

# The Right Tool for the Job: Contextualization of Cybersecurity Education and Assessment Methods

Daniel Köhler<sup>a</sup> and Christoph Meinel

Hasso Plattner Institute, University of Potsdam, Prof.-Dr.-Helmert-Str. 2-3, Potsdam, Germany

Keywords: Security, Awareness, Education, Assessment, Method Overview.

Abstract: Today, cybersecurity attacks are one of the significant threats companies face. Employees, often the weakest link in the cybersecurity chain, are sensitized to threats in cyberspace by implemented cybersecurity awareness and education programs in companies. Success is often rated using obligatory quizzes. Those, however, do not accurately depict actual employee behavior; they only test for knowledge. Companies often lack accurate measures to validate the success of cybersecurity awareness measures. We aggregate previous literature on measures for education and assessment in the context of cybersecurity awareness and present a taxonomy of education and assessment measures, categorizing them for context, applicability, and effort while summarizing (dis-) advantages identified in previous research. Thereby, we enable easier decisions on specific cybersecurity awareness education and assessment methods for decision-makers with specific restraints.

## 1 INTRODUCTION

Roughly 90% of data breaches in 2020 could be traced back to the initial access vector of phishing, an attack against human subjects, counterfeiting various technical defense mechanisms (Cisco, 2021). Therefore, many companies pursue cybersecurity education with their employees to foster security awareness (Lain et al., 2022). However, they often follow narrow principles for establishing awareness among their employees, providing educational videos or computer-based training paired with quizzes or phishing emails (Jaeger and Eckhardt, 2021).

The landscape of available and researched education measures for cybersecurity awareness and appropriate verification methods is vast. Therefore, deriving a complete overview of the advantages of different methods in specific situations is a daunting task. Further, an assessment of the different dimensions of cybersecurity awareness, from *Perception* to achieving *Behavior* change, is often omitted in previous work. Similarly neglected is often an appropriate differentiation between methods used for training and methods used for assessment of cybersecurity skills. Therefore, barely any company can adequately tackle the challenge to actively decide *for* or *against* a specific education method. Instead, they often rely on pre-


viously established, potentially lacking training measures, unaware of the potential for improvement in evaluating actual behavior changes.

This manuscript provides taxonomies of cybersecurity education and assessment methods to the community. To serve as a guideline for decision-makers to assess appropriate measures and to provide a starting point for fellow researchers to identify potentially under-researched topics, both incorporating:

- *Key Considerations* for each method and pointers towards previous research with in-depth examples having employed the respective methods.
- Contextualization of the methods along the dimensions of *effort*, *dependencies*, or the *context* in which they can be applied, to the best of our knowledge unavailable in previous literature.
- Verification of each assessment method along dimensions of cybersecurity awareness

## 2 BACKGROUND

In this work, we evaluate measures to teach or assess awareness of risks in information technology (IT) devices and systems. Such as risks on the internet. For the term of *cybersecurity awareness*, we build on the work by Jäger, who in his work reviewed 40 previous publications, synthesizing the relationship between

<sup>a</sup>  <https://orcid.org/0000-0003-3121-3888>

Information Security Awareness, its antecedents, and consequences (Jaeger, 2018): “*Security Awareness is a state of mind, derived by education and experience in which persons are capable of understanding and protecting themselves against security threats*”.

Regarding dimensions of cybersecurity awareness, the last years have shown many research articles and manuscripts proposing solutions and frameworks to capture the nature of cybersecurity awareness assessment. Already in 2006, *Kruger and Kearney* started to outline the field of research by providing a first model using three categories: Knowledge, Attitude, and Behavior (KAB) to measure awareness (Kruger and Kearney, 2006). In 2011, *Khan et al.* enhanced the KAB-Model into the Five-Step-Ladder-Model (Khan et al., 2011). They challenge the implicit expectation in the KAB-model that knowledge ultimately leads to behavior. By inducing the model with *Theory of Reasoned Action* and *Theory of Planned Behavior*, they derive two intermediate steps before the behavior change.

*Hänsch and Benenson* have further studied the phenomenon of missing concrete dimensions and scope of *Security Awareness* by analyzing more than 25 publications from the previous 15 years (Hänsch and Benenson, 2014). They highlight three interpretations of Security Awareness: (1) *Perception*, the fact that users know of dangers. (2) *Protection*, users shall know which dangers exist and which measures are needed to protect themselves. (3) *Behavior*, users know and apply security behavior best practices.

In this work, we follow the dimensions of cybersecurity awareness defined by Hänsch and Benenson. Compared to a few of the other dimensions derived in previous research, Hänsch’s dimensions allow easy explainability and understandability. With one of our target groups being decision-makers to bring theory into practice, these features are critical to allow easy application. Besides that, the framework has already been employed by various other researchers as the foundation for follow-up work, which we interpret as additional indicator for its validity (Espinha Gasiba et al., 2020; Maennel et al., 2018; Schütz, 2018).

### 3 RELATED WORK

Various authors have already provided an in-depth assessment of some education or assessment methods, e.g., (Kumaraguru et al., 2009; Zielinska et al., 2014; Caputo et al., 2014). However, with different research goals in the respective publications, they fell short of providing an overview of the landscape. We present a short overview of four related studies which have put

parts of the body of research into perspective.

In 2015, *Rahim et al.* conducted a structured literature review to identify (overarching) approaches in cybersecurity awareness measurement (Rahim et al., 2015). They recognized that cybersecurity assessment requires mixed quantitative and qualitative approaches. While the authors of the work discuss findings and the impact of their analyzed studies on a meta-level, their assessment cannot be used as a guideline for implementing further cybersecurity assessment, as they center their descriptions around the studied pieces of research literature.

In their 2020 literature review, *Jampen et al.* surveyed various previous works on phishing tests (Jampen et al., 2020). One of their fields of analysis covers the impact of education on phishing susceptibility in the context of cybersecurity education. However, while the authors identify 35 previous works that mention the effects of education, they do not provide enough details on the types of education to base a decision for an education methodology on their survey.

*Fertig and Schütz* performed a systematic literature review in 2020 identifying 34 relevant resources, which they assessed for the methods to measure Security Awareness (Fertig and Schütz, 2020). They recognized that most studies (>25) conducted awareness assessments based on questionnaires and surveys.

In 2022, *Zhang-Kennedy and Chiasson* (Zhang-Kennedy and Chiasson, 2022) surveyed more than 100 multimedia tools for cybersecurity education. They rate the tools and games available for cybersecurity education according to ten principles from learning science. The survey’s contribution is close to our contextualization in Table 1 and 2, however, only features multimedia content such as games or films.

While all the previous work has evaluated some aspects of education and assessment methods, they often do not provide a comparison and contextualization of the methods. As such, deriving real-world comparability and applicability from previous publications is difficult. Our manuscript targets the missing overview, comparison, and contextualization of concrete measures and methods for cybersecurity education and assessment.

### 4 TAXONOMY DIMENSIONS

To derive appropriate dimensions and constraints that need to be applied to potential methods in different contexts, we conducted a workshop with fellow researchers at the *ARES* conference<sup>1</sup> in 2023 (Köhler,

<sup>1</sup>The workshop *CS-EDU* was organized by *Gregor Langner (AIT)*. *Daniel Köhler*, first author of this

2023). Eighteen subject matter experts from research, industry, and governmental institutions participated in the workshop. Most participants had a background in education, e.g., from their time in a university or higher education institution. In the workshop, we led a series of smaller discussions with participants. Potential educative measures to be applied in a context, such as a university or a workplace, were initially brainstormed. Later discussions explored the applicability of these measures to changing scenarios, such as the COVID-19 pandemic, work-from-home, or remote teaching. Based on these discussions and the exploration, different dimensions and constraints were developed for education and assessment methods, as outlined in the following:

**Education Methods** are used to present knowledge to a learner. To decide which methods to use, it is critical to be aware of the **Context** in which a specific education should be employed. The discussion differentiated between a *Private* and *Professional* context. The professional contexts are employment or paid training programs, whereas private contexts could be, e.g., governmental education programs for their citizens. Alongside the context of an educational program, certain **Restrictions** are induced by the different education methods. Such restrictions cover *Time(ing)* of a particular education measure, the *location*, in which it is performed, or whether *scalability* to larger groups of learners is possible. When, e.g., assessing a classroom-based training program, restrictions towards both time, location, and hence scalability are high. However, other cases, e.g., when using posters for education, have a high restriction for the location of a (single) poster but are easily scalable by providing multiple posters across multiple locations. Finally, different education measures require a different level of effort for their implementation. We divide between *Preparation* and *Execution* effort, as both could influence a decision maker's willingness to decide for or against a method.

**Assessment Methods** similarly underly constraints in the categories of **Effort** and the differentiation between a professional or private **Context**. **Restrictions** towards Scalability, Time, and Location apply to assessment just as to education measures. Additionally, we assess the measures based on the dimensions of cybersecurity awareness covered. Examples would be quizzes, which are unlikely to provide realistic results when questioning users' behavior in specific situations. Therefore, we include a mapping towards the three dimensions of cybersecurity awareness proposed by *Hänsch and Benenson* (Hänsch and

manuscript, led the one-hour-long sub-part of the workshop discussing the topic presented in this manuscript.

Benenson, 2014), which we presented in Section 2: Perception, Protection, and Behavior.

- **Perception:** describes the fundamental understanding of security problems and dangers in omnipresent cyberspace; an example would be that a user knows that cybercriminals try to get hold of user passwords that are reused across services to perform actions in the user's name.
- **Protection:** describes user knowledge on solutions and mitigations for the problems; e.g., the user understands the concept of a Password manager, which allows them to use complex, different, and secure passwords for all services.
- **Behavior:** questions whether users apply the known security best practices, e.g., if the user *actually* uses complex and unique passwords.

For education measures, the assessment of dimensions of cybersecurity awareness is not applicable. The education measures define *how* the education is done. Sensitization for cybersecurity throughout the different dimensions requires providing appropriate content to educate the users specifically on that issue. An assessment of dimensions in education would hence rather be a question of *what* is taught, instead of *how* is taught, and is covered to some extent in various skill frameworks previously assessed, presented, or in development for cybersecurity, e.g. by (Caulkins et al., 2019; Furnell and Bishop, 2020).

## 5 EDUCATION METHODS

Education, generally, can be consumed in different contexts. Schools teach pupils who, later in life, potentially pursue higher education degrees. More formalized education in cybersecurity is encountered, e.g., in the context of professional training for a specific job role or (online-) courses that interested learners can take. Some education methods, such as online videos, can be applied in various contexts, independent of the target group or content.

Table 1 presents our collection of education methods, which we have observed primarily within cybersecurity education. We highlight key considerations for the different methods alongside references to literature in which more practical and in-depth resources on the respective method can be found.

The table further highlights our contextualization of the methods based on insights reported by previous researchers, our experience from (education) in industry and academia, and our discussion with subject matter experts during the workshop (Köhler, 2023). We contextualize based on the dimensions derived

Table 1: Overview of different education methods suitable for cybersecurity education, contextualized for the **effort** required for implementation, **restrictions** induced by the method, and **context** in which they could be applied.

	Effort		Restrictions			Context		Key Considerations	References and Examples
	Preparation	Execution	Time	Location	Scalability	Private	Professional		
<b>Text-Based</b>									
E-Mails and Newsletter	Low	Low	○	○	○	✓	✓	• Texts can be harder to <i>understand</i>	(Khan et al., 2011)
News Articles	Low	Low	●	○	●	✓	(✓)	• Current events increase interest in topic	(Nagelhout et al., 2012)
(e-) Books & Documents	Med.	Low	○	○	○	✓	✓	• Requires motivation to consume and learn	(Carella et al., 2017)
Security Tips	Low	Low	○	○	○	✓	✓	• Short tips are often not understood properly	(Orunsolu et al., 2017)
<b>Picture-Based</b>									
Comics	Med.	Low	○	○	○	✓	✓	• Ideally short, engaging and fun • Greater <i>accessibility</i> than some other methods	(Zhang-Kennedy and Chiasson, 2021)
Poster & Billboards	Low	Med.	○	●	●	✓	✓	• <i>Location</i> is critical • Best to <i>reiterate</i> knowledge	(Khan et al., 2011)
Social Media Posts	Low	Low	○	○	○	✓		• Used for shorter or less complex content	(Mavrodiava et al., 2019) (Hamid et al., 2017)
<b>Video-Based</b>									
Videos	Med.	Low	○	○	○	✓	✓	• Potentially very theoretical and not engaging	(Zhang-Kennedy and Chiasson, 2021)
Short Videos (Social Media)	Med.	Low	○	○	○	✓		• Less complex topics • Target group rather young people	(Mavrodiava et al., 2019)
Advertisement Campaigns	Med.	Med.	○	○	○	✓		• Can help reach diverse target groups	(Putte, 2009)
Online Courses (MOOCs)	High	Low	●	○	○	✓	✓	• Complex and diverse topics can be covered	(González-Manzano and de Fuentes, 2019)
<b>Social &amp; Group Activities</b>									
(Online) Presentations & Classroom Training	Med.	High	●	●	●		✓	• <i>Adjustable</i> to almost every situation or topic • <i>Inefficient</i> when trainee number increases • Sometimes ineffective	(Khan et al., 2011) (Al-Daeef et al., 2017) (Carella et al., 2017)
(Online) Group Discussions	Low	High	●	●	●		✓	• In small groups, <i>efficient</i> method • Learners can learn from each other	(Khan et al., 2011) (Al-Daeef et al., 2017)
<b>Gamified Learning</b>									
(Educational) Video Games	High	Med.	○	○	○	✓	✓	• Very <i>Engaging</i> • Allows to experience <i>real-world scenarios</i>	(Khan et al., 2011) (Zhang-Kennedy and Chiasson, 2021)
(Educational) Tabletop Games	High	Med.	●	●	●	✓		• Potentially rather <i>theoretical</i>	(Zhang-Kennedy and Chiasson, 2021)
Computer-Based Training	Med.	Low	○	○	○	✓		• Similar to Video Games, potentially less engaging • Allows more precise <i>real-world scenarios</i>	(Khan et al., 2011)
Serious Games	High	High	●	●	●	✓		• Immersive and sustainable sensitization for topics	(Hart et al., 2020)
<b>Miscellaneous</b>									
Radio Programmes	Low	Low	●	○	○	✓		• Can help reinforce knowledge	(O'Shea and Richmond, 2007)
Podcasts	Low	Low	○	○	○	✓	✓	• No visual components	(Köhler et al., 2022) (Goldman, 2018)

○: No Restriction ●: Limited Restriction, ●: Strong Restriction

in Section 4. For most dimensions, we have implemented a scale consisting of three values. **Effort** is categorized as *Low*, *Medium (Med.)*, or *High*. Usually, a high effort can be equalized by paying higher amounts of money to, e.g., a consulting company preparing and implementing the respective measure. One example would be an online course on a specific topic. Preparation of such a course can be daunting and thus rated as *High* effort (Hollands and Tirthali, 2014). Therefore, one could decide to buy (access to) online courses from established platforms such as Coursera, or EdX.

Regarding *Restrictions*, we highlight if the method induces strong restrictions (●), limited restrictions (●), or has no restrictions (○). Restrictions primarily apply to the time or location where a measure would be performed. Both limit the scalability of an education measure. An example would be designing an education measure for a worldwide company. Classroom-based training could be used but is

usually limited to a certain location where the activity happens. In the context of video calls, one could perform classroom-based training online (●) and would primarily be limited by the time slot (●), which has to fit all attendees. Hence, in the example of a worldwide organization, the company would have to offer many sessions covering the same content to enable all employees to participate. This would be considered limited scalability of the measure (●).

The following sections briefly highlight essential aspects of across the dimensions of the the table.

**Effort** particularly targets, how a measure is prepared and applied. As Lutz and Kc (Lutz and Kc, 2011) highlighted, the content of education programs can impact which presentation form would be efficient to use. Hence, each change regarding an education method could require new content to be *prepared*. As the table shows, most education measures require low or moderate preparation effort. However, more sophisticated methods, such as online courses, video

or tabletop games, and serious games, require tremendous preparation and effort. The content and material for these education measures can often be obtained from other companies or public sources such as online education platforms. The decision to use external content can drastically reduce the effort required for preparation. However, when using external resources, the exact coverage of suitable topics for the own situation can not be assured.

For the *execution* of an education method, significant differences in the effort are observable. While prerecorded videos are effortlessly distributed, classroom sessions require planning, preparation, personnel, and infrastructure, such as available rooms or space to be conducted. Overall, the majority of popular education methods require relatively low effort during execution.

**Restrictions** to education measures such as classroom-based training often depend on learners being in the same place at the same moment. Such measures are challenging to scale across a big organization potentially spread worldwide. Companies may not require scalability of their education programs. In such cases, relying on measures that are hard to scale should be of no issue. In contrast, most, e.g., video-based measures, do not depend on location, time, or scalability. Similarly effortlessly scale text- and picture-based measures that do not rely on a physical medium, such as emails or social media posts.

Many researchers have reported interactive and social types of training, such as serious games, discussions, and classroom training, to be very impactful towards the learning outcomes. However, at the same time, those are the education measures which's implementation strongly depends on a shared location and available time slot. The past years, though, have shown that many workshops can be performed in online contexts, rendering the dependency on a shared location less critical.

Regarding the **Context** of an education program, many methods can be observed for recipients in private (off-work) and professional contexts. Often, content is only consumed by those actively deciding to do so. An example is listening to podcasts. Broader communication channels, such as social media, radio programs, or advertisement campaigns on TV or during other podcast shows, would also reach those not enrolled or subscribed to educative material anywhere else. Those campaigns could be used in, e.g., government-sponsored education programs, to reach diverse recipient groups throughout the population.

On the other hand, some education methods are primarily seen in professional education. Such would be classroom-based training, e.g., in yearly manda-

tory security education. Similarly, computer-based training or serious games are primarily observed in professional contexts, mainly due to the high cost and effort of preparation required.

## 6 ASSESSMENT METHODS

Measuring and assessing learning success is essential for observing any impact provided by education measures and programs. However, the effect and fit of a particular assessment for a specific situation is often only studied little. Other researchers explicitly state shortcomings of their used measurement or teaching methods (Kruger and Kearney, 2006). We, put different methods and approaches into perspective to allow decision-makers and researchers to compare them and choose the most appropriate for their scenario.

Table 2 provides an overview of the different assessment approaches identified from previous research. As earlier, we contextualize the different methods alongside the dimensions outlined in Section 4. In addition to the previous table, however, this overview also provides an evaluation of dimensions of cybersecurity awareness that can be assessed using the respective methods.

Similarly to the other scales, we differentiate on a three-point scale between a Good (✓), Neutral (○), or Bad (×) fit of a respective method for assessing awareness in a particular dimension of cybersecurity awareness. An example would be quizzes, which can easily be used to assess an employee's understanding of a specific topic (*perception*) or whether they know how to *protect* themselves against various threats in cyberspace adequately but fail to measure *behavior*.

The following paragraphs provide an overview of the different dimensions assessed and the implications to practicality.

Accurate assessment of **Dimensions of Cybersecurity Awareness** is relevant to correctly interpret real-world situations. The chosen assessment method strongly determines the quality of answers for the specific dimensions in question. Choosing the wrong measurement for the dimension in question can result in inaccurate results and, in the worst cases, put, e.g., an overall company security posture at risk.

It is important to note that measures that actively question an employee or make them realize that an assessment is performed are usually only effective in assessing the dimensions of *perception* (of a threat) and *protection*. Other researchers have already reported on the danger of employees providing inaccurate answers in surveys on behavior because they assume that the employer *wants* to hear that answer (Kruger

Table 2: Overview of assessment methods proposed and applied in previous literature compared for the covered **dimension** of security awareness, **effort** required for implementation, **restrictions** implied by the method and applicable **context**.

	Dimension			Effort		Restrictions			Context		Key Considerations	References and Examples
	Perception	Protection	Behavior	Preparation	Execution	Time	Location	Scalability	Private	Professional		
<b>(Knowledge) Assessment</b>												
Quizzes	✓	✓	×	Low	Low	○	○	○	✓	✓	• Can only verify <i>theoretical</i> knowledge	(Kruger and Kearney, 2006) (Köhler et al., 2023)
Surveys, Questionnaires	×	✓	○	Low	Med.	○	○	●	✓	✓	• Danger that employees <i>answer dishonestly</i>	(Kruger and Kearney, 2006) (Marks and Rezgui, 2009)
Interviews	✓	✓	✓	Med.	High	●	○	●	✓	✓	• Exhaustive work for large groups	(Boujettif and Wang, 2010)
Observation	×	×	✓	Med.	High	●	●	●	✓	✓	• Potentially very time-consuming	(Marks and Rezgui, 2009)
<b>Technical Measures</b>												
Helpdesk Reports	×	×	✓	Low	Low	○	○	●	✓	✓	• Insights into processes known to employees	(Khan et al., 2011) (Gardner and Thomas, 2014)
(Monitoring) Internet Activity	×	×	✓	Med.	Med.	○	○	●	✓	✓	• Provides accurate information on employee behavior	(Khan et al., 2011)
(Monitoring) Password Policies	×	○	✓	Low	Low	○	○	○	✓	✓	• Measure if employees / customers <i>protect</i> accordingly	(Wolf et al., 2010)
Phishing Tests (E-Mails)	×	×	✓	Med.	Med.	○	○	○	✓	✓	• Monitor actual <i>behavior</i> precisely	(Jaeger and Eckhardt, 2021) (Köhler et al., 2023)
<b>Exercises</b>												
Red-Team Exercises	×	✓	✓	High	High	●	●	●	✓	✓	• Particularly study cybersecurity-teams	(Scholl et al., 2017)
Simulation Games	✓	✓	○	High	High	●	●	●	✓	✓	• Worst-case scenarios close to reality	(Jalali et al., 2019)

Appropriateness to evaluate dimension: ×: Bad Fit ○: Neutral, ✓: Good Fit  
○: No Restriction ●: Limited Restriction, ●: Strong Restriction

and Kearney, 2006; Fertig and Schütz, 2020).

Many technical methods, such as monitoring employees’ passwords or internet activity, can accurately assess the actual *behavior*. One of the most common methods is phishing email exercises with employees to validate the success of previous cybersecurity awareness campaigns.

The **Effort** required for preparation of assessment methods differs strongly. While techniques such as quizzes or surveys are easy to prepare and relatively easy to execute, other methods, such as interviews, require little effort during preparation but tremendous effort during execution. Additional examples are personal talks with employees or observations of their behavior, which would occupy many (human) resources. During the execution of the assessment measures, complex methods such as red-team exercises or security benchmarks require high effort. Such effort could be represented by monetary resources required to be spent or employees tasked with the individual assessment.

**Restrictions** to measures cover scalability, time, and location, particularly for in-person assessments. Instead, various measures relying on technical aspects, such as monitoring databases or internet activity, underly fewer restrictions. Highly specialized exercises such as red-teaming or simulation games underlie most restrictions. These measures promise to provide real-world insights into actual threat scenarios but, therefore, often imply more substantial re-

strictions for the time or location of the measure.

**Contexts** of assessment measures differ between personal and professional scenarios. Particularly for technical measures we observe a strong tendency to application in professional contexts only. Quizzes for behavior, e.g., in the context of online courses, can be completed by persons in their private lives, or interviews and observation for specific studies can be conducted with private persons. Those types of assessments rarely actually target people’s behavior. Most people would answer that they should use good passwords, however, the least users actually do (Yildirim and Mackie, 2019).

Technical measures for assessment are only implemented in professional work situations where employees are trained and assessed for their cybersecurity awareness. Proper studies using technical measures on private participants often observe substantial limitations regarding their internal validity, as study participants would need to be informed of the nature of the research and could, in turn, react differently when observed or questioned.

## 7 FUTURE WORK

Some of the presented methods lack research on their effectiveness. For future research in this area, we plan to build on the discussion with researchers from the field of cybersecurity education, as challenged by

this work. Based on feedback from the community, we aim to expand this taxonomy with additional education and assessment methods and further dimensions to contextualize these. While we derived our overview from a cybersecurity awareness perspective, we expect that practitioners and researchers from other domains can also apply teaching methods to their contexts. Promising examples could be other fields of awareness, such as fake news.

## 8 CONCLUSION

In this work, we challenge the problem of unsuitable cybersecurity awareness programs by providing decision-makers with taxonomies for choosing education and assessment methods.

In Table 1, we categorize 19 methods for education based on the *effort* needed for both preparation and execution, *restrictions* in terms of time, location, and scalability, and the method's *context* of private or professional education. Short summaries of critical findings and considerations on the methods accompany the presentation of the methods.

In Table 2, we highlight ten different cybersecurity awareness assessment methods used and considered in previous research. As previously, we categorize each measure according to the *effort* for preparation, restrictions, and execution and the *context* that we observed to be used. Particularly for the context of cybersecurity, we investigate the *dimension*, such as *Perception*, *Protection*, or *Behavior*, that can be assessed by the respective measure(s).

With both overviews, we provide decision-makers with a foundation for an educated decision on which measures to implement in their context. Similarly, the summary can inspire researchers when drafting further studies in the cybersecurity context.

## REFERENCES

- Al-Daeef, M. M., Basir, N., and Saudi, M. M. (2017). Security awareness training: A review. *Lecture Notes in Engineering and CS*.
- Boujettif, M. and Wang, Y. (2010). Constructivist Approach to Information Security Awareness in the Middle East. In *2010 International Conference on Broadband, Wireless Computing, Communication and Applications*, pages 192–199.
- Caputo, D. D., Pfleeger, S. L., Freeman, J. D., and Johnson, M. E. (2014). Going Spear Phishing: Exploring Embedded Training and Awareness. *IEEE Security & Privacy*, 12(1):28–38.
- Carella, A., Kotsoev, M., and Truta, T. M. (2017). Impact of security awareness training on phishing click-through rates. In *2017 IEEE International Conference on Big Data (Big Data)*, pages 4458–4466.
- Caulkins, B., Marlowe, T., and Reardon, A. (2019). Cybersecurity Skills to Address Today's Threats. In *Advances in Human Factors in Cybersecurity*, Advances in Intelligent Systems and Computing, pages 187–192. Springer International Publishing.
- Cisco (2021). Cybersecurity threat trends: phishing, crypto top the list.
- Espinha Gasiba, T., Lechner, U., and Pinto-Albuquerque, M. (2020). Sifu - a cybersecurity awareness platform with challenge assessment and intelligent coach. *Cybersecurity*, 3(1):24.
- Fertig, T. and Schütz, A. (2020). About the measuring of information security awareness: a systematic literature review. *Proceedings of the Hawaii International Conference on System Sciences*, 53.
- Furnell, S. and Bishop, M. (2020). Addressing cyber security skills: the spectrum, not the silo. *Computer Fraud & Security*, 2020(2):6–11. Publisher: Elsevier.
- Gardner, B. and Thomas, V. (2014). *Building an information security awareness program: defending against social engineering and technical threats*. Elsevier/Syngress, Amsterdam ; Boston.
- Goldman, T. (2018). The Impact of Podcasts in Education. *Pop Culture Intersections*.
- González-Manzano, L. and de Fuentes, J. M. (2019). Design recommendations for online cybersecurity courses. *Computers & Security*, 80:238–256. ISBN: 0167-4048 Publisher: Elsevier.
- Hamid, S., Ijab, M. T., Sulaiman, H., Md. Anwar, R., and Norman, A. A. (2017). Social media for environmental sustainability awareness in higher education. *International Journal of Sustainability in Higher Education*, 18(4):474–491.
- Hänsch, N. and Benenson, Z. (2014). Specifying it security awareness. In *25th International workshop on database and expert systems applications*. IEEE.
- Hart, S., Margheri, A., Paci, F., and Sassone, V. (2020). Riskio: A Serious Game for Cyber Security Awareness and Education. *Computers & Security*, 95.
- Hollands, F. M. and Tirthali, D. (2014). Resource Requirements and Costs of Developing and Delivering MOOCs. *International Review of Research in Open and Distributed Learning*, 15(5):113–133.
- Jaeger, L. (2018). Information security awareness: Literature review and integrative framework. In *Proceedings of the Annual Hawaii ICSS*, volume 2018, pages 4703–4712. IEEE Computer Society.
- Jaeger, L. and Eckhardt, A. (2021). Eyes wide open: The role of situational information security awareness for security-related behaviour. *Information Systems Journal*, 31(3):429–472.
- Jalali, M. S., Siegel, M., and Madnick, S. (2019). Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. *The Journal of Strategic Information Systems*, 28(1):66–82.

- Jampen, D., Gür, G., Sutter, T., and Tellenbach, B. (2020). Don't click: towards an effective anti-phishing training. A comparative literature review. *Human-centric Computing and Information Sciences*, 10(1):33.
- Khan, B., Khaled, S. A., Syed, I. N., and Muhammad, K. K. (2011). Effectiveness of information security awareness methods based on psychological theories. *African journal of business management*, 5(26).
- Köhler, D., Pünter, W., and Meinel, C. (2023). Fishing for Non-Professional Answers: Quantitative Study on Email Phishing Susceptibility in Private Contexts. In Review.
- Kruger, H. A. and Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & security*, 25(4):289–296.
- Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., and Pham, T. (2009). School of phish: a real-world evaluation of anti-phishing training. In *Proceedings of the 5th Symposium on Usable Privacy and Security*. ACM.
- Köhler, D. (2023). Discussion on Methods for Assessing Cybersecurity Awareness. Workshop Presentation.
- Köhler, D., Pünter, W., and Meinel, C. (2023). The “How” Matters: Evaluating Different Video Types for Cybersecurity MOOCs. In *Responsive and Sustainable Educational Futures*, Lecture Notes in Computer Science, pages 149–163, Cham. Springer Nature Switzerland.
- Köhler, D., Serth, S., Steinbeck, H., and Meinel, C. (2022). Integrating Podcasts into MOOCs: Comparing Effects of Audio- and Video-Based Education for Secondary Content. In *Educating for a New Future: Making Sense of Technology-Enhanced Learning Adoption*, volume 13450 of *LNCS*, pages 131–144. Springer International Publishing, Switzerland.
- Lain, D., Kostianen, K., and Čapkun, S. (2022). Phishing in organizations: Findings from a large-scale and long-term study. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 842–859. IEEE.
- Lutz, W. and Kc, S. (2011). Global Human Capital: Integrating Education and Population. *Science*, 333(6042).
- Maennel, K., Mäses, S., and Maennel, O. (2018). Cyber Hygiene: The Big Picture. In *Secure IT Systems*, Lecture Notes in Computer Science, pages 291–305, Cham. Springer International Publishing.
- Marks, A. and Rezgui, Y. (2009). A Comparative Study of Information Security Awareness in Higher Education Based on the Concept of Design Theorizing. In *2009 International Conference on Management and Service Science*, pages 1–7.
- Mavrodieva, A. V., Rachman, O. K., Harahap, V. B., and Shaw, R. (2019). Role of social media as a soft power tool in raising public awareness and engagement in addressing climate change. *Climate*, 7(10):122. ISBN: 2225-1154 Publisher: MDPI.
- Nagelhout, G. E., Van Den Putte, B., De Vries, H., Crone, M., Fong, G. T., and Willemsen, M. C. (2012). The influence of newspaper coverage and a media campaign on smokers' support for smoke-free bars and restaurants and on secondhand smoke harm awareness. *Tobacco Control*, 21.
- Orunsolu, A. A., Sodiya, A. S., Akinwale, A. T., Olajuwon, B. I., Alaran, M. A., Bamgboye, O. O., and Afolabi, O. A. (2017). An empirical evaluation of security tips in phishing prevention: A case study of nigerian banks. *International Journal of Electronics and Information Engineering*, 6(1):25–39.
- O'Shea, P. and Richmond, S. (2007). Radio Education: A Review of the Literature. Publisher: World Ag Info Project.
- Putte, B. v. d. (2009). What matters most in advertising campaigns?: The relative effect of media expenditure and message content strategy. *International Journal of Advertising*, 28(4):669–690.
- Rahim, N. H. A., Hamid, S., Mat Kiah, M. L., Shamshirband, S., and Furnell, S. (2015). A systematic review of approaches to assessing cybersecurity awareness. *Kybernetes*, 44(4):606–622.
- Scholl, M., Leiner, K. B., and Fuhrmann, F. (2017). Blind Spot: Do You Know the Effectiveness of Your Information Security Awareness-Raising Program? 15(4).
- Schütz, A. E. (2018). Information security awareness: it's time to change minds. In *Proceedings of International Conference on Applied Informatics Imagination, Creativity, Design, Development-ICDD*.
- Wolf, M. J., Haworth, D., and Pietron, L. (2010). *Measuring an information security awareness program*. University of Nebraska at Omaha.
- Yıldırım, M. and Mackie, I. (2019). Encouraging users to improve password security and memorability. *International Journal of Information Security*, 18(6).
- Zhang-Kennedy, L. and Chiasson, S. (2021). A systematic review of multimedia tools for cybersecurity awareness and education. *ACM Computing Surveys (CSUR)*, 54(1):1–39.
- Zhang-Kennedy, L. and Chiasson, S. (2022). A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education. *ACM Computing Surveys*, 54(1):1–39.
- Zielinska, O. A., Tembe, R., Hong, K. W., Ge, X., Murphy-Hill, E., and Mayhorn, C. B. (2014). One Phish, Two Phish, How to Avoid the Internet Phish: Analysis of Training Strategies to Detect Phishing Emails. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 58. Publisher: SAGE Publications.