Computers & Security 137 (2024) 103630

Contents lists available at ScienceDirect

Computers & Security

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

Design principles for cognitively accessible cybersecurity training

Joakim Kävrestad [a,*], Jana Rambusch [b], Marcus Nohlberg [b]

[a] Jönköping School of Engineering, Gjuterigatan 5, 551 11, Jönköping, Sweden
[b] University of Skövde, Högskolevägen, Box 408, 541 28 Skövde, Sweden

ARTICLE INFO

Keywords:
Cybersecurity training
Cognitive accessibility
Accessible security
Usable security
Cybersecurity training design

ABSTRACT

Exploiting human behavior to gain unauthorized access to computer systems has become common practice for modern cybercriminals. Users are expected to adopt secure behavior to avoid those attackers. This secure behavior requires cognitive processing and is often seen as a nuisance which could explain why attacks exploiting user behavior continues to be a fruitful approach for attackers. While adopting secure behavior can be difficult for any user, it can be even more difficult for users with cognitive disabilities. This research focuses on users with cognitive disabilities with the intent of developing design principles for the development of cognitively accessible cybersecurity training. The target group is estimated to include almost 10 % of all users but is previously understudied. The results show that the target group experience cybersecurity as cognitively demanding, sometimes to a degree that becomes incapacitating. Participating in cybersecurity training requires cognitive energy which is a finite resource. Cognitively accessible cybersecurity training requires a minimalist design approach and inclusion of accessibility functions. A minimalist design approach, in this case, means that both informative and design elements should be kept to a minimum. The rationale is that all such elements require cognitive processing which should be kept to a minimum.

1. Introduction

Establishing and maintaining a sufficient level of cybersecurity is paramount in modern-day computer systems. A crucial part of cybersecurity is defending the computer system from adversaries that come in many different forms, from nation-states to hacktivists and disgruntled employees (Sfakianakis et al., 2019; Stankovska, 2016). Those adversaries have a wide array of different options for how to carry out attacks. Those options, often referred to as attack vectors can be roughly categorized as technological, process-oriented, or human-oriented (Juliadotter and Choo, 2015). This paper is concerned with the human-oriented attack vector which is often considered to be the most frequently used (Joinson and van Steen, 2018; Soare, 2020; Zimmermann and Renaud, 2019). Adversaries exploit human nature to gain unauthorized access to data or otherwise perform ill deeds on a regular basis (Mashiane and Kritzinger, 2018).

Exploiting the human-oriented attack vector typically includes exploiting user behavior to the benefit of the attacker. This is made possible since users typically struggle to adopt secure behavior. Secure behavior includes, but is not limited to, adopting secure password practices, following security policies, and correctly distinguishing phishing e-mails (Hadlington, 2017). Previous research has suggested that users need to be supported to enable secure behavior and the common support mechanism suggested is training (Joinson and van Steen, 2018). As described by Aldawood and Skinner (2018) and Al-Daeef et al. (2017), there are several different training methods available. However, recent research argues that many training approaches fail to adequately support users toward secure behavior. The key reasons reported are that users are not actively participating in training delivered on demand and acquired knowledge is only retained for a limited time (Bada et al., 2019; Gjertsen et al., 2017; Reinheimer et al., 2020). Kävrestad et al. (2022) show that even if users do adopt a correct behavior, that does not always translate to a secure outcome. A method for cybersecurity training that is argued to overcome those problems is Context-Based Micro-Training (CBMT), which is adopted as the cybersecurity training methodology in this research (Kävrestad, 2022).

Researchers have started to investigate the cognitive effort needed to carry out cybersecurity tasks. Cognitive effort can be described as the effort spent on tasks that require cognitive processing, for instance, problem sampling, memory, and rational reasoning (Westbrook and Braver, 2015). As described by Lamond et al. (2022), many of the

[*] Corresponding author.
E-mail address: joakim.kavrestad@ju.se (J. Kävrestad).

https://doi.org/10.1016/j.cose.2023.103630
Received 21 August 2023; Received in revised form 16 November 2023; Accepted 28 November 2023
Available online 29 November 2023

activities users are supposed to engage in the name of cybersecurity do require cognitive effort. This includes creating and memorizing passwords, learning new security tools, and evaluating the legitimacy of e-mails (Gutzwiller et al., 2020; Reeves et al., 2021). Just by participating in cybersecurity training it is expected that users to learn and memorize, often while actively engaging in training sessions (Hu et al., 2022). Consequently, we argue cognitive effort to be an important factor in the development and evaluation of cybersecurity training.

Related to cognitive effort is cognitive accessibility which can be described as actions towards making something accessible for users with cognitive and learning disabilities (Mozilla, 2022). In addition to users with disabilities, other user groups such as seniors may face cognitive challenges while using digital technology (Burmeister, 2010). Cybersecurity training is not excluded from these technologies. Rather, Horcher and Tejay (2009) show that cognition plays a central role in a user's ability to comprehend cybersecurity training. As far as we know, no previous research has investigated cybersecurity training from the perspective of users with cognitive disabilities and/or impairments (from here on denoted "users with cognitive disabilities") . To that end, this paper reports on research into cybersecurity training through the lens of cognitive accessibility with the aim of *developing cybersecurity training for users with cognitive disabilities.* The following research questions were developed for the research.

RQ1: How can cognitive disabilities impact users' ability to adopt secure behavior?

RQ2: How can CBMT be used to implement cybersecurity training for users with cognitive disabilities?

RQ3: How can cybersecurity training for users with cognitive disabilities be developed?

RQ1 intends to review how cognitive disabilities impact on users' ability to adopt secure behavior. The rationale is to use existing knowledge to develop a cybersecurity training tool which can be evaluated with users who have cognitive disabilities. The training method adopted in this research is CBMT and RQ2 seeks to explore how the CBMT method can work for the target group. RQ3 seeks to develop and evaluate a training tool with the intention of generating knowledge about how such training should be designed with users with cognitive disabilities in mind. This knowledge is expressed as design principles which constitute the main contribution of this research. Further contributions include how cognitive disabilities can pose cybersecurity problems.

The remainder of this paper is structured as follows. The upcoming background will describe background concepts. The chosen methodology, design science, and how it has been implemented in this research is presented in Section 3. The results section will then elaborate on the research steps and outline results before the paper is concluded by highlighting contributions and outlining directions for future work.

2. Background

This section elaborates on core topics of relevance for the paper.

2.1. Cognitive abilities and disabilities

Cognitive abilities refer to an individual's perception, problem-solving ability and ability to plan and reason (Karwowski and Kaufman, 2017). Memory and ability to concentrate are also included in cognitive abilities (Oberauer et al., 2000). An individual's cognitive abilities are dynamic and impacted by numerous factors and conditions, and some of them can be both temporary and permanent (Palmer, 2013; Verhagen et al., 2019). Factors that can have a temporary impact include stress, fatigue, mood, anxiety and more (Verhagen et al., 2019). Conditions that have a more permanent impact include autism and attention deficit hyperactivity disorder (ADHD) (Happé et al., 2016; Young, 2005). While some people are diagnosed with a single cognitive disability, comorbidity is common. For instance, research shows that ADHD and autism are common comorbidities to each other (Antshel et al., 2013). It is estimated that over 9 % of all Americans have a cognitive disability while it can be expected that around 20 % of seniors have a cognitive impairment (FCC, 2016; Pais et al., 2020).

The research in this paper focuses on making cybersecurity training available for users with cognitive disabilities. Given the dynamic nature of cognitive abilities, pretty much anyone could be included in this user group given the right conditions (Olney and Kim, 2001; World Health Organization, 2022). Cognitive disabilities are highly individual with the common denominator of impacting the persons cognitive abilities in one or more way. Furthermore, the extent of impact is also individual (Lundin et al., 2012). A person with a cognitive disability will, according to Lundin et al. (2012), experience difficulties with at least one of the following; memory, problem-solving, attention, linguistic comprehension, math comprehension, or visual comprehension.

2.2. Secure behavior

Cybersecurity is a socio-technical property where the goal is to maintain confidentiality, integrity and availability of information and systems (International Organization for Standardization, 2012, 2020). This include a wide array of considerations where some are technical, some are organizational and some relate to the users themselves (Juliadotter and Choo, 2015). In fact, recent literature describes that attacks utilizing user behavior is one of, if not the, most commonly used way to execute a cyberattack (Anwar et al., 2017; Kritzinger et al., 2018; Zimmermann and Renaud, 2019). To ensure cybersecurity, users are expected to engage in secure behavior. What secure behavior entails is not entirely clear even if different sources offer advice to users. Based on a summary of advice from different research and practitioner sources the following is included in *secure behavior* (Al-Omari et al., 2012; Hadlington, 2017; Internetstiftelsen, 2016; MSB, 2021, 2022; Säkerhetskollen, 2023):

- Be attentive to details in incoming messages to avoid phishing, vishing, smishing etc.
- Maintain backups of important data to enable data recovery.
- Only use digital ID at your own initiative to avoid digital ID frauds.
- Use strong passwords and keep them to yourself to ensure they are not used by others.
- Use password manager and multi-factor authentication.
- Never log into accounts upon request from someone else.
- Keep software, anti-malware tools, and your router up to date to avoid susceptibility to zero-day vulnerabilities.
- Only install software from trusted sources to avoid malware.
- Control the identity of people you trade with online, to avoid fraudsters in online trade.
- Be critical of information to avoid disinformation.

For the purpose of this paper, *secure behavior* is defined as adopting practices outlined in regulations, policies and recommendations such as the list above.

2.3. Cognitive disabilities and cybersecurity

Although research that directly connects cybersecurity and cognitive disabilities is scarce, recent research in related areas suggests that cognitive disabilities may have negative cybersecurity implications. Security fatigue is one concept that has received attention from research (Reeves et al., 2021). In essence, Reeves et al. (2021) describe that high demands and exposure to those demands leads to user disengagement form cybersecurity tasks. Furthermore, Nobles (2022) describe that stress and burnout cause a lowered cognitive ability which results in lowered cybersecurity.

Previous research has tested how different cognitive abilities impact on certain aspects of cybersecurity aspects. Harrison et al. (2016) show a connection between attention and phishing susceptibility where users with higher attention are better at detection phishing. Katsini et al. (2018) show that cognitive ability impacts on how strong passwords user create. Reeves et al. (2021) describe that engaging in secure behavior is cognitively demanding. While those publications focus on neurotypical users, they showcase that cognitive effort is required to engage in secure behavior.

A reasonable, consequent, assumption is that a lowered cognitive ability inhibits a user's ability to comply with a cognitively demanding security task or requirement. With that follows that it will be easier for a user to comply with a suggested behavior that is less demanding. This has been tested, and found to be true, in the realm of passwords. In essence, previous research have shown that users are more prone to adopt guidelines perceived as easy to comply with (Al-Slais and El-Medany, 2022; Guo et al., 2019).

2.4. Cybersecurity training

The most common suggestion for how to support users towards secure behavior is through the use of training (Joinson and van Steen, 2018). Training intends to enable secure behavior by educating users on what that entails (Anwar et al., 2017; Safa et al., 2015). However, research shows that training interventions often fail to reach their intended target for several reasons, primarily:

- While users are informed about how to act, that does not always translate to secure behavior (Bada et al., 2019).
- Knowledge acquired during a training intervention is only retained for a limited amount of time (Reinheimer et al., 2020).
- Users are not actively participating in on-demand training (Gjertsen et al., 2017).
- Some research argues that many training practices are not based in theory, nor is their effect empirically evaluated (Abraham and Chengalur-Smith, 2019; Siponen and Baskerville, 2018).

Cybersecurity training has received quite a bit of attention from researchers in recent years. Hu et al., 2022 report on a literature review of 80 studies and conclude that cybersecurity training is fundamental to mitigate security risks. Chowdhury and Gkioulos (2021) reviewed 67 studies and conclude that there is no generally agreed upon delivery method for cybersecurity training, and that combining such training with practical activities seems advantageous. Even if there is no generally accepted set of guidelines for cybersecurity training, several publications contribute to the topic. The following guidelines frequently appear in recent literature (Alyami et al., 2023; Beuran et al., 2016; Haney and Lutters, 2018; Reeves et al., 2021):

- Training should be tailored to specific user groups.
- Training should account for differences in cultural background.
- The content should reflect the skills the training aims to develop.
- The content should be as easy as possible to use.
- The content should be aligned with technical constraints.
- Training should be consistent, relevant, and non-intrusive.
- Practical elements should be integrated with the training.

2.5. Context-Based micro-training

A recent method for cybersecurity training that seeks to meet the challenges presented above is Context-Based Micro-Training (CBMT) (Kävrestad and Nohlberg, 2020). CBMT suggests that cybersecurity training should be presented to users when they are in a situation where that training is of direct relevance. For instance, users should be trained in phishing detection when they are reading their e-mail. By presenting training in this way, Kävrestad and Nohlberg (2020) argues that the training includes an awareness increasing mechanism which is beneficial for secure behavior. Furthermore, the user will be reminded about the expected behavior every time they experience a risky situation. CBMT has shown to have good results for teaching users about phishing detection and password practices (Kävrestad, 2022). Kävrestad (2022) further show that CBMT has been compared to other training methods in terms of user appreciation with good results. However, Kävrestad (2022), emphasize that for users to accept cybersecurity training it must:

- Be presented in an easy to digest format.
- Focus on the most crucial information needed for the user.
- Be possible to opt out from training.
- Be short.

Practically, CBMT needs a way to detect when a user enters a situation where cybersecurity training is relevant and present training at that point. As shown in Fig. 1, the training should first provide the user with very brief information to make the user aware of a risky situation. It should then also provide the user with an option for more training.

CBMT has been selected as the cybersecurity training method for use in this research. We argue that the core ideas of CBMT align well with difficulties faced by persons with cognitive disabilities. When training is delivered repetitively in situations where it is of direct relevance, it should support users who have attention and memory problems. The user will be informed about concepts which are relevant to what the user is currently doing, which limits the need to switch between tasks. Furthermore, since the training is repetitive the user does not need to remember all provided information but can rely on the training method to provide the information as often as needed. By making the training short and focused, the user only needs to consume small chunks of information which limits the need for cognitive processing.

3. Methodology

Design science as described by Hevner et al. (2004) was adopted as the methodology for this research. Design science is suitable for research that seeks to develop theory through the study of artefacts (March and Smith, 1995). It emphasizes usefulness in practical application domains and research in those application domains. Hevner et al. (2004) argues that design science is appropriate for problems that may have several solutions and a goal is to develop and evaluate the artefact with the intent of finding one of those. This research considers Hevner et al. (2004) to describe the overall goals of design science with emphasis of cyclical design grounded in existing theories and tightly integrated with continuous evaluation. Peffers et al. (2007) provides a concrete research framework for design science which was used in the development of the research process. They suggest that design science should include the six phases of: identification and motivation of problem, definition of objectives for a solution, artefact development, artefact demonstration, artefact evaluation, and communication. The development, demonstration and evaluation phases are often explored iteratively (Peffers et al., 2007). Fig. 2 provides a graphical representation of the research process which is based on Peffers et al. (2007).

This research includes three distinct steps: explication of theoretical framework and two iterations of artefact development, demonstration and evaluation – design cycles. Each step corresponds to one research question. This research took a qualitative approach to data collection, using interviews. Gathered data was analyzed using thematic coding (Braun and Clarke, 2006). Table 1 provides an overview of the core activities and outputs related to the research questions.

A purposive sampling approach was used with the intention of including domain experts and users with cognitive disabilities (Etikan et al., 2016). Four domain experts were included in the initial research stage to provide a starting point for artifact development. The participants in the group interviews in design cycles 1 and 2 were users with congenital or acquired cognitive disabilities and are able to autonomously use computers. They are experienced in cognitive evaluations of digital systems as members of the organization Begripsam. Begripsam

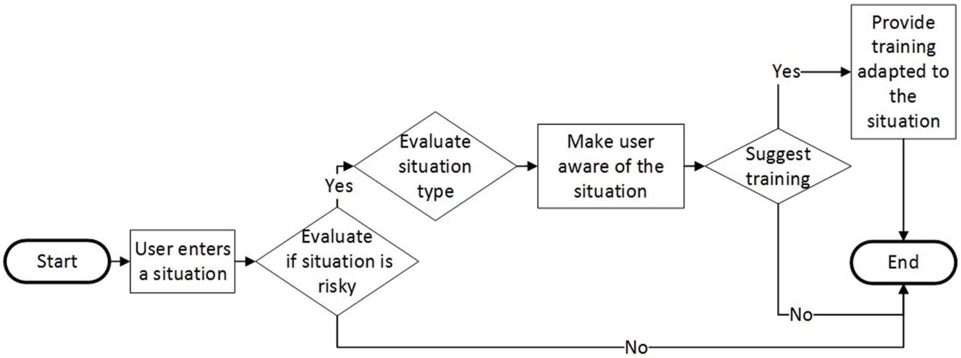

Start
User enters a situation
Evaluate if situation is risky
Yes
No
Evaluate situation type
Make user aware of the situation
Suggest training
Yes
No
Provide training adapted to the situation
End

Fig. 1. CBMT process.

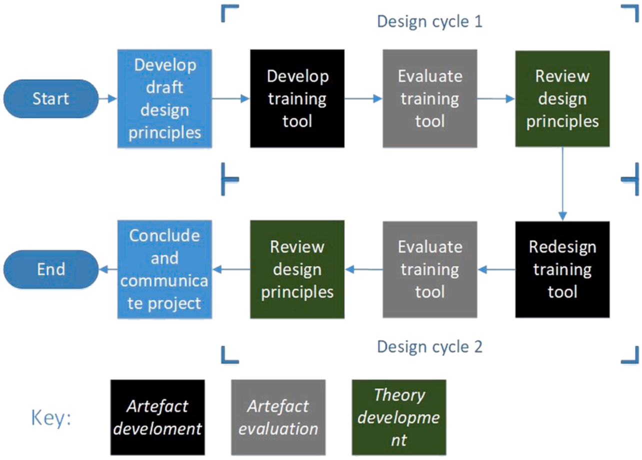


Fig. 2. Research process overview.

Table 1
Research activities related to research questions.

Activity	RQ	Data source	Outputs
Theoretical framework	How can cognitive disabilities impact users' ability to adopt secure behavior?	Related literature and interviews with four domain experts.	First draft of design principles.
Design cycle 1	How can CBMT be used to implement cybersecurity training for users with cognitive disabilities?	Design principles used to development. Group interviews with ten participants for evaluation.	Draft artefact and reviewed design principles
Design cycle 2	How can cybersecurity training for users with cognitive disabilities be developed?	Data from previous group interviews used for development. Group interviews with eleven participants used for evaluation.	Finalized artefact and reviewed design principles.

supported the research by organizing the evaluations. We acknowledge that including participants who are experienced evaluators is likely to impact the results. The decision to focus on this specific population is motivated twofold. First, as experienced evaluators and members of the target group, the participants can be expected to provide deep and valuable responses. Second, sampling through an organization which specializes in evaluations ensures recruitment of participants who are actively seeking to engage in evaluations. They are therefore voluntary participants, which is positive from a research ethical standpoint. The reasoning is that they are aware of what to expect when participating in evaluations which ensures that they are not signing up for something they then realize that they do not want to be a part of.

The upcoming section will describe each of the research activities, and related results, in detail.

4. Theoretical framework

The first research step was to explicate a theoretical framework as a set of design principles used to inform the first artifact design. The theoretical framework was based on the theoretical concepts presented in the background and interviews with four domain experts. The intention was to generate design principles grounded in research and practice.

4.1. Expert interviews

The expert interviews were conducted to gain practitioner insight into the research. The interviews were conducted as semi-structured interviews around topics derived from the concepts described in the background. The topics of the interviews, and a brief justification are presented in Table 2.

The four participants consisted of:

- A special education teacher with over 15 years of experience working with special pedagogy. Students with neurodevelopmental disorders are the focus of the participant.

Table 2
Expert interview topics.

Interview topic	Justification
Differences between people with cognitive disabilities and neurotypical with regards to secure behavior.	It can be assumed that lowered cognitive ability leads to lowered ability to comply with cybersecurity demands.
Differences between neurotypical and people with cognitive disabilities with regards to requirements on cybersecurity support.	People with cognitive disabilities process information differently from neurotypicals. Consequently, it is possible that they have other requirements on support services.
Cybersecurity training for people with cognitive disabilities.	This topic focused on cybersecurity training for people with cognitive disabilities. First, the participants were asked to outline their thoughts in general before they were asked about how specific cognitive abilities could impact on how people consumed cybersecurity training.
CBMT for people with cognitive disabilities.	The participants were introduced to CBMT and asked to comment on it from the perspective of users with cognitive disabilities. They were the asked about the reminding effect of CBMT and the fact that CBMT involved inserting training in the user's workflow.

- An interface design expert with 10 years of experience as a user experience designer and over 20 years of experience in non-profit organizations for persons with neurodevelopmental disorders.
- Two people who work with cognitive accessibility evaluations of digital services.

The expert interviews were conducted by researcher A and transcribed by researcher B. Researcher A then conducted the thematic analysis which was reviewed by the rest of the research team. The interviews revealed two main themes with several sub-themes. Those are outlined in Table 3.

In addition to the themes presented in Table 3, the participants stress that cognitive disabilities are very diverse and individual. For instance, a person with ADHD may struggle with impulse control while a person with autism typically does not. However, it is common to have more than one diagnosis and ADHD in autism in combination is not uncommon and how that is manifested is very individual. The participants did, however, suggest that keeping training short and to the point will help most people in the target group.

4.2. Drafting design principles

An important concept in the interviews was cognitive energy. The participants described that people with cognitive disabilities have a finite amount of cognitive energy and that cognitive processing required cognitive energy. Consequently, cybersecurity training should be developed so that it requires as little energy as possible. That notion influenced how three initial design principles were formed. The design principles were at this stage seen as initial inputs to the artifact design and then reviewed throughout the remainder of the research. The design principles are presented and justified below:

DP 1. Cybersecurity training for users with cognitive disabilities should be presented to users in context where the training is of direct relevance. This principle is intended to guide training towards being practical, to the point and expected. It is practical in the sense that when training is presented in a context of direct relevance it is directly relevant to the user's current tasks. Presenting information of relevance for the current task is also intended to make the training expected. Since it only presents information on a single subject rather than general cybersecurity topics it can also be short. This principle is guided by CBMT's emphasis on short training in contexts of relevance to the user. Presenting training in relevant situations makes it repetitive by nature, which can combat memory-related problems of the target group described in the background.

DP 2. Cybersecurity training for users with cognitive disabilities should focus on only the most important information. The interview participants stress that processing information demands a lot of cognitive energy, and this principle therefore stipulates that cybersecurity training should only present the most important information to avoid forcing the user to process to mush information. The principle is also in-line with CBMTs call for short and easy to digest training.

DP 3. Cybersecurity training for users with cognitive disabilities should only present information that is of relevance for the user. This principle seeks to minimize confusion by ensuring that only information related to a specific context is presented. It is derived from the interview responses which describe that users with cognitive disabilities often struggle with concentration, especially if different messages are presented at the same time. It also intended to make the information more expected since it is fit for a situation the user is currently experiencing.

Table 3
Results of expert interviews.

Theme	Sub-themes	Description
Secure behavior	Impulse control	It is common for some people with cognitive disabilities to act before they think. This could lead to higher susceptibility to, for instance, phishing.
	Anxiety	Some people want to know what is happening all the time and know everything about a subject. Not knowing what is happening may lead to anxiety for a task.
	Energy	The participants stress that a common denominator for persons with cognitive disabilities is that cognitive processing requires energy which is a finite resource. This may lead to persons not adopting security features which require cognitive processing.
	Concentration	It is common for some persons with cognitive disabilities to struggle with concentration needed to engage in, for instance password creation.
Training	To the point	The training should be focused on as few subjects as possible so that users do not lose focus or get confused.
	Clear	It is important that the information is clearly presented and free of distractions.
	Expected	It can be confusing and distracting if the participants are not aware that training may appear.
	Practical	If the training can be integrated with practical scenarios or real-world situations a feeling of relevance can occur.
	Short	Summarizing the most important information is important since it then requires less energy to consume.

5. Cycle 1: proposing a solution

The first design cycle sought to explore *How can CBMT be used to implement cybersecurity training for users with cognitive disabilities?* For this purpose, a training tool was developed according to CBMT and the developed design principles. It was then evaluated in group interviews with people with cognitive disabilities. The output of the interviews was used to review the design principles, as outlines in the remainder of this section.

5.1. Development and demonstration

In this step, a cybersecurity training tool that provided users with training on how to create strong passwords was created. The training was designed to be implemented at the account registration form of a web site and will appear to users when they click a create password field, in accordance with DP1. The training appears to users as a pop-up with text elements, as demonstrated in Fig. 2.

As seen in Fig. 2, the training is a dialogue with six steps. The first step contains minimal information and, in accordance with CBMT, allows the user to decide if they want more information or not. The information is based on Kävrestad et al. (2020). If the user continues, they will receive further information and may then test their knowledge in a short quiz before creating their password. By providing very condensed information relevant for password creation, the training complies with DP2 and DP3.

From a technical perspective, the tool was developed as a JavaScript which is included on a web page. It then appears to the user as a pop-up whenever the user clicks in the password field of an account registration page.

5.2. Evaluation of the training tool

The training tool was evaluated in two group interviews with the target group, users with cognitive disabilities. The first group interview included four participants and the second group interview included six participants. The participants were samples using a purposive sampling approach with the intent of recruiting participants from the target group who were used to participating in similar studies. The approach was decided on in cooperation with the organization Begripsam who specialize in usability evaluations focusing on cognitive accessibility. The rationale was that participants who are used to participating in usability evaluations will be more comfortable than users recruited using a random sampling technique. That was deemed important for the research ability to generate good results when targeting a population which often struggles with communication and social interaction, which is the case with people who are, for instance, autistic. All participants had one or more cognitive disabilities but were able to autonomously use digital devices. They lived independently with no or little assistance.

Each interview lasted for about two hours and during the interview the researcher demonstrated the training tool and the participants provided feedback about it. When the participants identified issues, they were asked about how the issue could be resolved. The group interviews were analyzed in a thematic fashion and three topics emerged: Perceived issues, proposed solutions, general about security functions. Several themes were identified for each topic and those are summarized in Table 3.

Topic	Theme	Description
Perceived issues with training tool	Unfocused design	Several participants mentioned that some design elements did not fill a purpose but required cognitive energy to process. For instance, the image at the start of the training was mentioned as energy consuming but unnecessary.
	Lack of availability functions	The participants described it as problematic that availability functions such as ability to enlarge text or use text-to-speech was missing.
	Inconsistency	The participants perceived an inconsistent use of colors and placements of design elements as problematic. This created a feeling of confusion.
	Language	The participants perceived several sentences as long and complicated. They mentioned that they got stuck on sentences they did not understand.
Proposed solutions	Minimalism design	The participants suggested to only include the information that was needed and remove everything “fancy”. They described that images and videos should only be included if they served an important purpose.
	Accessibility functions	The participant suggested adding Accessibility functions, at least text to speech.
	Media diversity	The participants disagreed on what type of media to present information in. Most participants preferred text, but some wanted an option to have information as video.
General about security functions	Energy consuming	Several participants described the issues they perceived as energy draining to the extent that they were not able to use it. One participant described that their energy was a limited source and they often had to plan their day so that they created an account or had energy to make dinner.
	Focus on usefulness	The participants described that security was important but that they had to handle it as something they want rather than something they need. The top priority was to be able to do what they needed to do online. Maintaining a high level of security is not always possible.
	Hindering functions	Some participants described some security functions as completely hindering. Captcha was described as such a service and some participants described that they simply could not use services who used captcha because they were too complicated.
	Reminders	The participants were positive towards the training appearing at an event. The participants described this as a beneficial warning and reminder when they are doing something. They also described that it is important they are aware of the warning in advance.

(continued on next column)
(continued)

5.3. Revising the design principles

Following the group interviews the design principles were revisited. The established principles were confirmed. It is noteworthy that DP2 and DP3 call for focused information relevant for the user. While this is covered by DP2 and DP3, the interviews showed how critical these principles are. The interview participants describe that irrelevant or unneeded information takes a lot of energy to process. The consequence of not adhering to those principles can be that users with cognitive disabilities are unable to use a tool. A property requested by the participants, but not reflected in the design principles, is that design elements should also be limited. The participants specifically described that tools often have a design that is too “flashy” and energy consuming. For that reason, a fourth design principle was added; *DP 4. Cybersecurity training for users with cognitive disabilities should not include design elements without a clear purpose.*

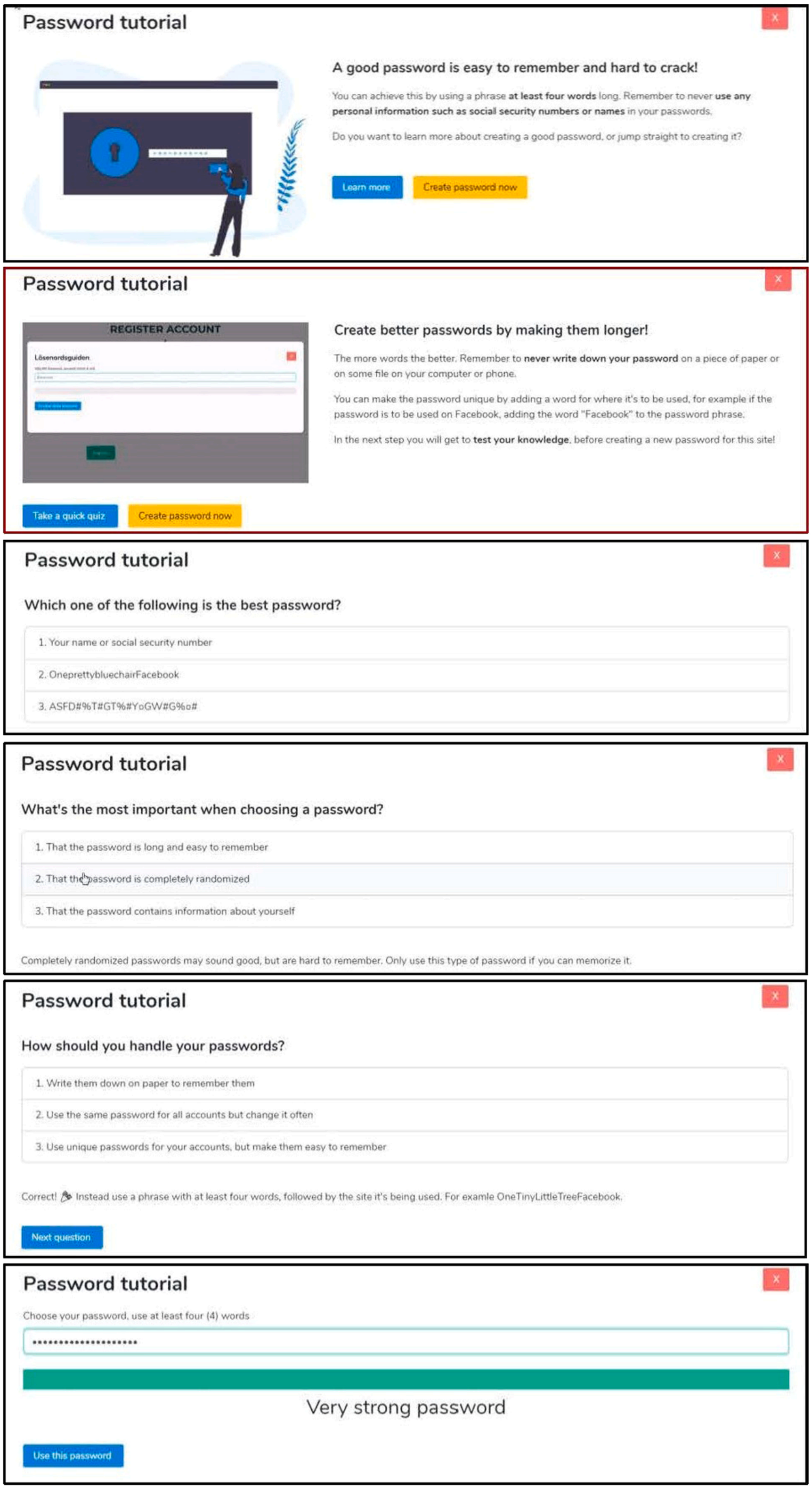
Furthermore, media diversity was discussed in several ways during the interviews where the most prominent discussion was that text element should be available in speech in some way. The important takeaway was that it must be possible for users to digest information in different ways, i.e. visually and auditory. Text-to-speech funtionality was given as an example of a service to include. A fifth design principle was established as; *DP 5. It should be possible for users with cognitive disabilities to consume cybersecurity training visually or auditory.*

6. Cycle 2: refining the solution

The training tool was redesigned following the evaluation. The tool was extended to not only provide training on password guidelines but also on phishing, online fraud and fake news. The following main design changes were made in this phase:

- The tool was designed as a browser extension to allow for a unified design for all security situations.
- The tool was designed to appear only as a textbox in the upper right screen corner, as shown in Fig. 3. The intention was to remove unnecessary design elements such as images, and to position the tool in a way that was less intrusive. The user can now opt for additional training and will then be presented with more extensive information, as shown in Fig. 4.
- A text to speech function was added to allow users to obtain auditory information.

The tool is designed to work for every website the user visits and contains functions to detect risky situations. The detection relies on a combination of content analysis matching based on web addresses. For instance, it detects when a user is about to create a password by looking for pages with two input fields for passwords, which is the typical layout for an account registration or password change page. To detect when a user could benefit from phishing training it attempts to identify if the user opens an inbox based on site content and uses a list of known mail services as a backup. The fraud and fake news functions relies on lists of known fraudulent or fake news websites. When one of the



Password tutorial

A good password is easy to remember and hard to crack!

You can achieve this by using a phrase **at least four words** long. Remember to never **use any personal information such as social security numbers or names** in your passwords.

Do you want to learn more about creating a good password, or jump straight to creating it?

Password tutorial

Create better passwords by making them longer!

The more words the better. Remember to **never write down your password** on a piece of paper or on some file on your computer or phone.

You can make the password unique by adding a word for where it's to be used, for example if the password is to be used on Facebook, adding the word "Facebook" to the password phrase.

In the next step you will get to **test your knowledge**, before creating a new password for this site!

Password tutorial

Which one of the following is the best password?

1. Your name or social security number
2. OneprettybluechairFacebook
3. ASFD#%T#GT%#YoGW#G%o#

Password tutorial

What's the most important when choosing a password?

1. That the password is long and easy to remember
2. That the password is completely randomized
3. That the password contains information about yourself

Completely randomized passwords may sound good, but are hard to remember. Only use this type of password if you can memorize it.

Password tutorial

How should you handle your passwords?

1. Write them down on paper to remember them
2. Use the same password for all accounts but change it often
3. Use unique passwords for your accounts, but make them easy to remember

Correct! 🎉 Instead use a phrase with at least four words, followed by the site it's being used. For examle OneTinyLittleTreeFacebook.

Password tutorial

Choose your password, use at least four (4) words

••••••••••••••••••••

Very strong password

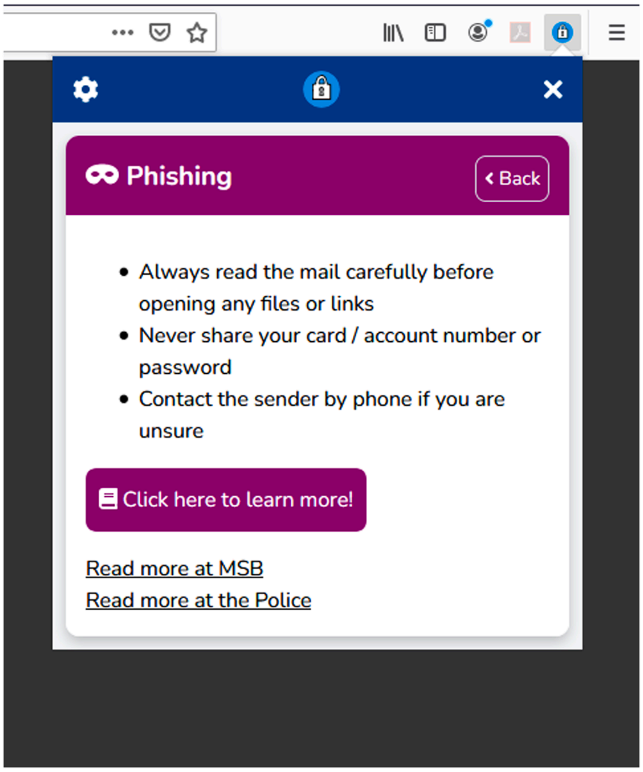
Fig. 3. Training tool in design cycle 1.

aforementioned situations is detected the tool presents brief training on the detected situation as a windows in the upper right corner, as shown in Fig. 4.

The user can opt for deeper information by selecting *Click here to learn more.* The tool will then open a new tab with more training on the topic at hand, as shown in Fig. 5.

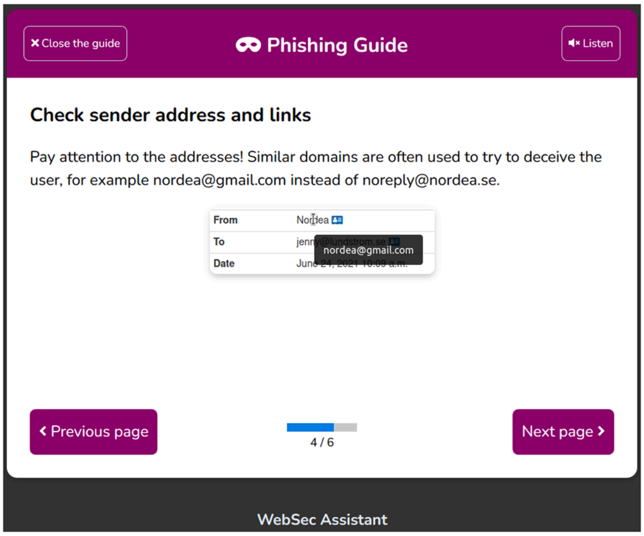
6.1. Evaluation

The training tool was evaluated in two group interviews with the target group, users with cognitive disabilities. The participant profile and interview organization were the same as for the group interviews in cycle 1. One group interview included five participants and the other



- Always read the mail carefully before opening any files or links
- Never share your card / account number or password
- Contact the sender by phone if you are unsure

Fig. 4. Demonstration of phishing warning from the training tool.



Check sender address and links

Pay attention to the addresses! Similar domains are often used to try to deceive the user, for example nordea@gmail.com instead of noreply@nordea.se.

From	Nordea
To	jenny@lundstrom.se
Date	June 24, 2021 10:09 a.m.

Fig. 5. Demonstration of phishing training from the training tool.

included six participants. Each interview took about two hours and during the interview the researcher demonstrated the training tool and the participants provided feedback about it. When the participants identified issues, they were asked about how the issue could be resolved. The group interviews were analyzed in a thematic fashion and two topics emerged: perceived issues with the tool and proposed solutions.

The results from the interviews were mostly the same as the interviews in design cycle 1 but the focus at this stage was on detailed issues such as choice of words, placements of buttons and individual design elements. This confirms the interview data previously gathered and highlights the importance of continuous user involvement during interface design. Furthermore, two new themes emerged in the analysis of those group interviews. The first new theme was *control* where the participants expressed an increased willingness to have control over how the tool behaved. This pertained mainly to the text to speech functionality where participants wanted to be able to control the pace of the speech. They also wanted to be able to mark a section of the text and have the function speak that selection. Under the theme of control, the participants also mentioned that it would be good if the tool could include options for configuring how often it appears. The second theme was *conflict* and highlights that the participants disagreed on several occasions. The disagreements were often about design options where they demonstrated different preferences. The disagreements were both about detailed design options such as placements of buttons, and about fundamental functional options such as the level of configuration that should be allowed or needed to use the tool. Most participants wanted a limited set of options to promote ease of use where some preferred to have full control over the tools' behavior. In conclusion, the evaluation confirmed the design principles previously outlined.

7. Conclusions and future work

This research is focused on cybersecurity training with cognitive disabilities in mind, a topic that has received little to no attention from researchers in the past. It adopted a user centric research approach by using design science to research how a cybersecurity training tool for users with cognitive disabilities could be developed. The research was guided by three research questions which are elaborated on next.

The first research question was "How can cognitive disabilities impact users' ability to adopt secure behavior?". The data collected in this research provides two main insights in relation to this question. First, several participants describe how they often experience cognitive fatigue during cognitively demanding tasks. Further, the participants describe security processes such as phishing detection and password management as high-demanding and difficult. While this aligns well with research into usable security which targets neurotypical users, e.g. Caputo et al. (2016) and Caulfield et al. (2019), the participants in this research describe the issues as close to incapacitating suggesting that usability issues are even more problematic for this user group. Second, the participants describe some functions, such as captchas, as completely incapacitating suggesting that some security functions are completely discriminating towards some users.

The second research question was "How can CBMT be used to implement cybersecurity training for users with cognitive disabilities?". The interviews during this research suggest that the fundamental concept of CBMT is a good fit for users with cognitive disabilities. CBMT emphasizes limited and easy to absorb information which is what the participants in this research requests. CBMT dictates that cybersecurity training should be provided to users as a warning in a situation with elevated cybersecurity risk. On this note the participants are positive to the warning function but stress the importance of being aware that a warning may appear.

The third research question, "How can cybersecurity training for users with cognitive disabilities be designed?", was answered by developing design principles for cybersecurity training for users with cognitive challenges and those are outlined in the coming section. As a practical contribution, this research developed cybersecurity training as a browser plugin which is freely available for anyone to use.[1]

7.1. Design principles

The main research contribution of this work is the development of design principles throughout the work. They provide a theoretical contribution to the field of cognitively accessible cybersecurity training

[1] https://chrome.google.com/webstore/detail/websec-coach/fppabiaolagdjpchoicgfikcjnilbdkl?hl=sv

and are explained as follows.

DP 1. Cybersecurity training for users with cognitive disabilities should be presented to users in context where the training is of direct relevance. This principle is guided by CBMT and intends to meet the need for practical training identified in the interviews. Presenting training in relevant situations makes it repetitive by nature, which can combat memory related problems of the target group. It is, however, important that users are aware that training may appear in situations with elevated risk.

DP 2. Cybersecurity training for users with cognitive disabilities should focus on only the most important information. The intention of this principle is to limit the need for cognitive processing which in turn reduces the energy needed to consume the training. The principle is also in-line with CBMTs call for short and easy to digest training.

DP 3. Cybersecurity training for users with cognitive disabilities should only present information that is of relevance for the user. This principle seeks to minimize confusion by ensuring that only information related to a specific context is presented. This is also intended to make the information more expected since it is fit for a situation the user is currently experiencing.

DP 4. Cybersecurity training for users with cognitive disabilities should not include design elements without a clear purpose. This principle is an extension to P2 and P3 which emphasizes focused and limited information. This principle continues by suggesting that design elements should also be minimized. The rationale is that everything that is presented to the user must be processed and visual elements which are not required to make the presented information tangible should be avoided as they require unnecessary cognitive processing.

DP 5. It should be possible for users with cognitive disabilities to consume cybersecurity training visually or auditory. This design principle responds to a need for consuming information in different ways. Some users struggle with reading and can benefit from auditory consumption and some users prefer reading. Allowing informative elements to be consumed visually or auditory, for instance using text to speech functionality is beneficial.

While the design principles are developed with a focus on users with cognitive disabilities, they intend to minimize the cognitive energy required to participate in cybersecurity training. Previous research suggest that to beneficial for neurotypical user groups as well (Reeves et al., 2021). To what extent those design principles are applicable for neurotypical users is, however, beyond the scope of this research.

7.2. Discussion

To the best of our knowledge, this is no previous research focusing on cybersecurity training for users with cognitive disabilities. For that reason, we adopted a design sciences methodology with continuous target group interviews with the intent of generating a deep understanding of the problem at hand. In total, 25 participants have been involved in this research where 21 are users from the target group and four are domain experts. For practical reasons, the research has been conducted in Sweden with Swedish participants. Hence, the target group is to some extent representative of Swedish users.

A second discussion related to the decisions about what theoretical frameworks to adopt. This research decided to adopt CBMT as the fundamental theory for cybersecurity training and the rationale was that CBMT has been extensively evaluated in other user groups with positive results. It is, nevertheless, possible that adopting some other cybersecurity training approach could have generated other results.

7.3. Limitation

As exemplified by Koutsouris et al. (2021) and Reeves et al. (2021), cybersecurity training can be evaluated based on:

- How the user perceives the training which is argued to be important for user adoption of the training.
- What the user learns using the training.
- How the training impacts on user behavior.

While all those aspects are important, the present research is focused on user perception by researching how to make users able to even participate in training. The rationale is that users must be able to participate in training for the training to have any effect. How the training impacts on the user's ability to adopt secure behavior is beyond the scope of this research.

This research was conducted as a design science project. Design science aims to create artifacts to solve problems within a specified domain (Hevner et al., 2004; Peffers et al., 2007). The domain for this research is users with cognitive disabilities and the participants in this research were exclusively selected from that domain. Consequently, the results are applicable to the domain and the degree to which the results can be generalized outside the domain is unknown.

7.4. Directions for future work

Given the lack of previous research on cybersecurity training for users with cognitive disabilities, this research provides a starting point for such research and opens an avenue of possible future directions. The most prominent discussion in the interviews concerned cognitive energy and workload, and how security functions sometimes depleted the participants' energy to the level of them being unable to follow security advice or use services at all. Cognitive workload has been a theme in previous research and it is clear that security functions can be cognitively exhaustive (Boyce et al., 2011; Nobles, 2022). Consequently, a future research agenda could be to quantify the cognitive cost of security to understand how much security users can be expected to engage with. That could be done by integrating theories from different fields, for instance from psychology and neurology. Such an agenda could also include an outline of how some security functions can be completely incapacitating for some user groups.

A second direction for future work would be to build on the present research. Such research could replicate this study in other populations or with other cybersecurity training approaches. One could also review the results of this research with a survey-based methodology to create a data sample which would allow for generalization of the results. Future work could also include an emphasis on the outcome of the training rather than the user's perception of it. That could be done by observing the implementation of cybersecurity training, and its effect on user behavior, in a longitudinal way.

As noted in the background, there is no generally agreed upon best practice for cybersecurity training for neurotypical users. This research is a first step towards such a theory for users with cognitive disabilities but does not account for the experience of neurotypical users. A third direction for future work would be to study how the design principles are perceived by neurotypical users.

Funding

This research was funded by the Swedish Post and Telecom Authority under grant number 19-10617.

CRediT authorship contribution statement

Joakim Kävrestad: Conceptualization, Methodology, Validation, Investigation, Writing – original draft, Project administration, Funding acquisition. **Jana Rambusch:** Conceptualization, Writing – review & editing, Supervision, Funding acquisition. **Marcus Nohlberg:** Conceptualization, Data curation, Writing – review & editing, Supervision, Funding acquisition.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Software developed is available and linked to. Interview data cannot be disclosed due to participant privacy concerns.

Acknowledgment

We want to acknowledge the organization Begripsam for assisting this research by providing access to valuable participants.

References

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

Al-Daeef, M.M., Basir, N., Saudi, M.M., 2017. Security awareness training: a review. In: Proceedings of the World Congress on Engineering, 1, pp. 5–7.

Al-Omari, A., El-Gayar, O., Deokar, A., 2012. Security policy compliance: user acceptance perspective. In: Proceeding of the 45th Hawaii International Conference on System Sciences. IEEE, pp. 3317–3326. https://doi.org/10.1109/HICSS.2012.516.

Al-Slais, Y., El-Medany, W.M., 2022. User-centric adaptive password policies to combat password fatigue. Int. Arab J. Inf. Technol. 19 (1), 55–62.

Aldawood, H., Skinner, G., 2018. Educating and raising awareness on cyber security social engineering: a literature review. In: Lee, M.J.W., Nikolic, S., Shen, J., Lei, L.C.U., Wong, G.K.W., Venkatarayalu, N. (Eds.), Proceedings of 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering, pp. 62–68.

Alyami, A., Sammon, D., Neville, K., Mahony, C., 2023. Critical success factors for Security Education, Training and Awareness (SETA) programme effectiveness: an empirical comparison of practitioner perspectives. Inf. Comput. Security.

Antshel, K.M., Zhang-James, Y., Faraone, S.V., 2013. The comorbidity of ADHD and autism spectrum disorder. Expert Rev. Neurother. 13 (10), 1117–1128.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., Xu, L., 2017. Gender difference and employees' cybersecurity behaviors. Comput. Hum. Behav. 69, 437–443. https://doi.org/10.1016/j.chb.2016.12.040.

Bada, M., Sasse, A.M., & Nurse, J.R. (2019). Cyber security awareness campaigns: why do they fail to change behaviour? *arXiv preprint* 10.48550/arXiv.1901.02672.

Beuran, R., Chinen, K.-i., Tan, Y., & Shinoda, Y. (2016). Towards effective cybersecurity education and training.

Boyce, M.W., Duma, K.M., Hettinger, L.J., Malone, T.B., Wilson, D.P., Lockett-Reynolds, J., 2011. Human performance in cybersecurity: a research agenda. In: Proceedings of the Human Factors and Ergonomics Society annual meeting.

Braun, V., Clarke, V., 2006. Using thematic analysis in psychology. Qual. Res. Psychol. 3 (2), 77–101.

Burmeister, O.K., 2010. Websites for seniors: cognitive accessibility. Int. J. Emerg. Technol. Soc. 8 (2), 99.

Caputo, D.D., Pfleeger, S.L., Sasse, M.A., Ammann, P., Offutt, J., Deng, L., 2016. Barriers to usable security? Three organizational case studies. IEEE Secur. Priv. 14 (5), 22–32. https://doi.org/10.1109/msp.2016.95.

Caulfield, T., Spring, J.M., & Angela Sasse, M. (2019). Why jenny can't figure out which of these messages is a covert information operation.

Chowdhury, N., Gkioulos, V., 2021. Cyber security training for critical infrastructure protection: a literature review. Comput. Sci. Rev. 40, 100361.

Etikan, I., Musa, S.A., Alkassim, R.S., 2016. Comparison of convenience sampling and purposive sampling. Am. J. Theor. Appl. Stat. 5 (1), 1–4. https://doi.org/10.11648/j.ajtas.20160501.11.

FCC. (2016). *Cognitive disabilities*. Retrieved 20230925 from https://www.fcc.gov/cognitive-disabilities.

Gjertsen, E.G.B., Gjære, E.A., Bartnes, M., Flores, W.R., 2017a. Gamification of information security awareness and training. In: Proceedings of the 3rd International Conference on Information Systems Security and Privacy, 2017, pp. 59–70. https://doi.org/10.5220/0006128500590070.

Gjertsen, E.G.B., Gjaere, E.A., Bartnes, M., Flores, W.R., 2017b. Gamification of information security awareness and training. In: Proceedings of the 3rd International Conference on Information Systems Security and Privacy, pp. 59–70. https://doi.org/10.5220/0006128500590070.

Guo, Y., Zhang, Z., Guo, Y., 2019. Optiwords: a new password policy for creating memorable and strong passwords. Comput. Security 85, 423–435.

Gutzwiller, R., Dykstra, J., Payne, B., 2020. Gaps and opportunities in situational awareness for cybersecurity. Digit. Threats: Res. Pract. 1 (3), 1–6. https://doi.org/10.1145/3384471.

Hadlington, L., 2017. Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon 3 (7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346.

Haney, J.M., Lutters, W.G., 2018. It's {Scary… It's}{Confusing… It's} Dull": how cybersecurity advocates overcome negative perceptions of security. In: Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018).

Happé, F.G., Mansour, H., Barrett, P., Brown, T., Abbott, P., Charlton, R.A., 2016. Demographic and cognitive profile of individuals seeking a diagnosis of autism spectrum disorder in adulthood. J. Autism Dev. Disord. 46 (11), 3469–3480.

Harrison, B., Svetieva, E., Vishwanath, A., 2016. Individual processing of phishing emails: how attention and elaboration protect against phishing. Online Inf. Rev. 40 (2), 265–281.

Hevner, A.R., March, S.T., Park, J., Ram, S., 2004. Design science in information systems research. MIS Q. 28 (1), 75–105.

Horcher, A.-M., Tejay, G.P., 2009. Building a better password: the role of cognitive load in information security training. In: 2009 IEEE International Conference on Intelligence and Security Informatics.

International Organization for Standardization. (2012). *ISO/IEC 27032:2012*.

International Organization for Standardization. (2020). *ISO/IEC TS 27100:2020 Information technology — Cybersecurity — Overview and concepts*. https://www.iso.org/obp/ui#iso:std:iso-iec:ts:27100:ed-1:v1:en:term:3.2.

Internetstiftelsen. (2016, 2016). *Skydda dig mot bedragare!*.

Hu, S., Hsu, C., Zhou, Z., 2022. Security education, training, and awareness programs: literature review. J. Comput. Inf. Syst. 62 (4), 752–764.

Joinson, A., van Steen, T., 2018. Human aspects of cyber security: behaviour or culture change? Cyber Security: Peer-Rev. J. 1 (4), 351–360.

Juliadotter, N.V., Choo, K.-K.R., 2015. Cloud attack and risk assessment taxonomy. IEEE Cloud Comput. 2 (1), 14–20. https://doi.org/10.1109/MCC.2015.2.

Karwowski, M., Kaufman, J.C., 2017. The Creative Self: Effect of Beliefs, Self-efficacy, Mindset, and Identity. Academic Press.

Katsini, C., Fidas, C., Raptis, G.E., Belk, M., Samaras, G., Avouris, N., 2018. Influences of human cognition and visual behavior on password strength during picture password composition. In: Proceedings of the 2018 CHI Conference on Human Factors in Computing systems.

Koutsouris, N., Vassilakis, C., Kolokotronis, N., 2021. Cyber-security training evaluation metrics. In: 2021 IEEE International Conference on Cyber Security and Resilience (CSR).

Kritzinger, E., Loock, M., Mwim, E.N., 2018. Cyber safety awareness and culture planning in South Africa. In: LNCS, Vol. 11161, pp. 317–326.

Kävrestad, J., 2022. Context-based Micro-Training: Enhancing Cybersecurity Training for End-Users. University of Skövde.

Kävrestad, J., Hagberg, A., Nohlberg, M., Rambusch, J., Roos, R., Furnell, S., 2022. Evaluation of contextual and game-based training for phishing detection. Fut. Internet 14 (4). https://doi.org/10.3390/fi14040104.

Kävrestad, J., Lennartsson, M., Birath, M., Nohlberg, M., 2020. Constructing secure and memorable passwords. Inf. Comput. Security 28 (5), 701–717. https://doi.org/10.1108/ICS-07-2019-0077.

Kävrestad, J., Nohlberg, M., 2020. Context based microtraining: a framework for information security training. In: Proceedings of the 14th International Symposium on Human Aspects of Information Security and Assurance (HAISA2020). Springer, pp. 71–81. https://doi.org/10.1007/978-3-030-57404-8_6.

Lamond, M., Renaud, K., Wood, L., Prior, S., 2022. SOK: young children's cybersecurity knowledge, skills & practice: a systematic literature review. In: Proceedings of the 2022 European Symposium on Usable Security.

Lundin, L., Mellgren, Z., Abrams, D., Conse, J., Harty, M., Magnusson, B., Möller, N., 2012. Psykiska Funktionshinder : Stöd Och Hjälp Vid Kognitiva Funktinsnedsättningar, 2 ed. Studentlitteratur.

March, S.T., Smith, G.F., 1995. Design and natural science research on information technology. Decis. Support Syst. 15 (4), 251–266. https://doi.org/10.1016/0167-9236(94)00041-2.

Mashiane, T., Kritzinger, E., 2018. Cybersecurity behaviour: a conceptual taxonomy. In: Proceedings of IFIP International Conference on Information Security Theory and Practice. Springer, pp. 147–156. https://doi.org/10.1007/978-3-030-20074-9_11.

Mozilla. (2022). *Cognitive accessibility*. https://developer.mozilla.org/en-US/docs/Web/Accessibility/Cognitive_accessibility.

MSB. (2021). *Informationssäkerhet för privatpersoner*.

MSB. (2022). *Tänk säkert - Alla kan bidra till Sveriges cybersäkerhet. Du också!*.

Nobles, C., 2022. Stress, burnout, and security fatigue in cybersecurity: a human factors problem. HOLISTICA–J. Bus. Public Admin. 13 (1), 49–72.

Oberauer, K., Süß, H.-M., Schulze, R., Wilhelm, O., Wittmann, W.W., 2000. Working memory capacity—Facets of a cognitive ability construct. Pers. Individ. Dif. 29 (6), 1017–1045.

Olney, M.F., Kim, A., 2001. Beyond adjustment: integration of cognitive disability into identity. Disabil. Soc. 16 (4), 563–583.

Pais, R., Ruano, L., P Carvalho, O., Barros, H, 2020. Global cognitive impairment prevalence and incidence in community dwelling older adults—a systematic review. Geriatrics 5 (4), 84.

Palmer, L., 2013. The relationship between stress, fatigue, and cognitive functioning. Coll. Stud. J. 47 (2), 312–325.

Peffers, K., Tuunanen, T., Rothenberger, M.A., Chatterjee, S., 2007. A design science research methodology for information systems research. J. Manag. Inf. Syst. 24 (3), 45–77.

Reeves, A., Delfabbro, P., Calic, D., 2021. Encouraging employee engagement with cybersecurity: how to tackle cyber fatigue. Sage Open 11 (1). https://doi.org/10.1177/21582440211000049.

Reinheimer, B., Aldag, L., Mayer, P., Mossano, M., Duezguen, R., Lofthouse, B., von Landesberger, T., Volkamer, M., 2020. An investigation of phishing awareness and education over time: when and how to best remind users. In: Proceedings of the Sixteenth Symposium on Usable Privacy and Security ({SOUPS} 2020). USENIX Association, pp. 259–284.

Safa, N.S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N.A., Herawan, T., 2015. Information security conscious care behaviour formation in organizations. Comput. Security 53, 65–78. https://doi.org/10.1016/j.cose.2015.05.012.

Sfakianakis, A., Douligeris, C., Marinos, L., Lourenço, M., & Raghimi, O. (2019). *Enisa threat landscape report 2018 15 top cyberthreats and trends*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018.

Siponen, M., Baskerville, R.L., 2018. Intervention effect rates as a path to research relevance: information systems security example. J. Assoc. Inf. Syst. 19 (4) https://doi.org/10.17705/1jais.00491.

Soare, B. (2020). *Vectors of attack*. Retrieved 20220217 from https://heimdalsecurity.com/blog/vectors-of-attack/.

Stankovska, A., 2016. Cyber threat actors and cyber threat management. Entrepreneurship 4 (1), 174–185.

Säkerhetskollen. (2023, 2023). *Bli trygg på internet | Säkerhetskollen*.

Verhagen, S.J., Daniëls, N.E., Bartels, S.L., Tans, S., Borkelmans, K.W., de Vugt, M.E., Delespaul, P.A., 2019. Measuring within-day cognitive performance using the experience sampling method: a pilot study in a healthy population. PLoS One 14 (12), e0226409.

Westbrook, A., Braver, T.S., 2015. Cognitive effort: a neuroeconomic approach. Cognit., Affect. Behav. Neurosci. 15 (2), 395–415.

World Health Organization. (2022). *International statistical classification of diseases and related health problems*. https://www.who.int/standards/classifications/classification-of-diseases#:~:text=International%20Statistical%20Classification%20of%20Diseases%20and%20Related%20Health%20Problems%20(ICD)&text=ICD%20serves%20a%20broad%20range,and%20coded%20with%20the%20ICD.

Young, S., 2005. Coping strategies used by adults with ADHD. Pers. Individ. Diff. 38 (4), 809–816.

Zimmermann, V., Renaud, K., 2019. Moving from a ‘human-as-problem" to a ‘human-as-solution" cybersecurity mindset. Int. J. Hum. Comput. Stud. 131, 169–187. https://doi.org/10.1016/j.ijhcs.2019.05.005.

Joakim Kävrestad is a senior lecturer in informatics at the University of Skövde. He obtained his PhD in 2022 with his dissertation titled "Context-Based Micro-Training - Enhancing cybersecurity training for end-users". He has been committed to working within usable and equal access to security for a decade and his main research interests revolve around how user abilities impact the ability to be secure. In addition to leading and participating in several research projects, he is involved in ENISA Ad-Hoc Working Group on Awareness Raising.

Jana Rambusch is a senior lecturer in cognitive sciences at the University of Skövde. She obtained her PhD in 2010 with her dissertation titled "Mind Games Extended: Understanding Gameplay as Situated Activity". Jana is a member of Swedish Cognitive Science Society and her research interest include Human-Computer interaction and user experience design.

Marcus Nohlberg is a senior lecturer and docent in informatics at the University of Skövde. He obtained his PhD in 2008 with his dissertation titled "Securing Information Assets: Understanding, Measuring and Protecting against Social Engineering Attacks". He has a diverse background in research, consulting, and entrepreneurship and has been active in several start-ups taking research results to product realization. He is active in research on a plethora of topics revolving around the human aspect of security.