Challenges for Designing Serious Games on Security and Privacy Awareness

Sebastian Pape[1,2][0000−0002−0893−7856]

[1] Chair of Mobile Business & Multilateral Security
Goethe University Frankfurt, Germany
sebastian.pape@m-chair.de
[2] Social Engineering Academy GmbH, Frankfurt, Germany

Abstract. Serious games seem to be a good alternative to traditional trainings since they are supposed to be more entertaining and engaging. However, serious games also create specific challenges: The serious games should not only be adapted to specific target groups, but also be capable of addressing recent attacks. Furthermore, evaluation of the serious games turns out to be challenging. While this already holds for serious games in general, it is even more difficult for serious games on security and privacy awareness. On the one hand, because it is hard to measure security and privacy awareness. On the other hand, because both of these topics are currently often in the main stream media requiring to make sure that a measured change really results from the game session. This paper briefly introduces three serious games to counter social engineering attacks and one serious game to raise privacy awareness. Based on the introduced games the raised challenges are discussed and partially existing solutions are presented.

Keywords: Serious Games · Security Awareness · Privacy Awareness · Social Engineering

1 Introduction

Huizinga [28] discusses the importance of the play element in culture and points out that games have a long history, animals already played long before humanity arose: ”Play is older than culture, for culture, however inadequately defined, always presupposes human society, and animals have not waited for man to teach them their playing.“ While one of the most significant aspects of play is that it is fun, it was only natural to explore the application of games for other purposes than entertainment. Abt [1] coined the term “serious games” in the 70s, although the idea was not new at that time. The “Landlord’s game”, a predecessor of Monopoly, was already created in 1902 to illustrate the dangers of capitalist approaches [39].

The main challenge of designing serious games is to keep the balance between entertainment and other purposes [20]. As the boundaries between playing and not playing are fuzzy [47], whether the designer succeeds will also depend on the players' target group of the game. However, compared to traditional forms of learning serious games are more entertaining and engaging, and have demonstrated a potential in industrial education and training disciplines [45].

To foster the discussion, selected games to counter social engineering attacks and raise privacy awareness will be sketched in Sect. 2. Sect. 3 discusses the challenge of creating appropriate content for a specific target group and to cope with permanently changing attacks. Sect. 4 discusses different types of evaluating the game along with specific challenges for evaluating security and privacy awareness. Sect. 5 concludes the paper.

2 Sample Serious Games to Prevent Social Engineering and Raise Privacy Awareness

Social Engineering is defined as a technique that exploits human weaknesses and aims to manipulate people into breaking normal security procedures [33]. It is expected that machine learning techniques surface as new powerful tools in the social engineering area [8] while defenders still have a lack of tool support [6].

In general, companies have two main strategies to defend against social engineering attacks: social engineering penetration testing [55] or raising the security awareness via campaigns or trainings. For social engineering penetration testing, the penetration testers are supposed to attack the employees and find vulnerabilities. Unfortunately, experiments have shown that this approach can lead to employees becoming demotivated when confronted with the results of the test [16]. Furthermore, the social engineering penetration tests may interfere with the employees' right of personality, resulting in ethical [25] and legal [56] issues.

While traditional security awareness training may prove successful in particular against phishing, often the training is conducted in a way that it does not have a long lasting effect [52]. As already discussed in the previous section, serious games may be a viable alternative.

There is a number of serious board games targeting different aspects of security awareness, such as Collect it All [30, 9, 31], Control Alt Hack [12, 13, 14, 23, 15], d0x3d [23, 22], Decisions and Disruptions [7], Elevation of Privileges [51, 50], Operation Digitale Schlange [44, 43], and the ISMS card game [54].

As a foundation for our discussion, we introduce the three serious games HATCH, PROTECT and the CyberSecurity Awareness Quiz in this section which all aim to counter social engineering attacks. Their relation is shown in Fig. 1 [34] and will be further elaborated in the next subsections. HATCH is a physical card game and PROTECT and the CyberSecurity Awareness Quiz are digital games which have also been integrated in the TREAT-ARREST project's cyber ranges platform [26]. Additionally to the serious security games, we also briefly introduce the serious game LEECH which is not connected to the previously described games and aims to increase the players' privacy awareness.

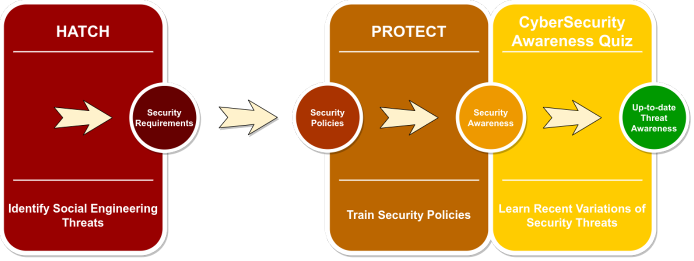
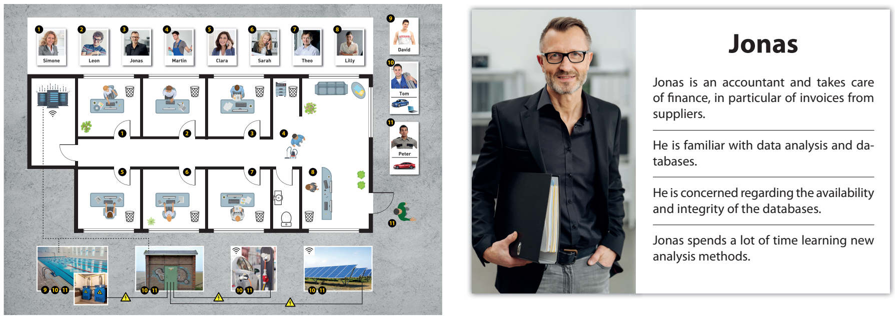

HATCH
Security Requirements
Identify Social Engineering Threats
PROTECT
Security Policies
Security Awareness
Train Security Policies
CyberSecurity Awareness Quiz
Up-to-date Threat Awareness
Learn Recent Variations of Security Threats

Fig. 1: Relation of HATCH, PROTECT and CyberSecurity Awareness Quiz [34]

2.1 HATCH

Schaab et al. [48] examined the psychological principles of social engineering and investigated which psychological techniques induce resistance to persuasion applicable for social engineering. Based on the identified gaps [49], the serious game HATCH [5] is proposed to foster the players' understanding of social engineering attacks. When playing HATCH, players attack personas in a virtual scenario based on cards with psychological principals and social engineering attacks. While personas are by definition imaginary, they provide a realistic descriptions of stakeholders or in this case employees, who have names, jobs, feelings, goals, and certain needs [18]. This way players can learn about the attackers' perspective, their vulnerabilities and get a better understanding of potential attack vectors. Fig. 2a shows a scenario plan for small energy providers [11, 38] and Fig. 2b describes one of the personas from the scenario.



Jonas

Jonas is an accountant and takes care of finance, in particular of invoices from suppliers.

He is familiar with data analysis and databases.

He is concerned regarding the availability and integrity of the databases.

Jonas spends a lot of time learning new analysis methods.

(a) Scenario Plan

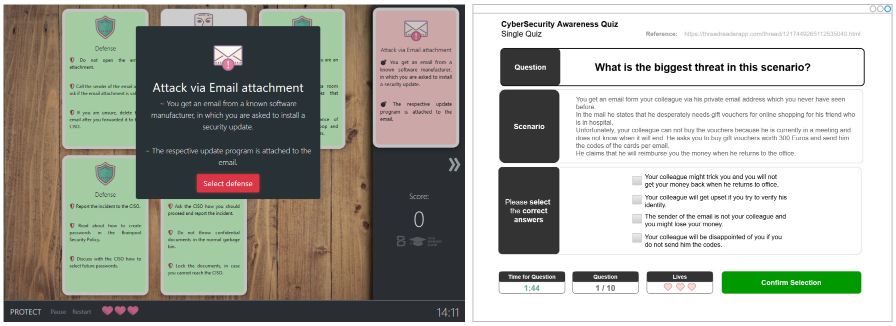
(b) Persona Card: Jonas, Accountant

Fig. 2: HATCH

However, HATCH can not only be used for training purposes but also to elicit security requirements to prevent social engineering [4]. Instead of the virtual personas, players describe social engineering attacks on their colleagues. Since players know their colleagues, no persona descriptions are necessary and players can exploit their knowledge about processes in their work environment, i. e. about how to cut through the red tape and informal ways of handling tasks. As a result, at the end of the game a list of potential attacks can be investigated by the IT department.

2.2 PROTECT

Based on the derived security requirements it is possible to adapt the organization's security policies. Since security policies are documents often unread by the users, the serious game PROTECT was developed to train users in behaving according to the organization's security policies [21]. PROTECT is the further development of PERSUADED [2] with the improvement of making the game more configurable and an improved graphical user interface as shown in Fig. 3a. Both games are digital card games where players have to defend against attacks with the correct defenses in a solitaire like game type. Special cards allow users to peak on the card pile and skip attack cards when they do not hold the corresponding defenses.



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.

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.

CyberSecurity Awareness Quiz
Single Quiz

Reference: https://threadreaderapp.com/thread/1217449265112535040.html

Question: What is the biggest threat in this scenario?

Scenario: You get an email form your colleague via his private email address which you never have seen before.
In the mail he states that he desperately needs gift vouchers for online shopping for his friend who is in hospital.
Unfortunately, your colleague can not buy the vouchers because he is currently in a meeting and does not know when it will end. He asks you to buy gift vouchers worth 300 Euros and send him the codes of the cards per email.
He claims that he will reimburse you the money when he returns to the office.

Please select the correct answers

- □ Your colleague might trick you and you will not get your money back when he returns to office.
- □ Your colleague will get upset if you try to verify his identity.
- □ The sender of the email is not your colleague and you might lose your money.
- □ Your colleague will be disappointed of you if you do not send him the codes.

Time for Question: 1:44
Question: 1 / 10
Lives: ♡ ♡ ♡

(a) PROTECT (b) CyberSecurity Awareness Quiz

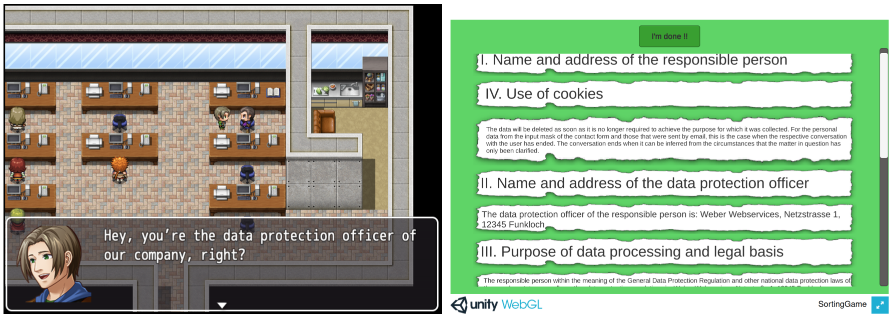
Fig. 3: Graphical User Interfaces for Serious Games

2.3 CyberSecurity Awareness Quiz

Attackers adapt their attacks based on recent events, e. g., such as the COVID-19 pandemic [46], and naturally security policies can not be adapted too often and fast enough. Therefore, it is also important to raise the employees' awareness about recent attacks or attack variations. For that purpose, we propose the CyberSecurity Awareness Quiz [35] which allows to add new content with only little effort. Fig. 3b shows the user interface for the players. We also propose a process for the timely development of new questions based on recent attacks. For that purpose, several relevant news feeds and websites are used as input. If adequate attacks are identified questions on the attack are derived along with correct and incorrect answers. The quiz content editor may then group selected questions to form a quiz or select all questions matching a certain keyword. In future work we intend to investigate by user studies if the implementation is also perceived as lightweight by the players and if players perceive the game suitable for occasional playing.

2.4 Leech

In contrast to the previous three games, Leech does not address security awareness, but privacy awareness. As a continuation to work on an assessment framework for privacy policies of Internet of Things Services [41] based on particular General Data Protection Regulation (GDPR) [42] requirements, the serious game Leech was developed. The aim of is Leech is to foster players' learning about the contents and structure of privacy policies so that they get a rough understanding what to expect in privacy policies. Leech is an adventure game (cf. Fig. 4a) and the player has to solve quests to complete the game. Two of the tasks are implemented as a mini game, i. e. sorting snippets of a privacy policy, (cf. Fig. 4b) to allow more complexity. Two pre-tests led to promising results and a quantitative evaluation of the game is planned as the next step by investigating players' online privacy literacy, demographics, values on privacy policies, actions within the game, and their in-game experience [37].



Hey, you're the data protection officer of our company, right?

I. Name and address of the responsible person

IV. Use of cookies

The data will be deleted as soon as it is no longer required to achieve the purpose for which it was collected. For the personal data from the input mask of the contact form and those that were sent by email, this is the case when the respective conversation with the user has ended. The conversation ends when it can be inferred from the circumstances that the matter in question has only been clarified.

II. Name and address of the data protection officer

The data protection officer of the responsible person is: Weber Webservices, Netzstrasse 1, 12345 Funkloch

III. Purpose of data processing and legal basis

The responsible person within the meaning of the General Data Protection Regulation and other national data protection laws of

(a) Main Game

(b) Mini Game

Fig. 4: Leech

3 Game Content Creation and Adaption

Even if the main idea and game mechanics of a serious game are already finished, the content of the game needs to be designed or may need to be adapted later. In this section, we discuss two challenges regarding the content: Adapting it to the appropriate target group and adapting it to recent attacks.

3.1 Adressing Target Groups

Similar to awareness campaigns, the scope of serious games should be as specific as possible to the target audience [3]. One can already see from the different nature of the proposed games, that each of the games needs different content. For HATCH scenarios and persona descriptions need to be created. For PROTECT attack descriptions and matching defense pairs need to be created and for the CyberSecurity Awareness Quiz a catalog of questions along with correct and not so easy to determine wrong answers needs to be created. We will cover the creation of quiz questions in the next subsection and further elaborate on the most difficult task: Creating scenarios for HATCH.

We propose a systematic approach based on grounded theory as proposed by Faily and Flechais [18] (cf. Fig. 5). By conducting interviews with relevant stakeholders, systematically coding the answers, and grouping the codes different properties for the personas can be derived [27]. We have evaluated the approach by building a virtual scenario for consultant companies. The approach worked well and we obtained a reasonable scenario. However, the approach was quite time consuming, thus we propose further research in lightweight approaches which allow the creation of appropriate scenarios with less effort.

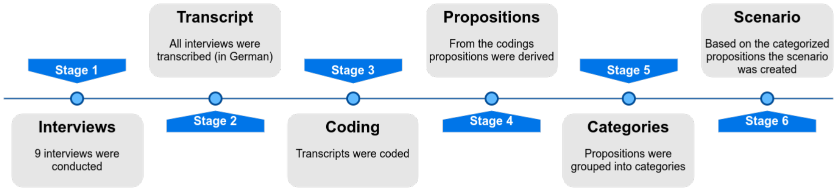

Stage 1
Interviews
9 interviews were conducted
Stage 2
Transcript
All interviews were transcribed (in German)
Stage 3
Coding
Transcripts were coded
Stage 4
Propositions
From the codings propositions were derived
Stage 5
Categories
Propositions were grouped into categories
Stage 6
Scenario
Based on the categorized propositions the scenario was created

Fig. 5: Content Creation Process for HATCH [27]

3.2 Addressing Recent Attacks

Another challenge is to address the attackers' adaption of attacks. Naturally, the time span from discovering new types of attack, adapting the security policies and training the players in the new security policy is too long to be an effective tool. During the process of improving the security policies, the attacker might already have changed their attack theme.

In general, one would not want to wait until recent attacks start attacking the organization's employees, but rather try to prepare them beforehand. As a consequence, relying on public available information on attacks already observed in the wild seems to be a viable option. For that purpose appropriate web resources like news and security websites, feeds, blogs or even twitter accounts which publish content related to social engineering attacks need to be collected. Content which is presented in a structured manner is in general preferable, as it might allow an automation. Figure 6 shows an overview of the steps for a possible information procurement [35] for the CyberSecurity Awareness Quiz:

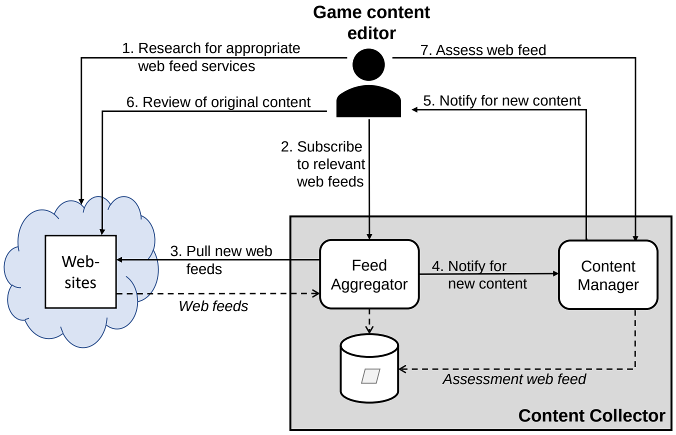

Game content editor
1. Research for appropriate web feed services
7. Assess web feed
6. Review of original content
5. Notify for new content
2. Subscribe to relevant web feeds
Web-sites
3. Pull new web feeds
Web feeds
Feed Aggregator
4. Notify for new content
Content Manager
Assessment web feed
Content Collector

Fig. 6: Transforming News about Attacks into Questions [35]

In the initial step of the process, the game content editor will search for sources which publish content about social engineering attacks and implement a web feed service. This step will be repeated periodically to check if new appropriate web resources are available. The information from the feed will be aggregated automatically and if new content is found, the game content editor will get the new feeds to assess them manually and create new content for the game, when appropriate.

The CyberSecurity Awareness Quiz was specifically built, to allow the fast creation of new content. The generation of appropriate question and answer pairs can be done much faster than the creation of new scenarios for HATCH or the adaption of the security policies along with the creation of new attack/defense pairs for PROTECT. This also demonstrates that the serious game does not only need to be adapted to a specific target group, but also to a specific purpose: Here, the possibility to react to new attacks in the wild as fast as possible.

4 Evaluation of Serious Games

There are numerous dimensions to evaluate for serious games. The most obvious dimensions are the entertainment factor and the effectiveness of the serious game. However, there are several other dimensions which are worthwhile to investigate also. One of the aspects is to ensure no harm is done to the players respectively employees. While this might sound surprising on a first glance, it can easily be possible that players may be bullied during the game or that their personal data is exposed. We deal in the next subsection with the challenge of measuring the effectiveness of the serious game and in the following subsection, we briefly cover legal and ethical aspects.

4.1 Effectiveness

To the best of our knowledge, regarding the general evaluation of serious games, there is not much literature. However, there is a literature survey in a related area on gamification [24], which observes that many papers only report descriptive statistics and only papers are published with either all or at least a part of the tests were positive (publication bias). Further problems reported were a small sample size, self-developed questionnaires omitting validated psychometric measurements, very short time frames, and the lack of control groups. The literature review also denotes several other points of criticism, such as lack of clarity in reporting the goals of the game and the results. A similar literature review was done on positive effects on computer games in general [10], which also includes a limited number of serious games. Their result was comparable, in particular, they only found one paper explicitly making use of correlations. The only study specifically on serious games for CSA from Tioh et al. [53] also found that evaluations were done with small sample sizes and rather informally. However, the study also covers only a small set of games.

Although, we did not do a systematic analysis, from the papers on serious games, we have investigated, we found a similar pattern. In particular, the patterns of a low number of participants, not explicitly and measurable formulated goals, short time frames of the experiment, i. e. measuring directly after the game, and the lack of control groups were often seen. In particular long term measurements, e. g. several weeks after playing the game, would yield in more interesting insights as many effects might be measurable immediately after the game, but will vanish when time elapses. Furthermore, since many main stream media report also about security and privacy incidents, control groups for long term measurements are unavoidable. This dramatically increases the necessary effort for evaluating the effectiveness of serious games on security and privacy awareness. Since the duration of the games can be between a couple of minutes and several days and participants not only need to play the game, but also participate in the evaluation procedure, e. g. filling a questionnaire, the evaluation of serious games requires significant resources. As a further problem, this may also lead to a selection bias, as not all potential players might be willing to participate in such a time consuming evaluation.

Security and Privacy Awareness One of the problems for security and privacy awareness is, that it they are hard to measure. Besides the idea of social engineering penetration testing of the employees, which we have already discussed, the best way of measuring security or privacy awareness are self-reported questionnaires such as human aspects of information security [40], security attitudes [19], security behaviour [17], and the online privacy literacy scale[32]. However, self-reported questionnaires might not be the most reliable measurement, as they might not only be influenced by the participants' mood, but participants also often get annoyed if they need to repeatedly answer the same questions, i. e. measuring before and after the game. As it is not well researched how repeatably answering the security and privacy awareness questionnaires might change the results, this might also effect the results.

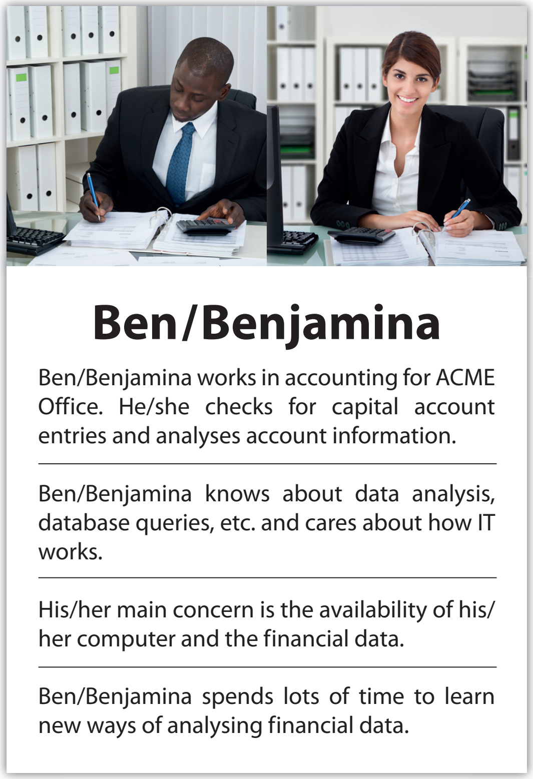
4.2 Legal and Ethical Assessment

For the three introduced serious games countering social engineering threats, HATCH is the most obvious candidate for a legal assessment. On the one hand, because with real scenarios it may be used with the players as victims in the game putting their personal data at risk. On the other hand, because PROTECT and the CyberSecurity Awareness Quiz are both single player games, and therefore face less risks, e. g. of players bullying each other.

When playing HATCH with a realistic scenario, the employees' personal information might be at risk if players use it to describe their attacks. Legal requirements demand a careful consideration of conditions the game can be used in. Therefore, we provide a legal analysis of the requirements to use HATCH for threat elicitation [29]. The main outcome is that the virtual scenario may be used without hesitation since players are not as victims part of the game, and therefore other players do not attack them in the game. The realistic scenario should only be used for threat elicitation since the risk of players accidentally or intentionally exposing other players is real.

While the assessment was specifically investigating HATCH and one would need to do a legal assessment for each considered serious security game before playing it in an official context, some general conclusions can be drawn. The most important question arising is if employees' personal characteristics are subject to the game. If they are, the organization needs a justification why a more gentle type of training without considering the employees' personal characteristics is not appropriate. This could be the case if the organization wants to conduct a threat analysis, for example because there already have been some incidents or the organization is specifically exposed social engineering attacks and wants to mitigate that [36].

From an ethical perspective, one needs to also carefully consider other aspects, i. e. discrimination. This in particular concerns the virtual scenarios. While



Ben/Benjamina

Ben/Benjamina works in accounting for ACME Office. He/she checks for capital account entries and analyses account information.

Ben/Benjamina knows about data analysis, database queries, etc. and cares about how IT works.

His/her main concern is the availability of his/her computer and the financial data.

Ben/Benjamina spends lots of time to learn new ways of analysing financial data.

Fig. 7: Gender Inclusive Persona Card for HATCH

it might be natural to develop personas which realistically reflect the situation in most companies, this might also lead to stereotypes discriminating certain groups, e. g. females when the managing positions are all modeled with males and subordinate positions such as cleaning staff are modeled with female personas. One solution to this problem is to design gender inclusive personas (cf. Fig. 7). However, this can only be the first step as this version only addresses gender, but does not consider any minorities.

5 Summary and Conclusion

We have briefly introduced serious games on security and privacy awareness. Based on the presented games, we have first discussed the challenged to create content which is appropriate for the players' target group and covers recent attacks. Furthermore, we have sketched, that the evaluation of serious games requires a lot of resources, such as long term experiments with a large sample size including control groups in order to be meaningful. Furthermore, in particular for security and privacy awareness, there is no automated measurement, resulting in self-reported questionnaires, which may cause problems if they are repeatedly answered. A systematic, standardized way to measure the outcomes of serious games may be desirable, although one of the remaining problems will probably still be to attract participants and in particular motivate them to participate in a long term study.

We have presented a legal assessment for HATCH. While some aspects can be transferred to other serious games, in order to use them in a broad manner in a professional context, individual assessments considering labor law might be necessary for each of the games. Further challenges of serious games include measuring dimensions which might not be expected at a first glance. This in particular refers to discrimination. While we have discussed gender inclusive persona cards for HATCH, gender was only addressed in a binary form. Future work could also try to cover further aspects of discrimination, e. g. consider minorities.

Acknowledgements

This work was supported by European Union's Horizon 2020 research and innovation program from the project CyberSec4Europe (grant agreement number: 830929) and from the project THREAT-ARREST (grant agreement number: 786890). We are also grateful to Kristina Femmer for designing plans and persona cards for HATCH.

Bibliography

[1] Abt, C.C.: Serious games. University press of America (1987)

[2] Aladawy, D., Beckers, K., Pape, S.: PERSUADED: Fighting Social Engineering Attacks with a Serious Game. In: Furnell, S., Mouratidis, H., Pernul, G. (eds.) Trust, Privacy and Security in Digital Business - 15th International Conference, TrustBus 2018, Regensburg, Germany, September 5-6, 2018, Proceedings. Lecture Notes in Computer Science, vol. 11033. Springer (2018), https://doi.org/10.1007/978-3-319-98385-1_8

[3] Bada, M., Sasse, A.M., Nurse, J.R.C.: Cyber security awareness campaigns: Why do they fail to change behaviour? CoRR abs/1901.02672 (2019), http://arxiv.org/abs/1901.02672

[4] Beckers, K., Pape, S.: 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), https://ieeexplore.ieee.org/document/7765507

[5] Beckers, K., Pape, S., 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), https://www.scienceopen.com/document?vid=ef4958b1-ff29-42e5-b58f-f66b8ef30a87

[6] Beckers, K., Schosser, D., Pape, S., Schaab, P.: A structured comparison of social engineering intelligence gathering tools. In: Trust, Privacy and Security in Digital Business - 14th International Conference, TrustBus 2017, Lyon, France, August 30-31, 2017, Proceedings. pp. 232–246 (2017), https://doi.org/10.1007/978-3-319-64483-7_15

[7] University of Bristol, B.C.S.G.: Decisions and disruptions homepage. http://www.decisions-disruptions.org/ (????)

[8] Canavese, D., Lioy, A., Pedone, I., Regano, L., Hatamian, M., Löbner, S., Pape, S., Arastouei, N., Skarmeta, A., Hita, A., Bernal, J.: Cybersecurity outlook 1. Tech. rep., CyberSec4Europe (09 2020), https://cybersec4europe.eu/wp-content/uploads/2021/01/D3.10-Cybersecurity-outlook-1-Submitted.pdf

[9] CIA: Cia: Collect it all - declassified training game. https://www.muckrock.com/foi/united-states-of-america-10/materials-for-the-game-collection-deck-35175/#file-162778 (????)

[10] Connolly, T.M., Boyle, E.A., MacArthur, E., Hainey, T., Boyle, J.M.: A systematic literature review of empirical evidence on computer games and serious games. Computers & education 59(2), 661–686 (2012)

[11] Dax, J., Hamburg, D., Pape, S., Pipek, V., Rannenberg, K., Schmitz, C., Sekulla, A., Terhaag, F.: Sichere informationsnetze bei kleinen und mittleren energieversorgern (sidate). In: Rudel, S., Lechner, U. (eds.) State of the Art: IT-Sicherheit für Kritische Infrastrukturen, chap. Sichere Informationsnetze

bei kleinen und mittleren Energieversorgern (SIDATE), p. 29. Universität der Bundeswehr, Neubiberg (2018)

[12] Denning, T., Kohno, T., Shostack, A.: Control-alt-hack: A card game for computer security outreach, education, and fun. Tech. Rep. UW-CSE-12-07-01, Department of Computer Science and Engineering University of Washington (July 2012)

[13] Denning, T., Kohno, T., Shostack, A.: Control-alt-hack™: a card game for computer security outreach and education (abstract only). In: Camp, T., Tymann, P.T., Dougherty, J.D., Nagel, K. (eds.) The 44th ACM Technical Symposium on Computer Science Education, SIGCSE '13, Denver, CO, USA, March 6-9, 2013. p. 729. ACM (2013), http://doi.acm.org/10.1145/2445196.2445408

[14] Denning, T., Lerner, A., Shostack, A., Kohno, T.: Control-alt-hack: the design and evaluation of a card game for computer security awareness and education. In: Sadeghi, A., Gligor, V.D., Yung, M. (eds.) 2013 ACM SIGSAC Conference on Computer and Communications Security, CCS'13, Berlin, Germany, November 4-8, 2013. pp. 915–928. ACM (2013), http://doi.acm.org/10.1145/2508859.2516753

[15] Denning, T., Shostack, A., Kohno, T.: Practical lessons from creating the control-alt-hack card game and research challenges for games in education and research. In: Peterson, Z.N.J. (ed.) 2014 USENIX Summit on Gaming, Games, and Gamification in Security Education, 3GSE '14, San Diego, CA, USA, August 18, 2014. USENIX Association (2014), https://www.usenix.org/conference/3gse14/summit-program/presentation/denning

[16] Dimkov, T., Van Cleeff, A., Pieters, W., Hartel, P.: Two methodologies for physical penetration testing using social engineering. In: Proceedings of the 26th annual computer security applications conference. pp. 399–408 (2010)

[17] Egelman, S., Peer, E.: Scaling the security wall: Developing a security behavior intentions scale (sebis). In: Proceedings of the 33rd annual ACM conference on human factors in computing systems. pp. 2873–2882 (2015)

[18] Faily, S., Flechais, I.: Persona cases: a technique for grounding personas. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. pp. 2267–2270 (2011)

[19] Faklaris, C., Dabbish, L.A., Hong, J.I.: A self-report measure of end-user security attitudes (sa-6). In: Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019). pp. 61–77 (2019)

[20] 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)

[21] Goeke, L., Quintanar, A., Beckers, K., Pape, S.: PROTECT - an easy configurable serious game to train employees against social engineering attacks. In: Fournaris, A.P., Athanatos, M., Lampropoulos, K., Ioannidis, S., Hatzivasilis, G., Damiani, E., Abie, H., Ranise, S., Verderame, L., Siena, A., Garcia-Alfaro, J. (eds.) Computer Security - ESORICS 2019 In-

ternational Workshops, IOSec, MSTEC, and FINSEC, Luxembourg City, Luxembourg, September 26-27, 2019, Revised Selected Papers. LNCS, vol. 11981, pp. 156–171. Springer International Publishing, Cham (09 2019), https://link.springer.com/chapter/10.1007/978-3-030-42051-2_11

[22] Gondree, M., Peterson, Z.N.J.: Valuing security by getting [d0x3d!]: Experiences with a network security board game. In: Kanich, C., Sherr, M. (eds.) 6th Workshop on Cyber Security Experimentation and Test, CSET '13, Washington, D.C., USA, August 12, 2013. USENIX Association (2013), https://www.usenix.org/conference/cset13/workshop-program/presentation/gondree

[23] Gondree, M., Peterson, Z.N.J., Denning, T.: Security through play. IEEE Security & Privacy 11(3), 64–67 (2013), http://dx.doi.org/10.1109/MSP.2013.69

[24] Hamari, J., Koivisto, J., Sarsa, H.: Does gamification work?–a literature review of empirical studies on gamification. In: 2014 47th Hawaii international conference on system sciences. pp. 3025–3034. Ieee (2014)

[25] Hatfield, J.M.: Virtuous human hacking: The ethics of social engineering in penetration-testing. Computers & Security 83, 354–366 (2019)

[26] Hatzivasilis, G., Ioannidis, S., Smyrlis, M., Spanoudakis, G., Frati, F., Braghin, C., Damiani, E., Koshutanski, H., Tsakirakis, G., Hildebrandt, T., Goeke, L., Pape, S., Blinder, O., Vinov, M., Leftheriotis, G., Kunc, M., Oikonomou, F., Magilo, G., Petrarolo, V., Chieti, A., Bordianu, R.: The threat-arrest cyber ranges platform. In: IEEE International Conference on Cyber Security and Resilience (CSR). IEEE (09 2021), https://ieeexplore.ieee.org/document/9527963

[27] Hazilov, V., Pape, S.: Systematic scenario creation for serious security-awareness games. In: Boureanu, I., Drâgan, C.C., Manulis, M., Giannetsos, T., Dadoyan, C., Gouvas, P., Hallman, R.A., Li, S., Chang, V., Pallas, F., Pohle, J., Sasse, A. (eds.) Computer Security - ESORICS 2020 International Workshops, DETIPS, DeSECSys, MPS, and SPOSE, Guildford, UK, September 17-18, 2020, Revised Selected Papers. LNCS, vol. 12580. Springer International Publishing, Cham (09 2020), https://link.springer.com/chapter/10.1007/978-3-030-66504-3_18

[28] Huizinga, J.: Homo ludens: A study on the play element in culture, reprint 1971 (1938)

[29] Kipker, D.K., Pape, S., Wojak, S., Beckers, K.: Juristische bewertung eines social-engineering-abwehr trainings. In: Rudel, S., Lechner, U. (eds.) State of the Art: IT-Sicherheit für Kritische Infrastrukturen, chap. Stand der IT-Sicherheit bei deutschen Stromnetzbetreibern, pp. 112–115. Universität der Bundeswehr, Neubiberg (2018)

[30] Liao, S.: The CIA made a magic: The gathering-style card game for training agents, and we played it. The Verge (May 2018), https://www.theverge.com/2018/5/21/17374054/cia-collect-it-all-declassified-training-tabletop-card-game

[31] Masnick, M.: Cia game kickstarter campaign. https://www.kickstarter.com/projects/mmasnick/cia-collect-it-all?ref=2fbwg2 (2019)

[32] Masur, P.K., Teutsch, D., Trepte, S.: Entwicklung und validierung der online-privatheitskompetenzskala (oplis). Diagnostica (2017)

[33] Papadaki, M., Furnell, S., Dodge, R.C.: Social engineering: Exploiting the weakest links. European Network & Information Security Agency (ENISA), Heraklion, Crete (2008)

[34] Pape, S.: Requirements engineering and tool-support for security and privacy (09 2020), http://publikationen.ub.uni-frankfurt.de/frontdoor/index/index/docId/59271

[35] Pape, S., Goeke, L., Quintanar, A., Beckers, K.: Conceptualization of a cybersecurity awareness quiz. In: Computer Security - ESORICS 2020 International Workshops MSTEC. LNCS, vol. 12512, pp. 61–76. Springer International Publishing, Cham (09 2020), https://link.springer.com/chapter/10.1007%2F978-3-030-62433-0_4

[36] Pape, S., Kipker, D.K.: Case study: Checking a serious security-awareness game for its legal adequacy. Datenschutz und Datensicherheit 45(5), 310–314 (05 2021), https://www.springerprofessional.de/en/case-study-checking-a-serious-security-awareness-game-for-its-le/19120160

[37] Pape, S., Klauer, A., 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) (06 2021), https://www.usenix.org/conference/soups2021/presentation/pape

[38] Pape, S., Schmitz, C., Kipker, D.K., Sekula, A.: On the use of information security management systems by german energy providers. In: Presented at the Fourteenth IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection (03 2020)

[39] Parlett, D.: The Oxford history of board games. Oxford University Press, USA (1999)

[40] Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., Jerram, C.: Determining employee awareness using the human aspects of information security questionnaire (hais-q). Computers & security 42, 165–176 (2014)

[41] Paul, N., Tesfay, W.B., Kipker, D.K., Stelter, M., Pape, S.: Assessing privacy policies of internet of things services. In: ICT Systems Security and Privacy Protection - 33rd IFIP TC 11 International Conference, SEC 2018, Held at the 24th IFIP World Computer Congress, WCC 2018, Poznan, Poland, September 18-20, 2018, Proceedings. pp. 156–169 (2018), https://doi.org/10.1007/978-3-319-99828-2_12

[42] Regulation, G.D.P.: Regulation eu 2016/679 of the european parliament and of the council of 27 april 2016. Official Journal of the European Union (2016)

[43] Rieb, A., Lechner, U.: Operation Digital Chameleon – Towards an Open Cybersecurity Method. In: Proceedings of the 12th International Sympo-

sium on Open Collaboration (OpenSym 2016). pp. 1–10. Berlin (2016), http://www.opensym.org/os2016/proceedings-files/p200-rieb.pdf

[44] Rieb, A., Lechner, U.: Towards Operation Digital Chameleon. In: Havârneanu, G., Setola, R., Nassopoulos, H., Wolthusen, S. (eds.) CRITIS 2016 - The 11th International Conference on Critical Information Infrastructures Security (to appear). pp. 1–6. Paris (2016)

[45] Riedel, J.C., Hauge, J.B.: State of the art of serious games for business and industry. In: 2011 17th International Conference on Concurrent Enterprising. pp. 1–8. IEEE (2011)

[46] Saleh, T.: Covidlock update: Deeper analysis of coronavirus android ransomware. https://www.domaintools.com/resources/blog/covidlock-update-coronavirus-ransomware (2020)

[47] Salen, K., Tekinbaş, K.S., Zimmerman, E.: Rules of play: Game design fundamentals. MIT press (2004)

[48] Schaab, P., Beckers, K., Pape, S.: A systematic gap analysis of social engineering defence mechanisms considering social psychology. In: 10th International Symposium on Human Aspects of Information Security & Assurance, HAISA 2016, Frankfurt, Germany, July 19-21, 2016, Proceedings. (2016), https://www.cscan.org/openaccess/?paperid=301

[49] Schaab, P., Beckers, K., Pape, S.: Social engineering defence mechanisms and counteracting training strategies. Information and Computer Security 25(2), 206–222 (2017), https://doi.org/10.1108/ICS-04-2017-0022

[50] Shostack, A.: Elevation of privilege: Drawing developers into threat modeling. Tech. rep., Microsoft, Redmond, U.S. (2012), http://download.microsoft.com/download/F/A/E/FAE1434F-6D22-4581-9804-8B60C04354E4/EoP_Whitepaper.pdf

[51] Shostack, A.: Threat Modeling: Designing for Security. John Wiley & Sons Inc., 1st edn. (2014)

[52] Stahl, S.: Beyond information security awareness training: It's time to change the culture. Information Security Management Handbook, Volume 3 3, 285 (2006)

[53] Tioh, J.N., Mina, M., Jacobson, D.W.: Cyber security training a survey of serious games in cyber security. In: 2017 IEEE Frontiers in Education Conference (FIE). pp. 1–5. IEEE (2017)

[54] UK, I.G.: The isms card game homepage. https://www.itgovernance.co.uk/shop/product/the-isms-card-game (2022)

[55] Watson, G., Mason, A., Ackroyd, R.: Social engineering penetration testing: executing social engineering pen tests, assessments and defense. Syngress (2014)

[56] Zimmer, M., Helle, A.: Tests mit Tücke– Arbeitsrechtliche Anforderungen an Social Engineering Tests. Betriebs-Berater 21(2016), 1269 (2016)