# A systematic review of current cybersecurity training methods

Prümmer J.; Steen, T. van; Berg, B. van den

Computers & Security 136 (2024) 103585

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

# A systematic review of current cybersecurity training methods

Julia Prümmer *, Tommy van Steen, Bibi van den Berg

*Institute of Security and Global Affairs, Faculty of Governance and Global Affairs, Leiden University, the Netherlands*

ARTICLE INFO

*Keywords:*
Cybersecurity
Systematic review
Cybersecurity interventions
Behaviour change
Training
Behavioural cybersecurity

ABSTRACT

Cybersecurity continues to be a growing issue, with cyberattacks causing financial losses and loss of productivity and reputation. Especially in an organisational setting, end-user behaviour plays an essential role in achieving a high level of cybersecurity. One way to improve end-user cybersecurity behaviour is through comprehensive training programmes.

There are many contradictory statements and findings with regard to the optimal way to conduct a behavioural cybersecurity training. We conducted a systematic review to create a comprehensive overview of the methods used in cybersecurity training and their effectiveness in improving organisational cybersecurity behaviours. Web of Science, ACM Digital Library, ProQuest, PubMed and PsycINFO were searched and 16,771 papers were identified. After title, abstract and full text screenings were conducted, 142 relevant papers were included in our analysis.

The analysis shows that the majority of studies report positive effects of training, regardless of the cybersecurity topic that was addressed or the training method that was employed. Game-based training methods were used most often. Most studies used a non-experimental design to test effectiveness, with pretest-posttest designs being the most frequent. Sample sizes were often small and many interventions were not tested on employees but other populations. Further findings with regard to intervention design, characteristics and evaluation are discussed.

## 1. Introduction

Cybersecurity and the prevention of cyberattacks, has been a growing security issue for organisations for a number of years (Ulsch, 2014). Organisations targeted through cyberattacks are diverse, ranging from large companies like Volkswagen (CNN, 2021), to critical infrastructures such as Colonial Pipeline (Reuters, 2021). According to the Cyber Security Breaches Survey published by the UK Government in 2022, higher education institutions were also affected, with 62 % experiencing attacks or breaches at least weekly (gov.uk, 2022).

Many of these cyberattacks are attributed to vulnerabilities associated with human actors within the organisation. For example, the incident at Volkswagen resulted from information stored in an unsecured file, and the attack on Colonial Pipeline was said to be caused by a reused password. Attacks on higher education institutions in the UK are reported to occur most often through phishing attacks (gov.uk, 2022). Damage as a result of human actions (or the omission thereof) can be severe, with outcomes including loss of productivity, monetary losses, and loss of credibility and reputation (Abawajy, 2014). Additionally, consequences are often not immediately visible. This negatively impacts the sense of urgency employees associate with cybersecurity (Dihoff et al., 2004).

One avenue to consider when attempting to improve cybersecurity is training the behaviour of end-users. Focusing on end-user behaviour is appealing in part due to the fact that many cybersecurity threats we are facing today cannot yet be solved entirely through technological solutions (Craigen et al., 2014). While protective measures such as firewalls, antivirus software and spam filters can reduce the occurrence of some threats, other threats still arise frequently and lead to disastrous consequences as those outlined above. Similarly, even if technological measures are implemented, they are not always practical when considering the tasks that employees and other types of end-users must perform. While employees are often aware of the security threats they may be confronted with, they also have to perform their job duties in a timely manner. In order to comply with both their job requirements and security policies as much as possible, shadow security behaviours are used (Kirlappos et al., 2014). Shadow security occurs when employees are not able to comply with the security policies and mechanisms that

* Corresponding author at: Leiden University, The Netherlands, Turfmarkt 99 Room 4.03, 2511 DP The Hague, the Netherlands.
*E-mail address:* j.prummer@fgga.leidenuniv.nl (J. Prümmer).

https://doi.org/10.1016/j.cose.2023.103585
Received 3 July 2023; Received in revised form 28 October 2023; Accepted 6 November 2023
Available online 9 November 2023

are set forth by their organisation, and therefore find and adopt alternative tools or solutions that are not approved by their organisation (Kirlappos et al., 2014). This suggests that when imposed guidelines and restrictions are unappealing to end-users, they will find a way to circumvent them. This also highlights that the behaviour of end-users is integral in preventing cyberattacks associated with human actions. One important way to do so is through training of these end-users with regard to threats that organisations and institutions face.

Organisational cybersecurity encompasses a number of topics where end-user behaviour is key in securing data, systems and locations. Ertan et al. (2020) identified four sets of behaviour that occur in organisational settings with regard to cybersecurity: compliance with security policy, phishing and email behaviour, password behaviour, and intergroup coordination and communication. The first set encompasses behaviours related to compliance with security policy. This broad category can contain a multitude of different behaviours that vary between different organisations. Topics related to this set may include screen locking behaviours, restrictions placed on file sharing, transfer of login credentials and 'bring your own device' guidelines. The second set entails phishing and email behaviour. Phishing attacks often employ social engineering mechanisms. They aim to manipulate individuals so that they provide sensitive data such as banking details, passwords or health records to the attacker (Salahdine and Kaabouch, 2019). The third set outlines password behaviour. Passwords are frequently used to access various kinds of information or data within organisations and can cause serious harm if mismanaged. Issues with password safety are most commonly associated with the way users generate these passwords (e.g., using short, easy-to-guess passwords or repeating the same password amongst platforms). Intergroup coordination and communication make up the final set identified in the review. Topics in this set mainly relate to organisational culture.

When attempting to improve the cybersecurity behaviour of end-users, the main focus is often on awareness campaigns to communicate issues on cybersecurity (e.g. Clark, 2013; Gundu and Flowerday, 2013; Rotvold, 2007). As found by van Steen et al. (2020), who analysed nineteen governmental cybersecurity awareness campaigns, the used materials were all of a similar nature. Information was exclusively provided via 'campaign stationery' such as posters or bookmarks and websites that at times included video material. The distribution of information through text-based methods is popular in these campaigns, as it is usually easier, quicker, and cheaper than other methods. However, research has shown that awareness campaigns are not very effective (Bada et al., 2019).

Though Mashiane et al. (2019) and Poepjes and Lane (2012) and many others rightfully state that awareness of cybersecurity threats is important, other researchers argue that it is only one of the many precursors leading to actual behavioural change. For one, Bada et al. (2019) found that merely providing information has a limited effect on changing users' behaviour. Similarly, Alruwaili (2019) expressed that training programs including information are simply too narrow and must include further guidelines on how to respond to threats. The translation of cybersecurity training programs into the workplace is a difficult undertaking in itself (He and Zhang, 2019). Employees often lack enthusiasm and have difficulty paying attention to the provided material (R. Adams, 2018; Gross, 2018; Kostadinov, 2018). When using methods with limited efficacy, effort and resources are often wasted.

A multitude of other training methods are available, including the application of new technologies such as Virtual Reality (Adinolf et al., 2019); or established techniques like serious gaming and nudging, the latter of which involves altering the choices available in such a way that a preferred option becomes more convenient and more likely to be chosen (Thaler and Sunstein, 2008; van Steen, 2022). Due to the fact that some of these training methods are newly applied to the field of cybersecurity, their application is often tested with regard to usability and clarity of the training program for the end-user, rather than how effective they are in changing behaviour (see for instance Adinolf et al., 2019; Alqahtani and Kavakli-Thorne, 2020).

The current study is not the first to synthesise research on end-user training in cybersecurity. Previous literature reviews on training in cybersecurity focused on specific circumstances, such as type of cybersecurity behaviour (Aldawood and Skinner, 2019a, 2019b; Chowdhury and Gkioulos, 2021) or type of training method (Coenraad et al., 2020; Hendrix et al., 2016; Katsantonis et al., 2017). Additionally, some reviews focused on only one particular country of interest (Alruwaili, 2019). While these are valuable contributions to the field, they often only analyse one of many facets necessary to understand the topic of cybersecurity training in general. In order to synthesise the literature that has been created on cybersecurity training in relation to digital technologies within organisational settings, this paper explores a wide range of current cybersecurity training methods, their design, and their effectiveness, by way of a systematic literature review. By conducting this systematic review, we aim to create a comprehensive overview of the field, identifying best practices and providing pointers regarding which avenues to explore further.

## 2. Methods

In order to facilitate transparency and completeness, the Preferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA) guidelines for systematic review reporting were followed (Moher et al., 2015; Page et al., 2021). The PRISMA guidelines provide checklists and protocols to aid in both the preparation and facilitation of systematic reviews. The elements of a systematic review to be considered according to the PRISMA guidelines outlined in Table A1 are adapted from Page et al. (2021) and include elements relevant to both systematic reviews and meta-analyses.

### 2.1. Information sources and search strategy

A systematic title and abstract search was conducted in November 2021, using the Web of Science, ACM Digital Library, ProQuest, PubMed and PsycINFO electronic databases. Search terms used were:

1) cyber* OR "cyber security" OR "information security" OR "digital security" OR "computer security" OR "social engineering" OR "IT security"
2) AND intervention* OR training OR awareness OR game* OR gamification

Table A2 shows the entered search queries for each database, as well as the number of results that were obtained.

Grey literature was covered by including the ProQuest Dissertations & Theses Sub-Database, as well as newspaper articles when available in the search. The initial search yielded 16,771 results.

### 2.2. Inclusion and exclusion criteria

Papers were included if they discussed training of end-users in relation to digital technologies within organisational settings aimed at improving their cybersecurity behaviour. Every training that focused on employee-to-employee behaviours, in which digital technologies are the means of interactions (e.g., to counter online harassment, sexting or bullying) were excluded, whereas those that focused on employees' direct interactions with the technology itself (e.g., to prevent phishing, increase screen locking, reduce shadow security or improve password management) were included. Eligible study designs included both empirical and non-empirical studies, as well as process evaluations and review papers. As the focus of the review is on organisational cybersecurity behaviour, training as part of a formal curriculum, such as university or high school courses related to cybersecurity, were excluded. Studies including any populations except minors were included, as long as the training was aimed at improving the above-mentioned

organisational cybersecurity behaviours. Additionally, studies where no English translation could be obtained were excluded.

### 2.3. Study selection and data extraction

Removing the duplicates reduced the number of articles from 16,771 to 9219. This number was reduced to 304 after the title and abstract screening. This screening was carried out by two authors (JP & TvS). Every article that was deemed relevant by at least one author was included at this stage. Next, a full-text screening was conducted by the same two authors using the inclusion and exclusion criteria outlined above. Here, disagreements between authors were discussed until consensus was reached, leading to 142 articles that were included in the review. A full overview of the article selection procedure is presented in Fig. A4. One author (JP) extracted the relevant data for all included papers. The extracted data included the cybersecurity topic discussed within the paper, the use of established theories to inform training creation, the method of training delivery, training properties i.e., training platform (online/in-person), presence of a trainer, social setting and training frequency, as well as methods of data collection, populations and sample sizes used for data collection, the degree of data manipulation and outcome measures used to assess effectivity. No risk of bias assessment was conducted as, to the best of our knowledge, there is no clear risk of bias assessment tool that is appropriate for the wide variety of study designs (experimental, pre-post, descriptive) and types of studies (theoretical contributions, review studies, empirical work and proposed methods) included in this systematic review. A full overview of the applied stages of the PRISMA guidelines can be found in Table A3.

## 3. Results

A total of 142 articles were included in this review. During the analysis, three separate categories of articles were identified. In the majority of articles, a training was presented and evaluated empirically. These articles were classified as empirical ($N = 89$). Articles that focused on cybersecurity training guidelines, theoretical frameworks, and literature reviews were classified as non-empirical/theoretical ($N = 38$). While some of the remaining articles could also be categorised as non-empirical, they distinguish themselves from others in the non-empirical category by proposing a concrete training or training development mechanisms. However, they also distinguished themselves from the articles in the empirical category in that they did not empirically evaluate the effectiveness of the training that was proposed. This third category will hereafter be referred to as proposed training/development ($N = 15$). See Table A4 for an overview of all included papers.

### 3.1. Literature reviews

Of the 38 non-empirical papers, nine were literature reviews (Aldawood and Skinner, 2019a, 2019b; Alruwaili, 2019; Chowdhury and Gkioulos, 2021; Coenraad et al., 2020; Fujs et al., 2020; Hendrix et al., 2016; Katsantonis et al., 2017; Khando et al., 2021). These papers reviewed and synthesised the literature and ongoing discourse on cybersecurity training. In doing so, they focused on more specific circumstances, instead of conducting a broader analysis of the field. For example, some papers were dedicated to distinct cybersecurity topics, as is seen in Aldawood and Skinner (2019a) and Aldawood and Skinner (2019b), where the focus is placed on training on social engineering. Similarly, Chowdhury and Gkioulos (2021) discussed literature on training dedicated to critical infrastructure protection. In some reviews, literature on game-based training techniques was highlighted and analysed (Coenraad et al., 2020; Hendrix et al., 2016; Katsantonis et al., 2017). One review focused on specific terminology (information security) used within cybersecurity (Khando et al., 2021), while another used bibliometric mapping to synthesise the data (Fujs et al., 2020). Lastly, Alruwaili (2019) chose to include studies centred on cybersecurity in Saudi Arabia. In these literature reviews, the growing importance of end-user training on cybersecurity is highlighted, while also identifying pitfalls and challenges that the field faces. While Aldawood and Skinner (2019b) identify a lack of financial resources as a primary challenge for many organisations, Alruwaili (2019) and Hendrix et al. (2016) highlight issues with regard to effectiveness evaluations.

### 3.2. Cybersecurity topics

We identified five distinct themes with regard to cybersecurity topics covered in the training literature: social engineering ($N = 42$), password safety ($N = 9$), workplace security ($N = 7$), malware ($N = 8$) and WiFi safety ($N = 1$). While some articles used the above-mentioned descriptions, which are often broader in scope, some were more specific when outlining the cybersecurity behaviours they were trying to address. Within social engineering, topics such as phishing (e.g. Abroshan et al., 2021; Jansson and von Solms, 2013; Martin, 2019) or fake web pages (e.g. Abraham and Chengalur-Smith, 2019) were identified. Articles focusing on workplace security were concerned with topics such as policy compliance (e.g. Goyal et al., 2019), 'bring your own device' regulations (Bada and Nurse, 2019) or insider threat (e.g. Carlson, 2020). Malware-related issues were sometimes concerned with user-orientated attacks or hacking (Hamoud and Aimeur, 2020; Lim et al., 2013). Within these topics and amongst the different categorisations or articles, social engineering, and more specifically phishing, was discussed most frequently. The remaining articles ($N = 86$) were either concerned with general cybersecurity (e.g. Amor, 2010; Dominguez, 2010; Kletenik et al., 2021), or did not further specify a certain behaviour or topic (e.g. Alshaikh et al., 2021; Bauer et al., 2017; González, 2019; Stefaniuk, 2020). Eight articles discussed more than one topic (e.g. Alotaibi, 2019; Bada and Nurse, 2019; Ikhalia et al., 2019). A more detailed description of topics is given in Table A5.

### 3.3. Theory-based training

Twenty-six studies relied on an established theory to create or evaluate the training. Theories occurring most frequently were the Protection Motivation Theory (PMT) ($N = 7$) and the Theory of Planned Behaviour (TPB) ($N = 7$). Other theories included the Theory of Reasoned Action ($N = 3$), Signal Detection Theory ($N = 2$), and General Deterrence Theory ($N = 2$). The concept of self-efficacy was also discussed in six articles. As an example, Salameh (2020) used the PMT factors of coping and threat appraisal to evaluate users' intentions after undergoing training. Gundu and Flowerday (2013) created a behavioural intention model based on the Theory of Reasoned Action and PMT that was used to create a training process that aims to help small to medium enterprises educate their employees. See Table A6 for exemplary articles that include the above-mentioned theories.

Amongst the non-empirical articles, six papers referenced an existing theory or established a new theory or framework. For instance, Khan et al. (2011) posited that using existing psychological theories of education, learning and behavioural change can make information security awareness methods more effective. In contrast, Younis and Musbah (2020) proposed a new framework called 'phishing detection framework' that aims to aid in training Arabic users to detect and report phishing attacks adequately.

### 3.4. Training methods

We identified seven distinct training methods in the empirical and proposed training categories that are listed here in decreasing frequency of appearance: game-based training ($N = 38$); presentation-based training ($N = 19$); simulation-based training ($N = 16$); information-based training, where information is presented via an unspecified method ($N = 15$); video-based training ($N = 14$); text-based training ($N$

= 13) and discussion-based training ($N = 6$). Some training methods did not fit into any of these categorisations, namely punishment-based training (Kim et al., 2020), training programs with different levels of media richness (Shaw et al., 2009) and knowledge maps (Shaw et al., 2011) amongst others. Fifteen articles did not specify which training method they used.

Game-based training methods were the most employed training method. One of the games developed to improve cybersecurity behaviour was a password protector game by Alotaibi (2019), where a user is required to create complex passwords. The password strength is indicated with visual cues such as colour bars and each level presents the trainees with different rules for password creation that they have to adhere to (e.g. number of characters, time limit). Afterwards, trainees needed to again enter the password they chose to demonstrate their ability to remember the password. Password strength ratings and awareness levels were significantly improved after the intervention. Another example is PhishI in Fatima et al. (2019). Here, players had to select a victim and gather information on them in order to draft a sophisticated phishing e-mail themselves. Awareness levels were improved and participants showed increased understanding of the effects of disclosure of information online. A similar example of players taking on the role of the attacker is the multiplayer card game SREG by Yasin et al. (2018). Players were instructed to assess vulnerabilities in a target organisation and compromise it by suggesting concrete attack scenarios. Both performance and feedback evaluations from players were positive. In the game created by van Steen and Deeleman (2021), players were given access to money that they could spend on assets to strengthen themselves against cybersecurity incidents. A reward in the form of a smiley was given when players chose the correct protective measures. Incorrect responses resulted in a lower score. They found that the implementation of the serious game had a positive significant effect on self-reported outcome evaluations, while merely providing information did not.

An example of a presentation-based training was given in Sykosch et al. (2020), where an instructor held a 60-minute lecture on perceivable artefacts in phishing, and how users are supposed to respond to them. This intervention led to a significant decrease in artefact reporting by users. Chatchalermpun and Daengsi (2021) made use of presentation-based training as well by holding a 'security day', which included instructor-led seminars on cyber risks. Findings showed that participant awareness increased from 77.75 % to 93.24 % after the training. Simulation-based training was employed by Jansson and von Solms (2013). Here, participants were exposed to a simulated phishing attack and, after they behaved insecurely, received several notifications informing them that they had partaken in such behaviour. The authors noted that after the intervention, users reacted more securely. A similar method was used in Baillon et al. (2019), where some participants were exposed to a phishing e-mail and subsequent feedback on their behaviour as part of the training. This intervention, as well as the provision of information to the remaining participants, had a large effect on participant probability to click on phishing links in the future. A second example of information-based training occurred in Hepp et al. (2018), where participants underwent a short online course that provided them with an overview of privacy legislations and other issues related to cybersecurity. The exact mechanisms used within the online course were not described further. After completion of the training, interviews and focus groups were held to analyse the participants' perceptions of the training modules.

Video-based training was used in Chin et al. (2016) and included a series of online videos that covered topics such as mobile security, password and data protection and many more. Here, the intervention group showed improvements in self-reported behaviour, but these were not statistically significant. Tschakert and Ngamsuriyaroj (2019) also made use of educational videos in their training on social engineering. Positive effects of the overall training, which also included a presentation, as well as game- and text-based methods, were reported. Another example of text-based training was given in Abawajy (2014), where participants were provided with a short web article detailing phishing and anti-phishing techniques. After the training, participants' ability to identify phishing e-mails increased significantly. Lastly, in Puhakainen and Siponen (2010) participants took part in a collaborative discussion about risks related to e-mail use as part of their training. Following, data on training usefulness and satisfaction was gathered from participants through interviews.

In 32 articles, more than one training method was employed. For example, Clark (2013) used a combination of discussion-, presentation- and text-based methods to create a multimethod cybersecurity training campaign. Informal Q&A sessions, newsletters, seminars and an information portal were provided, and participants were free to choose in which of the training activities they wanted to partake. In contrast, Baillon et al. (2019) compared the effectiveness of using information-based or simulation-based training with each other by using a $2 \times 2$ factorial design. More specifically, participants were divided into a control group that did not receive any training, one group that received information on phishing through infographics, one that underwent a simulated phishing test, and one group that received both the infographics and the simulated phishing.

### 3.5. Training properties

Twenty-four studies made use of an instructor in their training to explain training mechanisms or teach the relevant information (e.g. Oslejsek et al., 2021; Siponen et al., 2020; Wu et al., 2021). Extracted data on platforms, i.e., online vs. in-person training, and social settings, i.e., group vs. individual, provided further insights into the types of training that were offered. Online ($N = 72$) and individual ($N = 69$) training were used most frequently. For example, House (2013) implemented a video-based online training that participants could complete by themselves. The video provided them with information on what phishing is, how attacks using phishing occur and the best ways to prevent them. In contrast to that, Puhakainen (2006) used a mix of presentation- and discussion-based training to create an instructor-led group training that aimed to increase user attitudes towards information security. Shargawi (2017) aimed their training at phishing susceptibility by making use of both instructor-led presentations held on a group level and an online awareness model that participants could complete by themselves. In 20 articles, no information on platform or social setting was given (e.g. Bauer et al., 2017; Hammond, 2019; Younes, 2014). We also checked for explicit mentions of behavioural change techniques and found that fear appeal was used in four articles (Abraham, 2012; Cook et al., 2017; House, 2013; Martin, 2019). For example, Abraham (2012) included a message in their training on social engineering that outlines the possible occurrence of identity theft and its consequences. Additionally, a condition of graphic fear appeal also included showing the participants a video clip from the movie "The Net", which focuses on a victim of identity theft. They found that these fear appeal messages did not influence either participants' attitude levels or efficacy beliefs, nor their objective behaviour, while the training they employed alongside did. A small number of articles described platforms or software that simplify the creation of training for organisations and, more specifically, instructors. For example, Beuran et al. (2018) described their platform CyTrONE, where a coordinator adds training input into an e-learning system, which in turn generates training content and a training environment for the trainees. Similar solutions were proposed by Beuran et al. (2019) and Cone et al. (2007).

### 3.6. Study design

The majority of articles used employees ($N = 49$) or students ($N = 35$) as the sample population. Samples in the remaining articles could be categorised into young adults ($N = 2$), and a sample of the general population ($N = 8$). A more detailed description of sample populations

can be found in Table A7. Two articles did not provide information on the sample population. Multiple sample populations (students and employees) were used in seven articles. The number of participants used varied greatly across studies, from as small as a single participant (Aoyama et al., 2017), up to 20,260 participants (Chatchalermpun and Daengsi, 2021). This discrepancy is further highlighted when comparing the mean number of participants in all studies combined, which is 804, with the corresponding median of 96, showing that at least half of the analysed articles used less than 100 participants to evaluate effectiveness. Overall, only six articles explicitly mentioned a repetition of training materials at least two or more times (e.g. Curry et al., 2019; Gundu and Flowerday, 2013; Lim et al., 2016), while the rest conducted the training once before evaluation ($N = 53$) (e.g. Adinolf et al., 2019; Chen et al., 2020; Harta et al., 2020; Sykosch et al., 2020), or did not disclose that information ($N = 30$) (e.g. Briliyanti et al., 2019; Ikhalia et al., 2019; Wu et al., 2021).

Overall, quantitative data collection was used most frequently ($N = 62$), followed by qualitative ($N = 16$) and mixed ($N = 11$) data collection. A more detailed description of how data collection occurred is given in Table A7. Most articles used non-experimental manipulation when conducting evaluations ($N = 67$), i.e. a one-group pretest-posttest, case study or static group comparison design. An experimental design, i.e. a pretest-posttest control group or posttest control group design with randomisation between groups, was used 13 times. A quasi-experimental research design, i.e. a time series or pretest-posttest control group design without randomisation, was used nine times.

We also analysed the outcome measures used to assess training effectiveness. In total, seven distinct outcome measures were identified and are listed here in decreasing order of appearance: knowledge ($N = 32$), objective behaviour ($N = 27$), attitude ($N = 13$), intention ($N = 11$), perception ($N = 9$), self-reported behaviour ($N = 7$), and efficacy beliefs ($N = 3$). Data was collected using questionnaires, interviews and game scores. Furthermore, objective behaviour was mostly assessed by having participants identify phishing e-mails, or fake links or websites (e.g. Abraham, 2012; Baillon et al., 2019). For more information on how data for different outcome measures was created see Table A8.

### 3.7. Training effects

Instead of merely measuring the effectiveness of the various training initiatives, it is interesting to note that in some studies ($N = 22$), participants were asked to evaluate whether they appreciated the way the training was conducted, with regard to both enjoyment and perceived usefulness. A majority of these articles ($N = 15$) reported positive feedback, especially when employing techniques such as game-based or simulation-based training (e.g. Baxter et al., 2016; Loffler et al., 2021). A contrasting view was found by Abawajy (2014), where participants rated video-based training as their favourite, followed by text-based training. Game-based training was rated last and only 5 % of participants selected it as their favourite method. However, 60 % added that they still enjoyed the experience of undergoing a game-based training.

In terms of effectiveness, the majority of the empirical articles ($N = 62$) reported positive effects of training. Albrechtsen and Hovden (2010), who researched the effects of a discussion-based group training, found a significant change in awareness and self-reported behaviour in the experimental group in comparison with the control group. This effect translated to follow-up measures that were taken six months later. Van Steen and Deeleman (2021) found that after participants underwent a game-based training, self-reported Theory of Planned Behaviour scores were positively and significantly influenced. This change occurred in comparison to a control group that received no cybersecurity training, as well as a group that underwent text-based learning. Abawajy (2014) analysed and contrasted the effects of game-based, video-based and text-based training and found that awareness rates increased significantly in all conditions. They also found that participants showed improvements in different areas, depending on which training method they were assigned to. For example, those who participated in game-based training were able to establish website authenticity quicker than those in other conditions. Similarly, those in the video-based condition did particularly well when answering phishing-related questions. They concluded that different delivery methods could potentially have different benefits for the trainee. Other articles evaluated in the context of this review showed similar findings. Kim (2010) found that instructor-based trainees had higher levels of learning transfer, whereas computer-based trainees had higher levels of knowledge retention, suggesting that combining methods would be beneficial. The possibility of training personalisation is also discussed in Chowdhury and Gkioulos (2021).

Twelve articles report mixed results (e.g. Abraham, 2012; Al Zaidy, 2020; Gordon et al., 2019; Harta et al., 2020). Jenkins et al. (2013) found that training containing low extraneous stimuli resulted in significantly higher rates of secure behaviour than no training, whereas training with high extraneous stimuli did not. Additionally, users reported dissatisfaction with the high extraneous stimuli training. Both training variations were based on a narrated PowerPoint slide presentation. While the low extraneous stimuli training contained nothing else, other stimuli not directly related to the security policy information were added to the high extraneous stimuli training. This included a visible narrator and a greater variety of colours. Similarly, McCrohan et al. (2010) found that the effects of a high-information condition increased, while those of the low-information condition did not. This effect did not translate to a two-week follow-up. During the study, both groups took part in an online lecture. The low-information condition contained very general information on computer security, while the high-information condition included more details and a story-based presentation style.

Five articles report negative or no effects of training (Bernier, 2020; Harrison, 2018; Martin, 2019; Sykosch et al., 2020; Waly, 2013). Participants in Waly (2013) reported dissatisfaction with the training initiatives implemented by their organisations and described them as overloaded with information and uninteresting. No detailed description of the type of training they were referring to was provided. Both Martin (2019) and Harrison (2018) found no significant effect of training. The training methods used in their research were text-based and simulation-based training.

Ten articles gave a descriptive evaluation of their findings (e.g. Adinolf et al., 2019; Conrad, 2021; Hepp et al., 2018; Švábenský and Vykopal, 2018). For example, Adinolf et al. (2019) reported ideas participants had about security training. These ideas were related to themes, as well as stylistic and mechanical choices that could be implemented in a training. Others, such as Alshaikh et al. (2021), Aoyama et al. (2017) and Dominguez (2010), gave descriptions of training programs that were utilised at the various organisations they assessed.

## 4. Discussion

Cybersecurity training in relation to digital technologies within organisational settings is a growing topic of conversation in academic literature. A large amount of research has already been conducted on the topic, as evidenced by the 142 articles included in this systematic literature review. Cybersecurity topics addressed within the training were varied and ranged from cybersecurity as a general concept (e.g. Hepp et al., 2018; Kletenik et al., 2021; Yasin et al., 2019) to more specific topics such as phishing (e.g. Dixon et al., 2019; Gordon et al., 2019), insider threat (Muhirwe, 2016) and others. Similarly, a multitude of training methods was presented using a variety of platforms (e.g. DeCarlo, 2021; Fatima et al., 2019) and social settings (e.g. Dixon et al., 2019; Heid et al., 2020; Wu et al., 2021). In contrast to some articles employing more 'traditional' methods of training (e.g. Nicolas-Rocca, 2010; Sardar and Wahsheh, 2020; Sykosch et al., 2020), others made use of more creative techniques such as serious gaming (e.g. Jansen and Fischbach, 2020; Lim et al., 2013; Oslejsek et al., 2021) or virtual reality

(e.g. Adinolf et al., 2019; Veneruso et al., 2020) to design an engaging environment for learning to take place. While objective measurements of improvement of behaviour after training administration were observed frequently (e.g. Baillon et al., 2019; Jansson and von Solms, 2013; Martin, 2019), the majority of articles chose to focus on other facets such as knowledge gained through the training (e.g. Cook et al., 2017; Ghazvini and Shukur, 2018; Kletenik et al., 2021), attitudes towards cybersecurity (e.g. Dixon et al., 2019; Kim et al., 2016; Wu et al., 2021) or intentions to act more securely in the future (e.g. Anzaldua Jr, 2016; Bernier, 2020; Salameh, 2020). The majority of results reported in articles that were included in this review are positive and promising (e.g. Hammond, 2019; Lamour, 2008; Robbins, 2020; van Steen and Deeleman, 2021; Younes, 2014). However, many aspects of training in the context of cybersecurity remain unclear. This lack of clarity is both with regard to the design and implementation of interventions, as well as the evaluation of effectiveness.

### 4.1. Intervention design

A significant observation made while analysing the selected articles was an underwhelming reliance on theory when creating training material. Based on the descriptions encountered within the selected articles, it often appears as if methods used during the intervention were not included consciously and deliberately with a theoretical underpinning as part of the design process, but rather through 'common sense' or for practical reasons. Similarly, the use of traditional techniques of awareness-raising – e.g. through posters and newsletters – was observed frequently. The effectiveness of this style of campaign is questioned with regard to both non-cybersecurity behaviours (Dumesnil and Verger, 2009; Leavy et al., 2011) and cybersecurity behaviours (Bada et al., 2019). Cybersecurity behaviours and the reasons for unsafe behaviour can be varied and complex, especially in an organisational setting (Pogrebna and Skilton, 2019), and cannot be reduced to a lack of awareness or unwillingness of the 'human factor' to act in accordance with guidelines and protocols. The lack of theoretical underpinning is surprising, given the complexities associated with human action, especially when considering that the effect of the use of theory to inform training creation has been extensively recognised in other disciplines such as psychology, sociology and healthcare (Eccles et al., 2005; Green and Glasgow, 2006). This notion of training creation through theory can already be observed in the field of health psychology, as shown through a meta-analysis conducted by Gourlan et al. (2016), which outlines the effectiveness and robustness of theory-based approaches in improving physical activity. Similar observations were made with regard to studies conducted in the domains of work and school behaviour, nutrition, and sexual behaviour, as identified in a meta-analysis conducted by Steinmetz et al. (2016), that analysed the effectiveness of behaviour change interventions based on the Theory of Planned Behaviour. It would be worthwhile to implement similar solutions and test their effectiveness in the context of cybersecurity education.

Observations related to intervention design were also made in terms of the training methods authors chose to implement. As outlined above, game-based training methods are used most frequently. While some authors (e.g. Chen et al., 2020; DeCarlo, 2021; Loffler et al., 2021; Weanquoi et al., 2017) have described positive feedback from participants after implementing games, Cook et al. (2017) noted that several participants propositioned that the game that they implemented should be accompanied by some form of presentation. This would suggest that games are not an alternative, but should rather be used in conjunction with other training methods. However, due to a lack of specification on why participants favoured one method over others, conclusions with regard to training type preferences should be drawn with caution. While design ideas such as the implementation of an accelerated feedback cycle (Adams and Makramalla, 2015; Chen et al., 2020), personalisation of training (Hamoud and Aimeur, 2020; Heid et al., 2020) or a strategic combination of training methods (Abawajy, 2014; Kim, 2010) are discussed in a handful of articles, their effect is often not evaluated empirically. Although the personalisation of training has been extensively studied in other disciplines such as educational science (Prain et al., 2013) and has been shown to be more effective when facilitated through technology rather than traditional learning techniques (Zheng et al., 2022), the effect in the field of cybersecurity education is still unclear. Still, as shown by Li and Wong (2019), in the period from 2009 to 2018 between 50 % to 57 % of studies on personalised learning were concerned with issues of effectiveness. Taking the conclusions drawn from these studies and implementing them with regard to end-user cybersecurity education could be a good starting point for exploring this topic further.

### 4.2. Intervention characteristics

Similar to the issues outlined above of intervention design, there appears to be no discernible pattern in how specific behaviours are trained. For example, presentation-based training was used when addressing concerns related to password safety (McCoy and Fowler, 2004; McCrohan et al., 2010; Nicolas-Rocca, 2010), social engineering (Al-Hamar, 2010; Chatchalermpun and Daengsi, 2021; Shargawi, 2017; Sykosch et al., 2020) and malware (Chowdhury and Gkioulos, 2021; Sardar and Wahsheh, 2020). Other articles do not make a distinction between these behaviours and instead address general cybersecurity as one overarching concept (Amor, 2010; Hepp et al., 2018; Kletenik et al., 2020; Yasin et al., 2019). Similar observations can be made with regard to the properties of the interventions. Again, no clear pattern emerges with regards to when authors choose to conduct a training online (Arain et al., 2019; Filipczuk et al., 2019) or in-person (Aoyama et al., 2017; Yasin et al., 2019), with a trainer (Briliyanti et al., 2019; Nicolas-Rocca, 2010), in a group (Cook et al., 2017; Harta et al., 2020) or individually (Chen et al., 2020; Heid et al., 2020). As previously discussed in relation to intervention design, these inconsistencies in characteristics also point to a lack of deliberation and suggest that practicality has a large influence on choices made with regard to training characteristics. This is evidenced further by the large majority of studies in this review choosing to conduct an online training that participants can undergo without supervision (e.g. Harrison, 2018; Kletenik et al., 2021). Compared to in-person and/or instructor-led training, self-guided online training appears easier to implement and less costly. As shown in Zheng et al. (2022) online training has been shown to contribute to increased levels of effectiveness when compared to traditional methods such as classroom settings. Unfortunately, similar conclusions cannot be drawn based on the information provided in the articles analysed here, indicating that further evaluation is warranted.

### 4.3. Intervention evaluation

Observations were also made concerning how the interventions were evaluated. This includes the number of participants that were used, the frequency of training repetition before evaluation and which outcome measures were evaluated. The majority of articles administered their suggested training only once before evaluation occurred, as seen in Alqahtani and Kavakli-Thorne (2020), where data was collected after a one-time administration of a serious game, or Shaw et al. (2011), where knowledge levels were assessed after one training session. In addition, a median number of participants of $N = 96$ suggests a lack of large-scale studies. While Kim et al. (2020) and Gordon et al. (2019) administered their training to 1248 & 5416 participants respectively, many studies used between 10 & 100 participants. In addition to a lack of long-term, large-scale evaluations, outcome measurements were often not concerned with cybersecurity behaviour, but focused instead on behavioural intentions, changes in attitudes and perceptions, or other metrics. While many theories of behaviour have identified these factors as predictors of behaviour change, for example in the Theory of Planned Behaviour (Ajzen, 1991), this association is often weak (Bhattacherjee

and Sanford, 2009). The ambiguity of the term awareness is a related issue. In many of the articles analysed for this review, the term awareness is used when describing the effects of the training. Unfortunately, it is often unclear what the implication of awareness is in the context of training effectiveness. Improvements in attitude, increased levels of knowledge, higher intentions with regard to security guideline adherence or objectively improved behaviour could all indicate increases in awareness. This diversity in measurement is shown in Al Zaidy (2020), Albrechtsen and Hovden (2010) and Puhakainen (2006), who measure knowledge, self-reported behaviour and attitude respectively, all within the context of raising awareness.

### 4.4. Gaps in the literature and areas for future research

With regard to the above-highlighted themes, several gaps in the literature were observed. In general, the field would benefit from a stronger focus on the design of the interventions, as the goals and target metrics of a specific training program were not always apparent. One significant observation therein is the limited use of theory to support training creation. As stated previously, choices made during the training design process seemed to lack deliberation, contributing to the frequent occurrence of traditional text- or video-based training methodologies. Similar observations were made concerning other design choices, such as personalisation of training or training method combination. Whether or not these choices affected end-user behaviour was often not evaluated. Addressing these questions, both theoretically and empirically, would help the field move forward.

Most studies identified in this review are empirical in nature, with the majority of them conducting quantitative evaluations. Unfortunately, the empirical evaluations conducted in the selected studies were limited in several ways. For example, long-lasting behaviour change could not be evaluated with certainty, since the majority of studies measured effectiveness after a single training session and did not include a follow-up measurement. This is unfortunate, given that long-term behaviour change and habit formation are often associated with continued repetition of an activity (Lally and Gardner, 2013). Additionally, half of the articles that conducted an empirical evaluation used fewer than 100 participants, suggesting that a training was set up that might be difficult to scale up for use in large organisations. Furthermore, many interventions were not tested on employees themselves, but rather on students or other populations (Abraham and Chengalur-Smith, 2019; Filipczuk et al., 2019), even when the training was designed for an organisational setting. While that is not inappropriate for the early stages of intervention development, field validation in the context where the training should be implemented would strengthen the practical implementations of successful training methods. External factors such as time pressure and intense job requirements could play a role in how employees interact with cybersecurity risks and should therefore be considered when evaluating the effectiveness of cybersecurity training. Lastly, the majority of articles measured the effectiveness of cybersecurity training not through objective behavioural measurements, but by assessing behavioural intentions, increases in knowledge or other measurements. As outlined above, while these factors are related to behaviour change, they do not constitute a true alternative to objective behavioural measurements. The missing focus on developing objective behavioural measurements is therefore the final gap that this literature review uncovered.

Overall, further analysis is needed to understand why employees act insecure, in order to create effective interventions dedicated to minimising unsafe acts in cyberspace (Kirlappos et al., 2014). Additionally, while some articles base their intervention and training techniques on theory, a more explicit reliance on theories of behaviour change is encouraged. Training initiatives that used theories such as the protection motivation theory and the theory of planned behaviour showed positive results, suggesting that the field would benefit from a more theory-driven approach to cybersecurity training (e.g. Alqahtani and Kavakli-Thorne, 2020; Cook et al., 2017). Future research should also examine individual difference in the types of methods employees prefer when undergoing training.

Additional avenues for future research should be focused on intervention design specifications, especially to determine if specific training properties or delivery methods are more appropriate for specific cybersecurity behaviours. Furthermore, large-scale field evaluations with a focus on long-lasting behaviour change, as well as the implementation of objective behavioural measurements to assess effectiveness are encouraged.

## 5. Conclusion

The field of cybersecurity training for end-users is diverse in training design, methods of delivery, cybersecurity topics and measurements of effectiveness. We found promising results in improving cybersecurity behaviour through training for a variety of cybersecurity behaviours through a wide range of means. Still, many aspects of training design are uncertain and could benefit from changes in structure and deliberation during the design process. Furthermore, outcome measures used for effectiveness evaluation are often removed from behaviour and instead focus on related factors such as attitudes and intentions. This review highlights a need for further research, especially with regard to theory-based training development, as well as the design of the training environment. Furthermore, continued critical evaluation of long-term training effects is necessary to build a cyber-resilient workforce.

## CRediT authorship contribution statement

**Julia Prümmer:** Conceptualization, Methodology, Formal analysis, Data curation, Writing – original draft, Visualization. **Tommy van Steen:** Conceptualization, Formal analysis, Writing – review & editing, Supervision. **Bibi van den Berg:** Conceptualization, Writing – review & editing, Supervision.

## Declaration of Competing Interest

The authors of this article have no conflicting interests to declare. No external funding was sought with regard to this project.

## Data availability

Data will be made available on request.

## Appendix A

Fig. A4 and Tables A1-A8

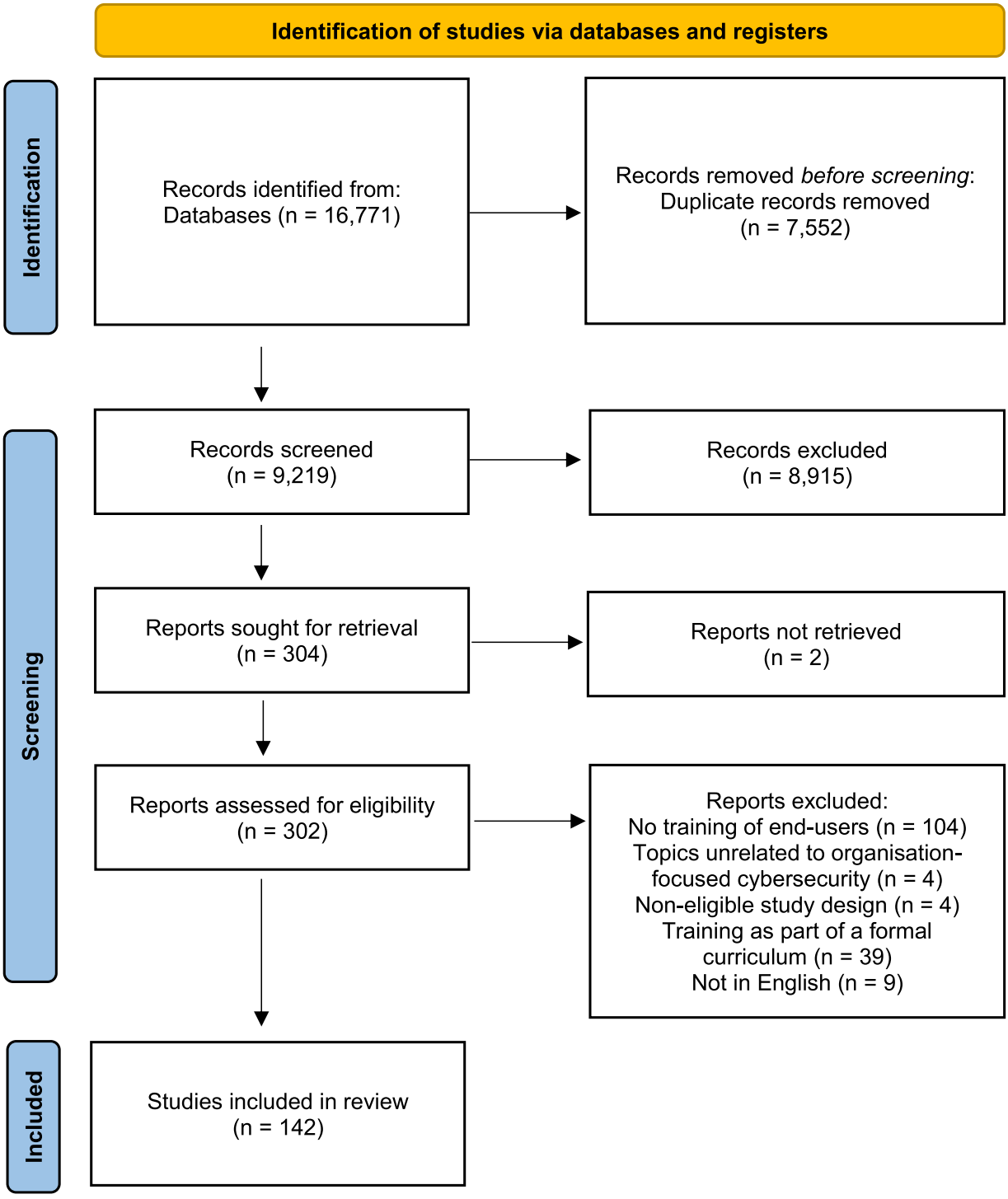


**Fig. A4.** Flow chart for identification of eligible studies.

**Table A1**
PRISMA guidelines adapted from Page et al. (2021).

| Checklist item | Explanation |
|---|---|
| Eligibility criteria | Specify the inclusion and exclusion criteria for the review and how studies were grouped for the syntheses. |
| Information sources | Specify all databases, registers, […] and other sources searched or consulted to identify studies. Specify the date when each source was last searched or consulted. |
| Search strategy | Present the full search strategies for all databases, registers and websites, including any filters and limits used. |

(*continued on next page*)

**Table A1** (*continued*)

| Checklist item | Explanation |
|---|---|
| Selection process | Specify the methods used to decide whether a study met the inclusion criteria of the review, including how many reviewers screened each record and each report retrieved, whether they worked independently, and if applicable, details of automation tools used in the proces. |
| Data collection process | Specify the methods used to collect data from reports, including how many reviewers collected data from each report, whether they worked independently, any processes for obtaining or confirming data from study investigators, and if applicable, details of automation tools used in the process. |
| Data items | a. List and define all outcomes for which data were sought. Specify whether all results that were compatible with each domain in each study were sought (e.g. for all measures, time points, analyses), and if not, the methods used to decide which results to collect.<br>b. List and define all other variables for which data were sought (e.g. participant and intervention characteristics, funding sources). Describe any assumptions made about any missing or unclear information. |
| Study risk of bias assessment | Specify the methods used to assess risk of bias in the included studies […]. |
| Effect measures | Specify for each outcome the effect measure(s) (e.g. risk ratio, mean difference) used in the synthesis or presentation of results. |
| Synthesis methods | […] Describe any methods used to tabulate or visually display results of individual studies and syntheses. […] |
| Reporting bias assessment | Describe any methods used to assess risk of bias due to missing results in a synthesis (arising from reporting biases). |
| Certainty assessment | Describe any methods used to assess certainty (or confidence) in the body of evidence for an outcome. |

**Table A2**
Search queries and results per database.

| Database | Search query | Results |
|---|---|---|
| Web of Science | AB=(cyber* OR "cyber security" OR "information security" OR "digital security" OR "computer security" OR "social engineering" OR "IT security") AND AB=(intervention* OR training OR awareness OR game* OR gamification) | 6298 |
| ACM Digital Library | [[*Abstract: cyber**] OR [*Abstract*: "*cyber security*"] OR [*Abstract*: "*information security*"] OR [*Abstract*: "*digital security*"] OR [*Abstract*: "*computer security*"] OR [*Abstract*: "*social engineering*"] OR [*Abstract*: "*it security*"]] AND [[Abstract: intervention*] OR [*Abstract: training*] OR [*Abstract: awareness*] OR [*Abstract: game**] OR [*Abstract: gamification*]] | 1405 |
| ProQuest | ab(cyber* OR "cyber security" OR "information security" OR "digital security" OR "computer security" OR "social engineering" OR "IT security") AND ab(intervention* OR training OR awareness OR game* OR gamification) | 4896 |
| PubMed | (cyber*[Title/Abstract] OR "cyber security"[Title/Abstract] OR "information security"[Title/Abstract] OR "digital security"[Title/Abstract] OR "computer security"[Title/Abstract] OR "social engineering"[Title/Abstract] OR "IT security"[*Title/Abstract*]) AND (intervention*[Title/Abstract] OR training[Title/Abstract] OR awareness[Title/Abstract] OR game*[Title/Abstract] OR gamification[*Title/Abstract*]) | 1562 |
| PsycINFO | AB (cyber* OR "cyber security" OR "information security" OR "digital security" OR "computer security" OR "social engineering" OR "IT security") AND AB (intervention* OR training OR awareness OR game* OR gamification) | 2610 |
| Total | | 16,771 |

**Table A3**
PRISMA guidelines adapted from Page et al. (2021) and their application.

| Checklist item | Explanation | Application |
|---|---|---|
| Eligibility criteria | Specify the inclusion and exclusion criteria for the review and how studies were grouped for the syntheses. | Inclusion and exclusion criteria were specified prior to data collection. An exact description of these criteria can be found in Section 2.2. For the synthesis, studies were grouped according to their study design, namely non-empirical/theoretical, empirical and proposed training/development. |
| Information sources | Specify all databases, registers, […] and other sources searched or consulted to identify studies. Specify the date when each source was last searched or consulted. | Databases searched were Web of Science, ACM Digital Library, ProQuest, PubMed & PsycINFO. The search was carried out on 26th November 2021. |
| Search strategy | Present the full search strategies for all databases, registers and websites, including any filters and limits used. | Full search strategy for each database can be seen in Table A2. |
| Selection process | Specify the methods used to decide whether a study met the inclusion criteria of the review, including how many reviewers screened each record and each report retrieved, whether they worked independently, and if applicable, details of automation tools used in the proces. | During initial title and abstract screening, records were screened for general thematical relevance. During full-text screening, records were screened more thorougly, using the inclusion and exclusion criteria specified in Section 2.2. Title and abstract, as well as a full-text screening were carried out by two authors (X & X (masked for peer review)). Disagreements were discussed until consensus was reached. No automation tools were used. |
| Data collection process | Specify the methods used to collect data from reports, including how many reviewers collected data from each report, whether they worked independently, any processes for obtaining or confirming data from study investigators, and if applicable, details of automation tools used in the process. | Data was extracted by thorough analysis of each record and relevant information was transcribed into an Excel file. This extraction was carried out by author X (masked for peer review). Due to the nature of the data sought, all sought data was available in the source records. No automation tools were used. |
| Data items | a. List and define all outcomes for which data were sought. Specify whether all results that were compatible with each domain in each study were sought (e.g. for all measures, time points, analyses), and if not, the methods used to decide which results to collect.<br>b. List and define all other variables for which data were sought (e.g. participant and intervention characteristics, funding sources). Describe any assumptions made about any missing or unclear information. | a. Outcomes for which data was sought included cybersecurity topics, use of theories, training delivery methods, trainer presence, platform, social setting, training frequency, use of behavioural change methods, sample population, sample size, data collection method, degree of data manipulation, outcome measures & method of evaluation, as well as an overview of the findings. For some records, mainly non-empirical, not all information was present. In those cases, a more detailed description of findings was extracted.<br>b. Other information extracted for the purposes of completeness included a detailed description of training mechanisms. |

(*continued on next page*)

**Table A3** (*continued*)

| Checklist item | Explanation | Application |
|---|---|---|
| Study risk of bias assessment | Specify the methods used to assess risk of bias in the included studies […]. | Risk of bias of the selected records was not assessed due to considerable methodological differences between the selected records. A further explanation is provided in Section 2.3. |
| Effect measures | Specify for each outcome the effect measure(s) (e.g. risk ratio, mean difference) used in the synthesis or presentation of results. | Effect measures were not explicitly considered in this systematic review as statistical analysis of training effectiveness is beyond the scope of this paper. |
| Synthesis methods | […] Describe any methods used to tabulate or visually display results of individual studies and syntheses. […] | Outcomes deemed most relevant and informative by the authors were displayed in Table A5 for all individual studies. |
| Reporting bias assessment | Describe any methods used to assess risk of bias due to missing results in a synthesis (arising from reporting biases). | As no statistical analysis of the study findings were conducted, the missing effect measures do not pose a bias to the findings in this review. |
| Certainty assessment | Describe any methods used to assess certainty (or confidence) in the body of evidence for an outcome. | All records included in this review have been published in peer-reviewed journals or were approved by a dissertation committee. |

**Table A4**
Data extracted from studies included in the review.

| Author & Year | Topic | Training delivery method | Training properties[1] | Sample[2] | Data collection | Outcome measures | Country |
|---|---|---|---|---|---|---|---|
| Abawajy (2014) | social engineering (phishing) | game-based<br>text-based<br>video-based | no trainer<br>online<br>individual | 60<br>general | quantitative<br>non-experimental | objective behaviour<br>enjoyment of training | Australia[4] |
| Abraham (2012) | social engineering (fake web-pages) | video-based<br>text-based | no trainer<br>online<br>individual | 151<br>students | quantitative<br>non-experimental | attitude<br>efficacy belief<br>objective behaviour | United States |
| Abraham and Chengalur-Smith (2019) | social engineering (fake web-pages and links) | text-based | no trainer<br>online<br>individual | 206<br>students | quantitative<br>experimental | perception<br>efficacy belief<br>intention | United States |
| Abroshan et al. (2021) | social engineering (phishing) | – | – | – | – | – | Belgium[4] |
| Adams and Makramalla (2015) | social engineering | game-based | no trainer<br>online<br>individual | – | – | – | Canada[4] |
| Adinolf et al. (2019) | not specified | simulation-based | not specified<br>in-person<br>group | 20<br>employees | qualitative<br>non-experimental | ideas for cybersecurity training using Virtual Reality | Australia |
| Ahmmed (2019) | WIFI safety | text-based | no trainer<br>online<br>individual | 100<br>not specified | quantitative<br>non-experimental | objective behaviour | United Kingdom |
| Al Zaidy (2020) | not specified | not specified | not specified | 75<br>employees | quantitative<br>non-experimental | knowledge<br>self-reported behaviour | United States |
| Al-Hamar (2010) | social engineering (phishing) | text-based<br>game-based<br>presentation-based | trainer & no trainer<br>online & in-person<br>group & individual | 209<br>employees | mixed<br>quasi-experimental | knowledge<br>objective behaviour | United Kingdom & Qatar |
| Albrechtsen and Hovden (2010) | not specified | discussion-based | trainer<br>in-person<br>group | 197<br>employees | mixed<br>experimental | self-reported behaviour<br>attitude | Norway |
| Aldawood and Skinner (2019a) | social engineering | – | – | – | – | – | Australia[4] |
| Aldawood and Skinner (2019b) | social engineering | – | – | – | – | – | Australia[4] |
| Alotaibi (2019) | password safety<br>malware | game-based | no trainer<br>online<br>individual | 100<br>general | quantitative<br>non-experimental | knowledge<br>usability<br>enjoyment of training | Saudi Arabia |
| Alqahtani and Kavakli-Thorne (2020) | not specified | game-based | no trainer<br>online<br>individual | 91<br>students | quantitative<br>non-experimental | usability<br>intention | Australia |
| Alruwaili (2019) | not specified | – | – | – | – | – | Saudi Arabia |
| Alshaikh et al. (2021) | not specified | not specified | not specified | not specified<br>employees | qualitative<br>non-experimental | – | Saudi Arabia & Australia[4] |
| Alzahrani and Johnson (2019) | workplace security (policy compliance) | game-based | trainer<br>in-person<br>group | 30<br>students | quantitative<br>non-experimental | intention | United Kingdom |
| Amor (2010) | general information security | – | – | – | – | – | United States[4] |
| Anzaldua Jr (2016) | not specified | video-based | no trainer<br>online<br>individual | 32<br>students | quantitative<br>experimental | attitude<br>intention | United States |
| Aoyama et al. (2017) | not specified | discussion-based<br>simulation-based | not specified<br>in-person | 4 groups<br>containing 1–5 | qualitative<br>non-experimental | level of incident preparedness | Japan[4] |

(*continued on next page*)

**Table A4** (*continued*)

| Author & Year | Topic | Training delivery method | Training properties[1] | Sample[2] | Data collection | Outcome measures | Country |
|---|---|---|---|---|---|---|---|
| | | | group & individual | participants employees | | | |
| Arain et al. (2019) | not specified | not specified | no trainer online individual | 586 employees | quantitative non-experimental | knowledge | Canada |
| Armstead (2017) | not specified | simulation-based | not specified | 8 employees | qualitative non-experimental | perceived effectiveness | United States |
| Ashenden and Lawrence (2013) | not specified | – | – | – | – | – | United Kingdom[4] |
| Awojana et al. (2018) | not specified | – | – | – | – | – | United States[4] |
| Bada and Nurse (2019) | workplace security (bring your own device) social engineering | video-based | not specified | 20 employees | mixed non-experimental | usability perceived effectiveness | United Kingdom |
| Baillon et al. (2019) | social engineering (phishing) | info-based simulation-based | no trainer online individual | 10,929 employees | quantitative experimental | objective behaviour | The Netherlands |
| Bakalovic (2020) | not specified | – | – | – | – | – | United States[4] |
| Banfield (2016) | not specified | not specified | not specified | 99 employees | quantitative non-experimental | intention usability perceived effectiveness | United States[4] |
| Bauer et al. (2017) | not specified | not specified | not specified | 33 employees | qualitative non-experimental | perception knowledge | Austria[4] |
| Baxter et al. (2016) | not specified | game-based info-based | not specified online individual | 116 students | quantitative experimental | enjoyment of training attitude knowledge | United States |
| Bernier (2020) | social engineering | not specified | not specified | 54 employees | qualitative non-experimental | knowledge intention | United States |
| Beuran et al. (2018) | not specified | simulation-based | no trainer online individual | – | – | – | Japan |
| Beuran et al. (2019) | not specified | not specified | not specified | – | – | – | Japan |
| Bishop (2002) | not specified | – | – | – | – | – | United States[4] |
| Black et al. (2018) | not specified | info-based | no trainer online individual | – | – | – | United States[4] |
| Briliyanti et al. (2019) | not specified | simulation-based | trainer online & in-person group | 19 employees | quantitative non-experimental | usability knowledge | United States |
| Byrne (2020) | social engineering | – | – | – | – | – | United States[4] |
| Carlson (2020) | workplace security (insider threat) | – | – | – | – | – | United States[4] |
| Chatchalermpun and Daengsi (2021) | social engineering (phishing) | info-based presentation-based | trainer & no trainer online & in-person individual | 20,260 employees | quantitative non-experimental | objective behaviour | Thailand |
| Chen et al. (2019) | not specified | game-based | no trainer online individual | – | – | – | United States |
| Chen et al. (2020) | not specified | game-based | no trainer online individual | 178 general | quantitative experimental | perception attitude efficacy beliefs | United States |
| Chin et al. (2016) | general information security | video-based | no trainer online individual | 347 students | quantitative non-experimental | self-reported behaviour | United States |
| Chowdhury and Gkioulos (2021) | malware (critical infrastructure protection) | – | trainer & no trainer online & in-person group & individual | – | – | – | Norway[4] |
| CJ et al. (2018) | social engineering (phishing) | game-based | no trainer online individual | 8071 general | quantitative non-experimental | objective behaviour knowledge | India[4] |
| Clark (2013) | not specified | discussion-based presentation-based text-based | trainer & no trainer online & in-person group & individual | 202 employees | quantitative non-experimental | knowledge attitude perception | United States[4] |

(*continued on next page*)

**Table A4** (*continued*)

| Author & Year | Topic | Training delivery method | Training properties[1] | Sample[2] | Data collection | Outcome measures | Country |
|---|---|---|---|---|---|---|---|
| Coenraad et al. (2020) | not specified | – | no trainer<br>online<br>individual | – | – | – | United States[4] |
| Cone et al. (2007) | not specified | game-based | no trainer<br>online<br>individual | – | – | – | United States[4] |
| Conrad (2021) | not specified | not specified | not specified | 7<br>employees | qualitative<br>non-experimental | subjective views on what makes cybersecurity successful | United States |
| Cook et al. (2017) | not specified | game-based<br>presentation-based | no trainer<br>online<br>group | not specified | quantitative<br>non-experimental | knowledge | United Kingdom[4] |
| Cooper (2008) | not specified | – | – | – | – | – | United States |
| Cooper (2009) | password safety<br>malware<br>social engineering | – | – | – | – | – | United States |
| Curry et al. (2019) | password safety | info-based | no trainer<br>online<br>individual | 238<br>students | mixed<br>non-experimental | self-reported behaviour | United States[4] |
| DeCarlo (2021) | not specified | game-based<br>presentation-based | no trainer<br>online<br>individual | 300<br>employees | quantitative<br>experimental | objective behaviour<br>knowledge | United States[4] |
| Denning et al. (2013) | not specified | game-based | no trainer<br>in-person<br>group | 450<br>students | qualitative<br>non-experimental | enjoyment of training<br>perceived effectiveness | United States[4] |
| Dixon et al. (2019) | social engineering (phishing) | game-based | no trainer<br>online & in-person<br>group | 9<br>young adults | qualitative<br>non-experimental | usability | United Kingdom[4] |
| Dominguez (2010) | general information security | presentation-based<br>text-based<br>video-based | not specified<br>online & in-person<br>group & individual | study 1 - 55; study 2 - 4<br>employees | qualitative<br>non-experimental | general evaluation of security programs | Puerto Rico |
| Dugan (2018) | not specified | – | – | – | – | – | United States[4] |
| Fatima et al. (2019) | social engineering (phishing) | game-based | no trainer<br>in-person<br>group | 63<br>students | quantitative<br>non-experimental | perception<br>objective behaviour | China |
| Filipczuk et al. (2019) | social engineering (phishing) | game-based<br>info-based | no trainer<br>online<br>individual | 17<br>employees & students | qualitative<br>non-experimental | knowledge | United Kingdom[4] |
| Fleming (2017) | not specified | not specified | not specified | 15<br>employees | qualitative<br>non-experimental | participant experiences in addressing cybersecurity | United States |
| Fujs et al. (2020) | not specified | – | – | – | – | – | Slovenia[4] |
| Ghazvini and Shukur (2016) | not specified | – | – | – | – | – | Malaysia |
| Ghazvini and Shukur (2017) | not specified | – | – | – | – | – | Malaysia |
| Ghazvini and Shukur (2018) | workplace security<br>malware | game-based | no trainer<br>online<br>individual | 5<br>employees | quantitative<br>non-experimental | knowledge | Malaysia |
| González (2019) | not specified | – | – | – | – | – | United States[4] |
| Goode (2018) | not specified | presentation-based<br>video-based<br>text-based | trainer & no trainer<br>online & in-person<br>group & individual | 250<br>employees | quantitative<br>experimental | knowledge | United States |
| Gordon et al. (2019) | social engineering (phishing) | info-based | no trainer<br>online<br>individual | 5416<br>employees | quantitative<br>quasi-experimental | knowledge<br>objective behaviour | United States |
| Goyal et al. (2019) | workplace security (policy compliance) | game-based | no trainer<br>online<br>group & individual | 30<br>general | quantitative<br>non-experimental | perceived effectiveness<br>objective behaviour | United States[4] |
| Gundu and Flowerday (2013) | not specified | info-based | no trainer<br>online<br>individual | 28<br>employees | mixed<br>non-experimental | knowledge<br>attitude<br>self-reported behaviour | South Africa |
| Hammond (2019) | not specified | not specified | not specified | 340<br>employees | quantitative<br>quasi-experimental | perception | United States, Germany, |

(*continued on next page*)

**Table A4** (*continued*)

| Author & Year | Topic | Training delivery method | Training properties[1] | Sample[2] | Data collection | Outcome measures | Country |
|---|---|---|---|---|---|---|---|
| | | | | | | | Venezuela, India & Brazil |
| Hamoud and Aimeur (2020) | malware (user-orientated attacks) | simulation-based<br>info-based | trainer<br>online<br>individual | – | – | – | Canada & Algeria[4] |
| Harrison (2018) | social engineering (phishing) | text-based<br>simulation-based | no trainer<br>online<br>individual | 559<br>employees | quantitative<br>experimental | knowledge<br>objective behaviour | United States |
| Harta et al. (2020) | social engineering | game-based | no trainer<br>in-person<br>group | 54<br>employees & students | quantitative<br>non-experimental | perceived effectiveness | United Kingdom |
| Hatzivasilis et al. (2020) | not specified | – | no trainer<br>online<br>individual | – | – | – | Greece[4] |
| Häußinger (2015) | not specified | not specified | not specified | 444<br>general | quantitative<br>non-experimental | not specified | Germany[4] |
| He and Zhang (2019) | not specified | – | – | – | – | – | United States[4] |
| Heid et al. (2020) | not specified | game-based | no trainer<br>online<br>individual | – | – | – | Germany[4] |
| Hendrix et al. (2016) | not specified | – | – | – | – | – | United Kingdom[4] |
| Hepp et al. (2018) | general information security | info-based | not specified<br>online<br>not specified | 191<br>employees | qualitative<br>non-experimental | perceived effectiveness | Canada |
| House (2013) | social engineering (phishing) | video-based | no trainer<br>online<br>individual | 59<br>students | quantitative<br>non-experimental | perception<br>intention<br>objective behaviour | United States |
| Ikhalia et al. (2019) | social engineering<br>malware | video-based<br>info-based | no trainer<br>online<br>individual | 40<br>students | mixed<br>non-experimental | enjoyment of training<br>usability<br>objective behaviour | United Kingdom |
| Jansen and Fischbach (2020) | social engineering | game-based | no trainer<br>online<br>individual | – | – | – | Germany[4] |
| Jansson and von Solms (2013) | social engineering (phishing) | simulation-based | no trainer<br>online<br>individual | week 1 - 9273;<br>week 2 - 8231<br>employees & students | quantitative<br>non-experimental | objective behaviour | South Africa |
| Jeffers (2016) | not specified | – | – | – | – | – | United States[4] |
| Jenkins et al. (2013) | not specified | video-based | no trainer<br>online<br>individual | 238<br>students | quantitative<br>non-experimental[3] | usability<br>objective behaviour | United States[4] |
| Katsantonis et al. (2017) | not specified | – | – | – | – | – | Greece[4] |
| Kennedy (2016) | not specified | – | – | – | – | – | United States[4] |
| Khan et al. (2011) | not specified | – | – | – | – | – | Saudi Arabia[4] |
| Khando et al. (2021) | not specified | – | – | – | – | – | Sweden[4] |
| Kießling et al. (2021) | not specified | game-based | no trainer<br>in-person<br>group | – | – | – | Germany[4] |
| Kim et al. (2017) | social engineering (malicious email and files) | simulation-based | no trainer<br>online<br>individual | – | – | – | South Korea[4] |
| Kim et al. (2020) | social engineering (phishing) | punishment-based | not specified | 1248<br>employees | quantitative<br>experimental for punishment condition<br>non-experimental for comparison condition | objective behaviour | South Korea |
| Kim (2010) | not specified | presentation-based<br>info-based | trainer & no trainer<br>online & in-person<br>group & individual | 212<br>employees | quantitative<br>quasi-experimental | knowledge<br>perceived effectiveness | United States |
| Kim et al. (2016) | general information security | simulation-based | no trainer<br>online<br>individual | 347<br>students | quantitative<br>non-experimental | attitude | South Korea[4] |
| Kletenik et al. (2020) | general information security | game-based | no trainer<br>not specified<br>individual | 75<br>students | quantitative<br>non-experimental | knowledge | United States |
| Kletenik et al. (2021) | general information security | game-based | no trainer<br>online<br>individual | 75<br>students | quantitative<br>non-experimental | knowledge | United States |

(*continued on next page*)

**Table A4** (*continued*)

| Author & Year | Topic | Training delivery method | Training properties[1] | Sample[2] | Data collection | Outcome measures | Country |
|---|---|---|---|---|---|---|---|
| Knopik (2021) | not specified | game-based<br>video-based | not specified | 100<br>general | quantitative<br>non-experimental | not specified | United States |
| Korpela (2015) | not specified | – | – | – | – | – | Canada[4] |
| Lamour (2008) | not specified | presentation-based<br>info-based | trainer<br>online & in-person<br>group & individual | 120<br>students | quantitative<br>experimental | objective behaviour<br>knowledge | United States |
| Legárd (2021) | not specified | – | – | – | – | – | Hungary[4] |
| Lim et al. (2016) | social engineering (phishing) | simulation-based | no trainer<br>online<br>individual | training 1 & 2 - 481; training 3 & 4 - 1045<br>employees | quantitative<br>non-experimental | objective behaviour | South Korea[4] |
| Lim et al. (2013) | malware (hacking) | game-based | no trainer<br>online<br>individual | – | – | – | South Korea[4] |
| Loffler et al. (2021) | not specified | simulation-based | no trainer<br>online<br>group | 81<br>students | mixed<br>non-experimental | usability | Switzerland |
| Martin (2019) | social engineering (phishing) | text-based | no trainer<br>online<br>individual | 139<br>employees | quantitative<br>non-experimental | objective behaviour | United States |
| Mayhorn and Nyeste (2011) | social engineering (phishing) | game-based<br>simulation-based | no trainer<br>online<br>individual | 84<br>students | quantitative<br>experimental | objective behaviour | United States |
| McCarthy (2021) | not specified | – | – | – | – | – | United States[4] |
| McCoy and Fowler (2004) | password safety<br>workplace security<br>social engineering | presentation-based<br>text-based | trainer & no trainer<br>online & in-person<br>group & individual | – | – | – | United States |
| McCrohan et al. (2010) | password safety | low-information<br>high-information - story style | no trainer<br>online<br>individual | 396<br>students | quantitative<br>experimental | objective behaviour | United States |
| Muhirwe (2016) | social engineering (phishing)<br>workplace security (insider threat) | – | – | – | – | – | United States[4] |
| Nicolas-Rocca (2010) | password safety | presentation-based | trainer<br>in-person<br>group | 30<br>employees | mixed<br>non-experimental | objective behaviour | United States |
| Oslejsek et al. (2021) | not specified | – | trainer<br>online<br>group & individual | – | – | – | Czech Republic[4] |
| Puhakainen (2006) | not specified | presentation-based<br>discussion-based | trainer<br>in-person<br>group | 17<br>employees | mixed<br>non-experimental | attitude | Finland[4] |
| Puhakainen and Siponen (2010) | not specified | discussion-based<br>presentation-based | trainer<br>in-person<br>group | 16<br>employees | qualitative<br>non-experimental | usability<br>perceived effectiveness<br>enjoyment of training | Finland |
| Robbins (2020) | not specified | not specified | not specified | 200<br>employees | quantitative<br>non-experimental | knowledge<br>attitude<br>self-reported behaviour | United States |
| Rotvold (2007) | general information security | presentation-based<br>text-based<br>video-based | not specified<br>online & in-person<br>group & individual | study 1 - 85; study 2 - 144<br>employees | quantitative<br>non-experimental | general evaluation of security programs | United States |
| Sabillon et al. (2019) | not specified | info-based<br>video-based | trainer<br>online & in-person<br>group | not specified<br>employees | qualitative<br>non-experimental | not specified | Canada |
| Salameh (2020) | not specified | game-based | no trainer<br>online<br>individual | 122<br>general | quantitative<br>non-experimental | intention | United States |
| Sardar and Wahsheh (2020) | password safety<br>social engineering (phishing)<br>malware | presentation-based | trainer<br>in-person<br>group | – | – | – | United States[4] |

(*continued on next page*)

**Table A4** (*continued*)

| Author & Year | Topic | Training delivery method | Training properties[1] | Sample[2] | Data collection | Outcome measures | Country |
|---|---|---|---|---|---|---|---|
| Shargawi (2017) | social engineering (phishing) | presentation-based<br>info-based<br>discussion-based | trainer & no trainer<br>online & in-person<br>group & individual | 100 students | quantitative<br>quasi-experimental | perception<br>knowledge | Saudi Arabia, United Kingdom & United States |
| Shaw (2020) | social engineering (phishing) | – | – | – | – | – | United States[4] |
| Shaw et al. (2009) | social engineering (e-mail management) | hypermedia (high media richness)<br>multimedia (middle media richness)<br>hypertext (low media richness) | no trainer<br>online<br>individual | 153 students | quantitative<br>quasi-experimental | knowledge | Taiwan |
| Shaw et al. (2011) | not specified | knowledge-map based training<br>browse-based training | no trainer<br>online<br>individual | 78 students | quantitative<br>quasi-experimental | knowledge | Taiwan[4] |
| Siponen et al. (2020) | password safety | simulation-based | trainer<br>in-person<br>group | 83 employees | quantitative<br>quasi-experimental | intention<br>objective behaviour | United Arab Emirates |
| Stefaniuk (2020) | not specified | not specified | not specified | 98 employees | quantitative<br>non-experimental | evaluation of current practices in organisation | Poland[4] |
| Sumner and Yuan (2019) | social engineering (phishing) | – | – | – | – | – | United States[4] |
| Švábenský and Vykopal (2018) | not specified | game-based | not specified<br>online<br>individual | 67 employees & students | quantitative<br>non-experimental | perceived effectiveness<br>usability | Austria, Slovakia, Czech Republic & Switzerland |
| Sykosch et al. (2020) | social engineering (phishing) | presentation-based | trainer<br>in-person<br>group | phase 1 - 196;<br>phase 2 - 163 employees | quantitative<br>quasi-experimental | objective behaviour | Germany[4] |
| Talib (2014) | not specified | visual<br>aural<br>reading/writing<br>kinaesthetic | no trainer<br>in-person<br>individual | 40 employees & students | quantitative<br>non-experimental | knowledge | United Kingdom |
| Tan et al. (2020) | not specified | – | – | – | – | – | Japan[4] |
| Thornton and Turley (2020) | password safety | game-based | no trainer<br>online<br>individual | 28 students | quantitative<br>non-experimental | attitude<br>knowledge<br>objective behaviour | United States[4] |
| Tschakert and Ngamsuriyaroj (2019) | social engineering (phishing) | video-based<br>game-based<br>text-based<br>presentation-based | trainer & no trainer<br>online & in-person<br>group & individual | 33 students | quantitative<br>non-experimental | objective behaviour<br>usability<br>enjoyment of training | Thailand |
| van Steen and Deeleman (2021) | not specified | game-based | no trainer<br>online<br>individual | 258 employees & students | quantitative<br>experimental | attitude<br>perception<br>intention<br>self-reported behaviour | The Netherlands |
| van Steenburg (2017) | not specified | – | – | – | – | – | United States[4] |
| Veneruso et al. (2020) | not specified | simulation-based | no trainer<br>online<br>individual | 40 young adults | quantitative<br>non-experimental[3] | knowledge | Italy[4] |
| Waly (2013) | not specified | not specified | not specified | 40 employees | qualitative<br>non-experimental | perceived effectiveness | United Kingdom |
| Weanquoi et al. (2017) | social engineering (phishing) | game-based | no trainer<br>online<br>individual | 30 students | quantitative<br>non-experimental | not specified | United States |
| Wen et al. (2017) | social engineering (phishing) | game-based | no trainer<br>online<br>individual | – | – | – | United States[4] |
| Wu et al. (2021) | not specified | game-based<br>presentation-based | trainer<br>online & in-person<br>group & individual | 110 students | quantitative<br>non-experimental[3] | attitude<br>knowledge<br>intention | Taiwan |
| Yasin et al. (2018) | not specified | game-based | trainer<br>in-person<br>group | 16 students | mixed<br>non-experimental | knowledge<br>usability<br>enjoyment of training<br>perceived effectiveness | China[4] |

(*continued on next page*)

**Table A4** (*continued*)

| Author & Year | Topic | Training delivery method | Training properties[1] | Sample[2] | Data collection | Outcome measures | Country |
|---|---|---|---|---|---|---|---|
| Yasin et al. (2019) | general information security | game-based | no trainer in-person group | 96 employees & students | quantitative non-experimental | enjoyment of training usability knowledge | China[4] |
| Younes (2014) | not specified | not specified | not specified | 20 employees | mixed non-experimental[3] | experiences of employees with cybersecurity and training | United States |
| Younis and Musbah (2020) | social engineering (phishing) | – | – | – | – | – | Lybia[4] |

[1] Contains information on presence of trainer, platform and social setting.
[2] Contains information on sample sizes and sample population.
[3] Randomisation is not explicitly stated and it is therefore assumed that it did not occur.
[4] Country of residence of the corresponding author.

**Table A5**
Topics covered in the selected articles.

| Cybersecurity Topics | Cybersecurity Subtopics | N[1] | Example Reference | Described Training Approach | Findings[2] |
|---|---|---|---|---|---|
| General Cybersecurity/Not Specified | | 86 | Chin et al. (2016) | Training included a series of videos covering topics such as mobile security, social networking, password protection and data protection. | mixed |
| Social engineering | | 42 | Jansen and Fischbach (2020) | In Social Engineer Game, player is tasked with performing a social engineering penetration test by applying convention SE attack methods. | N/A |
| | Phishing | 27 | Tschakert and Ngamsuriyaroj (2019) | Training on phishing susceptibility through multiple training methods including educational videos, the game anti-phishing phil and instructor-led lectures. | positive |
| | Fake web-pages | 4 | Abraham and Chengalur-Smith (2019) | A text-based online training covering web security best practices, such as checking URLs, padlock icons and other indicators of fake web-pages. | positive |
| Password safety | | 9 | Siponen et al. (2020) | Educational training sessions on password policies, as well as education on neutralisation techniques, such as 'denial of responsibility', and why they do not excuse insecure password behaviour. | positive |
| Workplace security | | 7 | Ghazvini and Shukur (2018) | Serious game for healthcare industry, in which employees are tasked with answering questions related to different infosec policy topics. | positive |
| | Policy compliance | 2 | Alzahrani and Johnson (2019) | In the described game, players are tasked with managing the security of a small utility company. After each round success/failure of the investments made before is assessed. | positive |
| | Insider threat | 2 | Muhirwe (2016) | Outline of a student-centred approach to cyber-security training based on three dimensions. Students should be seen as college users, home users, and future corporate users. | N/A |
| | "Bring your own device" | 1 | Bada and Nurse (2019) | Creation of a cybersecurity awareness program for SMEs based on a literature review and case study. The program outlines guidelines for engagement with the SMEs, program resources and how to improve security practices and culture, amongst others. | positive |
| Malware | | 8 | Alotaibi (2019) | In malware guardian game, players are instructed to scan files for malware for potential security risks. If incorrect evaluation is made, player is punished. | positive |
| | User-orientated attacks | 1 | Hamoud and Aimeur (2020) | Creation of a theoretical user-based security training model (STRIM). In the model, user reports are generated based on a users' response to a training program. Report is sent to ethical hacker, who creates a personalised practical test for the user. The users' response to this test is analysed and informs future training programs. | N/A |
| | Critical infrastructure protection | 1 | Chowdhury and Gkioulos (2021) | Literature review of cybersecurity training targeted at critical infrastructure protection. Simulation-based solutions show highest amount of research. | N/A |
| | Hacking | 1 | Lim et al. (2013) | In game, attackers are tasked with hacking defenders personal information. If defender is not successful, information is revealed. Afterwards, defender can reflect on how well their data was protected. | N/A |
| Wifi Safety | | 1 | Ahmmed (2019) | Design of interface to aid in wifi network selection. Interface included security metre, indicating the security level of the network. | positive |

[1] Subtopic N's are included in general topic N's. If a more specific subtopic was addressed in the article, a general categorisation was still assigned.
[2] Articles marked with N/A were either theoretical or proposed a training mechanism without conducting an empirical evaluation.

**Table A6**
Theories used in selected articles.

| Theory use | N | Example Reference | Described Theory Implementation |
|---|---|---|---|
| Protection motivation theory | 7 | Gundu and Flowerday (2013) | PMT is used in conjunction with other theories to create the 'behavioural intention model', which is used to create training material. The material communicated the organisations' subjective norms on information security. |
| Theory of planned behaviour | 7 | Banfield (2016) | The survey to assess program effectiveness was based on TPB. They found that perceived behavioural control has a significant effect on security intention. |

(*continued on next page*)

**Table A6** (*continued*)

| Theory use | N | Example Reference | Described Theory Implementation |
|---|---|---|---|
| Theory of reasoned action | 3 | Al Zaidy (2020) | TRA is used in conjunction with other theories to create a study-specific framework. TRA factors were found to lead to more secure action. |
| Signal detection theory | 2 | Tschakert and Ngamsuriyaroj (2019) | SDT was used to measure increases in phishing detection ability caused by training. A decrease of the rate of false negatives was related to participants' ability to detect phishing, rather than a general increase in alertness, as the false-positive rate did not increase. |
| General deterrence theory | 2 | Bernier (2020) | GDT is used in conjunction with TPB to create a study-specific framework of awareness training. The effectiveness of including deterrents in the training was measured. |

**Table A7**
Representation of study characteristics including sample population and evaluation method.

| Study characteristics | N | Example Reference | Content |
|---|---|---|---|
| **Sample population** | | | |
| Employees | 49 | Kim et al. (2020) | Data was collected at a public organisation with over 3700 employees located in Korea. |
| Students | 35 | Weanquoi et al. (2017) | Data was collected from students in two classes at Winston-Salem State University. |
| Young adults | 2 | Dixon et al. (2019) | The participants in this study were sampled based on their gaming habits. |
| General | 8 | Chen et al. (2020) | Data was collected through Amazon Mechanical Turk (AMT). |
| **Method of evaluation** | | | |
| Quantitative | 62 | Mayhorn and Nyeste (2011) | Quantitative data collection occurred through participant interaction with trustworthy and untrustworthy e-mails. |
| Qualitative | 16 | Adinolf et al. (2019) | Qualitative data was collected through two ideation workshops. |
| Mixed | 11 | Curry et al. (2019) | Mixed-method evaluation occurred via close- and open-ended questions. |

**Table A8**
Outcome measures used for empirical evaluation.

| Outcome measures | N | Example Reference | Method of evaluation |
|---|---|---|---|
| Knowledge | 32 | Filipczuk et al. (2019) | Knowledge levels were collected through quizzes as part of the game-play. |
| Objective behaviour | 27 | Gordon et al. (2019) | Objective behaviour assessment occurred through the calculation of phishing e-mail click rates before and after the training program. |
| Attitude | 13 | Robbins (2020) | Attitude levels were measured through a questionnaire, namely the Human Aspects of Information Security Questionnaire (HAIS-Q). |
| Intention | 11 | Salameh (2020) | Intention was measured through a questionnaire, namely the Cybersecurity Intended Behaviour Variables (CIBV) scale based on Van der Linden (2014). |
| Perception | 9 | Hammond (2019) | Perception was assessed through an online questionnaire developed by Ifinedo (2012). |
| Self-reported behaviour | 7 | Gundu and Flowerday (2013) | Self-reported behaviour assessment occurred through an online test based on the three components of enhanced security identified by Kruger & Kearney (2006). |
| Efficacy beliefs | 3 | Chen et al. (2020) | Efficacy beliefs were evaluated through a questionnaire, namely Witte's Risk Behaviour Diagnosis Scale (Witte, 1996). |

## References


Abawajy, J., 2014. User preference of cyber security awareness delivery methods. Behav. Inf. Technol. 33 (3), 3 https://doi.org/10.1080/0144929X.2012.708787.

Abraham, S., 2012. Exploring the effectiveness of information security training and persuasive messages. ProQuest Dissertations and Theses. State University of New York at Albany.

Abraham, S., Chengalur-Smith, I., 2019. Evaluating the effectiveness of learner controlled information security training. Comput. Secur. 87 https://doi.org/10.1016/j.cose.2019.101586.

Abroshan, H., Devos, J., Poels, G., Laermans, E., 2021. A phishing mitigation solution using human behaviour and emotions that influence the success of phishing attacks. In: Adjunct Proceedings of the 29th ACM Conference on User Modeling, Adaptation and Personalization, pp. 345–350. https://doi.org/10.1145/3450614.3464472.

Adams, M., Makramalla, M., 2015. Cybersecurity skills training: an attacker-centric gamified approach. Technol. Innov. Manag..Rev. 5–14.

Adams, R., 2018. Our approach to employee security training. Pager Duty.

Adinolf, S., Wyeth, P., Brown, R., Altizer, R., 2019. Towards designing agent based virtual reality applications for cybersecurity training. In: Proceedings of the 31st Australian Conference on Human-Computer-Interaction, pp. 452–456. https://doi.org/10.1145/3369457.3369515.

Ahmmed, N.M.A., 2019. An evaluation of targeted security awareness for end users. PQDT - UK & Ireland. University of Plymouth, (United Kingdom).

Ajzen, I., 1991. The theory of planned behavior. Organ. Behav. Hum. Decis. Process. 50 (2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T.

Al Zaidy, A., 2020. Impact of training on employee actions and information security awareness in academic institutions. ProQuest Dissertations and Theses. Northcentral University.

Albrechtsen, E., Hovden, J., 2010. Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. Comput. Secur. 29 (4), 4 https://doi.org/10.1016/j.cose.2009.12.005.

Aldawood, H., Skinner, G., 2019a. An academic review of current industrial and commercial cyber security social engineering solutions. In: Proceedings of the 3rd International Conference on Cryptography, Security and Privacy, pp. 110–115. https://doi.org/10.1145/3309074.3309083.

Aldawood, H., Skinner, G., 2019b. Reviewing cyber security social engineering training and awareness programs—pitfalls and ongoing issues. Fut. Internet 11 (3), 3. https://doi.org/10.3390/fi11030073.

Al-Hamar, M.K., 2010. Reducing the risk of e-mail phishing in the state of qatar through an effective awareness framework. PQDT - UK & Ireland. Loughborough University, (United Kingdom).

Alotaibi, F.F.G., 2019. Evaluation and enhancement of public cyber security awareness. PQDT - UK & Ireland. University of Plymouth, (United Kingdom).

Alqahtani, H., Kavakli-Thorne, M., 2020. Design and evaluation of an augmented reality game for cybersecurity awareness (CybAR). Information 11 (2), 2. https://doi.org/10.3390/info11020121.

Alruwaili, A., 2019. A review of the impact of training on cybersecurity awareness. Int. J. Adv. Res. Comput. Sci. 10 (5), 5 https://doi.org/10.26483/ijarcs.v10i5.6476.

Alshaikh, M., Maynard, S.B., Ahmad, A., 2021. Applying social marketing to evaluate current security education training and awareness programs in organisations. Comput. Secur. 100 https://doi.org/10.1016/j.cose.2020.102090.

Alzahrani, A., Johnson, C., 2019. Autonomy motivators, serious games, and intention toward ISP compliance. Int. J. Serious Games 6 (4), 4. https://doi.org/10.17083/ijsg.v6i4.315.

Amor, H., 2010. Training general users on the non-policy side of the IS program. In: 2010 Information Security Curriculum Development Conference, pp. 141–144. https://doi.org/10.1145/1940941.1940970.

Anzaldua Jr, R., 2016. Does information security training change hispanic students' attitudes toward the perception of risk in the management of data security. ProQuest Dissertations and Theses. Northcentral University.
Aoyama, T., Nakano, T., Koshijima, I., Hashimoto, Y., Watanabe, K., 2017. On the complexity of cybersecurity exercises proportional to preparedness. J. Disast. Res. 12 (5, SI), 5 https://doi.org/10.20965/jdr.2017.p1081.
Arain, M.A., Tarraf, R., Ahmad, A., 2019. Assessing staff awareness and effectiveness of educational training on IT security and privacy in a large healthcare organization. J. Multidiscip. Healthc. 12, 73–81. https://doi.org/10.2147/JMDH.S183275.
Armstead, S.K., 2017. The effectiveness of information technology simulation and security awareness training on U.S. military personnel in Iraq and Afghanistan. ProQuest Dissertations and Theses. Capella University.
Ashenden, D., Lawrence, D., 2013. Can we sell security like soap? A new approach to behaviour change. In: Proceedings of the 2013 New Security Paradigms Workshop, pp. 87–94. https://doi.org/10.1145/2535813.2535823.
Awojana, T., Chou, T.-S., Hempenius, N., 2018. Review of the existing game based learning system in cybersecurity. In: Proceedings of the 19th Annual SIG Conference on Information Technology Education, 144. https://doi.org/10.1145/3241815.3241839.
Bada, M., Nurse, J.R.C., 2019. Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). Inf. Comput. Secur. 27 (3), 3 https://doi.org/10.1108/ICS-07-2018-0080.
Bada, M., Sasse, A.M., Nurse, J.R.C., 2019. Cyber Security Awareness Campaigns: why do they fail to change behaviour? CoRR. http://arxiv.org/abs/1901.02672.
Baillon, A., Bruin, J.de, Emirmahmutoglu, A., Veer, E.van de, Dijk, B.van, 2019. Informing, simulating experience, or both: a field experiment on phishing risks. PLoS One 14 (12), 12. https://doi.org/10.1371/journal.pone.0224216.
Bakalovic, A., 2020. The importance of cybersecurity education. ProQuest Dissertations and Theses. Utica College.
Banfield, J.M., 2016. A study of information security awareness program effectiveness in predicting end-user security behavior. ProQuest Dissertations and Theses. Eastern Michigan University.
Bauer, S., Bernroider, E.W.N., Chudzikowski, K., 2017. Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. Comput. Secur. 68, 145–159. https://doi.org/10.1016/j.cose.2017.04.009.
Baxter, R.J.E.W., Holderness Jr, D.K., Wood, D.A, 2016. Applying basic gamification techniques to IT compliance training: evidence from the lab and field. J. Inf. Syst. 30 (3), 3 https://doi.org/10.2308/isys-51341.
Bernier, C., 2020. Evaluating the effectiveness of deterrents and training methods to decrease effectiveness of social engineering on corporate users within large insurance providers. ProQuest Dissertations and Theses. Northcentral University.
Beuran, R., Tang, D., Pham, C., Chinen, K., Tan, Y., Shinoda, Y., 2018. Integrated framework for hands-on cybersecurity training: cyTrONE. Comput. Secur. 78, 43–59. https://doi.org/10.1016/j.cose.2018.06.001.
Beuran, R., Tang, D., Tan, Z., Hasegawa, S., Tan, Y., Shinoda, Y., 2019. Supporting cybersecurity education and training via LMS integration: cyLMS. Educ. Inf. Technol. 24 (6), 6 https://doi.org/10.1007/s10639-019-09942-y.
Bhattacherjee, A., Sanford, C., 2009. The intention–behaviour gap in technology usage: the moderating role of attitude strength. Behav. Inf. Technol. 28 (4), 389–401. https://doi.org/10.1080/01449290802121230.
Bishop, M., 2002. Computer security education: training, scholarship, and research. Computer, S.
Black, M., Chapman, D., Clark, A., 2018. The enhanced virtual laboratory: extending cyber security awareness through a web-based laboratory. Inf. Syst. Educ. J. 16 (6), 6.
Briliyanti, A., Rojewski, J., Van Nguyen, T.J., Luchini-Colbry, K., Colbry, D., 2019. The CyberAmbassador training program. In: Proceedings of the Practice and Experience in Advanced Research Computing on Rise of the Machines (Learning). https://doi.org/10.1145/3332186.3332218.
Byrne, R., 2020. The importance of cybersecurity awareness training on small corporations to reduce the risk of a social engineering attack. ProQuest Dissertations and Theses. Utica College.
Carlson, A., 2020. Combating insider threat with proper training. ProQuest Dissertations and Theses. Utica College.
Chatchalermpun, S., Daengsi, T., 2021. Improving cybersecurity awareness using phishing attack simulation. IOP Conf. Ser. 1088 (1), 1 https://doi.org/10.1088/1757-899X/1088/1/012015.
Chen, T., Hammer, J., Dabbish, L., 2019. Self-efficacy-based game design to encourage security behavior online. In: Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems, pp. 1–6. https://doi.org/10.1145/3290607.3312935.
Chen, T., Stewart, M., Bai, Z., Chen, E., Dabbish, L., Hammer, J., 2020. Hacked time: design and evaluation of a self-efficacy based cybersecurity game. In: Proceedings of the 2020 ACM Designing Interactive Systems Conference, pp. 1737–1749. https://doi.org/10.1145/3357236.3395522.
Chin, A.G., Etudo, U., Harris, M.A., 2016. On mobile device security practices and training efficacy: an empirical study. Inform. Educ. 15 (2), 2 https://doi.org/10.15388/infedu.2016.12.
Chowdhury, N., Gkioulos, V., 2021. Cyber security training for critical infrastructure protection: a literature review. Comput. Sci. Rev. 40 https://doi.org/10.1016/j.cosrev.2021.100361.
CJ, G., Pandit, S., Vaddepalli, S., Tupsamudre, H., Banahatti, V., Lodha, S., 2018. PHISHY - a serious game to train enterprise users on phishing awareness. In: Proceedings of the 2018 Annual Symposium on Computer-Human Interaction in Play Companion Extended Abstracts, pp. 169–181. https://doi.org/10.1145/3270316.3273042.
Clark, C.Y., 2013. A study on corporate security awareness and compliance behavior intent. ProQuest Dissertations and Theses. Pace University.
CNN, 2021. Volkswagen hack: 3 Million Customers Have Had Their Information Stolen. CNN. https://edition.cnn.com/2021/06/11/cars/vw-audi-hack-customer-information/index.html.
Coenraad, M., Pellicone, A., Ketelhut, D.J., Cukier, M., Plane, J., Weintrop, D., 2020. Experiencing cybersecurity one game at a time: a systematic review of cybersecurity digital games. Simul Gaming 51 (5), 5. https://doi.org/10.1177/1046878120933312.
Cone, B.D., Irvine, C.E., Thompson, M.F., Nguyen, T.D., 2007. A video game for cyber security training and awareness. Comput. Secur. 26 (1), 1 https://doi.org/10.1016/j.cose.2006.10.005.
Conrad, M., 2021. Standardizing cybersecurity training in the healthcare industry using qualitative nominal group technique. ProQuest Dissertations and Theses. University of Phoenix.
Cook, A., Smith, R.G., Maglaras, L., Janicke, H., 2017. SCIPS: using experiential learning to raise cyber situational awareness in industrial control system. International J. Cyber Warfare Terror. 7 (2), 2 https://doi.org/10.4018/IJCWT.2017040101.
Cooper, M.H., 2008. Information security training: lessons learned along the trail. In: Proceedings of the 36th Annual ACM SIGUCCS Fall Conference: Moving Mountains, Blazing Trails, pp. 207–212. https://doi.org/10.1145/1449956.1450020.
Cooper, M.H., 2009. Information security training: what will you communicate?. In: Proceedings of the 37th Annual ACM SIGUCCS Fall Conference: Communication and Collaboration, pp. 217–222. https://doi.org/10.1145/1629501.1629541.
Craigen, D., Diakun-Thibault, N., Purse, R., 2014. Defining cybersecurity. Technol. Innov. Manag. Rev. 4, 13–21. https://doi.org/10.22215/timreview/835.
Curry, M., Marshall, B., Correia, J., Crossler, R.E., 2019. InfoSec Process Action Model (IPAM): targeting insiders' weak password behavior. J. Inf. Syst. 33 (3), 3 https://doi.org/10.2308/isys-52381.
DeCarlo, S.M., 2021. Measuring the application of knowledge gained from the gamification of cybersecurity training in healthcare. Dissertation Abstracts International: Section B: The Sciences and Engineering. ProQuest Information & Learning (Vol. 82, Issues 5-B).
Denning, T., Lerner, A., Shostack, A., Kohno, T., 2013. Control-alt-hack: the design and evaluation of a card game for computer security awareness and education. In: Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, pp. 915–928. https://doi.org/10.1145/2508859.2516753.
Dihoff, R.E., Brosvic, G.M., Epstein, M.L., Cook, M.J., 2004. Provision of feedback during preparation for academic testing: learning is enhanced by immediate but not delayed feedback. Psychol. Rec. 54 (2), 207–231. https://doi.org/10.1007/BF03395471.
Dixon, M., Arachchilage, N.A.G., Nicholson, J., 2019. Engaging users with educational games: the case of phishing. In: Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems, pp. 1–6. https://doi.org/10.1145/3290607.3313026.
Dominguez, C.M.F., 2010. Risk reduction by implementing security awareness programs in Puerto Rico metro area companies. ProQuest Dissertations and Theses. Universidad del Turabo (Puerto Rico).
Dugan, N., 2018. Security awareness training in a corporate setting. ProQuest Dissertations and Theses. Iowa State University.
Dumesnil, H., Verger, P., 2009. Public awareness campaigns about depression and suicide: a review. Psychiatr. Serv. 60 (9), 1203–1213.
Eccles, M., Grimshaw, J., Walker, A., Johnston, M., Pitts, N., 2005. Changing the behavior of healthcare professionals: the use of theory in promoting the uptake of research findings. J. Clin. Epidemiol. 58 (2), 107–112. https://doi.org/10.1016/j.jclinepi.2004.09.002.
Ertan, A., Crossland, G., Heath, C., Denny, D., Jensen, R.B., 2020. Cyber security behaviour in organisations. CoRR abs/2004.11768.
Fatima, R., Yasin, A., Liu, L., Wang, J., 2019. How persuasive is a phishing email? A phishing game for phishing awareness. J. Comput. Secur. 27 (6), 6 https://doi.org/10.3233/JCS-181253.
Filipczuk, D., Mason, C., Snow, S., 2019. Using a game to explore notions of responsibility for cyber security in organisations. In: Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems, pp. 1–6. https://doi.org/10.1145/3290607.3312846.
Fleming, A., 2017. Exploring information security awareness training to reduce unauthorized disclosure of information in public schools. ProQuest Dissertations and Theses. Northcentral University.
Fujs, D., Vrhovec, S., Vavpotic, D., 2020. Bibliometric mapping of research on user training for secure use of information systems. J. Univers. Comput. Sci. 26 (7), 7.
Ghazvini, A., Shukur, Z., 2016. Awareness training transfer and information security content development for healthcare industry. Int. J. Adv. Comput.r Sci. Appl. 7 (5), 5.
Ghazvini, A., Shukur, Z., 2017. Information security content development for awareness training programs in healthcare. Int. J. Secur. Appl. 11 (7), 7 https://doi.org/10.14257/ijsia.2017.11.7.07.
Ghazvini, A., Shukur, Z., 2018. A serious game for healthcare industry: information security awareness training program for hospital Universiti Kebangsaan Malaysia. Int. J. Adv. Comput.r Sci. Appl. 9 (9), 9.
González, J.M.R., 2019. Building Information Security Awareness and Training for Older Adults. ProQuest Dissertations and Theses. Utica College.
Goode, J., 2018. Comparing training methodologies on employee's cybersecurity countermeasures awareness and skills in traditional vs. socio-technical programs. ProQuest Dissertations and Theses. Nova Southeastern University.
Gordon, W.J., Wright, A., Glynn, R.J., Kadakia, J., Mazzone, C., Leinbach, E., Landman, A., 2019. Evaluation of a mandatory phishing training program for high-

risk employees at a US healthcare system. J. Am. Med. Inform. Assoc. 26 (6), 6 https://doi.org/10.1093/jamia/ocz005.
Gourlan, M., Bernard, P., Bortolon, C., Romain, A.J., Lareyre, O., Carayol, M., Ninot, G., Boiché, J., 2016. Efficacy of theory-based interventions to promote physical activity. A meta-analysis of randomised controlled trials. Health Psychol Rev 10 (1), 50–66. https://doi.org/10.1080/17437199.2014.981777.
gov.uk, 2022. Educational Institutions Findings Annex—Cyber Security Breaches Survey 2022. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/educational-institutions-findings-annex-cyber-security-breaches-survey-2022#chapter-2-key-findings.
Goyal, S., Ajmeri, N., Singh, M.P., 2019. Applying norms and sanctions to promote cybersecurity hygiene. In: *Proceedings of the 18th International Conference on Autonomous Agents and MultiAgent Systems*, 1991–1993.
Green, L.W., Glasgow, R.E., 2006. Evaluating the relevance, generalization, and applicability of research: issues in external validation and translation methodology. Eval. Health Prof. 29 (1), 126–153.
Gross, A., 2018. Effective security training requires change in employee behavior. Health IT Answ.
Gundu, T., Flowerday, S.V., 2013. Ignorance to awareness: towards an information security awareness process. SAIEE Afr. Res. J. 104 (2), 2 https://doi.org/10.23919/SAIEE.2013.8531867.
Hammond, S.T., 2019. Threat and coping appraisals on information security awareness training effectiveness: a quasi-experimental study. ProQuest Dissertations and Theses. Capella University.
Hamoud, A., Aimeur, E., 2020. Handling user-oriented cyber-attacks: STRIM, a user-based security training model. Front. Comput. Sci. 2 https://doi.org/10.3389/fcomp.2020.00025.
Harrison, B., 2018. Does anti-phishing training protect against organizational cyber attacks?: an empirical assessment of training methods and employee readiness. ProQuest Dissertations and Theses. State University of New York at Buffalo.
Harta, S., Margheri, A., Paci, F., Sassonea, V., 2020. Riskio: a Serious game for cyber security awareness and education. Comput. Secur. 95 https://doi.org/10.1016/j.cose.2020.101827.
Hatzivasilis, G., Ioannidis, S., Smyrlis, M., Spanoudakis, G., Frati, F., Goeke, L., Hildebrandt, T., Tsakirakis, G., Oikonomou, F., Leftheriotis, G., Koshutanski, H., 2020. Modern aspects of cyber-security training and continuous adaptation of programmes to trainees. Appl. Sci. 10 (16), 16 https://doi.org/10.3390/app10165702.
Häußinger, F., 2015. Studies on employees' information security awareness. PQDT - Global. Georg-August-Universitaet Goettingen, Germany.
He, W., Zhang, Z., 2019. Enterprise cybersecurity training and awareness programs: recommendations for success. J. Organ. Comput. Electron. Commerce 29 (4), 4. https://doi.org/10.1080/10919392.2019.1611528.
Heid, K., Heider, J., Qasempour, K., 2020. Raising security awareness on mobile systems through gamification. In: Proceedings of the European Interdisciplinary Cybersecurity Conference. https://doi.org/10.1145/3424954.3424958.
Hendrix, M., Al-Sherbaz, A., Bloom, V., 2016. Game based cyber security training: are serious games suitable for cyber security training? Int. J. Serious Games 3 (1), 1. https://doi.org/10.17083/ijsg.v3i1.107.
Hepp, S.L., Tarraf, R.C., Birney, A., Arain, M.A., 2018. Evaluation of the awareness and effectiveness of IT security programs in a large publicly funded health care system. Health Inf. Manag. J. 47 (3), 3 https://doi.org/10.1177/1833358317722038.
House, D., 2013. An assessment of user response to phishing attacks: the effects of fear and self-confidence. ProQuest Dissertations and Theses. The University of Texas at Arlington.
Ikhalia, E., Serrano, A., Bell, D., Louvieris, P., 2019. Online social network security awareness: mass interpersonal persuasion using a Facebook app. Inf. Technol. People 32 (5), 5. https://doi.org/10.1108/ITP-06-2018-0278.
Jansen, P., Fischbach, F., 2020. The social engineer: an immersive virtual reality educational game to raise social engineering awareness. In: Extended Abstracts of the 2020 Annual Symposium on Computer-Human Interaction in Play, pp. 59–63. https://doi.org/10.1145/3383668.3419917.
Jansson, K., von Solms, R., 2013. Phishing for phishing awareness. Behav. Inf. Technol. 32 (6), 6 https://doi.org/10.1080/0144929X.2011.632650.
Jeffers, T.M., 2016. Maximizing adult learning methodologies in corporate cyber security training programs. ProQuest Dissertations and Theses. Utica College.
Jenkins, J.L., Durcikova, A., Burns, M.B., 2013. Simplicity is bliss: controlling extraneous cognitive load in online security training to promote secure behavior. J. Organ. End User Comput. 25 (3), 3 https://doi.org/10.4018/joeuc.2013070104.
Katsantonis, M.N., Fouliras, P., Mavridis, I., 2017. Conceptualization of game based approaches for learning and training on cyber security. In: Proceedings of the 21st Pan-Hellenic Conference on Informatics. https://doi.org/10.1145/3139367.3139415.
Kennedy, S.E., 2016. The pathway to security—Mitigating user negligence. Inf. Comput. Secur. 24 (3, SI), 3 https://doi.org/10.1108/ICS-10-2014-0065.
Khan, B., Alghathbar, K.S., Nabi, S.I., Khan, M.K., 2011. Effectiveness of information security awareness methods based on psychological theories. Afr. J. Bus. Manag. 5 (26), 26 https://doi.org/10.5897/AJBM11.067.
Khando, K., Gao, S., Islam, S.M., Salman, A., 2021. Enhancing employees information security awareness in private and public organisations: a systematic literature review. Comput. Secur. 106 https://doi.org/10.1016/j.cose.2021.102267.
Kießling, S., Hanka, T., Merli, D., 2021. Salt&Pepper: spice up security behavior with cognitive triggers. In: European Interdisciplinary Cybersecurity Conference, pp. 26–31. https://doi.org/10.1145/3487405.3487656.
Kim, B., Lee, D.-Y., Kim, B., 2020. Deterrent effects of punishment and training on insider security threats: a field experiment on phishing attacks. Behav. Inf. Technol. 39 (11), 11 https://doi.org/10.1080/0144929X.2019.1653992.
Kim, B.-H., Kim, K.-C., Hong, S.-E., Oh, S.-Y., 2017. Development of cyber information security education and training system. Multimed. Tools Appl. 76 (4), 4 https://doi.org/10.1007/s11042-016-3495-y.
Kim, P., 2010. Measuring the effectiveness of information security training: a comparative analysis of computer -based training and instructor -based training. ProQuest Dissertations and Theses. Robert Morris University.
Kim, S.R., Yang, J.H., Kim, S.B., 2016. A cybercrime prevention program based on simulation and quiz game: applying item response theory for effective information security learning. Int. J. Secur. Appl. 10 (5), 5 https://doi.org/10.14257/ijsia.2016.10.5.16.
Kirlappos, I., Parkin, S., Sasse, M.A., 2014. Learning from 'Shadow Security': why understanding non-compliance provides the basis for effective security. Workshop On Usable Security. Workshop on Usable Security. https://doi.org/10.14722/usec.2014.23007.
Kletenik, D., Butbul, A., Chan, D., Kwok, D., LaSpina, M., 2020. Cyber secured: a serious game for cybersecurity novices. In: Proceedings of the 51st ACM Technical Symposium on Computer Science Education, p. 1307. https://doi.org/10.1145/3328778.3372611.
Kletenik, D., Butbul, A., Chan, D., Kwok, D., LaSpina, M., 2021. Game on: teaching cybersecurity to novices through the use of a serious game. J. Comput. Sci. Coll. 36 (8), 8.
Knopik, C., 2021. A comparative analysis of video-based training and game-based training on information security. Dissertation Abstracts International: Section B: The Sciences and Engineering. ProQuest Information & Learning. Vol. 82, Issues 2-B.
Korpela, K., 2015. Improving cyber security awareness and training programs with data analytics. Inf. Secur. J. 24 (1–3), 1–3 https://doi.org/10.1080/19393555.2015.1051676.
Kostadinov, D., 2018. The components of a successful security awareness program. InforSec Inst.
Lally, P., Gardner, B., 2013. Promoting habit formation. Health Psychol. Rev. 7 (sup1), S137–S158. https://doi.org/10.1080/17437199.2011.603640.
Lamour, J., 2008. Impact of user awareness and training of infosec practitioners on data security. Dissertation Abstracts International Section A: Humanities and Social Sciences. ProQuest Information & Learning. Vol. 68, Issues 12-A.
Leavy, J.E., Bull, F.C., Rosenberg, M., Bauman, A., 2011. Physical activity mass media campaigns and their evaluation: a systematic review of the literature 2003–2010. Health Educ. Res. 26 (6), 1060–1085. https://doi.org/10.1093/her/cyr069.
Legárd, I., 2021. Effective methods for successful information security awareness. Pro Publico Bono - Magyar Kozigazgatas 1, 1. https://doi.org/10.32575/ppb.2021.1.7.
Li, K.C., Wong, B.T.-M., 2019. How learning has been personalised: a review of literature from 2009 to 2018. In: Cheung, S.K.S., Lee, L.-K., Simonova, I., Kozel, T., Kwok, L.-F. (Eds.), Blended Learning: Educational Innovation For Personalized Learning. Springer International Publishing, pp. 72–81.
Lim, I.K., Park, Y.G., Lee, J.K., 2016. Design of security training system for individual users. Wirel. Pers. Commun. 90 (3), 3 https://doi.org/10.1007/s11277-016-3380-z.
Lim, W.T., Yang, M.B., Kim, S.B., 2013. A novel card-based information security game development on SNS. Int. J. Secur. Appl. 7 (6), 6 https://doi.org/10.14257/ijsia.2013.7.6.13.
Loffler, E., Schneider, B., Asprion, P.M., Zanwar, T., 2021. CySecEscape 2.0-a virtual escape room to raise cybersecurity awareness. Int. J. Serious Games 8 (1), 1. https://doi.org/10.17083/ijsg.v8i1.413.
Martin, J., 2019. Phishing in dark waters: a Quasi-experimental approach with evaluating cyber-security training for end-users. ProQuest Dissertations and Theses. University of South Florida.
Mashiane, T., Dlamini, Z., Mahlangu, T., 2019. A rollout strategy for cybersecurity awareness campaigns. In: Proceedings of the 14th International Conference on Cyber Warfare and Security (ICCWS 2019), Stellenbosch, South Africa, pp. 243–250.
Mayhorn, C.B., Nyeste, P.G., 2011. Training users to counteract phishing. ProQuest Dissertations and Theses. North Carolina State University.
McCarthy, K., 2021. Cybersecurity awareness training methods and user behavior. ProQuest Dissertations and Theses. Utica College.
McCoy, C., Fowler, R.T., 2004. 'You Are the Key to Security': establishing a successful security awareness program. In: Proceedings of the 32nd Annual ACM SIGUCCS Conference on User Services, pp. 346–349. https://doi.org/10.1145/1027802.1027882.
McCrohan, K., Engel, K., Harvey, J., 2010. Influence of awareness and training on cyber security. J. Internet Commerce 9 (1), 1. https://doi.org/10.1080/15332861.2010.487415.
Moher, D., Shamseer, L., Clarke, M., Ghersi, D., Liberati, A., Petticrew, M., Shekelle, P., Stewart, L.A., PRISMA-P Group, 2015. Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015 statement. Syst. Rev. 4 (1), 1. https://doi.org/10.1186/2046-4053-4-1.
Muhirwe, J., 2016. Towards a 3-D approach to cybersecurity awareness for college students. In: Proceedings of the 17th Annual Conference on Information Technology Education, 105. https://doi.org/10.1145/2978192.2978203.
Nicolas-Rocca, T.S., 2010. Identification and access management: an action research approach to develop a training strategy for higher education. ProQuest Dissertations and Theses. The Claremont Graduate University.
Oslejsek, R., Rusnak, V., Burska, K., Svabensky, V., Vykopal, J., Cegan, J., 2021. Conceptual model of visual analytics for hands-on cybersecurity training. IEEE Trans. Vis. Comput. Graph 27 (8), 8. https://doi.org/10.1109/TVCG.2020.2977336.
Page, M.J., McKenzie, J.E., Bossuyt, P.M., Boutron, I., Hoffmann, T.C., Mulrow, C.D., Shamseer, L., Tetzlaff, J.M., Akl, E.A., Brennan, S.E., Chou, R., Glanville, J.,

Grimshaw, J.M., Hróbjartsson, A., Lalu, M.M., Li, T., Loder, E.W., Mayo-Wilson, E., McDonald, S., Moher, D., 2021. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. Int. J. Surg. 88, 105906 https://doi.org/10.1016/j.ijsu.2021.105906.
Poepjes, R., Lane, M., 2012. An Information Security Awareness Capability Model (ISACM).
Pogrebna, G., Skilton, M., 2019. Cybersecurity threats: past and Present. In: Pogrebna, G., Skilton, M. (Eds.), Navigating New Cyber Risks: How Businesses Can Plan, Build and Manage Safe Spaces in the Digital Age. Springer International Publishing, pp. 13–29. https://doi.org/10.1007/978-3-030-13527-0_2.
Prain, V., Cox, P., Deed, C., Dorman, J., Edwards, D., Farrelly, C., Keeffe, M., Lovejoy, V., Mow, L., Sellings, P., Waldrip, B., Yager, Z., 2013. Personalised learning: lessons to be learnt. Br. Educ. Res. J. 39 (4), 654–676. https://doi.org/10.1080/01411926.2012.669747.
Puhakainen, P.P., 2006. A design theory for information security awareness. ProQuest Dissertations and Theses. Oulun Yliopisto, Finland.
Puhakainen, P.P., Siponen, M., 2010. Improving employees' compliance through information systems security training: an action research study. MIS Quart. 34 (4), 4.
Reuters, 2021. One Password Allowed Hackers to Disrupt Colonial Pipeline, CEO Tells Senators. https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/.
Robbins, M.S., 2020. Exploring the impact of information security awareness training on knowledge, attitude, and behavior: a K-12 study. ProQuest Dissertations and Theses. Northcentral University.
Rotvold, G.M., 2007. Status of security awareness in business organizations and colleges of business: an analysis of training and education, policies, and social engineering testing. ProQuest Dissertations and Theses. The University of North Dakota.
Sabillon, R., Serra-Ruiz, J., Cavaller, V., Cano, J.J.M., 2019. An effective cybersecurity training model to support an organizational awareness program: the Cybersecurity Awareness TRAining Model (CATRAM). A case study in Canada. J. Cases Inf. Technol. 21 (3), 3 https://doi.org/10.4018/JCIT.2019070102.
Salahdine, F., Kaabouch, N., 2019. Social engineering attacks: a survey. Fut. Internet 11 (4). https://doi.org/10.3390/fi11040089.
Salameh, R., 2020. The relationship between engagement levels and players' intended behaviors in game-based training for cybersecurity. Dissertation Abstracts International Section A: Humanities and Social Sciences. ProQuest Information & Learning. Vol. 81, Issues 9-A.
Sardar, T., Wahsheh, L.A., 2020. Design of a cyber security awareness campaign to be implemented in a quarantine laboratory. J. Comput. Sci. Coll. 35 (9), 9.
Shargawi, A., 2017. Understanding the human behavioural factors behind online learners' susceptibility to phishing attacks. PQDT - UK & Ireland. Lancaster University, United Kingdom.
Shaw, C., 2020. Why phishing works and the detection needed to prevent it. ProQuest Dissertations and Theses. Utica College.
Shaw, R.S., Chen, C.C., Harris, A.L., Huang, H.-J., 2009. The impact of information richness on information security awareness training effectiveness. Comput. Educ. 52 (1), 1 https://doi.org/10.1016/j.compedu.2008.06.011.
Shaw, R.S., Keh, H.C., Huang, N.C., Huang, T.C., 2011. Information security awareness on-line materials design with knowledge maps. Int. J. Distance Educ. Technol. 9 (4), 4 https://doi.org/10.4018/jdet.2011100104.
Siponen, M., Puhakainen, P., Vance, A., 2020. Can individuals' neutralization techniques be overcome? A field experiment on password policy. Comput. Secur. 88 https://doi.org/10.1016/j.cose.2019.101617.
Stefaniuk, T., 2020. Training in shaping employee information security awareness. Entrepr. Sustain. Issues 7 (3), 3. https://doi.org/10.9770/jesi.2020.7.3(26.
Steinmetz, H., Knappstein, M., Ajzen, I., Schmidt, P., Kabst, R., 2016. How effective are behavior change interventions based on the theory of planned behavior? Z. Psychol. 224 (3), 216–233. https://doi.org/10.1027/2151-2604/a000255.
Sumner, A., Yuan, X., 2019. Mitigating phishing attacks: an overview. In: Proceedings of the 2019 ACM Southeast Conference, pp. 72–77. https://doi.org/10.1145/3299815.3314437.
Švábenský, V., Vykopal, J., 2018. Challenges arising from prerequisite testing in cybersecurity games. In: Proceedings of the 49th ACM Technical Symposium on Computer Science Education, pp. 56–61. https://doi.org/10.1145/3159450.3159454.
Sykosch, A., Doll, C., Wübbeling, M., Meier, M., 2020. Generalizing the phishing principle: analyzing user behavior in response to controlled stimuli for IT security awareness assessment. In: Proceedings of the 15th International Conference on Availability, Reliability and Security. https://doi.org/10.1145/3407023.3409205.
Talib, S., 2014. Personalising information security education. PQDT - UK & Ireland. University of Plymouth, (United Kingdom).
Tan, Z., Beuran, R., Hasegawa, S., Jiang, W., Zhao, M., Tan, Y., 2020. Adaptive security awareness training using linked open data datasets. Educ. Inf. Technol. 25 (6), 6 https://doi.org/10.1007/s10639-020-10155-x.
Thaler, R.H., Sunstein, C.R., 2008. Nudge: Improving Decisions About Health, Wealth, and Happiness. Yale University Press.
Thornton, D., Turley, F., 2020. Analysis of player behavior and EEG readings in a cybersecurity game. In: Proceedings of the 2020 ACM Southeast Conference, pp. 149–153. https://doi.org/10.1145/3374135.3385276.
Tschakert, K.F., Ngamsuriyaroj, S., 2019. Effectiveness of and user preferences for security awareness training methodologies. Heliyon 5 (6), 6. https://doi.org/10.1016/j.heliyon.2019.e02010.
Ulsch, M., 2014. Cyber Threat!: How to Manage the Growing Risk of Cyber Attacks. Wiley Online Library.
van Steen, T, 2022. When choice is (not) an option: nudging and techno-regulation approaches to behavioural cybersecurity. In: Schmorrow, D.D., Fidopiastis, C.M. (Eds.), Augmented Cognition. Springer International Publishing, pp. 120–130.
van Steen, T., Deeleman, J.R.A., 2021. Successful gamification of cybersecurity training. Cyberpsychology, Behavior, and Social Networking. https://doi.org/10.1089/cyber.2020.0526.
van Steen, T., Norris, E., Atha, K., Joinson, A., 2020. What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use? J. Cybersecur. 6 (1) https://doi.org/10.1093/cybsec/tyaa019.
van Steenburg, M., 2017. Applications of serious gaming to cybersecurity training and awareness. ProQuest Dissertations and Theses. Utica College.
Veneruso, S.V., Ferro, L.S., Marrella, A., Mecella, M., Catarci, T., 2020. CyberVR: an interactive learning experience in virtual reality for cybersecurity related issues. In: Proceedings of the International Conference on Advanced Visual Interfaces. https://doi.org/10.1145/3399715.3399860.
Waly, N.S., 2013. Organisational information security management: the impact of training and awareness: evaluating the socio-technical impact on organisational information security policy management. PQDT - UK & Ireland. University of Bradford, (United Kingdom).
Weanquoi, P., Johnson, J., Zhang, J., 2017. Using a game to teach about phishing. In: Proceedings of the 18th Annual Conference on Information Technology Education, 75. https://doi.org/10.1145/3125659.3125669.
Wen, Z.A., Li, Y., Wade, R., Huang, J., Wang, A., 2017. What.Hack: learn phishing email defence the fun way. In: Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems, pp. 234–237. https://doi.org/10.1145/3027063.3048412.
Wu, T., Tien, K.-Y., Hsu, W.-C., Fu-Hsiang, W., 2021. Assessing the effects of gamification on enhancing information security awareness knowledge. Appl. Sci. 11 (19), 19 https://doi.org/10.3390/app11199266.
Yasin, A., Liu, L., Li, T., Fatima, R., Jianmin, W., 2019. Improving software security awareness using a serious game. IET Softw. 13 (2, SI), 2 https://doi.org/10.1049/iet-sen.2018.5095.
Yasin, A., Liu, L., Li, T., Wang, J., Zowghi, D., 2018. Design and preliminary evaluation of a cyber Security Requirements Education Game (SREG). Inf. Softw. Technol. 95, 179–200. https://doi.org/10.1016/j.infsof.2017.12.002.
Younes, W., 2014. Cybersecurity education (training and awareness) for K-12 faculty and staff in allegheny county. Dissertation Abstracts International Section A: Humanities and Social Sciences. ProQuest Information & Learning. Vol. 75, Issues 4-A(E).
Younis, Y.A., Musbah, M., 2020. A framework to protect against phishing attacks. In: Proceedings of the 6th International Conference on Engineering & MIS 2020. https://doi.org/10.1145/3410352.3410825.
Zheng, L., Long, M., Zhong, L., Gyasi, J.F., 2022. The effectiveness of technology-facilitated personalized learning on learning achievements and learning perceptions: a meta-analysis. Educ. Inf. Technol. 27 (8), 11807–11830. https://doi.org/10.1007/s10639-022-11092-7.

**Julia Prümmer, MSc** is a PhD Candidate in Cybersecurity Governance at the Institute of Security and Global Affairs and a member of the Cybersecurity Governance research group. Her research focus includes behavioural change approaches to cybersecurity, cybersecurity behaviour of end-users and cyberpsychology. The title of her dissertation is: Designing and testing an evidence-based cybersecurity training for employees.

**Tommy van Steen, PhD**: is Assistant Professor in Cybersecurity Governance at the Institute of Security and Global Affairs and a member of the Cybersecurity Governance research group. His research interests include: cybersecurity behaviour of end-users, behavioural change, cyberpsychology, and organisational cybersecurity behaviour.

**Prof.dr. Bibi van den Berg, PhD**: is full professor of Cybersecurity Governance at Leiden University, and the head of the Cybersecurity Governance research group at the Institute of Security and Global Affairs of this university. Her research and teaching focus on several themes: (1) cybersecurity governance, (2) governance of security and safety and (3) regulating human behaviour through the use of technologies (techno-regulation and nudging).