Technische Hochschule Wildau [FH]
Technical University of Applied Sciences

Prof. Dr. Margit Scholl

Keynote: Participative Dialogue with Schools

Raising Information Security Awareness 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
   - Results of the gender-based school project “Security”
   - Results of the project “SecAware4school”

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

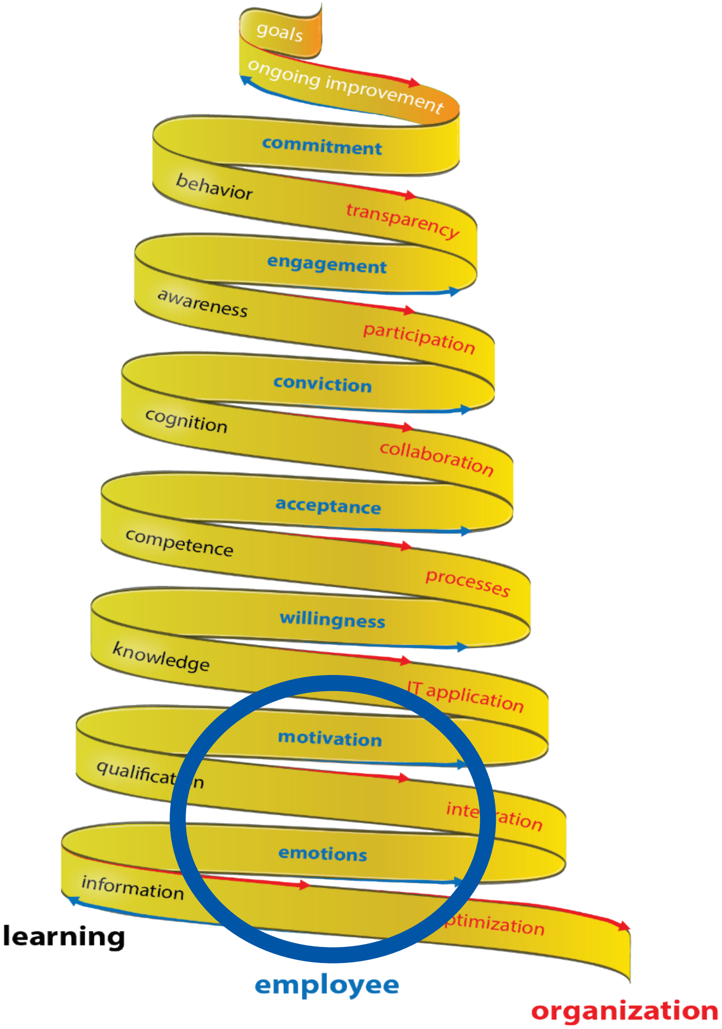
Integrity

Availability

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

Verfügbarkeit
Integrität
Vertraulichkeit
Authentizität
Nichtabstreitbarkeit
Verbindlichkeit
Gesetze
Standards & Norm

1. Introduction: Spiral of transformative interaction



Interaction between top-down specifications and individual bottom-up influence on the establishment of an organizational security culture

Organization: Place where information security is to be lived and which is characterized by guidelines, procedures and structures.
Employees: Actors whose attitudes and behavior make it possible to create an authentic security culture.
Learning process: Employees and the organization as a whole acquire information-security-relevant knowledge and awareness and practice appropriate behavior. Security culture is lived.

Explanation of the spiral (excerpt)
Formation of an awareness of information security and corresponding behavior requires emotional interest and motivation, as well as the willingness of the individual - systematic approach of operational security and privacy awareness.
As a result, higher acceptance and persistence of policies and measures to secure critical information.
Ideally active commitment and self-commitment for information security.

See [Scholl, M., & Fuhrmann, F. (2016). Analog – digital? Wie sich mithilfe analoger Methoden Bewusstsein für Informationssicherheit in der digitalen Welt fördern lässt In D. Rätz, M. Breidung, D. Lück-Schneider, S. Kaiser, & E. Schweighofer (Eds.), *Digitale Transformation: Methoden, Kompetenzen und Technologien für die Verwaltung* (pp. 101-112). Bonn: Gesellschaft für Informatik e.V. (GI) (Lecture Notes in Informatics (LN), Band 261)].

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):

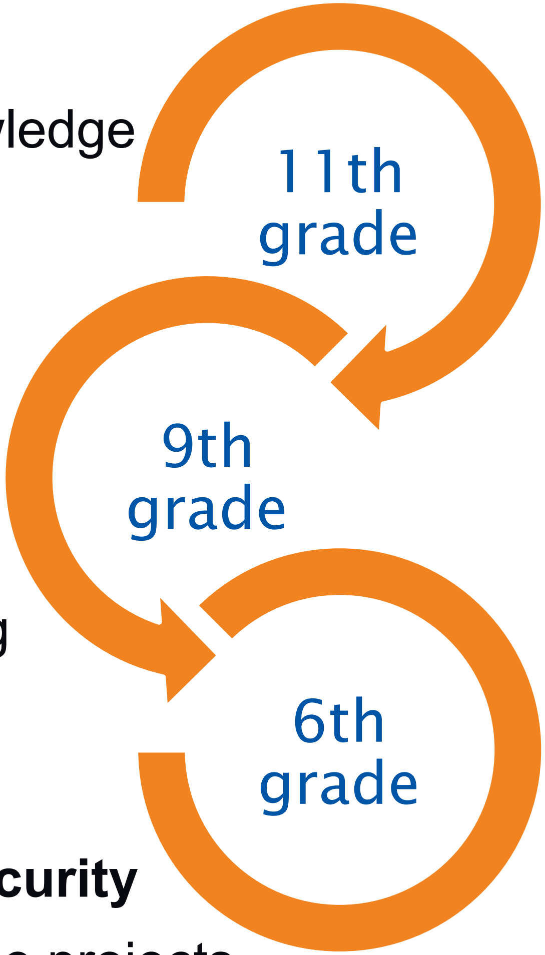
AuL focuses on the application of knowledge in real contexts and situations. The central aspect here is learning from experience, from real or simulated problems [Sc16].

2. ISA in everyday school life

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

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 two research projects “Security” and “SecAware4school,” various phases were defined 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.

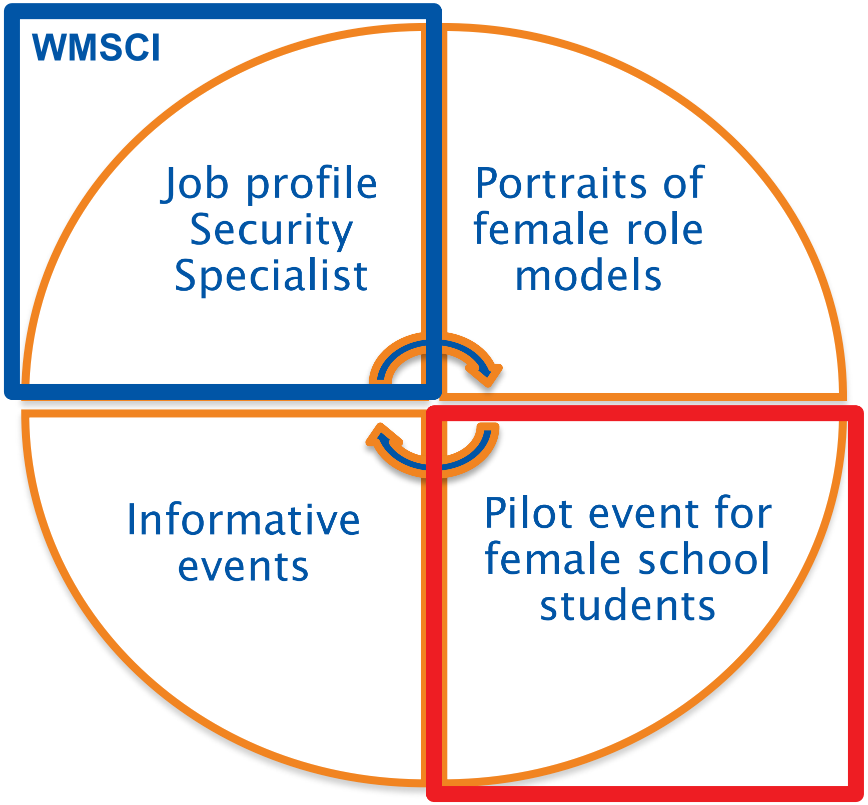
Creative workshops were the starting point for participative brainstorming and scenario development. The actual task of **game development** was left to the project team and then **tested** in the schools.

The gender-based project Security

The **Security project** focused on grade 9 and developed the following six analogue game-based learning scenarios, which can be borrowed by schools after the project ends in December 2019:

Fuhrmann, F., & Scholl, M. (2019). Does a Career In Information Security Appeal to Women?

1. *Security and safety on the road on school trips*
2. *Encryption principles*
3. *Image acquisition and image rights for usage/modification*
4. *Apps and their risks*
5. *Phishing mails*
6. *Password hacking*


WMSCI
Job profile Security Specialist
Portraits of female role models
Informative events
Pilot event for female school students

SPONSORED BY THE
Federal Ministry of Education and Research

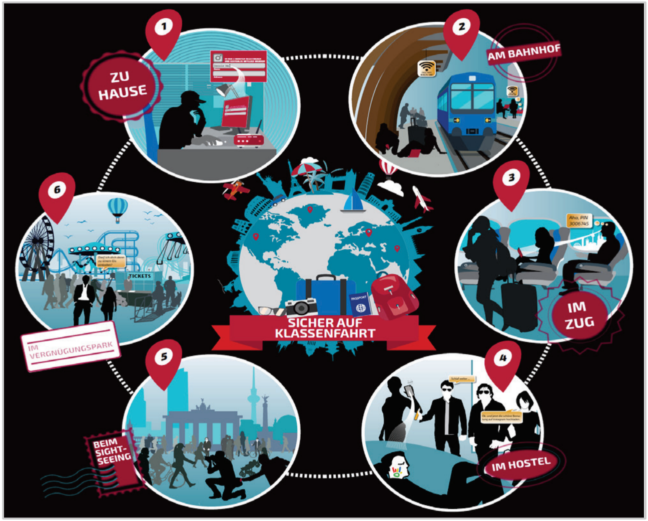
Security/safety on school trips

Objective of the learning scenario:
Awareness and knowledge of potential safety hazards and corresponding protective measures in public spaces. Issues relating to both information security and physical security are addressed.

Task:
What dangers are shown in the situations?
Which protective measures can reduce the risks?

- Read the dangers out loud. Identify the situation in which the danger is pictorially represented. Place the **Big Danger Card (red)** in the space.
- What would you tell your friends to help them protect themselves from this danger?

Assign the **Protective Cards (blue)** to the Big Danger Cards.



Offene Funkverbindungen

Bekanntmachung persönlicher Daten

Datensparsamkeit
Du überlegst genau, welche deiner Daten ein Anbieter wirklich benötigt. Im Zweifelsfall verzichtest du auf ein Angebot.

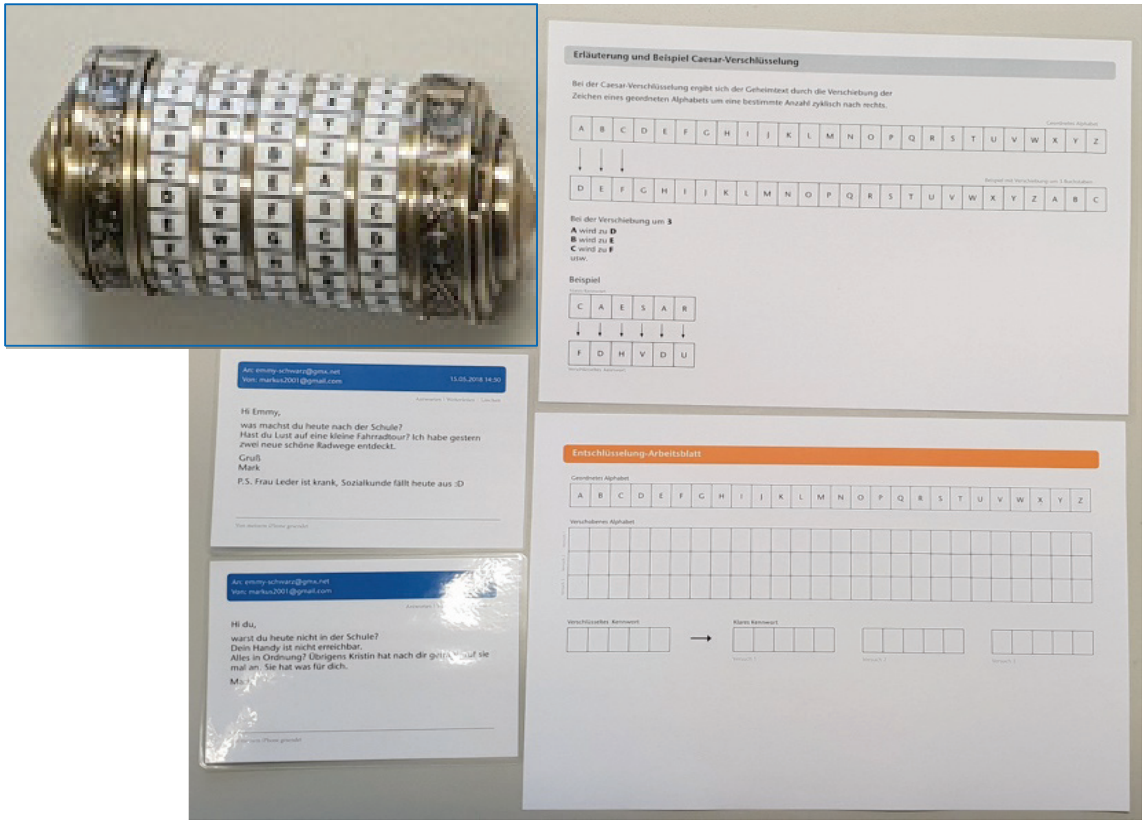
Mobile Datenverbindung
Unterwegs verbindest du dich über dein mobiles Internet anstatt über öffentlich zugängliche Internetverbindungen. Solltest du sie doch einmal nutzen, gibst du keine Login-Daten ein.

Encrytion principles

Objective of the learning scenario:
Basic knowledge of encryption and its possible uses with experience of a simple encryption method. Awareness of the importance of encryption.

Task:
Open the secret box!

- Find references to the Caesar shift in the emails.
- Write down possible displaced alphabets.
- Write down possible clear passwords.
- Try out the passwords.



Erläuterung und Beispiel Caesar-Verschlüsselung

Bei der Caesar-Verschlüsselung ergibt sich der Geheimtext durch die Verschiebung der Zeichen eines geordneten Alphabets um eine bestimmte Anzahl zyklisch nach rechts.

Geordnetes Alphabet

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Beispiel mit Verschiebung um 3 Buchstaben

Bei der Verschiebung um **3**
A wird zu **D**
B wird zu **E**
C wird zu **F**
usw.

Beispiel

Klares Kennwort

C	A	E	S	A	R
F	D	H	V	D	U

Verschlüsseltes Kennwort

An: emmy-schwarz@gmx.net
Von: markus2001@gmail.com
15.05.2018 14:50

Antworten | Weiterleiten | Löschen

Hi Emmy,

was machst du heute nach der Schule?
Hast du Lust auf eine kleine Fahrradtour? Ich habe gestern zwei neue schöne Radwege entdeckt.

Gruß
Mark

P.S. Frau Leder ist krank, Sozialkunde fällt heute aus :D

Von meinem iPhone gesendet

An: emmy-schwarz@gmx.net
Von: markus2001@gmail.com

Antworten

Hi du,

warst du heute nicht in der Schule?
Dein Handy ist nicht erreichbar.
Alles in Ordnung? Übrigens Kristin hat nach dir gefragt. Ruf sie mal an. Sie hat was für dich.

Mark

Von meinem iPhone gesendet

Entschlüsselung-Arbeitsblatt

Geordnetes Alphabet

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Verschobenes Alphabet

Verschlüsseltes Kennwort → Klares Kennwort

Versuch 1

Versuch 2

Versuch 3

Image acquisition and image rights

Objective of the learning scenario:
Awareness and knowledge of what can be photographed without permission or not.
Knowledge of the “right to one’s own image.”
Consideration of according “house rules” or similar documents.

Task I:
Which photos may be photographed without permission?

- Place the photos, which may be taken without permission or without asking, on the green cloth.

- Place the photos that **require permission**, such as asking for someone, on the red cloth.

- Justify your choices.

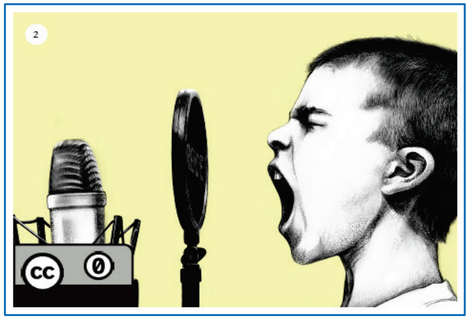
Image acquisition and image rights

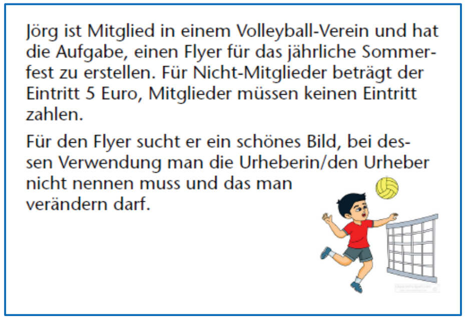
Securi♀y

TH WILDAU

Objective of the learning scenario:
Basic knowledge of copyright. Awareness and knowledge that images that can be found on the Internet, not just used. Knowledge about free images and their conditions of use (**C**reative **C**ommons license).

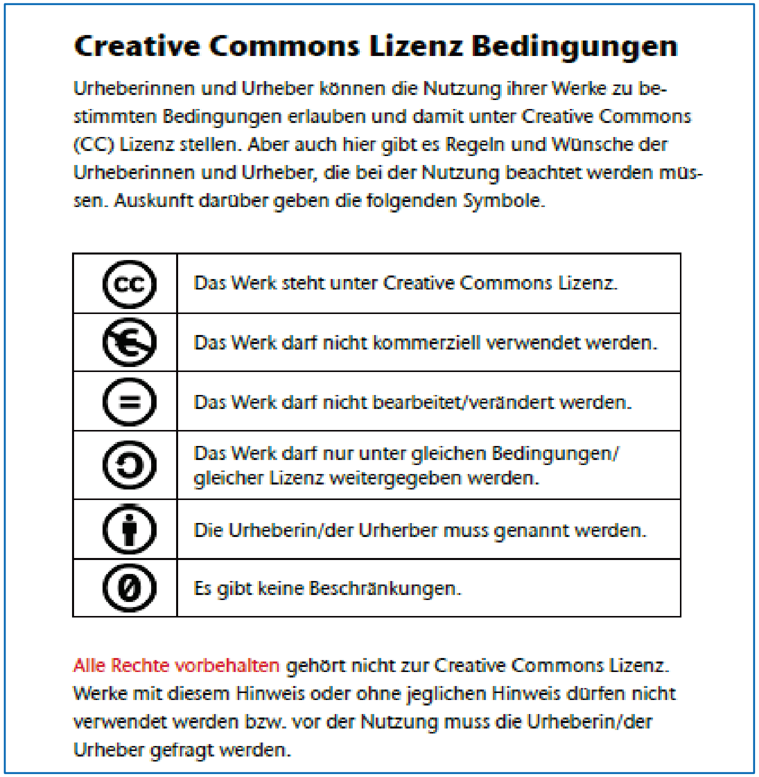
Task II:
Which image is the pupil allowed to use?
- Read the situation descriptions aloud and consider together which image(s) are suitable for it.
- Pay attention to the CC symbols in the pictures.





Jörg ist Mitglied in einem Volleyball-Verein und hat die Aufgabe, einen Flyer für das jährliche Sommerfest zu erstellen. Für Nicht-Mitglieder beträgt der Eintritt 5 Euro, Mitglieder müssen keinen Eintritt zahlen.

Für den Flyer sucht er ein schönes Bild, bei dessen Verwendung man die Urheberin/den Urheber nicht nennen muss und das man verändern darf.



Creative Commons Lizenz Bedingungen

Urheberinnen und Urheber können die Nutzung ihrer Werke zu bestimmten Bedingungen erlauben und damit unter Creative Commons (CC) Lizenz stellen. Aber auch hier gibt es Regeln und Wünsche der Urheberinnen und Urheber, die bei der Nutzung beachtet werden müssen. Auskunft darüber geben die folgenden Symbole.

(cc)	Das Werk steht unter Creative Commons Lizenz.
(€)	Das Werk darf nicht kommerziell verwendet werden.
(=)	Das Werk darf nicht bearbeitet/verändert werden.
(↻)	Das Werk darf nur unter gleichen Bedingungen/ gleicher Lizenz weitergegeben werden.
(i)	Die Urheberin/der Urheber muss genannt werden.
(0)	Es gibt keine Beschränkungen.

Alle Rechte vorbehalten gehört nicht zur Creative Commons Lizenz. Werke mit diesem Hinweis oder ohne jeglichen Hinweis dürfen nicht verwendet werden bzw. vor der Nutzung muss die Urheberin/der Urheber gefragt werden.

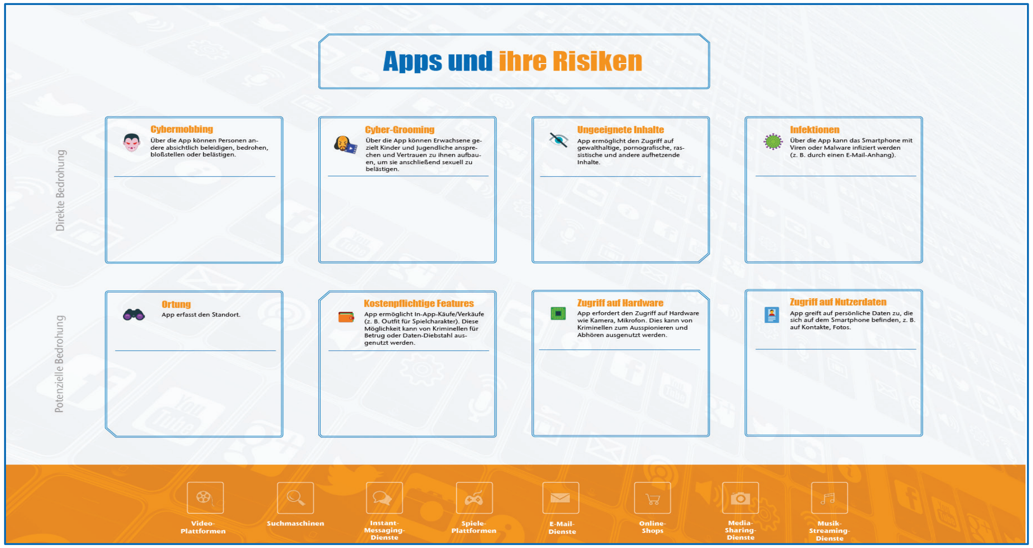
SPONSORED BY THE
Federal Ministry
of Education
and Research

Apps and their risks

Objective of the learning scenario:
Sensitization and understanding of potential risks of apps.
Rethinking the use of certain apps or consciously addressing the risks.

Task:
Which specific apps are associated with which risks?

- Does each app chip have the right category?
- Think about the risks associated with each app. Put an app chip on all these risks.



Apps und ihre Risiken

Direkte Bedrohung

Cybermobbing
Über die App können Personen andere absichtlich beleidigen, bedrohen, bloßstellen oder belästigen.

Cyber-Grooming
Über die App können Erwachsene gezielt Kinder und Jugendliche ansprechen und Vertrauen zu ihnen aufbauen, um sie anschließend sexuell zu belästigen.

Ungeeignete Inhalte
App ermöglicht den Zugriff auf gewalthaltige, pornografische, rassistische und andere aufhetzende Inhalte.

Infektionen
Über die App kann das Smartphone mit Viren oder Malware infiziert werden (z. B. durch einen E-Mail-Anhang).

Potenzielle Bedrohung

Ortung
App erfasst den Standort.

Kostenpflichtige Features
App ermöglicht In-App-Käufe/Verkäufe (z. B. Outfit für Spielcharakter). Diese Möglichkeit kann von Kriminellen für Betrug oder Daten-Diebstahl ausgenutzt werden.

Zugriff auf Hardware
App erfordert den Zugriff auf Hardware wie Kamera, Mikrofon. Dies kann von Kriminellen zum Ausspionieren und Abhören ausgenutzt werden.

Zugriff auf Nutzerdaten
App greift auf persönliche Daten zu, die sich auf dem Smartphone befinden, z. B. auf Kontakte, Fotos.

Video-Plattformen
Suchmaschinen
Instant-Messaging-Dienste
Spiele-Plattformen
E-Mail-Dienste
Online-Shops
Media-Sharing-Dienste
Musik-Streaming-Dienste

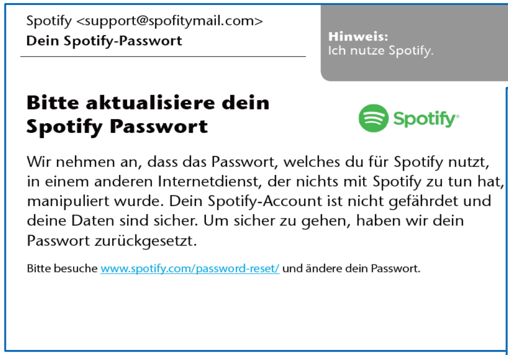
SPONSORED BY THE
Federal Ministry
of Education
and Research

Phishing mails

Objective of the learning scenario:
Awareness of the danger of phishing. Understanding and detection of phishing scams and training awareness of phishing scouting.

Task:
Which card is a phishing email?

- 1 or 2 people fishing emails.
- Read the emails in 2/3 groups and put phishing emails on the red cloth (**phishing mail**). Normal emails go on the green blanket (no phishing mail).


Spotify <support@spofitymail.com>
Dein Spotify-Passwort

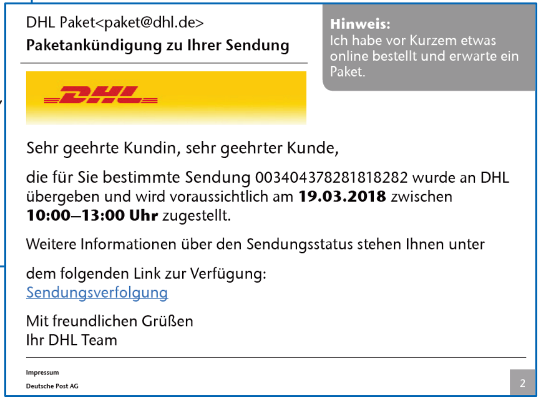
Hinweis:
Ich nutze Spotify.

Bitte aktualisiere dein Spotify Passwort

Spotify

Wir nehmen an, dass das Passwort, welches du für Spotify nutzt, in einem anderen Internetdienst, der nichts mit Spotify zu tun hat, manipuliert wurde. Dein Spotify-Account ist nicht gefährdet und deine Daten sind sicher. Um sicher zu gehen, haben wir dein Passwort zurückgesetzt.

Bitte besuche www.spotify.com/password-reset/ und ändere dein Passwort.


DHL Paket<paket@dhl.de>
Paketankündigung zu Ihrer Sendung

Hinweis:
Ich habe vor Kurzem etwas online bestellt und erwarte ein Paket.

DHL

Sehr geehrte Kundin, sehr geehrter Kunde,

die für Sie bestimmte Sendung 003404378281818282 wurde an DHL übergeben und wird voraussichtlich am **19.03.2018** zwischen **10:00–13:00 Uhr** zugestellt.

Weitere Informationen über den Sendungsstatus stehen Ihnen unter

dem folgenden Link zur Verfügung:
Sendungsverfolgung

Mit freundlichen Grüßen
Ihr DHL Team

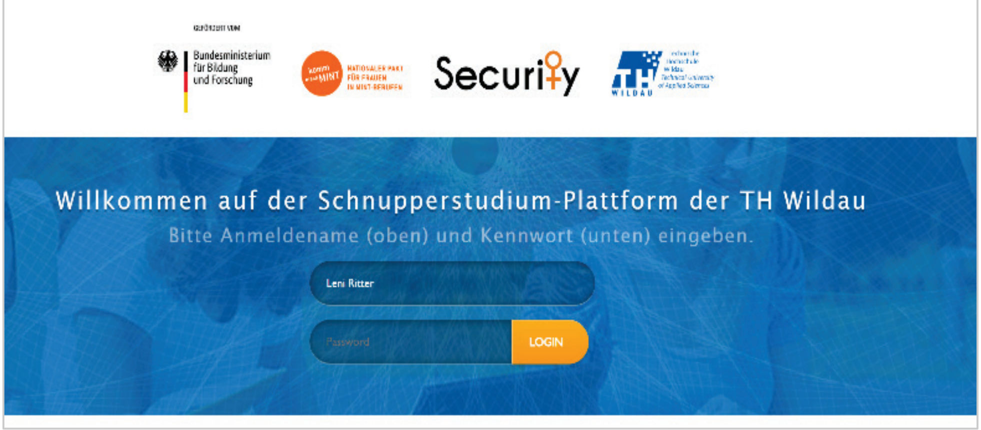
Impressum
Deutsche Post AG

2

Password hacking

Objective of the learning scenario:
Awareness of secure passwords and how to create secure passwords and easily remember them.

Task:
Crack the password!
- Read the fictitious profile of Leni Ritter.
- Use the profile to guess possible passwords for Leni Ritter and enter them into the fictitious platform.


Gefördert vom
Bundesministerium für Bildung und Forschung
komm mach MINT
NATIONALER PAKT FÜR FRAUEN IN MINT-BERUFEN
Security
TH WILDAU

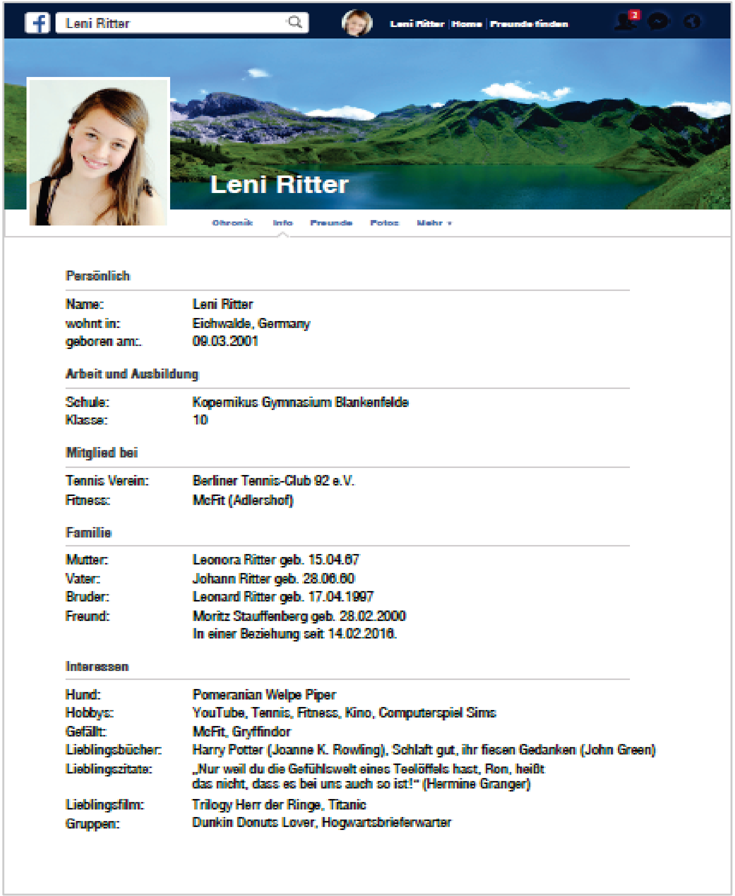
Willkommen auf der Schnupperstudium-Plattform der TH Wildau

Bitte Anmeldename (oben) und Kennwort (unten) eingeben.

Leni Ritter

Password

LOGIN



Persönlich

Name:	Leni Ritter
wohnt in:	Eichwalde, Germany
geboren am:.	09.03.2001

Arbeit und Ausbildung

Schule:	Kopernikus Gymnasium Blankenfelde
Klasse:	10

Mitglied bei

Tennis Verein:	Berliner Tennis-Club 92 e.V.
Fitness:	McFit (Adlershof)

Familie

Mutter:	Leonora Ritter geb. 15.04.67
Vater:	Johann Ritter geb. 28.06.60
Bruder:	Leonard Ritter geb. 17.04.1997
Freund:	Moritz Stauffenberg geb. 28.02.2000 In einer Beziehung seit 14.02.2016.

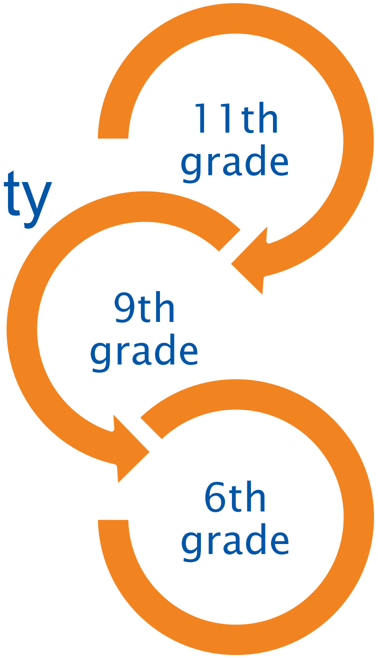
Interessen

Hund:	Pomeranian Welpe Piper
Hobbys:	YouTube, Tennis, Fitness, Kino, Computerspiel Sims
Gefällt:	McFit, Gryffindor
Lieblingsbücher:	Harry Potter (Joanne K. Rowling), Schlaft gut, ihr fiesen Gedanken (John Green)
Lieblingszitate:	„Nur weil du die Gefühlswelt eines Teelöffels hast, Ron, heißt das nicht, dass es bei uns auch so ist!" (Hermine Granger)
Lieblingsfilm:	Trilogy Herr der Ringe, Titanic
Gruppen:	Dunkin Donuts Lover, Hogwartsbrieferwarter

The Project "SecAware4school"

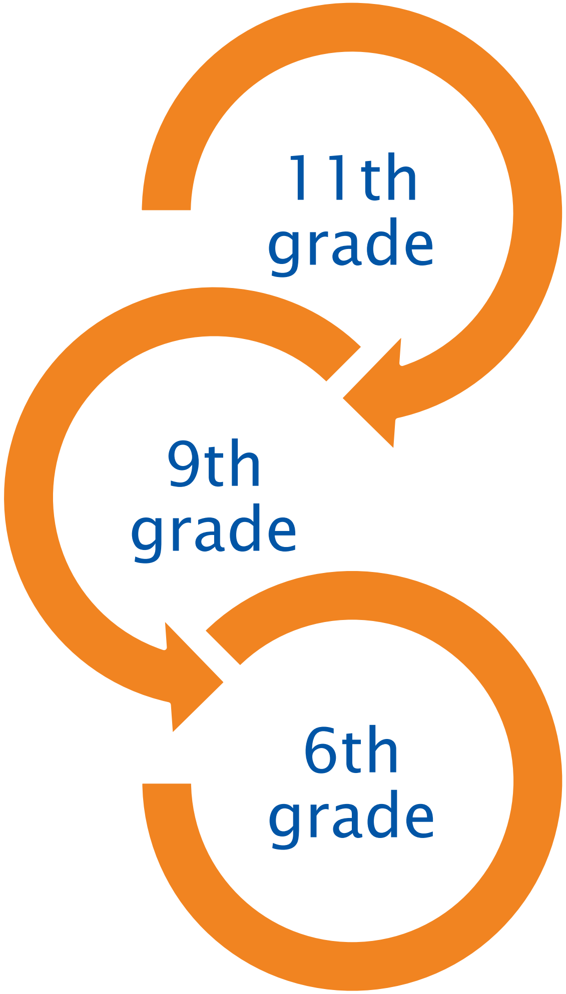
The **SecAware4school project** also includes lower (6th) and higher (11th) grades, developing a total of 10 learning scenarios at three different levels of difficulty for a total of 30 analogue and digital learning scenarios:

- 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.



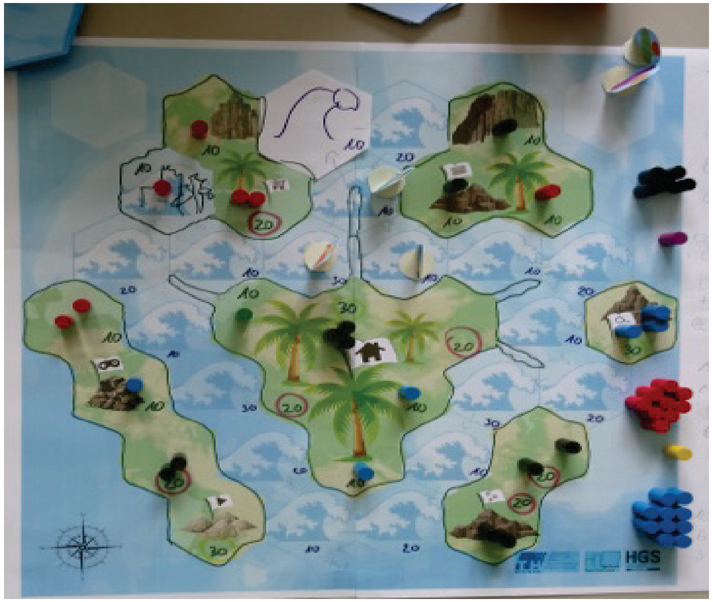
SPONSORED BY THE HGS Horst Görtz Stiftung

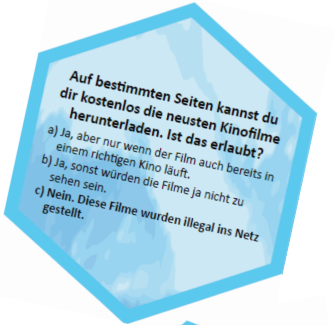
Hazards and protective measures (analogue)



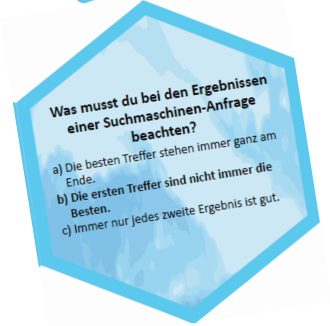
Objective of the learning scenario:
Knowledge of threats and safeguards for information security
Expansion of knowledge of information security

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



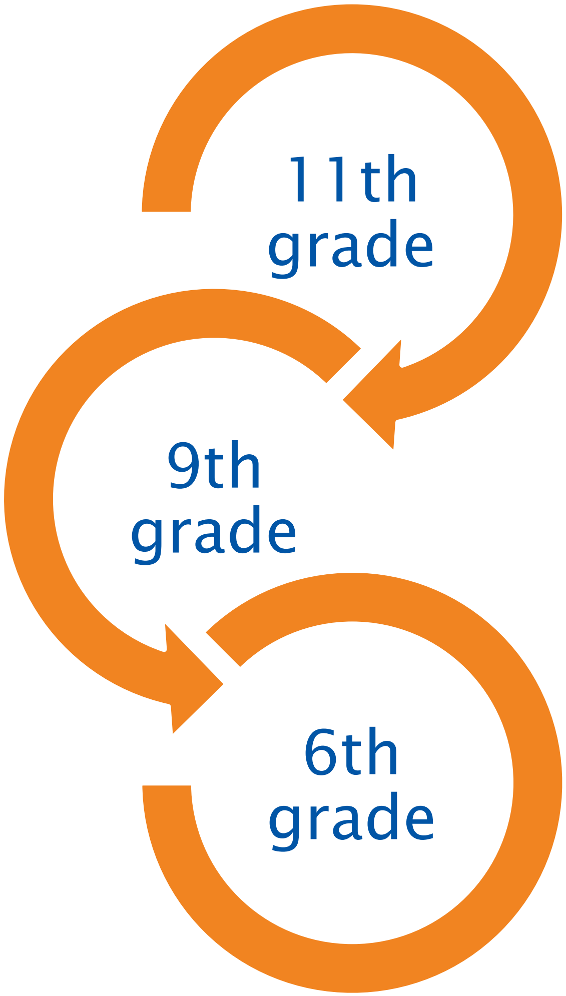


Auf bestimmten Seiten kannst du dir kostenlos die neusten Kinofilme herunterladen. Ist das erlaubt?
a) Ja, aber nur wenn der Film auch bereits in einem richtigen Kino läuft.
b) Ja, sonst würden die Filme ja nicht zu sehen sein.
c) Nein. Diese Filme wurden illegal ins Netz gestellt.



Was musst du bei den Ergebnissen einer Suchmaschinen-Anfrage beachten?
a) Die besten Treffer stehen immer ganz am Ende.
b) Die ersten Treffer sind nicht immer die Besten.
c) Immer nur jedes zweite Ergebnis ist gut.

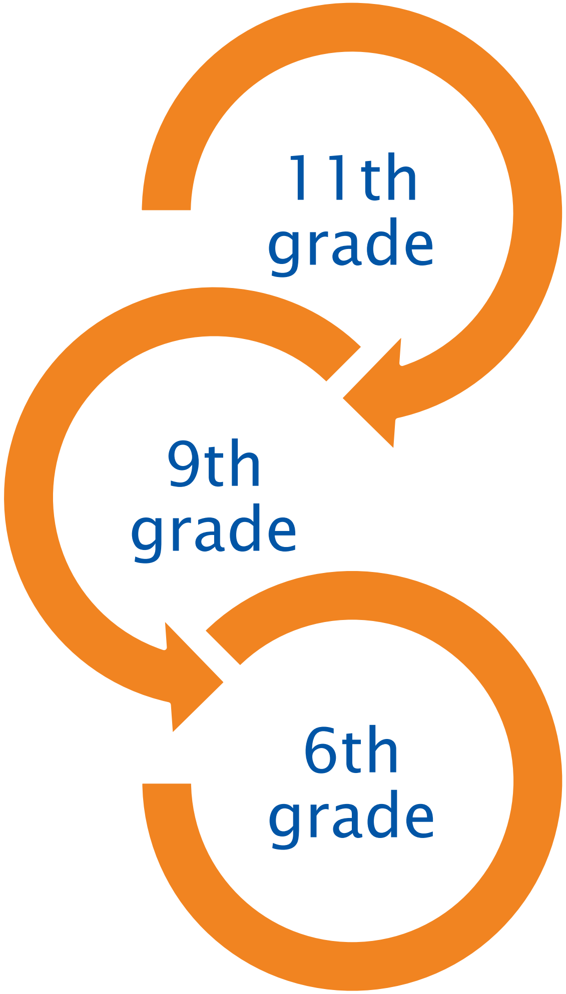
Recognize the internet norms (analogue)



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.

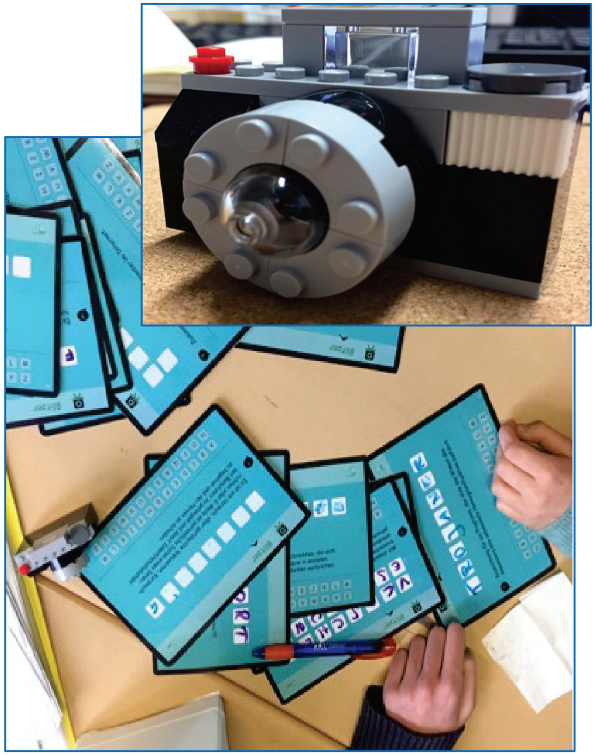
Task:
Hints and rules from the puzzle to remember.

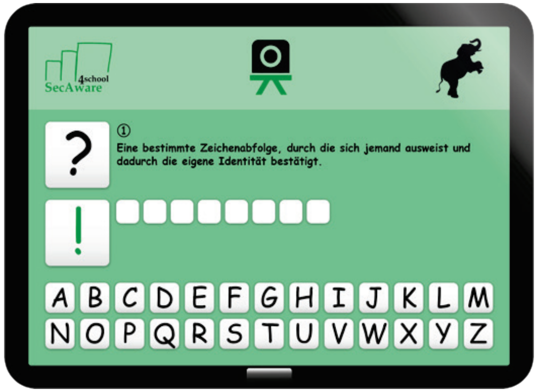
Rapid Guessing
(analogue + digital)



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

Task:
Guess important information security terms with discussion.

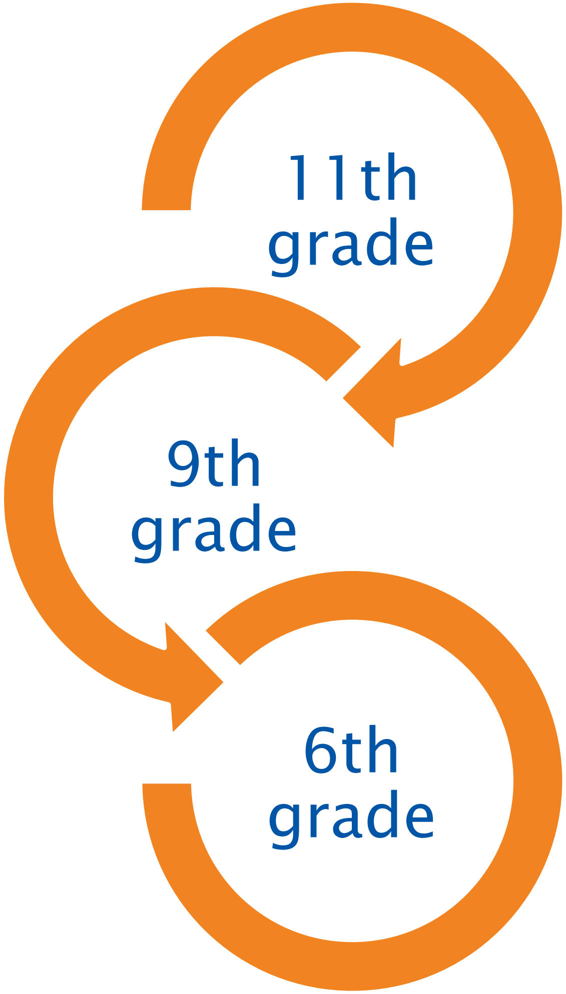




① Eine bestimmte Zeichenabfolge, durch die sich jemand ausweist und dadurch die eigene Identität bestätigt.

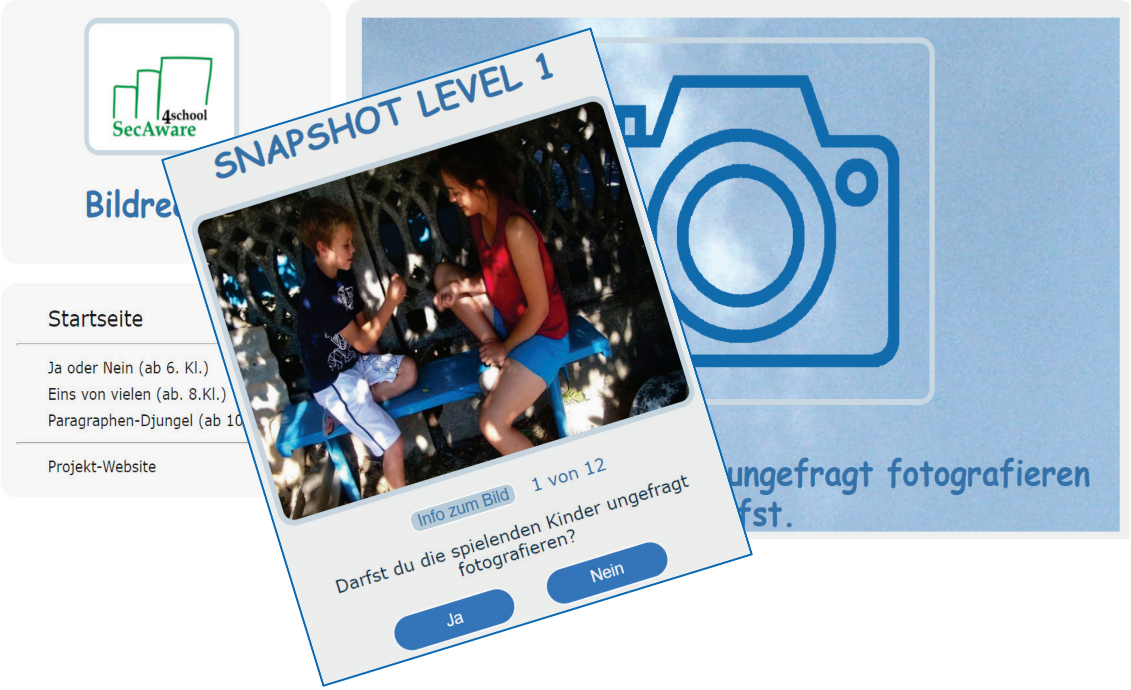
SPONSORED BY THE
HGS
Horst Görtz Stiftung

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.

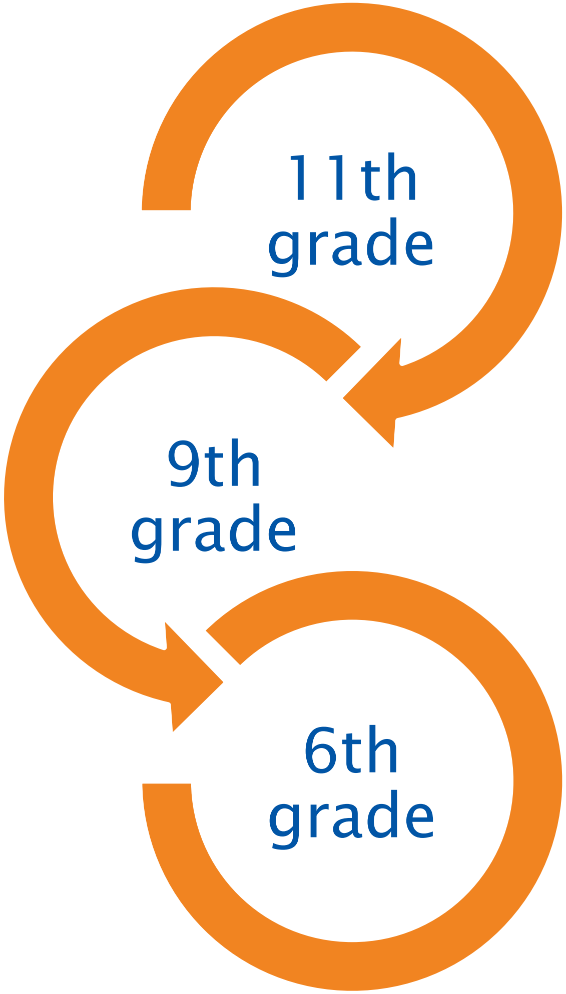


Darfst du die spielenden Kinder ungefragt fotografieren?

ungefragt fotografieren
fst.

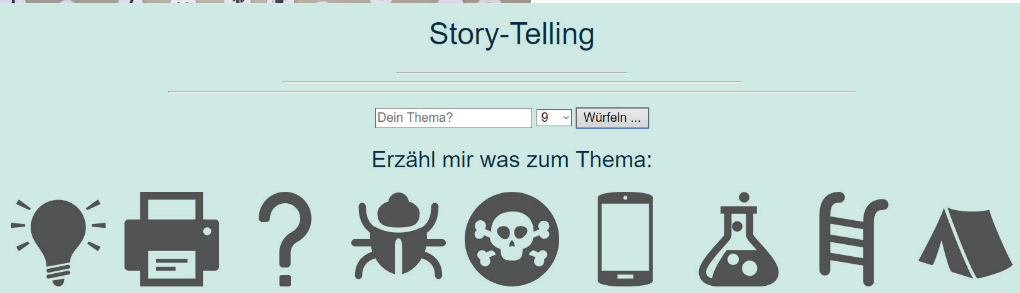
Storytelling in information security

(analogue + digital)



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

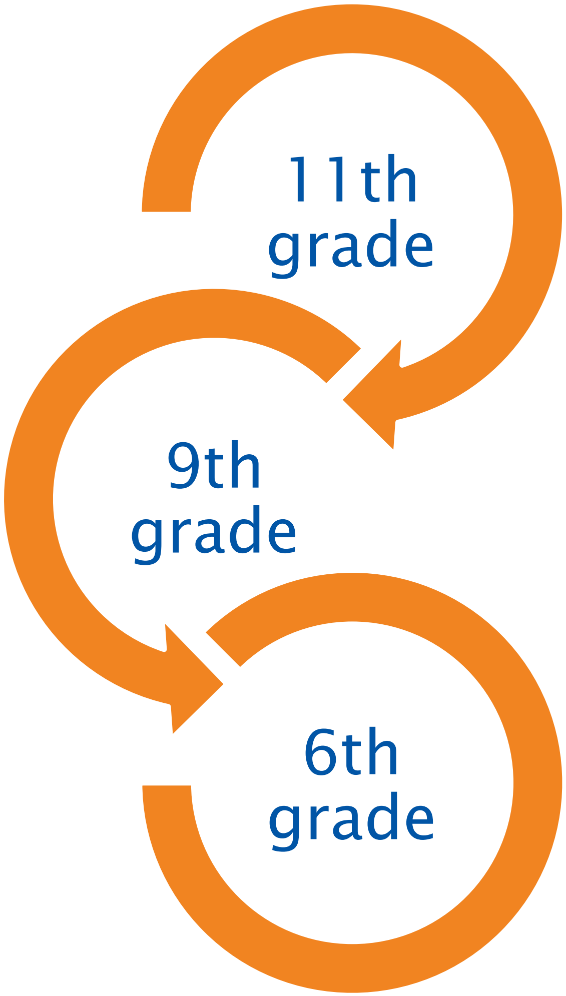
Task:
Use random symbols to write down a realistic story of information security using important and real technical terms.



Story-Telling

Erzähl mir was zum Thema:

Behavior in social networks (analogue)

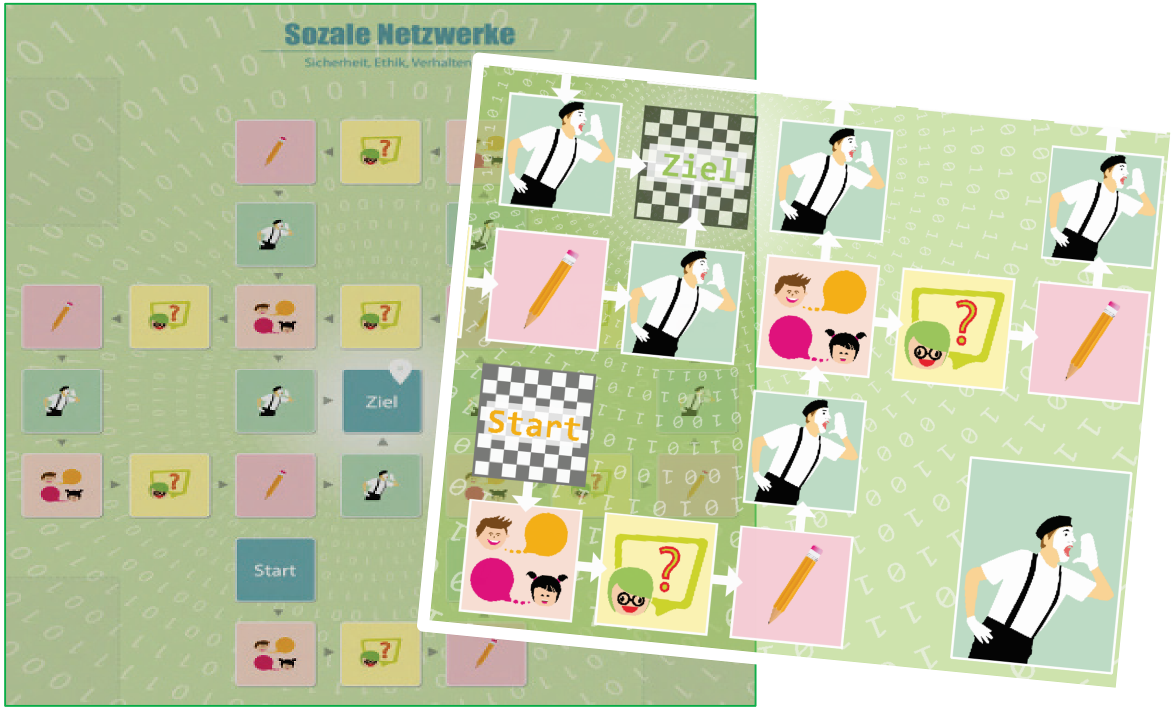

11th grade

9th grade

6th grade

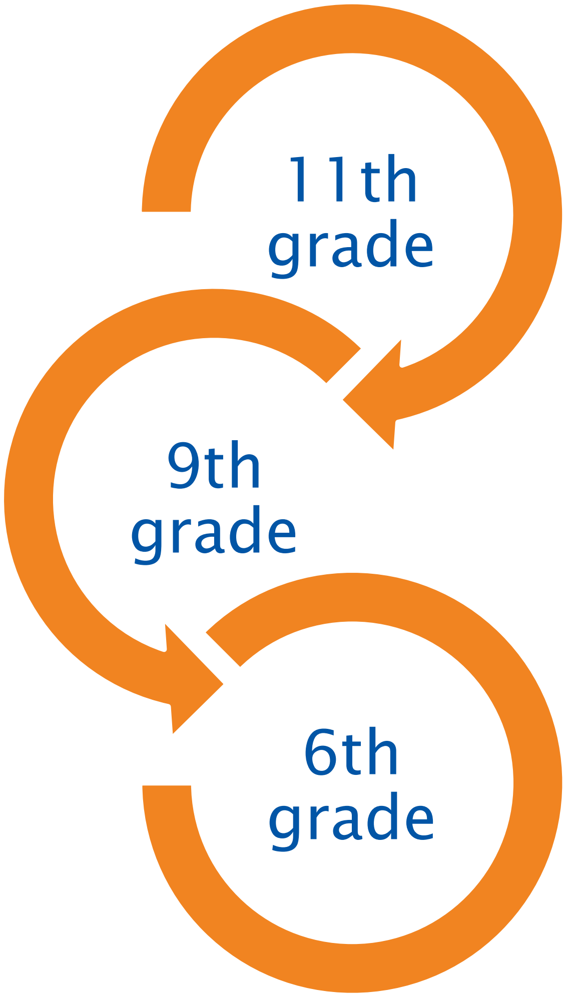
Objective of the learning scenario:
Awareness of safe security behavior in social networks.

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



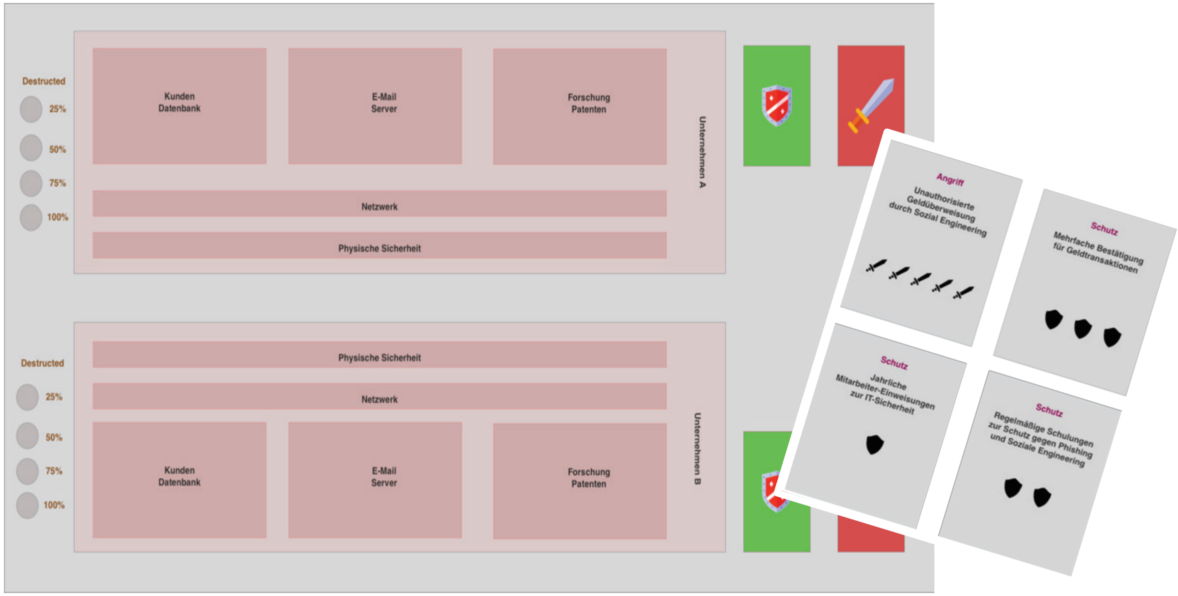
SPONSORED BY THE
HGS Horst Görtz Stiftung

Security duell in job situations (analogue)



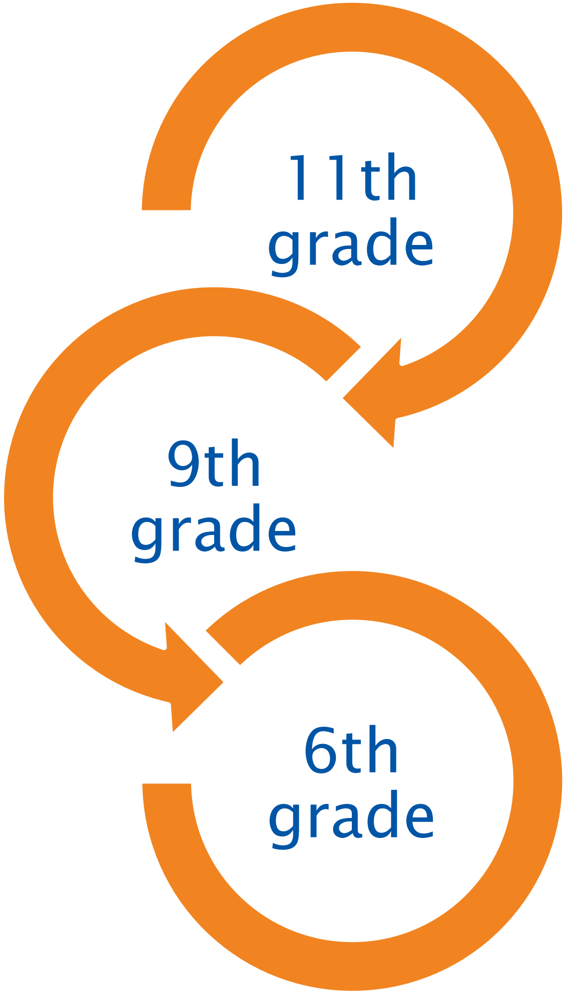
Objective of the learning scenario:
Information on security-relevant decision situations, possible consequences and possible protective measures.

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



SPONSORED BY THE
HGS
Horst Görtz Stiftung

Fake news
(analogue + digital)

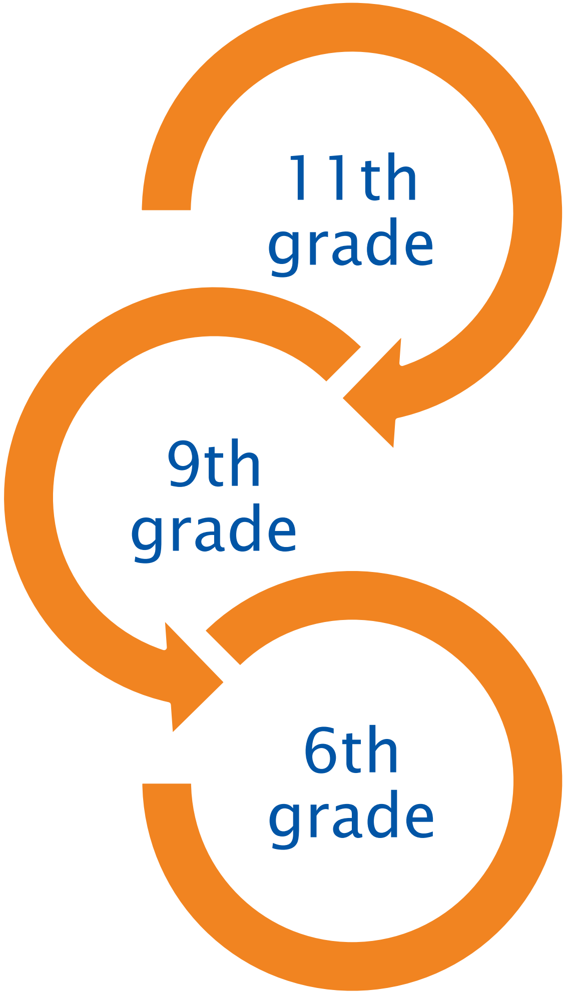


Objective of the learning scenario:
Sensitization to information collection and manipulation.

Task:
Identify fake messages based on examples.

SPONSORED BY THE
HGS Horst Görtz Stiftung

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?

SPONSORED BY THE
HGS Horst Görtz Stiftung

5. Outlook

Security

SPONSORED BY THE

Federal Ministry
of Education
and Research

The project ends on December 31, 2019.
All six experience-based learning scenarios can be borrowed by schools. Other materials to inspire girls' interest in information security are in place and usable.
https://www.security.wildau.biz

SecAware4school

SPONSORED BY THE

HGS
Horst Görtz Stiftung

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.

ACKNOWLEDGMENTS

The author would like to thank both research teams for their dedicated support in conducting the study and assisting in the process of game development:

- Operational project leader **Frauke Prott (Fuhrmann)** and her team **Security**
- Operational project leader **Regina Schuktomow** and her team **SecAware4school**

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

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

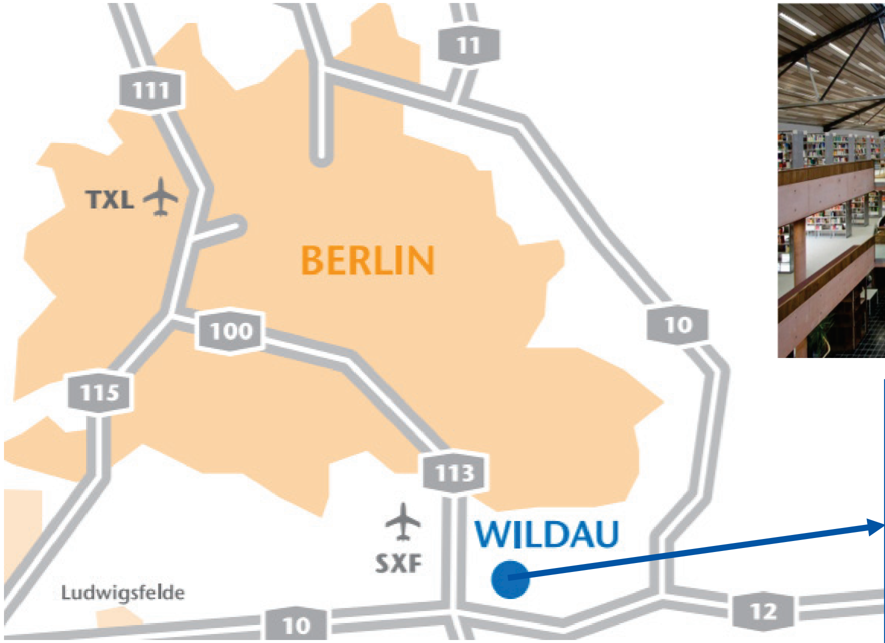
[Si17] Silic, M.; Back, A.: Impact of Gamification on User’s Knowledge-Sharing Practices: Relationships between Work Motivation, Performance Expectancy and Work Engagement. Proceedings of the 50th Hawaii International Conference on System Sciences, S. 1308-1317, 2017.

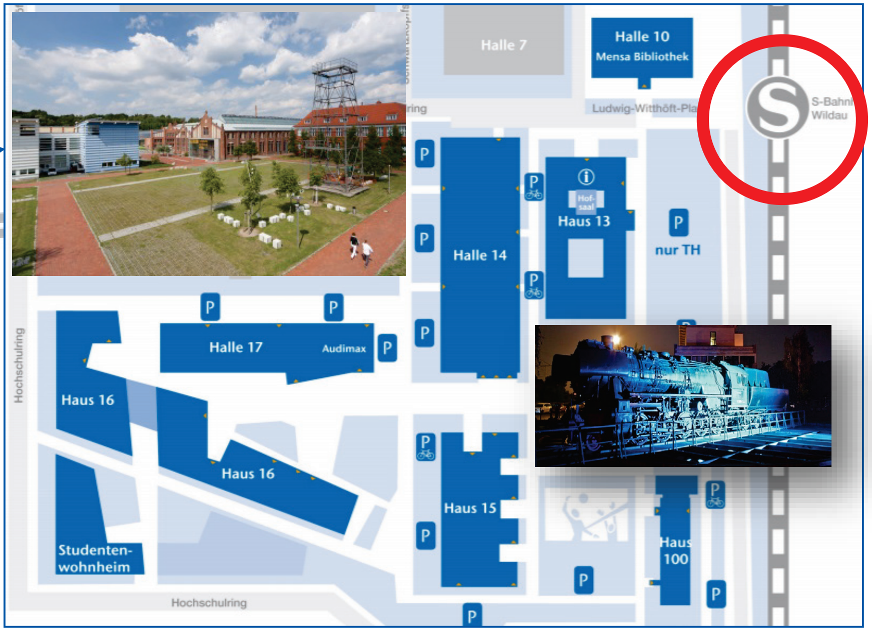
[St13] Styles M.: Constructing Positive Influences for User Security Decisions to Counter Corporate or State Sponsored Computer Espionage Threats. In: (Marinos L.; Askoxylakis, I. Hrsg.): HAS 2013, Lecture Notes in Computer Science, Vol. 8030. Berlin/Heidelberg, Springer, S. 197-206, 2013.

[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.

Where is the TUAS Wildau located?


111
11
TXL
BERLIN
100
10
115
113
SXF
WILDAU
Ludwigsfelde
10
12


Halle 7
Halle 10
Mensa Bibliothek
Ludwig-Witthöft-Pla
S-Bahn
Wildau
ring
P
Halle 14
Hof-
saal
Haus 13
nur TH
Halle 17
Audimax
Haus 16
Haus 16
Haus 15
Studenten-
wohnheim
Hochschulring
Haus
100