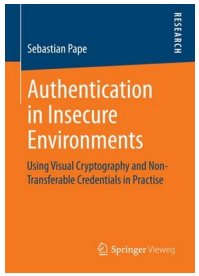
Serious Games for Security and Privacy Awareness

PD Dr. Sebastian Pape

PD Dr. Sebastian Pape

- Studies
  - Dipl.-Math.
  - Dipl.-Inform.



- PhD
  - Dr. rer. nat.
  - "Authentication in Insecure Environments"
- Habilitation
  - "Requirements Engineering and Tool-Support for Security and Privacy"

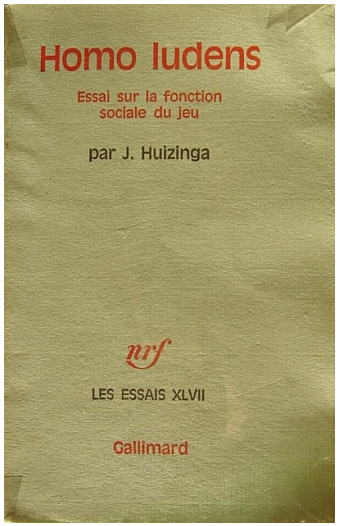
Interests:
Security & Privacy

- Post-Doc / Privatdozent
  - Group "Mobile Business & Multilateral Security"
- Founder
  - Social Engineering Academy GmbH

Agenda

- Introduction to Serious Games
- Serious Games Raising Awareness Against Social Engineering
  - HATCH
  - PROTECT
  - CyberSecurity Awareness Quiz
- Serious Games Raising Privacy Awareness
  - LEECH
- Open Questions and Challenges
- Discussion

- Book Homo Ludens
  - written in 1938 by Johan Huizinga



Source: https://de.wikipedia.org/wiki/Johan_Huizinga

- Discusses importance of the play element of culture
- Animals played before humans

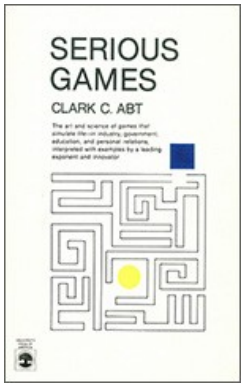
- One of the most significant aspects of play is that it is fun

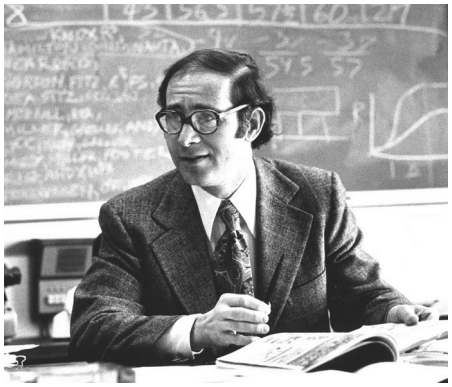
Huizinga, J.: Homo Ludens: A Study of the Play-Element in Culture. Beacon Press, Boston (1938)

Introduction to Serious Games II

- Term contrib. to Clark Abt (1971)

- Exploring the application of games for other purposes than entertainment





Source: https://www.abtassociates.com/who-we-are/our-people/clark-c-abt-phd

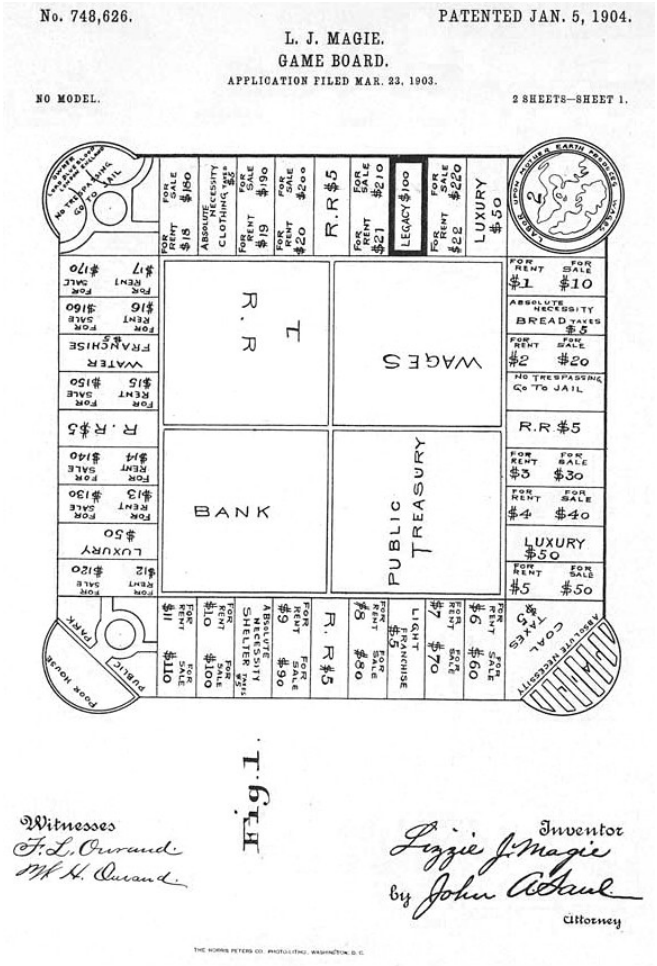
- Boundaries between playing and not playing are “fuzzy and permeable”

Salen, K., Zimmerman, E.: Rules of Play: Game Design Fundamentals. The MIT Press, Cambridge (2003)

→ inherent tension of balancing fun and purpose in Serious Games design.

Franzwa, C., Tang, Y., Johnson, A.: Serious game design: motivating students through a balance of fun and learning. In: 2013 5th International Conference on Games and Virtual Worlds for Serious Applications (VS-GAMES), pp. 1–7. IEEE (2013)

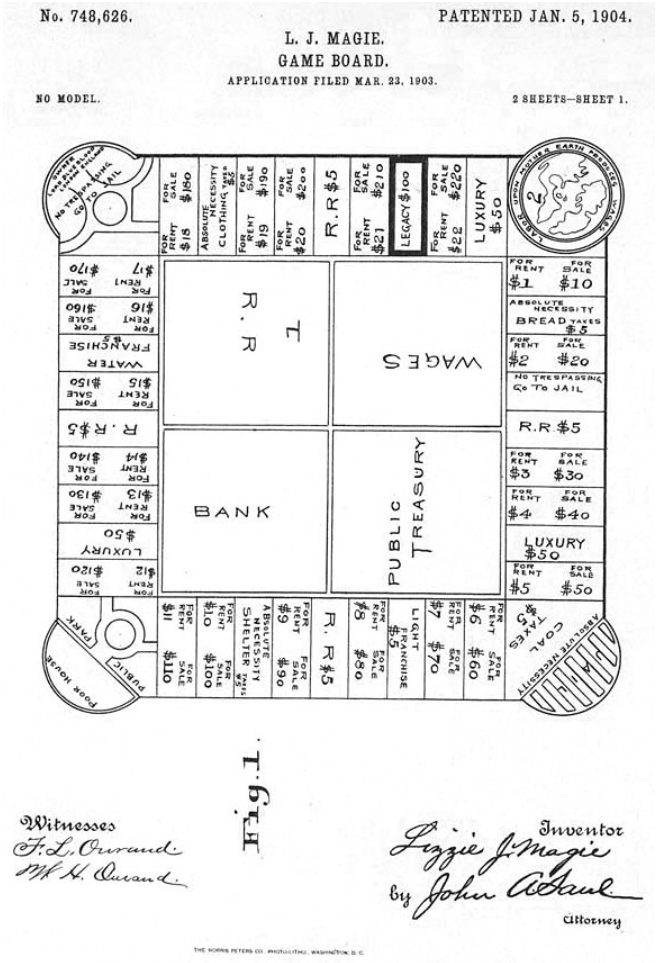
Who knows this game?



Parlett, D.S.: Oxford History of Board Games. Oxford University Press, Oxford (1999)

Serious Games Example

- Landlord's Game
  - created in 1902
  - precursor to Monopoly
  - was designed to illustrate the dangers of capitalist approaches to land taxes and property renting



Parlett, D.S.: Oxford History of Board Games. Oxford University Press, Oxford (1999)

Definition: Serious Games / Gamification

Serious Game

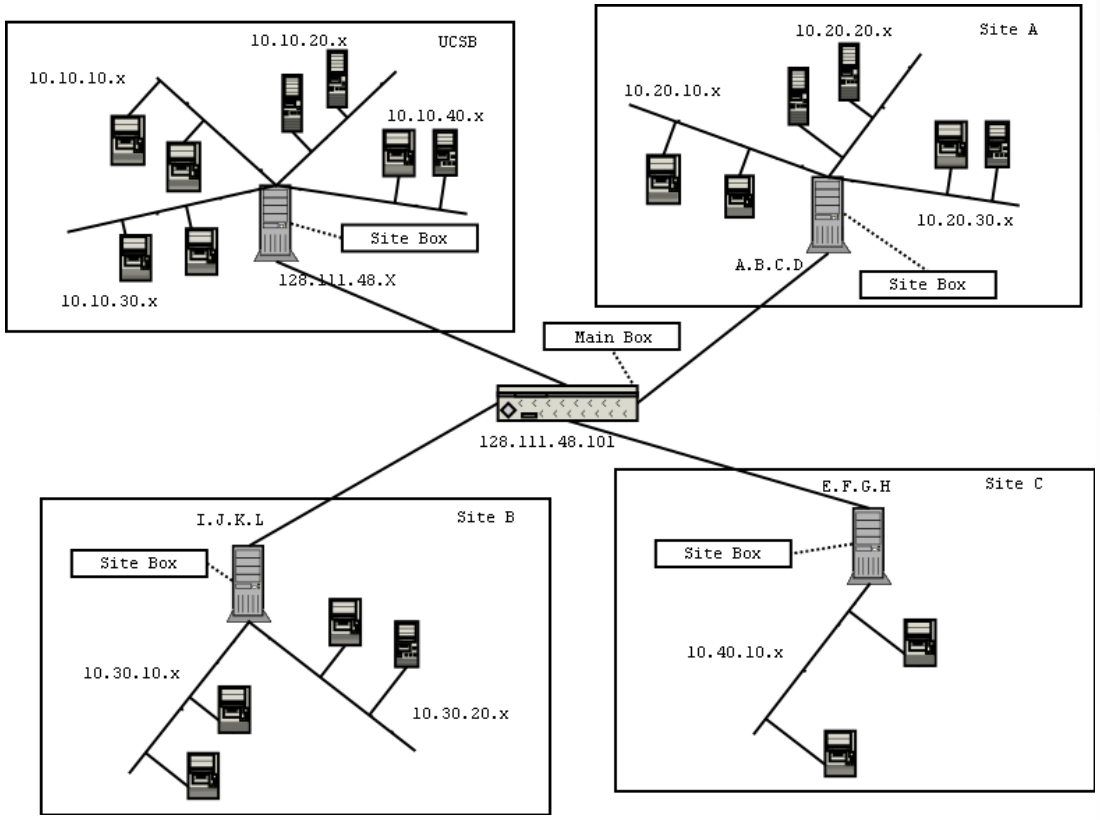
- A game designed for a primary purpose other than pure entertainment
- Often used as umbrella term
  - Edutainment
  - (Digital) Game-Based Learning
  - Good digital games
  - Epistemic Games
  - Persuasive Games

Gamification

- Application of game-design elements (e.g. point scoring, competition with others, rules of play) to other areas of activity / in non-game contexts.
- Typically used as an online marketing technique to encourage engagement with a product or service
- Other applications:
  - Organizational productivity
  - Crowdsourcing
  - Employee recruitment
  - Physical exercise
  - ...

Serious Games in Security

Source: https://ctfd.io/



Source: https://ictf.cs.ucsb.edu/archive/2004/site/

6. Deutscher IT-Sicherheitspreis 2016
3. Preis

- Beckers, K. and Pape, S.: A Serious Game for Eliciting Social Engineering Security Requirements. In Proceedings of the 24th IEEE International Conference on Requirements Engineering, IEEE Computer Society, RE '16 , 2016, Acceptance Rate: 22/79 = 27.8%.
- Beckers, K.; Pape, S. and Fries, V.: HATCH: Hack And Trick Capricious Humans -- A Serious Game on Social Engineering. In Proceedings of the 2016 British HCI Conference, Bournemouth, United Kingdom, July 11-15, 2016, 2016.

Introduction: Social Engineering

Source: cybertec-security.com

Breach vectors leading to compromise:

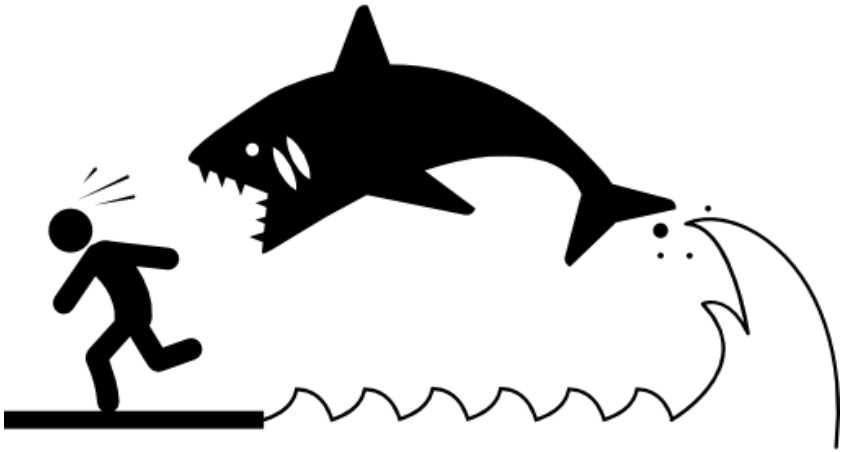
Source: PWC Information Security Breaches Survey 2017

Problems with SE Trainings

- Social engineering attacks are difficult to predict:
  - Based on human behaviour
- Awareness often trainings are ...
  - forced
  - have no lasting effect
  - not specific

Problems with Social Engineering Pentesting

- Lots of effort beforehand to address legal issues
- Involves the deception of employees and a possible violation of their privacy rights
- Provides only a small fraction of all attack vectors.
- Humans can easily be demotivated when confronted with the results



G. Watson, A. Mason, and R. Ackroyd, Social Engineering Penetration Testing: Executing Social Engineering Pen Tests, Assessments and Defense. Syngress, 2011.

T. Dimkov, A. van Cleeff, W. Pieters, and P. Hartel, “Two methodologies for physical penetration testing using social engineering,” in Proceedings of the 26th Annual Computer Security Applications Conference, ser. ACSAC ’10. ACM, 2010, pp. 399–408.

HATCH: Motivation

- Games can be fun
  → gets employees involved
- Games provide a realm
  → encourages employees to be creative
- Fictional situations are discussed in the game
  → no one is to blame
- Games are intended to be engaging and entertaining
  → which gets employees to play again and again

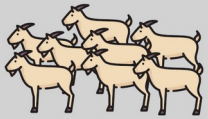
HATCH: Idea

Attack Scenarios

Dumpster Diving

Dumpster Diving is the act of analysing the documents and other things in a garbage bin of an organisation to reveal sensitive information.

Principles



The Herd Principle

Even the most suspicious victims will let their guard down when everyone next to them appears to share the same risk.
Exploit your victims by following a herd that you control.

Attacker Type

Inside Attacker

An insider is a known member of the organization who has already established trust.

Design: Kristina Femmer

HATCH
Real World Scenario

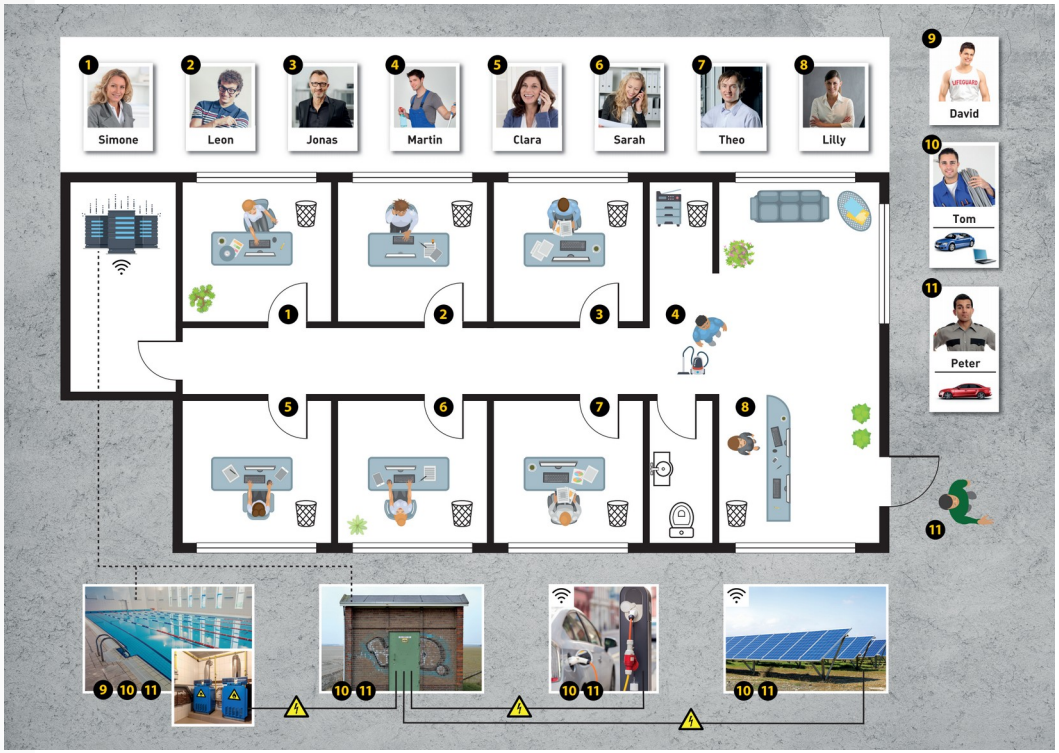
Kristian Beckers and Sebastian Pape. A serious game for eliciting social engineering security requirements. In Proceedings of the 24th IEEE International Conference on Requirements Engineering, RE '16. IEEE Computer Society, 2016

HATCH
Real World Scenario

Nr.	Context Knowledge	Attack	Asset	Principle	Attack Scenario
1	Tim is seeking for attention and likes to be admired for his achievements.	A member of an intranet security discussion board invites Tim to participate in an honorary event and asks the Tim to log in with his credentials to the intranet side using a specific link.	Credentials	Distraction	Waterholing
2	Jim flies to the United States from Germany with Lufthansa and they just announced a strike. Jim is watching his email closely to get any information about delays quick and deal with them.	The attacker fakes a Lufthansa email with an updated travel itinerary and attaches some malware to this email. The malware would gain him access to the Jim's PC and all digital assets on it.	Notebook Data	Time Pressure	Mail Attachment
3	Bob is using Yahoo Mail, which forces him to re-enter his credentials after 2 weeks continuously being logged in.	Bob proposes to attack himself using the outlined weakness in Yahoo Mail. If an attacker would fake the popup, he would probably (re-)enter his credentials	Email Data	Ignorance and Carelessness	Popup Window
4	Steve always leaves his office door and computer unlocked. The cleaning guy is quite dominant when cleaning the rooms.	An attacker can just enter his office pretending to be a (new) cleaning guy, so he can just enter and send an email using his computer and open an attachment with a Trojan.	Notebook Data	Laziness	Support Staff
5	Robert's family is about to arrive in the city to celebrate his PhD submission. He also is printing his Phd-thesis at the moment. Robert gets a call from his family who arrives by train.	The attacker would be around and offer him to finish copying his dissertation. Due to Robert's stress with his dissertation and family arriving he would welcome help. The attacker would then steal data from his dissertation.	Dissertation	Trust Principle	Direct Approach

Nr.	Threat	Security Requirement
1	A member of an intranet security discussion board invites Tim to participate in an honorary event and asks the boss to log in with his credentials to the intranet side using a specific link.	A security awareness training has to teach Tim and other employees to investigate links from unknown sources, even when under time pressure. These investigations can be delegated, e.g., to the IT security team.

Virtual Scenario: Training



Design: Kristina Femmer

- Overview diagram
  - room structure
  - employees and their offices
  - communication channels
  - assets have to be chosen and reasoned by the players

Tom

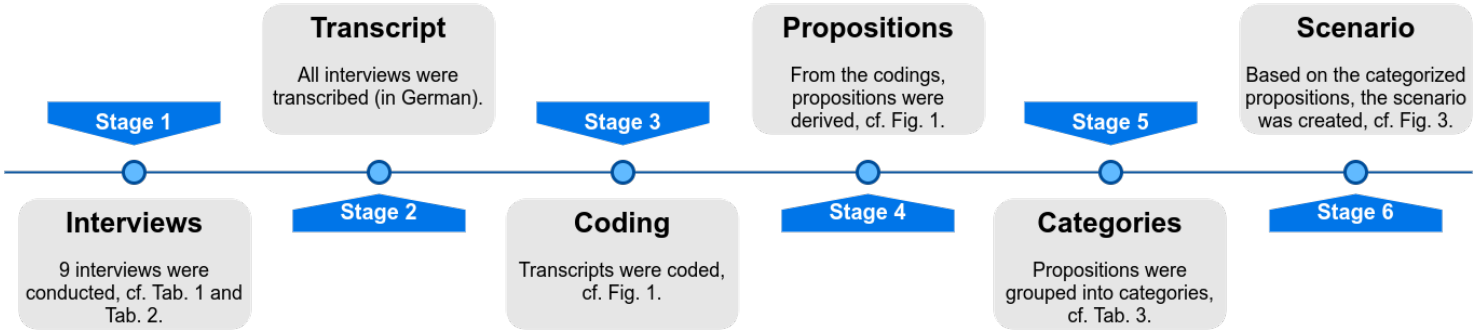
Tom is an electrician at SIDATE. He works in the field service and maintains the systems.

He knows the network structure of SIDATE by heart.

Tom tries to drive as little as possible and to shorten the distances.

Tom spends a lot of time to inform himself about new systems.

HATCH: Scenario Creation



- Based on Faily, S., Flechais, I.: Persona cases: a technique for grounding personas. In:Proceedings of the SIGCHI Conference on Human Factors in ComputingSystems. pp. 2267–2270 (2011)

Vera Hazilov and Sebastian Pape. Systematic scenario creation for serious security-awareness games. In Computer Security - ESORICS 2020 International Workshops, 2nd Workshop on Security, Privacy, Organizations, and Systems Engineering (SPOSE), to appear, 09 2020

Training: Law in General (Germany)

- **On the one hand:**
  - Management: Compliance IT-Security
  - Includes training against Social Engineering attacks (§ 43 Abs. 1 GmbHG und § 91 Abs. 1 AktG)

- **On the other hand:**
  - What exactly does the employee need to accept?
  - Freedom vs. Security
  - Consideration: Labour law, Data privacy law, Corporate compliance, Corporate Governance

→ **Differentiation between real and virtual scenario necessary**

Pape, S. and Kipker, D-K.: Case Study: Checking a Serious Security-Awareness Game for its Legal Adequacy. In Datenschutz und Datensicherheit, 45 (5): 310-314, 2021.

Real Scenario: Legal Aspects (Germany)

- Simulated attacks aim at real persons
- Employer has to protect employees from exposure
- Real scenario is particular risky for exposure

- **Fair balance between corporate interests and personal rights of the employee needed**

- Depends on
  - Industrial sector
  - Previous incidents
  - Purpose of the game
  - Just for training → virtual scenario
  - Threat elicitation → if necessary, ok
- Defence against SE also preserves workplaces

Virtual Scenario: Legal Aspects (Germany)

- Simulated attacks do **not** aim at real persons
- Employer has to protect employees from exposure
- Virtual scenario is **not** particular risky for exposure
- Employees can be trained before
- Clear rules (maybe even for communication)

- **Fair balance between corporate interests and personal rights of the employee needed**

- Low burden on employee
  → in general ok

  → Valid training

HATCH: Summary

Virtual Scenario

- Imaginary plan
- Personas

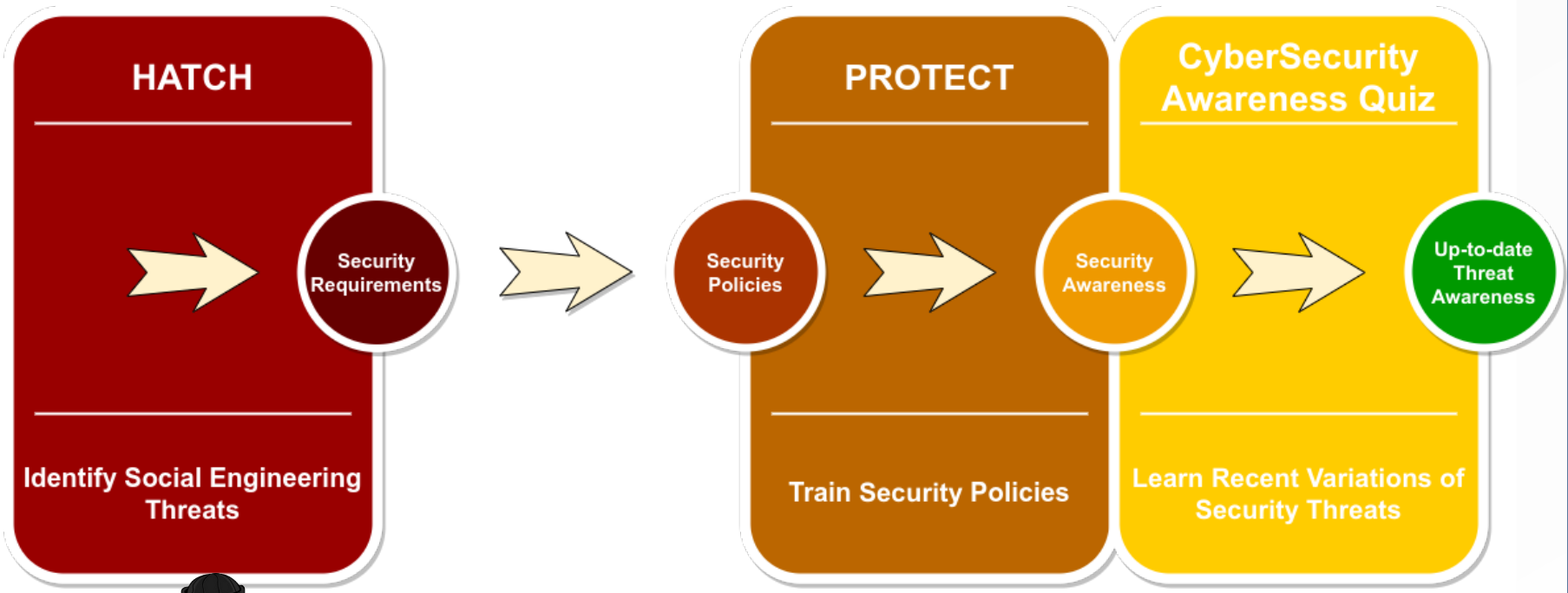
- Awareness Training
- Implications to real work environment?

Real World Scenario

- Real department plan
- Colleagues

- Threat Analysis
- Reasonable for employees?

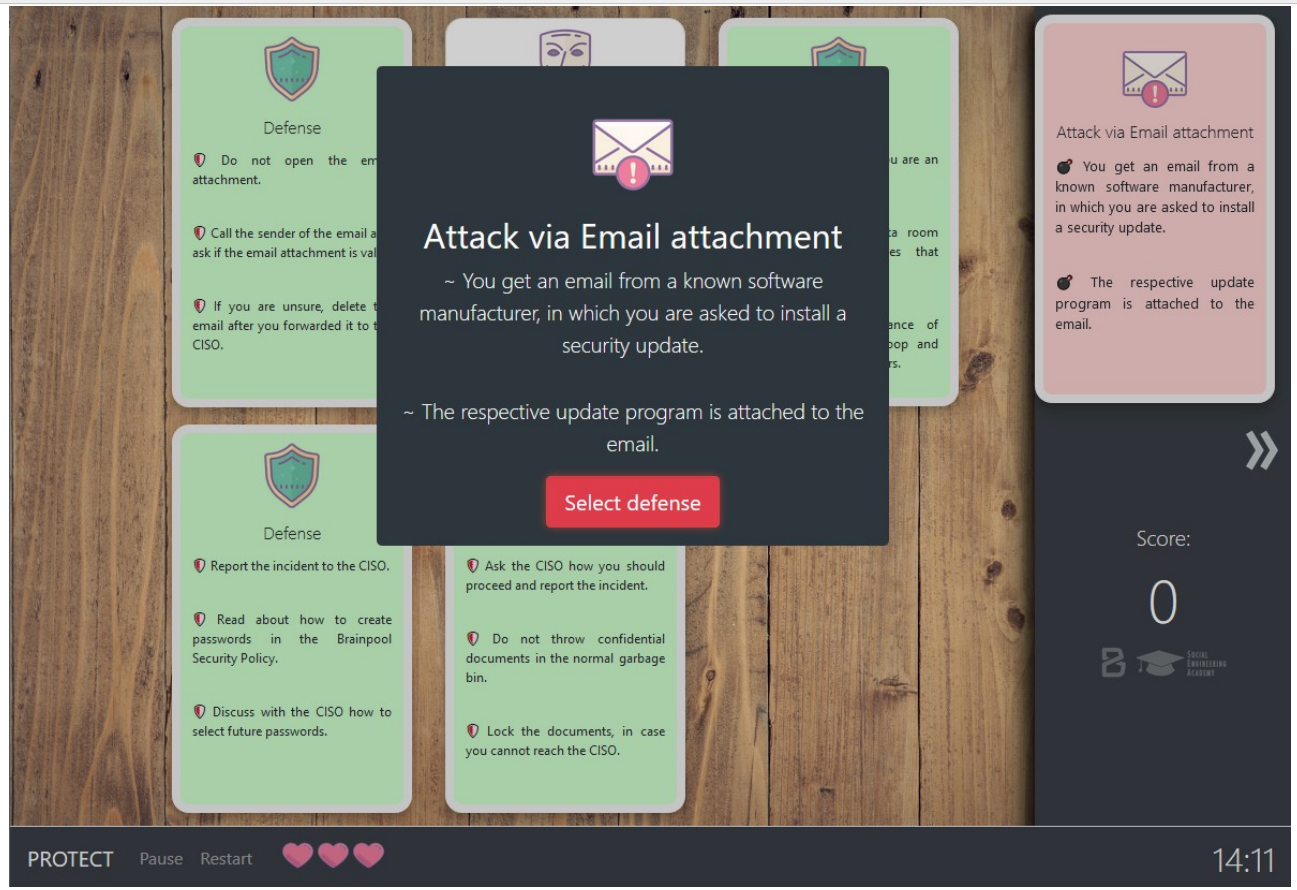
Serious Games Cascade



PR  TECT

Ludger Goeke, Alejandro Quintanar, Kristian Beckers, and Sebastian Pape. PROTECT - an easy configurable serious game to train employees against social engineering attacks. In Computer Security - ESORICS 2019 International Workshops, IOSec, MSTEC, and FINSEC, Luxembourg, September 26-27, 2019, Revised Selected Papers, volume 11981 of Lecture Notes in Computer Science, pages 156–171, Cham, 2019.

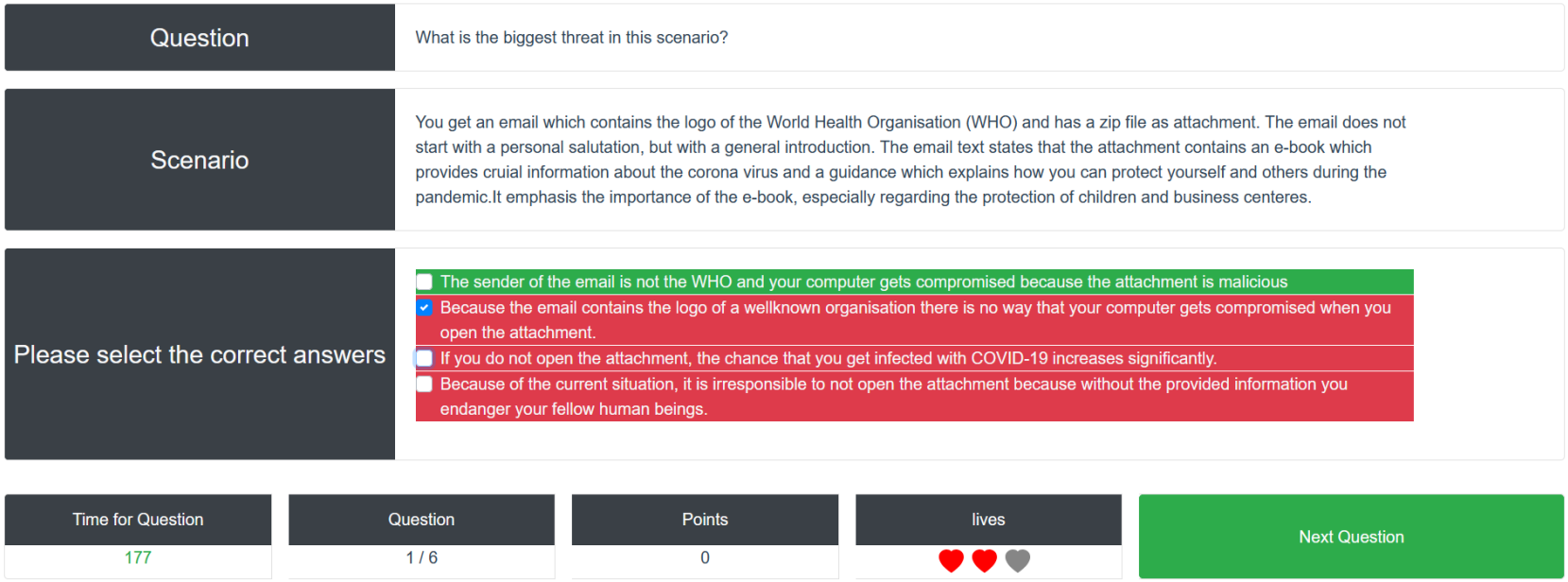
PROTECT


Defense
Do not open the em
attachment.
Call the sender of the email a
ask if the email attachment is val
If you are unsure, delete t
email after you forwarded it to t
CISO.
Attack via Email attachment
~ You get an email from a known software manufacturer, in which you are asked to install a security update.
~ The respective update program is attached to the email.
Select defense
Attack via Email attachment
You get an email from a known software manufacturer, in which you are asked to install a security update.
The respective update program is attached to the email.
Defense
Report the incident to the CISO.
Read about how to create passwords in the Brainpool Security Policy.
Discuss with the CISO how to select future passwords.
Ask the CISO how you should proceed and report the incident.
Do not throw confidential documents in the normal garbage bin.
Lock the documents, in case you cannot reach the CISO.
Score:
0
PROTECT
Pause
Restart
14:11

CyberSecurity
Awareness Quiz

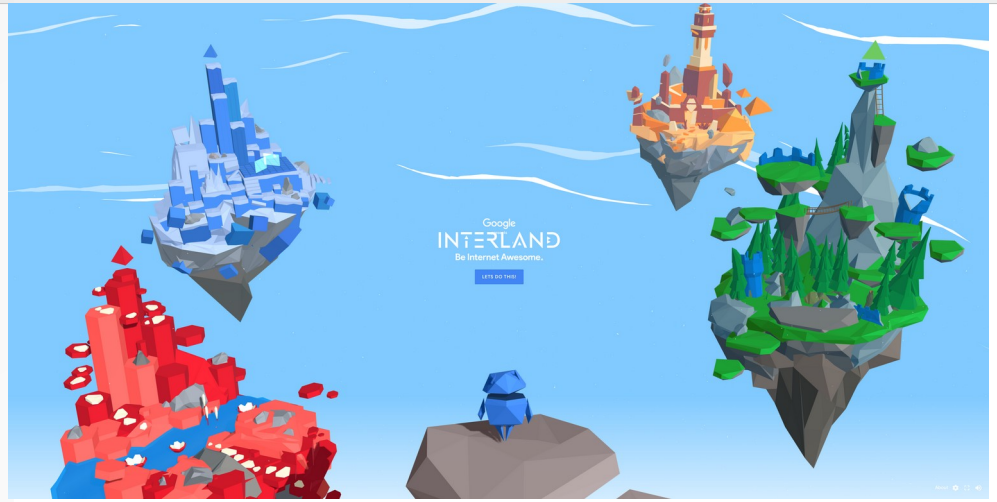
Sebastian Pape, Ludger Goeke, Alejandro Quintanar, and Kristian Beckers. Conceptualization of a cybersecurity awareness quiz. In Computer Security - ESORICS 2020 International Workshops MSTEC, to appear, 2020.

CyberSecurity Awareness Quiz



Sebastian Pape, Ludger Goeke, Alejandro Quintanar, and Kristian Beckers. Conceptualization of a cybersecurity awareness quiz. In Computer Security - ESORICS 2020 International Workshops MSTEC, 2020.

Serious Games Raising Privacy Awareness



Screenshot sources:

- https://beinternetawesome.withgoogle.com/
- https://www.datak.ch/
- https://datadealer.com/

Pape, S.; Klauer, A. and Rebler, M.: Leech: Let's Expose Evidently bad data Collecting Habits - Towards a Serious Game on Understanding Privacy Policies (Poster). In 17th Symposium on Usable Privacy and Security (SOUPS 2021), 2021.

Leech: Let's Expose Evidently bad data Collecting Habits

Towards a Serious Game on Understanding Privacy Policies

Sebastian Pape[1,2], Alexander Klauer[3,4] and Michaela Rebler[3]

[1]Goethe University Frankfurt [2]Social Engineering Academy [3]University of Regensburg [4]University College London

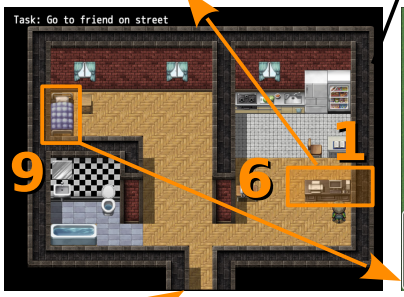
Abstract

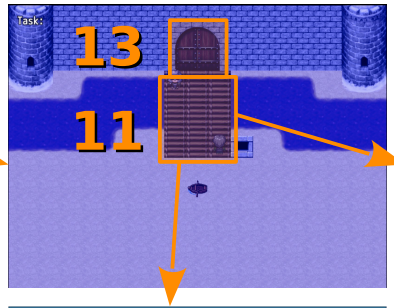
Most privacy policies are incomprehensive and largely unreadable. Thus, most users do not bother to read them. We propose **Leech**, a serious game for learning about the contents and structure of privacy policies so that users get a rough understanding what to expect in privacy policies.

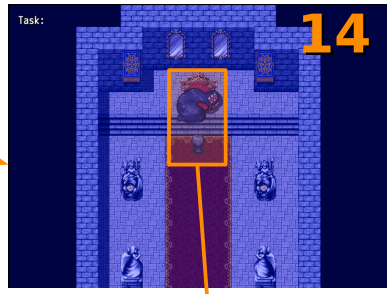
Leech is an adventure game and the player has to solve quests to complete the game. Two pretests led to promising results and we intend to quantitatively evaluate the game in the next step by investigating players' online privacy literacy, demographics, values on privacy policies, actions within the game, and their in-game experience.

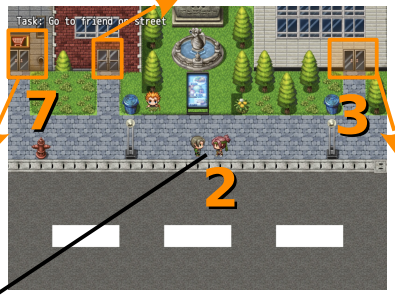
Players' actions and choices have consequences later in the game to learn about delayed consequences of accepting a privacy policy.

Main game is developed with **RPG Maker**



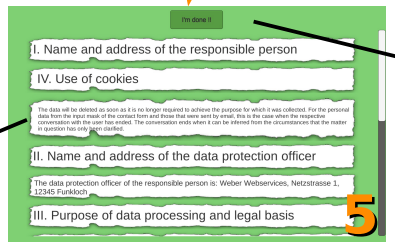






Task descriptions lead the player through the game.

Ingame Characters explain effects of ignoring privacy policies and how they work.



Sort Policy: the player has to sort snippets of a privacy policy to learn about relevant parts and the structure of privacy policies.

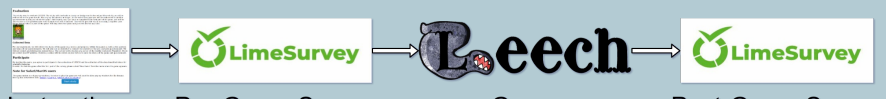
Minigames are embedded in the main story to allow for extra **interactivity**.

Sort Policy and Quiz are developed with **Unity.**

Quiz: to cover more broadly different topics from the GDPR.

Evaluation

- 2 Pre-tests with in total 18 persons
  - Positive feedback
  - Led to several improvements
- Quantitative evaluation planned including
  - Demographics
  - Online Privacy Literacy [1]
  - Values on Privacy Policies [2]
  - In-Game Experience Questionnaire [3]



https://leech.pallas.net/

References

1) Sabine Trepte, Doris Teutsch, Philipp K Masur, Carolin Eicher, Mona Fischer, Alisa Hennhöfer, and Fabienne Lind. Do people know about privacy and data protection strategies? Towards the "online privacy literacy scale"(OPLIS). In Reforming European data protection law, pages 333–365. Springer, 2015.
2) Julia Brande Earp, Annie I Antón, Lynda Aiman-Smith, and William H Stufflebeam. Examining internet privacy policies within the context of user privacy values. IEEE Transactions on Engineering Management, 52(2):227–237, 2005.
3) Wijnand A IJsselsteijn, Yvonne AW de Kort, and Karolien Poels. The game experience questionnaire. Eindhoven: Technische Universiteit Eindhoven, 46(1), 2013.

Acknowledgements

This work was supported by the EU's Horizon 2020 research and innovation program under grant agreements 786890 (THREAT-ARREST) and 830929 (CyberSecurity4Europe).

Challenges / Open Problems

- Fun vs. Serious Learning
- Game type suitable for Goal
- Clearly defined goal
  - Fun
  - Learning outcome
  - Behaviour Change
  - Persuasion
  - Artifact
  - ...
- Evaluation
  - Games: Especially Multiplayer: Lack of reproduceability
  - Privacy and Security Awareness are hard to measure

Literature Study on Gamification

Affordance	Included in the study
Points	[4][13][15][16][23][27][34] [37][41]
Leaderboards	[4][10][13][15][16][21][23] [27][37][41]
Achievements/ Badges	[2][8][10][17][20][22][25][27] [34]
Levels	[11][15][16][21][27][37]
Story/Theme	[12][18][21][23][33][36]
Clear goals	[11][27][33][32]
Feedback	[4][11][21][27][32][33]
Rewards	[12][18][33][36]
Progress	[14][18][27][33]
Challenge	[4][13][18][21][23][27][33]

Results	Paper
All tests positive	[13][37]
Part of the tests positive	[8][10][12][14][15][16][18] [22][23][25][27][32][33]
All tests not significant	-
Only descriptive statistics	[2][4][17][20][21][36][41]

Dependent variable	Paper
Psychological outcomes	[4][8][10][11][12][17][18][21] [27][33][34][41]
Behavioral outcomes	[2][4][8][10][11][13][14][15] [16][17][18][20][21][22][23] [25][27][32][33][36][37]

Source: Hamari, J., Koivisto, J., & Sarsa, H. (2014, January). Does gamification work?--a literature review of empirical studies on gamification. In 2014 47th Hawaii international conference on system sciences (HICSS) (pp. 3025-3034). IEEE.

Literature Study on Gamification: Limitations

1) Small sample sizes (around N=20)
2) Proper, validated psychometric measurements were not used
   (when surveying experiences and attitudes)
3) Some experiments lacked control groups and relied solely on user evaluation
4) Controls between implemented motivational affordances were often lacking and multiple affordances were investigated as a whole
   (i.e. no effects from individual motivational affordances could be established)
5) Many presented only descriptive statistics –
   although they could have easily also inferred about the relationship between constructs
6) Experiment timeframes were in most cases very short
   (novelty might have skewed the test subjects' experiences in a significant way)
7) Lack of clarity in reporting the results

   ...

Source: Hamari, J., Koivisto, J., & Sarsa, H. (2014, January). Does gamification work?--a literature review of empirical studies on gamification. In 2014 47th Hawaii international conference on system sciences (HICSS) (pp. 3025-3034). IEEE.

Evaluation of Serious Games

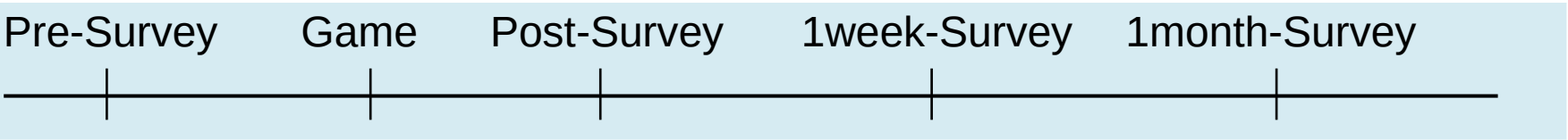
- Awareness Hard to measure
  - Questionnaires (SeBIS, OPLIS)
  - Many Questionnaires not public
  - Participants refuse to answer same questions again
  - Quiz: Learning through repetition?
- Self-Assessments
  - Might Introduce Bias
  - Assessment can change
  - Time / Date of Execution

Serge Egelman and Eyal Peer. Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS). In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '15). ACM, 2015.
Masur, P. K., Teutsch, D. & Trepte, S. (2017). Entwicklung und Validierung der Online-Privatheitskompetenzskala (OPLIS). Diagnostica, 63, 256-268.
Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. computers & security, 25(4), 289-296.

Evaluation of Serious Games

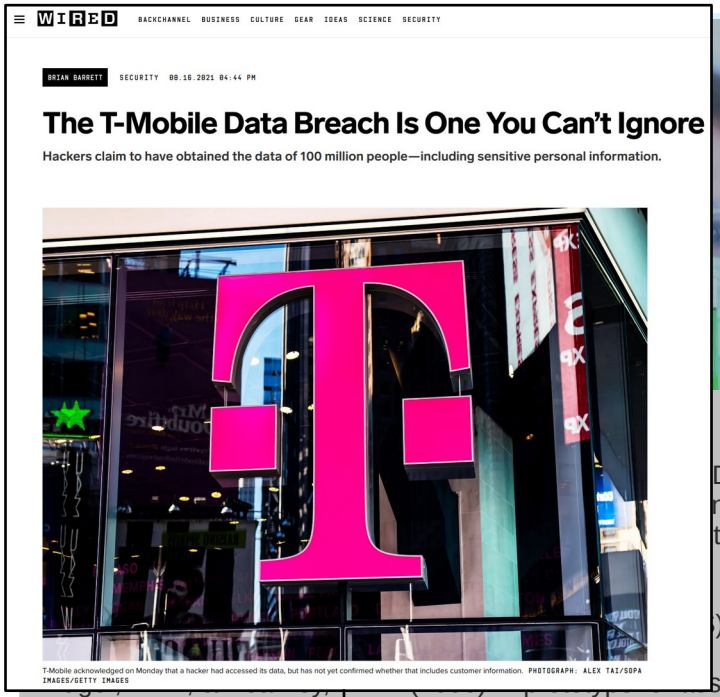
- Awareness Hard to measure
  - Questionnaires (SeBIS, OPLIS)
  - Many Questionnaires not public
  - Participants refuse to answer same questions again
  - Quiz: Learning through repetition?
- Self-Assessments
  - Might Introduce Bias
  - Assessment can change
  - Time / Date of Execution

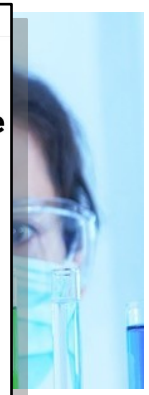
Serge Egelman and Eyal Peer. Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS). In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '15). ACM, 2015.
Masur, P. K., Teutsch, D. & Trepte, S. (2017). Entwicklung und Validierung der Online-Privatheitskompetenzskala (OPLIS). Diagnostica, 63, 256-268.
Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. computers & security, 25(4), 289-296.



Evaluation of Serious Games

- Awareness Hard to measure
  - Questionnaires (SeBIS, OPLIS)
  - Many Questionnaires not public
  - Participants refuse to answer same questions again
  - Quiz: Learning through repetition?
- Self-Assessments
  - Might Introduce Bias
  - Time / Date of Execution
  - Assessment can change

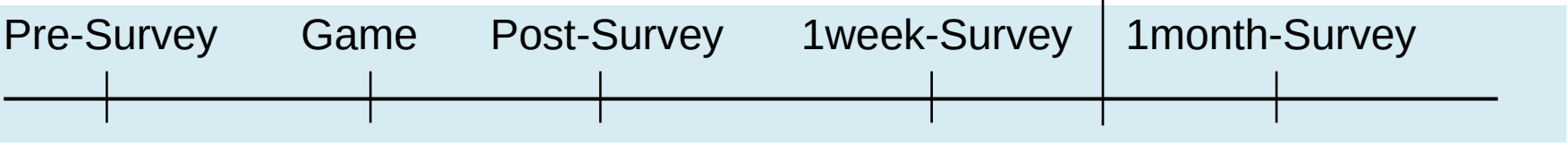




Developing
ngs of the
tems (CHI

und
).

sessing
information security awareness. computers & security, 25(4), 289-296.



Conclusion

- Serious Games are an interesting tool
- Already dozens of games for security
- Far less exist for privacy
- When used in corporate context
  - legal assessment needed
- Scientific evaluation is effortful and hard

Chair of Mobile Business & Multilateral Security

PD Dr. Sebastian Pape
Goethe University Frankfurt
Theodor-W.-Adorno-Platz 4
60629 Frankfurt, Germany

Phone +49 (0)69 798 34668
Fax +49 (0)69 798 35004

E-Mail: sebastian.pape@m-chair.de
WWW: www.m-chair.de