Evaluation Strategies for Cybersecurity Training Methods: A Literature Review

Joakim Kävrestad, Marcus Nohlberg

Evaluation strategies for cybersecurity training methods: a literature review

Joakim Kävrestad[1][0000−0003−2084−9119] and Marcus Nohlberg[1][0000−0001−5962−9995]

University of Skövde, Sweden *firstname.lastname*@his.se

Abstract. The human aspect of cybersecurity continues to present challenges to researchers and practitioners worldwide. While measures are being taken to improve the situation, a vast majority of security incidents can be attributed to user behavior. Security and Awareness Training (SAT) has been available for several decades and is commonly given as a suggestion for improving the cybersecurity behavior of end-users. However, attackers continue to exploit the human factor suggesting that current SAT methods are not enough. Researchers argue that providing knowledge alone is not enough, and some researchers suggest that many currently used SAT methods are, in fact, not empirically evaluated. This paper aims to examine how SAT has been evaluated in recent research using a structured literature review. The result is an overview of evaluation methods which describes what results that can be obtained using them. The study further suggests that SAT methods should be evaluated using a variety of methods since different methods will inevitably provide different results. The presented results can be used as a guide for future research projects seeking to develop or evaluate methods for SAT.

Keywords: Security · evaluation · methods · awareness · training · user

1 Introduction

It is well-established that insecure user behavior is one of the major challenges in cybersecurity [36]. Targeting users rather than technology is common practice for many attackers, and the need to make users more resilient to social engineering is apparent. As such, there is an obvious need to improve user behavior in regards to cybersecurity [6]. To this end, users must be helped to understand the consequences of their actions and learn how to act more securely [13]. For that purpose, user training is the go-to solution suggested in scientific research and offered by practitioners [23, 32].

Security and Awareness Training (SAT) has been discussed in the scientific literature for at least two decades [38]. However, recurring reports of attacks suggest that the problem of insecure user behavior is nowhere near being solved. On the contrary, industry reports describe that human-related attacks are the most common attacks, suggesting that up to 95% of attacks include the human element[12, 15, 39]. Some researchers even suggest that organizations' training

programs are often not grounded in empirical evidence of their effectiveness [1, 2]. Seeing how the problem of insecure user behavior is certainly not resolved, the need for further research into this area is apparent.

The goal of any SAT effort is to convey knowledge to the user so that she knows what to do, understands why to do it and how to do it [38]. As such, the ultimate goal is to improve the user behavior regarding security by providing the user with knowledge and understanding. Recent research suggests that providing knowledge is not enough as knowing what to do does not necessarily translate to correct behavior [31, 4]. It is easy to argue that the proper way to evaluate SAT efforts would be to evaluate the actual outcome, the effect on cybersecurity behavior. However, such studies bring practical as well as ethical concerns. Studies on human behavior must adhere to rigorous ethical principles that impact what can be done and how, as exemplified by [35]. Practically, experimental evaluations are hard to perform, leaving room for the use of other evaluation methods [46].

This paper aims to explore recently published work in the domain of end-user cybersecurity training to identify how such training methods are evaluated and outline considerations related to the identified evaluation methods. This was done through a structured literature review where included papers were analyzed using thematic coding. The results provide insight into what evaluation methods that are used for the evaluation of SAT and what results that can be expected from them. As such, it can be used to guide future research into SAT development by providing a reference for making informed methodological decisions and respond to the need for empirically evaluated SAT methods. The results also identify what SAT methods that have been evaluated in recent research.

2 Methodology

The study was performed as a structured literature review (SLR) which followed the process outlined by [30]:

1. Formulate a research question or aim.
2. Perform literature searches.
3. Apply inclusion and exclusion criteria.
4. Perform quality assessment.
5. Extract data.
6. Analyze data.

As described by [27, 22], selecting search terms and databases are essential tasks in an SLR. The search term used in this study was designed to be inclusive and capture all papers discussing end-user cybersecurity training. While a more restrictive query could have been designed, we argue that a broad search is more likely to capture all relevant studies, even if it results in a higher manual workload regarding the application of selection criteria. The query was expressed as follows: *security AND (training OR education) AND user*. Note that the query was modified to match the syntax of the databases used in the study. The search

term was applied to titles, abstracts, and keywords to focus the results. This was motivated by the argument that papers that do provide important information concerning the aim of the study are focused on cybersecurity training of end-users and will therefore include all search words in the metadata. To increase the chance that the study includes all important papers on the topic, an inclusive mindset was applied in choosing databases resulting in the use of *Scopus, Web of Science (core collection), Science Direct, dblp, and Usenix.*

All identified papers were evaluated against inclusion criteria. As suggested by [48], the criteria were established before the search process started to avoid bias during the selection process. The criteria were first applied to the abstracts of the identified papers. Paper that clearly failed to meet the criteria were excluded before the criteria were applied to the full remaining papers. Papers written by the authors of this paper were also excluded from the study to minimize bias. The criteria for inclusion were the following:

1. Published 2015 or later.
2. Not a duplication of another included paper.
3. Published in peer-reviewed journal or conference.
4. Free to access for the author.
5. Written in English.
6. Discusses the topic of this study.
7. Reports on one or more evaluations of SAT methods.

The first five criteria were used to limit the body of included papers to recent high-quality research and were, to some extent, applied automatically during the search process where publication year, language, and outlet could be configured during the search. The last two criteria were included to ensure that identified papers specifically discussed end-user training in the cybersecurity context and that they reported on findings based on their own data rather than conclusions based on cited material or similar. The included papers were analyzed using thematic coding in an open fashion, as described by [5]. During the analysis process, the papers were read and categorized in three steps:

1. All papers were read and individual methods of cybersecurity training were identified.
2. The papers were reread with the focus of identifying individual ways of evaluating training methods.
3. The goal and outcome of the evaluations presented in the papers were analyzed. At this stage, the papers were positioned according to what method they evaluated and how with the intent of analyzing how various evaluation methods are used.

EndNote Desktop was used for the categorization and coding of included papers.

3 Results

The searches, conducted on 2020-09-07, resulted in a total of 3664 papers, distributed among the included databases as follows:

- Scopus: 1997 hits
- Web of science: 1495 hits
- Science Direct: 129 hits
- dblp: 13 hits
- Usenix: 30 hits

All papers and their abstracts were loaded into EndNote, and duplicate papers were removed automatically during this process. Next, the titles and abstracts of all papers were scanned, and papers that clearly failed to meet the inclusion criteria were removed from the study, leaving 106 candidate papers. The inclusion criteria were then applied to the full body of those papers, resulting in 28 papers that were included in this study. Those papers were analyzed using thematic coding as described throughout the rest of this section.

3.1 Initial categorization of included papers

During the first analysis stage, the papers were first categorized according to what type of cybersecurity training they evaluated, resulting in an overview of what SAT methods have been evaluated in recent work. An overview and listing of papers included in the review are presented in Table 1. Included papers will from hereon be referenced by the label (Ax) provided in Table 1; the number in brackets point to the entry in the reference list that provides a full reference to the respective papers.

Papers	Category	Category description
A1:[34], A2:[3], A3:[40], A4:[44], A5:[19]	Several	Papers evaluating several training categories
A6:[14], A7:[20], A8:[17], A9:[10], A10:[28], A11:[21], A12: [18], A13:[37], A14:[47]	Gamification	Papers evaluating gamified training.
A15:[7],A16:[41]	Interactive online	Papers evaluating interactive material delivered online
A17:[45], A18:[25], A19:[42]	Lecture	Papers evaluating instructor-led lectures
A20:[26], A21:[49], A22:[11], A23:[51], A24:[24], A25:[9], A26:[50]	Situation aware	Papers evaluating training delivered in a situation where it is usable
A27: [29]	General_1	Evaluates the impact of progression in difficulty of material
A28: [33]	General_2	Evaluated how a variety of simultaneous methods affected phishing resilience in an organization

Table 1. List of included papers and initial categorization

3.2 Identification of evaluation methods

Following the identification of cybersecurity training types, the papers were once again analyzed focusing on what kind of evaluations they contained. At this point, four distinct methods of evaluation were identified in the papers:

- Perception evaluations: Evaluations that focused on users' perception of a training method. This included usability studies and typically aimed to evaluate if users liked the proposed method.
- Knowledge evaluations: Evaluations that measured the knowledge gained by participants using a certain method of training.
- Simulation: Evaluations that measured security outcomes, such as phishing resilience or password behavior in a simulated scenario.
- Experimental: Evaluations that measured security outcomes, such as phishing resilience or password behavior in a naturalistic setting.

3.3 Analysis of evaluation methods

The included papers were analyzed once again, focusing on the methods the papers used for evaluation, the author's comments on the used evaluation methods, and the rationale for adopting certain methods. The result in this step is an overview of what research goals are addressed using the four distinct methods of evaluation. Table 2 provides an overview of which evaluation methods are discussed in the included papers, and the remainder of this section describes the evaluation methods in more detail.

Evaluation type	**Papers**
Perception	A3, A4, A6, A7, A8, A9, A10, A12, A16, A23
Knowledge	A5, A11, A16, A17, A19
Simulation	A1, A2, A3, A4, A7, A12, A14, A15, A18, A21, A23, A24, A27
Experiment	A4, A5, A6, A13, A20, A22, A25, A26, A28

Table 2. Overview of evaluation types presented in the included papers

Ten of the included papers report on evaluations based on assessing participants *perception* using interviews or surveys. Two main types of studies can be identified where one evaluates users' perception of their own skill or knowledge. In contrast, the other evaluates the users' perception of a SAT method often in terms of how enjoyable or usable it is. A rationale provided as a motivation for perception evaluations is that a more enjoyable SAT is more likely to be used by the intended users in a naturalistic setting. The most frequently discussed shortcoming is that it cannot assess the actual effect on user behavior.

A similar type of evaluation is *knowledge based evaluation* where the participants' knowledge is measured, often using a survey. The rationale is that knowledge about correct behavior is a pre-condition for correct behavior. Similar to

perception evaluations, a shortcoming is that actual behavior is not assessed. However, a potential benefit compared to evaluation based on perception is that risk of response bias can be lesser.

Simulations measure the effect of SAT on security behavior but in a simulated environment. Simulations are presented in 13 of the included papers. The most commonly presented study type measures the participants' ability to distinguish between legitimate and fraudulent emails after being subjected to SAT. A few studies employ a pre-validated security awareness instrument to measure the SAT's effect on security awareness. A1 mentions that participants will likely be primed since they know that they participate in a study, and A21 argues that as a reason for why a simulation cannot fully mimic a natural scenario. However, the rationale for using simulations over naturalistic experiments is that simulations can provide insight into behavioral change without ethical and procedural difficulties that are often associated with experiments.

Experiments are used in nine of the included papers and measure security behavior in a naturalistic setting. Experiments are often performed using penetration testing techniques or by monitoring behavior in an organization after SAT is deployed. A rationale for using experiments is that the effect on actual behavior can be measured and observed, but several included papers demonstrate that experiments present ethical and procedural challenges. The ethical challenges stem from the fact that participants are often involved without explicit informed consent, or with informed consent that does not disclose the full extent of the experiment. The argument is that telling participants that their security behavior will be studied may influence their behavior (A11, A22, A26, A28). A workaround is to use limited informed consent and debrief participants upon study completion. Another workaround is to perform the study in an organizational setting and get permission from the organization. A practical difficulty involves that experiments with deceptive components need to consider ethical clearance.

In addition to the distinct evaluation types, the coding process identified several additional methodological considerations, and those are accounted for next. The first consideration relates to the study design, where the included papers demonstrate diversity. Between-group, pre-post, and one-shot case studies are present for all four evaluation methods. One-shot case studies report on the evaluation of a single SAT method, and an obvious drawback is that it cannot provide insight into how the SAT compares to other SAT methods. One-shot case studies are most prominently used when evaluating the users' perception of a single SAT method. Pre-post tests typically involve a study design where participants are subjected to a measure, then presented with SAT before they are again measured. The rationale is that the effect of the SAT is then isolated. Finally, the Between-group design includes subjecting different groups to different SAT methods to compare the effects, often including one group that is not subjected to any SAT method. A rationale for using a between-group design over a pre-post test is that the pre-post test design provides an increased risk of par-

ticipation bias which is arguably especially risky in studies evaluating security awareness and behavior.

Another aspect discussed in several included papers (e.g., A6, A7, A14, A15, A18) is knowledge retention, but this is only evaluated in a few of the included studies. In relation to knowledge retention, studies report that the effect of several SAT methods seems to wear off after a certain amount of time (A6). A second aspect considered in some of the included papers is if the participants would have participated in SAT if it was voluntary (A8, A10). Assessing if participants would participate voluntarily is important since prospective users need to participate in SAT for the training to be able to provide its intended effect. The effect of user unwillingness to participate in SAT is hard to account for in evaluations. A related consideration mentioned in A18 is a possible bias stemming from the participants' participation itself. Participants who know that they participate in an awareness evaluation are likely to be more aware compared to when they are not informed about the evaluation.

3.4 Discussion on the results

This paper reports on a structured literature review where 28 papers evaluating SAT methods were included. The evaluation methods used are classified as *Perception evaluations, knowledge evaluations, simulations, and experiments.* The analysis of how they are used and argued for demonstrates that they all have different benefits and shortcomings. While the end goal of any SAT is to improve user behavior, and experiments are arguably the only method that is fully capable of evaluating effects on behavior, they are practically and ethically challenging to perform. Simulations provide a less complicated alternative but are also argued to be less reliable [43, 16]. A second benefit of simulations is that the controlled nature of them allows for follow-up interviews with participants. Further, voluntary user participation is argued to be an important aspect of SAT, and perhaps the only evaluation method that captures that is *perception evaluations.* As such, an insight from this SLR is that an extensive SAT development project should evaluate its outcomes using diverse evaluation methods.

The results further demonstrate that bias and ethics present tough challenges for the evaluation of SAT. In addition to sources of bias common to most research on human subjects, SAT evaluations essentially evaluate awareness. A participant who participates in an awareness evaluation is bound to be more aware than the regular user. The results demonstrate that the study design is of high importance and aligns with previous publications in research methodology [8]. Concerning research ethics, true experiments are likely to involve deception and can include handling sensitive data, which is ethically challenging and highlights the importance of ethical reviews and ongoing ethical discussions.

As for the limitations of this particular study, an SLR is dependant on its included papers and therefore on its search and selection process. The process in this study was designed to include research published from the past five years in five different databases. While a broader selection of papers could have generated a larger empirical base, we argue that the included 28 papers are enough

to provide insight into the evaluation methods used in recent research in this domain. This was also demonstrated by saturation experienced by the researchers during the analysis. A second possible risk in qualitative research is researcher bias, given the researchers' heavy involvement in the analysis process. While difficult to minimize, researcher bias was handled in this study by ensuring that it was reported on in a way that enabled replication. The search, selection, and analysis process have been documented to ensure that it can be replicated and scrutinized by others.

4 Conclusions

This paper aimed to explore recently published work in the domain of end-user cybersecurity training to identify how such training methods are evaluated and outline considerations related to the identified evaluation methods. The paper identifies the four distinctive methods of *Perception evaluations, knowledge evaluations, simulations, and experiments* and shows that all are used in different evaluations of SAT with different challenges and benefits. As such, this study concludes that all identified evaluating types should ideally be used during the development of SAT methods. On this note, experiments and simulations are needed to provide empirical evidence as to how efficiently SAT methods can improve cybersecurity behavior while studying user perceptions of SAT methods is important in order to analyze the likelihood that users will opt to use the SAT voluntarily. The study further suggests that SAT evaluations should pay great attention to ethical challenges and bias stemming from mere participation in such studies, not least when deciding what study design to employ. This review also demonstrates that interactive and gamified training has received significant interest from researchers over the past five years.

The contribution of this paper is to the scientific community, where it provides an overview of evaluation methods used for the evaluation of SAT. The results can support future studies by providing insight into what results to expect from different evaluation methods and important considerations related to the use of the different methods. Consequently, the paper can contribute to the quality of future SAT development projects, and in the long run, to the practitioner community, which will receive even better guidelines for how to implement SAT.

This study identified participation bias and ethical challenges as two difficulties that are to be considered when evaluating SAT methods. A suggested direction for future work would be further studies into the design of ethically sound evaluation methodologies where bias is minimized. A second direction for future work is more studies concerning the retention of knowledge gained from SAT methods. While knowledge retention is mentioned in several of the papers included in this study, it is only evaluated in a few of those.

References

1. Al-Daeef, M.M., Basir, N., Saudi, M.M.: Security awareness training: A review. In: Proceedings of the World Congress on Engineering. vol. 1, pp. 5–7 (2017)
2. Alshaikh, M., Maynard, S.B., Ahmad, A., Chang, S.: An exploratory study of current information security training and awareness practices in organizations. In: Proceedings of the 51st Hawaii International Conference on System Sciences (2018)
3. Ayyagari, R., Figueroa, N.: Is seeing believing? training users on information security: Evidence from java applets. Journal of Information Systems Education **28**(2), 115–120 (2017)
4. Boss, S., Galletta, D., Lowry, P.B., Moody, G.D., Polak, P.: What do systems users have to fear? using fear appeals to engender threats and fear that motivate protective security behaviors. MIS Quarterly (MISQ) **39**(4), 837–864 (2015)
5. Braun, V., Clarke, V.: Using thematic analysis in psychology. Qualitative research in psychology **3**(2), 77–101 (2006)
6. Bulgurcu, B., Cavusoglu, H., Benbasat, I.: Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS quarterly **34**(3), 523–548 (2010)
7. Burris, J., Deneke, W., Maulding, B.: Activity Simulation for Experiential Learning in Cybersecurity Workforce Development, Lecture Notes in Computer Science, vol. 10923, pp. 17–25
8. Campbell, D.T.: Factors relevant to the validity of experiments in social settings. Psychological bulletin **54**(4), 297 (1957)
9. Choi, K.H., Lee, D.H.: A study on strengthening security awareness programs based on an rfid access control system for inside information leakage prevention. Multimedia Tools and Applications **74**(20), 8927–8937
10. Cole, J.R., Pence, T., Cummings, J., Baker, E.: Gamifying security awareness: A new prototype. vol. 11594 LNCS, pp. 115–133
11. Cuchta, T., Blackwood, B., Devine, T.R., Niichel, R.J., Daniels, K.M., Lutjens, C.H., Maibach, S., Stephenson, R.J.: Human risk factors in cybersecurity. pp. 87–92
12. Cybint: (2020), https://www.cybintsolutions.com/cyber-security-facts-stats/
13. Desman, M.B.: The ten commandments of information security awareness training. Inf. Secur. J. A Glob. Perspect. **11**(6), 39–44 (2003)
14. Dincelli, E., Chengalur-Smith, I.: Choose your own training adventure: designing a gamified seta artefact for improving information security and privacy through interactive storytelling. European Journal of Information Systems
15. EC-Council: (2019), https://blog.eccouncil.org/the-top-types-of-cybersecurity-attacks-of-2019-till-date/
16. Eck, J.E., Liu, L.: Contrasting simulated and empirical experiments in crime prevention. Journal of Experimental Criminology **4**(3), 195–213 (2008)
17. Gjertsen, E.G.B., Gjaere, E.A., Bartnes, M., Flores, W.R.: Gamification of Information Security Awareness and Training. Icissp 2017
18. Gokul, C.J., Pandit, S., Vaddepalli, S., Tupsamudre, H., Banahatti, V., Lodha, S., Acm: PHISHY - A Serious Game to Train Enterprise Users on Phishing Awareness. Proceedings of the 2018 Annual Symposium on Computer-Human Interaction in Play Companion Extended Abstracts
19. Gundu, T.: Acknowledging and Reducing the Knowing and Doing gap in Employee Cybersecurity Compliance, pp. 94–102. International Conference on Cyber Warfare and Security (2019)

20. Huynh, D., Luong, P., Iida, H., Beuran, R.: Design and Evaluation of a Cybersecurity Awareness Training Game, Lecture Notes in Computer Science, vol. 10507, pp. 183–188
21. Jayakrishnan, G.C., Sirigireddy, G.R., Vaddepalli, S., Banahatti, V., Lodha, S.P., Pandit, S.S.: Passworld: A serious game to promote password awareness and diversity in an enterprise. In: (SOUPS 2020). pp. 1–18 (2020)
22. Jesson, J., Matheson, L., Lacey, F.M.: Doing your literature review: Traditional and systematic techniques. Sage (2011)
23. Joinson, A., van Steen, T.: Human aspects of cyber security: Behaviour or culture change? Cyber Security: A Peer-Reviewed Journal **1**(4), 351–360 (2018)
24. Kunz, A., Volkamer, M., Stockhardt, S., Palberg, S., Lottermann, T., Piegert, E.: Nophish: Evaluation of a web application that teaches people being aware of phishing attacks. vol. P-259, pp. 509–518 (2016)
25. Lastdrager, E., Gallardo, I.C., Hartel, P., Junger, M.: How effective is anti-phishing training for children? pp. 229–239 (2017)
26. Lim, I.K., Park, Y.G., Lee, J.K.: Design of security training system for individual users. Wireless Personal Communications **90**(3), 1105–1120
27. Meline, T.: Selecting studies for systematic review: Inclusion and exclusion criteria. Contemporary issues in communication science and disorders **33**(21-27) (2006)
28. Micallef, N., Arachchilage, N.A.G.: Involving users in the design of a serious game for security questions education. arXiv preprint arXiv:1710.03888 (2017)
29. Moreno-Fernández, M.M., Blanco, F., Garaizar, P., Matute, H.: Fishing for phishers. improving internet users' sensitivity to visual deception cues to prevent electronic fraud. Computers in Human Behavior **69**, 421–436
30. Paré, G., Kitsiou, S.: Methods for literature reviews. In: Handbook of eHealth Evaluation: An Evidence-based Approach [Internet]. University of Victoria (2017)
31. Parsons, K., Butavicius, M.A., Lillie, M., Calic, D., McCormac, A., Pattinson, M.R.: Which individual, cultural, organisational and interventional factors explain phishing resilience? In: HAISA. pp. 1–11 (2018)
32. Puhakainen, P., Siponen, M.: Improving employees' compliance through information systems security training: an action research study. MIS quarterly pp. 757–778 (2010)
33. Rastenis, J., Ramanauskaitė, S., Janulevičius, J., Čenys, A.: Impact of information security training on recognition of phishing attacks: A case study of vilnius gediminas technical university. vol. 1243 CCIS, pp. 311–324
34. Reinheimer, B., Aldag, L., Mayer, P., Mossano, M., Duezguen, R., Lofthouse, B., von Landesberger, T., Volkamer, M.: An investigation of phishing awareness and education over time: When and how to best remind users. In: (SOUPS 2020). pp. 259–284
35. Renaud, K., Zimmermann, V.: Ethical guidelines for nudging in information security & privacy. International Journal of Human-Computer Studies **120**, 22–35 (2018)
36. Safa, N.S., Von Solms, R.: An information security knowledge sharing model in organizations. Computers in Human Behavior **57**, 442–451 (2016)
37. Silic, M., Lowry, P.B.: Using design-science based gamification to improve organizational security training and compliance. Journal of Management Information Systems **37**(1), 129–161
38. Siponen, M.T.: A conceptual foundation for organizational information security awareness. Information Management & Computer Security (2000)
39. Soare, B.: (2020), https://heimdalsecurity.com/blog/vectors-of-attack/

40. Stockhardt, S., Reinheimer, B., Volkamer, M., Mayer, P., Kunz, A., Rack, P., Lehmann, D.: Teaching Phishing-Security: Which Way is Best?, IFIP Advances in Information and Communication Technology, vol. 471, pp. 135–149
41. Takata, T., Ogura, K., Ieee: Confront Phishing Attacks - from a Perspective of Security Education, pp. 10–13. International Conference on Awareness Science and Technology (2019)
42. Taneski, V., Heričko, M., Brumen, B.: Impact of security education on password change. pp. 1350–1355
43. Tichy, W.F.: Should computer scientists experiment more? Computer **31**(5), 32–40 (1998)
44. Tschakert, K.F., Ngamsuriyaroj, S.: Effectiveness of and user preferences for security awareness training methodologies. Heliyon **5**(6)
45. Van Rensburg, W.J., Thomson, K.L., Futcher, L.: An Educational Intervention Towards Safe Smartphone Usage. HAISA 2018 (2018)
46. Vroom, C., Von Solms, R.: Towards information security behavioural compliance. Computers & security **23**(3), 191–198 (2004)
47. Wen, Z.A., Lin, Z.Q., Chen, R., Andersen, E., Assoc Comp, M.: What.Hack: Engaging Anti-Phishing Training Through a Role-playing Phishing Simulation Game. Chi 2019
48. Wohlin, C., Runeson, P., Höst, M., Ohlsson, M.C., Regnell, B., Wesslén, A.: Experimentation in software engineering. Springer Science & Business Media (2012)
49. Xiong, A.P., Proctor, R.W., Yang, W.N., Li, N.H.: Embedding training within warnings improves skills of identifying phishing webpages. Human Factors **61**(4), 577–595
50. Yang, W., Xiong, A., Chen, J., Proctor, R.W., Li, N.: Use of phishing training to improve security warning compliance: Evidence from a field experiment. vol. Part F127186, pp. 52–61
51. Zhou, L.M., Parmanto, B., Alfikri, Z., Bao, J.: A mobile app for assisting users to make informed selections in security settings for protecting personal health data: Development and feasibility study. Jmir Mhealth and Uhealth **6**(12)