

## Cognitively available cybersecurity: A Systematic Literature Review

Kävrestad Joakim, Naqvi Bilal

This is a Author's accepted manuscript (AAM) version of a publication  
published by Springer, Cham

in Human-Centered Software Engineering. HCSE 2024. Lecture Notes in Computer Science

**DOI:** 10.1007/978-3-031-64576-1\_9

### **Copyright of the original publication:**

© 2024 IFIP International Federation for Information Processing

### **Please cite the publication as follows:**

Kävrestad, J., Naqvi, B. (2024). Cognitively Available Cybersecurity: A Systematic Literature Review. In: Lárusdóttir, M.K., Naqvi, B., Bernhaupt, R., Ardito, C., Sauer, S. (eds) Human-Centered Software Engineering. HCSE 2024. Lecture Notes in Computer Science, vol 14793. Springer, Cham. [https://doi.org/10.1007/978-3-031-64576-1\\_9](https://doi.org/10.1007/978-3-031-64576-1_9)

**This is a parallel published version of an original publication.  
This version can differ from the original published article.**

# **Cognitively available cybersecurity: A Systematic Literature Review**

Joakim Kävrestad<sup>1</sup>[0000-0003-2084-9119] and Bilal Naqvi<sup>2</sup>[0000-0001-5271-5604]

<sup>1</sup> Jönköping School of Engineering, Jönköping, Sweden  
Joakim.kaverestad@ju.se

<sup>2</sup> Lappeenranta University of Technology: Lappeenranta, Finland  
Syed.Naqvi@lut.fi

**Abstract.** Cybersecurity is imperative to safeguard the digital systems on which the world has come to rely. A core part of cybersecurity is users' ability to adopt protective behavior by using security functions and adhering to security policies. Protective behavior requires cognitive effort, and some research suggests that users with cognitive challenges may struggle. There is no cohesive body of knowledge addressing those struggles and that gap is addressed in this research. A systematic literature was conducted to review how cognitive challenges are discussed in relationship to end-users' cybersecurity. The findings reveal that the research on the topic is limited but agrees that adopting protective behavior is cognitively demanding. That hinders both users with cognitive disabilities and neurotypical users from being secure. While addressing cognitive challenges in the cybersecurity domain is identified as an important future challenge, limiting the effort put on users to minimize the required cognitive energy is identified as a starting point.

**Keywords:** cognition, cognitive disabilities, cybersecurity, usability, usable security.

## **1 Introduction**

Today's digital landscape offers a multitude of services which modern society has become reliant on. Continued digitalization is a cornerstone for the for all aspects of society and bring increased ability to communication, improved access to entertainment and improved access to public services [34]. Bringing more parts of our lives to the digital world does, however, also increase the exposure to digital threats [13]. Different threat agents, including hacktivist, adversarial states, and organized criminals leverage the highly digitalized world for ill-doing [42]. Those malicious activities are carried out with various intentions including financial gain, promotion of disinformation, destabilizing of society and more. There are many different ways, called attack vectors, that the treats agents can use and those can be classified as technological, process-oriented or human-oriented [21]. The domain of this research is the human-oriented attack vector which is typically described as the most frequently used [20, 41].

The human attack vector can be described as exploiting users to carry out attacks. In essence, attackers leverage the facts that users are expected to adopt protective

behaviors by, for instance, using strong passwords, follow security rules, and correctly distinguish between phishing email and legitimate email but in practice often fail to do so [18]. Explaining why users fail to adopt protective behavior has been a topic of research for a long time. Two main explanations has been lack of user knowledge (e.g. [1, 2]) and lack of usability in cybersecurity tools and rules (e.g. [4, 12]). The lack of user knowledge explanations suggests that users are not informed about the threats posed in the digital world or equipped with the skills needed to mitigate the threats. The usability explanation suggests that the expectations, tools and rules presented to users are inherently difficult to use which discourages users from using them or hinders correct use. A common example is password complexity guidelines which promote long and complex passwords. Those are intended to result in passwords that are difficult to guess, but users often employ coping strategies to remember their passwords which results in the opposite [43].

As part of the usability research in the cybersecurity domain, researchers started to analyze the cognitive effort needed to adopt protective behavior. Many activities included in this protective behavior requires memory (password creation and use), problem solving (captchas, phishing), or learning and therefore require cognitive effort [17, 27, 39]. The current research landscape agrees that users are more likely to adopt protective behavior which requires less cognitive effort. A further, and less studied topic is how users' ability to adopt protective behavior is impacted by cognitive disabilities. While some studies suggest that a cognitive disability may negatively impact a user's ability to adopt a protective behavior (e.g. [23, 32]) the extent of the effect, and how to handle it is unknown. With the intent of enabling a future research agenda on cognitively accessible cybersecurity, this research seeks to summarize how cognitive challenges has been discussed in cybersecurity research so far by answering the research question *How are cognitive challenges discussed in relation to end-user cybersecurity in research?*

A systematic literature review was conducted to identify how cognitive disabilities in relation to end-user cybersecurity have been discussed in the extant literature. The initial search revealed (n=248) papers that have been published to date, however, only twelve papers satisfied the inclusion criteria set for this research. From the analysis of (n=12) papers, it was identified that cognitive abilities are acknowledged as a prerequisite for secure end-user behaviour. The included papers demonstrate that differences in cognitive functioning cause differences in the ability to adopt secure behaviour and pinpoint that memory, and attention as problem-solving is paramount for cybersecurity. The research shows that research into the domain is scarce but in agreement that adopting a secure behaviour is cognitively demanding. Furthermore, cybersecurity functions can sometimes exclude users from using services altogether. While solutions are scarce, usable design is described as positive in the analysed literature.

The remainder of the paper is organized as follows: Section 2 presents the background, Section 3 presents the research method, Section 4 presents the findings from

the systematic literature review, Section 5 presents the findings from the interviews, Section 6 presents the discussion, and Section 7 concludes the paper.

## 2 Background

Cognitive abilities involve perception and people's ability to solve problems, plan, and reason [22]. Concentration and memory are also cognitive abilities [33]. Those abilities are important precursors for cybersecurity behavior where users are expected to follow security plans and procedures, reason and make decisions about the legitimacy of emails, create, and memorize passwords, and more. In the cybersecurity domain, Gutzwiller et al. [17] describe cybersecurity as involving cognitively demanding tasks with cybersecurity fatigue as a possible consequence. Similarly, Boyce et al., [7] describe minimizing cognitive workload as an important usability factor for cybersecurity functions and interfaces.

People's cognitive abilities are dynamic and individual and can be impacted on both a temporary and permanent basis [37, 44]. Several conditions can have a permanent impact on a person's cognitive abilities including autism, dyslexia, stroke, brain injury, and dementia [14]. How a certain condition will impact a person's cognitive abilities is highly individual [28]. However, a person with a cognitive disability will experience limitations in one or more of the cognitive abilities. Estimating the prevalence of cognitive disabilities is cumbersome [36]. However, CDC [10] suggests that 12.8% of U.S. adults are affected by a cognitive disability while Gauchard et al., [16] suggested that the prevalence in a French sample was between 3.0% and 4.7% in 2006. Further, Pais et al. [36] found a median prevalence of 19% for cognitive impairment which refers to loss of memory, learning difficulties, and decreased ability to concentrate among the elderly.

Given the prevalence of cognitive disabilities and the individual nature of how they are manifested, a large portion of people with cognitive disabilities are part of the workforce. It is common to have employees with cognitive disabilities without even knowing about them. Subsequently, it is paramount that cybersecurity functions and processes work for users with cognitive disabilities. Previous research demonstrated that cognitive ability impacts a user's ability to detect phishing and use cybersecurity functions such as captchas [6, 45]. Furthermore, users with cognitive disabilities do have difficulties while authenticating using the current range of authentication options available, for instance remembering complex passwords without writing them down can prove to be a cumbersome task for users with cognitive disabilities, similarly, the use of biometrics such as fingerprints can be difficult for a user who has had stroke resulting in disability or paralysis of arms and hands. A pertinent aspect to consider is either to leave cognitively challenged users reliant on their caregivers to perform cybersecurity functions or to develop solutions that consider cognitive factors in the design and development of cybersecurity functions. Consequently, cognitively acces-

sible cybersecurity is an important security matter since it allows all users to efficiently use cybersecurity functions. It is also an equality and inclusivity concern because it works towards equal access to digital technology.

### 3 Methodology

A systematic literature review (SLR) was conducted to explore the state of the art of how cognitive disabilities have been considered in cybersecurity research. The SLR methodology described by Paré and Kitsiou [38] was adopted for the review. The upcoming sections will elaborate on the search and selection process and the analysis of the included publications.

#### 3.1 Search protocol

As suggested by Jesson et al., [19], an inclusive search query was developed to capture publications discussing cognitive abilities, disabilities, and disorders in a cybersecurity context. The following query was used:

*cybersecurity AND (cognition OR cognitive) AND (ability OR abilities OR disorder OR function OR functions)*

It is important to note that different databases and digital libraries (considered during this SLR) have their specific syntax for the resultant search queries. Therefore, the query above was reformatted (while retaining the meaning) across the following databases and digital libraries:

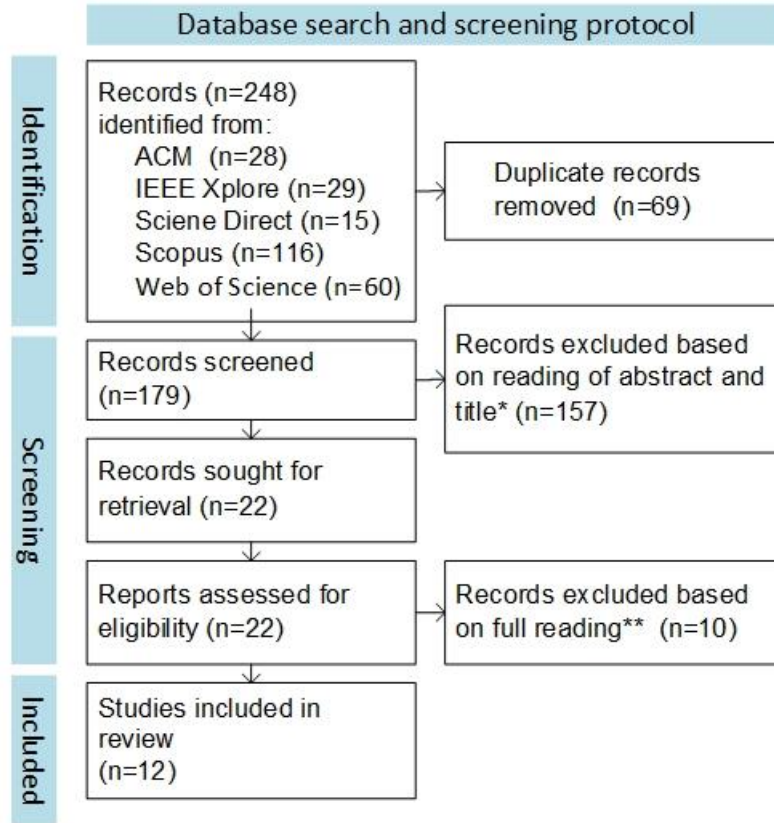
- ACM
- IEEE
- Scopus
- Science Direct
- Web of Science

#### 3.2 Screening for inclusion

The criteria for inclusion were defined to retain only the items that align with the goals of the study and help answer the research question. The following inclusion criteria (IC) were defined and applied for this study.

- IC 1: All papers that report any solutions, developmental approach, guidelines, principles, or recommendations for considering cognitive functions/challenges in the development of cybersecurity functions.
- IC 2: The language of the publication is English.
- IC 3: The publication has been published in a peer-reviewed journal or a conference.

The screening process is presented in Figure ; it is based on Page et al., [35] and Sarkis-Onofre et al., [40]. Firstly, the search results were scanned based on title and abstract, and irrelevant publications were discarded. The full body of the remaining papers was scanned again. Both scans were conducted independently by two researchers to minimize researcher bias. After scanning titles and abstracts, records kept by at least one researcher were kept for the scanning of the full papers. After the scanning of the full papers, the researchers discussed papers with conflicting judgments until a consensus was reached. Titles and authors of included publications are listed in Table 1. Searching and screening were conducted in two rounds, in October 2022 and in 2024. Figure 1 provides the combined results of both rounds. The rationale for searching in two rounds was that the initial searching yielded limited results and it was decided to pause the study for two years and then try again. The search and screening process in 2022 resulted in 8 publications selected for inclusion and another 4 were added in 2024.



\*Researcher A and B screened the records individually. All records included by at least one researcher were kept.

\*\* Researcher A and B screened the records individually. All records with disagreements were discussed until a joint decision was made.

**Fig. 1.** Screening process for the systematic literature review

**Table 1.** Titles and authors of included publications

Record title	Authors
An intelligent agent architecture to influence home users' risky behaviours [15]	Foroughi & Luksch, 2019
Neural correlates of gender differences and color in distinguishing security warnings and legitimate websites: A neurosecurity study [3]	Anderson et al., 2015
Leveraging digital intelligence in generation alpha [5]	Avci & Adigüzel, 2020
SOK: young children's cybersecurity knowledge, skills & practice: A systematic literature review [27]	Lamond et al., 2022

Modelling effective cybersecurity training frameworks: A Delphi method-based study [11]	Chowdhury et al., 2022
Cybersecurity as a social phenomenon [29]	McAlaney & Benson, 2019
Usable Privacy and Security from the Perspective of Cognitive Abilities [25]	Kävrestad et al., 2022
Upside and downside risk in online security for older adults with mild cognitive impairment [30]	Mentis et al., 2019
Aging online: Rethinking the aging decision-maker in a digital era [31]	Ebner et al., 2022
An Interdisciplinary Perspective on Mis/Disinformation Control [9]	Caramancion, 2023
Design principles for cognitively accessible cybersecurity training [24]	Kävrestad et al., 2024
Personality and Cognitive Factors in Password Security Behaviors [26]	Kennison & Chan-Tin, 2023

## 4 Results

The twelve included publications was analyzed in a thematic fashion inspired by Braun and Clarke [8]. First, individual concept of relevance for the research question was identified. Those concepts were then combined into three overarching themes. The themes are further described below.

### 4.1 Cognition is central to enable protective behaviour

The analysis of the included publications revealed that cognition has a central role to play in making accurate security decisions, may it be detecting and reporting an attack, responding to security warnings, or complying with a security policy. Foroughi & Luksch [15] acknowledge cognitive processing as central to users' cybersecurity decision-making. The authors propose a model to support cybersecurity decision-making by gathering information on user actions. While the publication does not explicitly describe how cognitive functioning impacts cybersecurity behavior, it showcases cognition as central to cybersecurity decision-making. Furthermore, Anderson et al., [3] describe that cognitive processing is central to cybersecurity behavior and that many such processes are automatic. Using electroencephalography, [3] examine users' brain activity when subjected to malware warnings and identify an increase in brain activity related to decision-making compared to when users are subjected to benign stimuli. While Anderson et al., focuses on neurotypical users, it demonstrates the importance of cognitive processing in cybersecurity decision-making. A similar perspective is presented by Ebner et al., [31] argue that age-related changes in cognitive functions can lead to poor decision-making online. Kävrestad et al., [24] describe that furthers the discussion by describing cognitive energy as a resource needed for cybersecurity tasks. Cognitive energy is finite and users with cognitive disabilities

may have less cognitive energy than neurotypical users, and cybersecurity tasks are therefore more costly.

In addition, Avci & Adigüzel, [5] describe the concept of digital intelligence as a set of cognitive, meta-cognitive, and socio-emotional skills and argue that users differ in the level of digital intelligence. The authors specifically focus on Generation Alpha as a group that needs to be trained differently from other users because of their life-long exposure to technology. While the paper does not specifically address differences in cognitive abilities, it does highlight cognitive processing as an important part of digital intelligence, and cybersecurity skills as important for digital users. Furthermore, Lamond et al., [27] stipulate that cybersecurity actions require mature cognitive abilities in a study on cybersecurity behavior among children. The paper finds that children often display poor cybersecurity behavior and attributes that, at least in part, to their cognitive functioning is not yet fully developed. Memory, literacy, attention, and problem-solving are described as cognitive functions that are important for cybersecurity activities. Similarly, Kennison & Chan-Tin [26] show that memory is connected to password creation so that users with lower memory ability create weaker passwords.

#### **4.2 Need for training and cognitive heuristics**

The current cybersecurity training regime does not consider the abilities, behavioral characteristics, and disabilities people have when developing the training content [24, 25]. Chowdhury et al., [11] Kennison & Chan-Tin [26] and question the effect of many current cybersecurity training programs and suggest that one reason is a lack of consideration of user's cognitive abilities in the development of such programs. Chowdhury et al., [11] then develop a framework for cybersecurity training those accounts for individual differences in different areas, including cognitive abilities. Such training needs to be designed to fortify the cognitive ability of users [9].

Furthermore, McAlaney & Benson, [29] discuss the role of cognitive heuristics in cybersecurity decision-making. Cognitive heuristics can be seen as mental shortcuts taken because cognitive processes require cognitive energy, which is a finite resource. The authors describe that the use of cognitive heuristics is a fundamental human function but that it can lead us to make incorrect cybersecurity decisions.

#### **4.3 Towards accessible and inclusive design**

In addition to the findings discussed earlier, the literature identifies the need for using accessible design approaches for inclusivity concerns and addressing the needs of users with cognitive disabilities. This is related to the finding just discussed that cognition is central to cybersecurity decision-making, which means that there is a need to support the cognitively challenged users of security functions thereby also reducing

the cybersecurity risks. Kävrestad et al., [24] present an interview study that aims to research usability requirements important for users with cognitive challenges. The main conclusion was that users with cognitive challenges face similar challenges as neurotypical users but often perceive the challenges as significantly more severe. The authors stress that cybersecurity tasks require energy, and that energy is a finite resource. Consequently, cybersecurity functions should strive to be as effortless as possible to use. The paper concludes that using accessible design and easy-to-follow instructions are important for users with cognitive challenges and beneficial for all user groups. Furthermore, Mentis et al., [30] studied how older users with mild cognitive impairments (MCI) are addressing cybersecurity concerns by interviewing users with MCI and their caregivers. They acknowledge that users with MCI may be more susceptible to cyber risks but describe that removing access to online services is also problematic since it reduces autonomy. The authors discuss using systems where a user's activity may be reviewed or monitored by a caregiver as one option, although such a solution would also reduce autonomy. The authors also discuss that services need to be designed to be secure and privacy-preserving without elaborating on how.

In conclusion, the SLR demonstrates that while research on cognitive abilities in relation to cybersecurity is scarce, the existing research does support the notion of cybersecurity activities as cognitively demanding. A few studies further demonstrate that users with cognitive challenges face difficulties when asked to engage in cybersecurity activities. Consequently, not accounting for cognitive challenges when developing cybersecurity functions and routines risks excluding users with cognitive challenges from being secure or using the services altogether.

## 5 Discussion

This research aimed to review how cognitive challenges in relation to cybersecurity are considered in current state-of-the-art research. The research comprised a systematic literature review to find out how cognitive disabilities are accounted for in cybersecurity research. Briefly, the result shows that academia acknowledge that cognitive disabilities are important to consider in relation to cybersecurity. However, the extent to which they have been considered so far is limited. Although the set of included publications is limited, it is notable that more than half the included publications are published from 2022 and onwards which could suggest an increasing research interest in the topic.

The SLR resulted in a limited set of included publications (n=12) which was quite surprising given that the initial searches generated 248 hits. However, many of those publications discussed cognitive aspects related to the cybersecurity workforce rather than end-user activities, or cognitive modeling as a computerized model which simulates human behavior. The twelve included publications show a distinctive pattern where most of them (seven) acknowledge cognitive processing or functioning as imperative for cybersecurity behavior. Five papers further showed that differences in

cognitive functioning result in different abilities to carry out cybersecurity activities. Only two papers provides insights on how to account for cognitive challenges in the development of cybersecurity routines and functions and suggest ease of use as the most important factor.

Cognitively accessible cybersecurity is important for users who suffer from cognitive disabilities. As discussed earlier, the cognitive ability of neurotypical users may be negatively impacted by temporary conditions such as ‘burnout’. Even stress and weariness can cause a person's cognitive abilities to be temporarily lowered. Consequently, cognitively accessible cybersecurity functions can be beneficial for all users.

## 6 Conclusions

This research shows that cognitive accessibility is important for making all users able to use cybersecurity functions. However, it also shows that research in the domain is limited. While explored research identifies that cognitive accessibility lowers the bar for the adoption of cybersecurity functions, how to do that remains unknown. A suggestion, considering this research, is that decision-makers and standardization bodies include cognitive accessibility into governing documents,

This research shows that cognitive accessibility is an important cybersecurity topic and reveals that both research and practitioner insight are scarce. Consequently, there are several avenues for further research. One such avenue would be to focus on the cognitive energy required to engage with cybersecurity functions. Being able to measure how much energy a certain tool or process requires would be beneficial and developing such a metric could be a direction for future work. Another possibility is to focus on the needs of the industry by researching the industry's preparedness to include cognitive accessibility in cybersecurity practices.

**Disclosure of Interests.** The authors have no competing interests to declare that are relevant to the content of this article.

## References

1. Al-Daeef, M.M. et al.: Security awareness training: A review. In: Proceedings of the World Congress on Engineering. pp. 5–7 (2017).
2. Aldawood, H., Skinner, G.: Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review. In: Proceedings of 2018 Ieee International Conference on Teaching, Assessment, and Learning for Engineering. pp. 62–68 IEEE (2018). <https://doi.org/10.1109/TALE.2018.8615162>.
3. Anderson, B.B. et al.: Neural correlates of gender differences and color in distinguishing security warnings and legitimate websites: a neurosecurity study. *Journal of Cybersecurity*. 1, 1, 109–120 (2015). <https://doi.org/10.1093/cybsec/tyv005>.

4. Atwater, E. et al.: Leading Johnny to Water: Designing for Usability and Trust. Presented at the Eleventh Symposium On Usable Privacy and Security (SOUPS) (2015).
5. Avci, H., Adigüzel, T.: Leveraging digital intelligence in generation alpha. In: The Teacher of Generation Alpha. pp. 119–132 (2020).
6. Belk, M. et al.: Do human cognitive differences in information processing affect preference and performance of CAPTCHA? *International Journal of Human-Computer Studies*. 84, 1–18 (2015).
7. Boyce, M.W. et al.: Human performance in cybersecurity: a research agenda. Presented at the Proceedings of the Human Factors and Ergonomics Society annual meeting (2011).
8. Braun, V., Clarke, V.: Using thematic analysis in psychology. *Qualitative research in psychology*. 3, 2, 77–101 (2006). <https://doi.org/10.1191/1478088706qp063oa>.
9. Caramancion, K.M.: An Interdisciplinary Perspective on Mis/Disinformation Control. In: 2023 3rd International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME). pp. 1–6 (2023). <https://doi.org/10.1109/ICECCME57830.2023.10253252>.
10. CDC: Disability Impacts All of Us, <https://www.cdc.gov/ncbddd/disabilityandhealth/infographic-disability-impacts-all.html>.
11. Chowdhury, N. et al.: Modeling effective cybersecurity training frameworks: A delphi method-based study. *Computers & Security*. 113, 102551 (2022). <https://doi.org/10.1016/j.cose.2021.102551>.
12. Das, S. et al.: A qualitative study on usability and acceptability of Yubico security key. Presented at the Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust (2018).
13. ENISA: ENISA Threat Landscape 2023, <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>, last accessed 2023/12/07.
14. FCC: Cognitive Disabilities, <https://www.fcc.gov/cognitive-disabilities>.
15. Foroughi, F., Luksch, P.: An intelligent agent architecture to influence home users' risky behaviours. *Advances in Intelligent Systems and Computing*. 797, 883–892 (2019). [https://doi.org/10.1007/978-981-13-1165-9\\_79](https://doi.org/10.1007/978-981-13-1165-9_79).
16. Gauchard, G.C. et al.: Prevalence of sensory and cognitive disabilities and falls, and their relationships: a community-based study. *Neuroepidemiology*. 26, 2, 108–118 (2006).
17. Gutzwiller, R. et al.: Gaps and opportunities in situational awareness for cybersecurity. *Digital Threats: Research and Practice*. 1, 3, 1–6 (2020). <https://doi.org/10.1145/3384471>.
18. Hadlington, L.: Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*. 3, 7, (2017). <https://doi.org/10.1016/j.heliyon.2017.e00346>.
19. Jesson, J. et al.: *Doing your literature review: Traditional and systematic techniques*. Sage (2011).
20. Joinson, A., van Steen, T.: Human aspects of cyber security: Behaviour or culture change? *Cyber Security: A Peer-Reviewed Journal*. 1, 4, 351–360 (2018).
21. Juliadotter, N.V., Choo, K.-K.R.: Cloud attack and risk assessment taxonomy. *IEEE Cloud Computing*. 2, 1, 14–20 (2015). <https://doi.org/10.1109/MCC.2015.2>.
22. Karwowski, M., Kaufman, J.C.: *The creative self: Effect of beliefs, self-efficacy, mindset, and identity*. Academic Press (2017).

23. Katsini, C. et al.: Eye Gaze-driven Prediction of Cognitive Differences during Graphical Password Composition. (2018). <https://doi.org/10.1145/3172944.3172996>.
24. Kävrestad, J. et al.: Design principles for cognitively accessible cybersecurity training. *Computers & Security*. 137, 103630 (2024). <https://doi.org/10.1016/j.cose.2023.103630>.
25. Kävrestad, J. et al.: Usable Privacy and Security from the Perspective of Cognitive Abilities. In: *Privacy and Identity Management. Between Data Protection and Security: 16th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2. 2 International Summer School, Privacy and Identity 2021, Virtual Event, August 16–20, 2021, Revised Selected Papers*. pp. 105–121 Springer International Publishing Cham (2022).
26. Kennison, S.M., Chan-Tin, D.E.: Personality and Cognitive Factors in Password Security Behaviors. *North American Journal of Psychology*. 25, 3, 599–599 (2023).
27. Lamond, M. et al.: SOK: young children’s cybersecurity knowledge, skills & practice: a systematic literature review. Presented at the Proceedings of the 2022 European Symposium on Usable Security (2022).
28. Lundin, L. et al.: *Psykiska funktionshinder: stöd och hjälp vid kognitiva funktionsnedsättningar*. Studentlitteratur (2012).
29. McAlaney, J., Benson, V.: Cybersecurity as a social phenomenon. In: *Cyber Influence and Cognitive Threats*. pp. 1–8 (2019). <https://doi.org/10.1016/B978-0-12-819204-7.00001-4>.
30. Mentis, H.M. et al.: Upside and downside risk in online security for older adults with mild cognitive impairment. In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. pp. 1–13 (2019).
31. Natalie Ebner et al.: Aging online: Rethinking the aging decision-maker in a digital era. In: *A Fresh Look at Fraud*. Routledge (2022).
32. Nobles, C.: Stress, Burnout, and Security Fatigue in Cybersecurity: A Human Factors Problem. *HOLISTICA—Journal of Business and Public Administration*. 13, 1, 49–72 (2022).
33. Oberauer, K. et al.: Working memory capacity—facets of a cognitive ability construct. *Personality and individual differences*. 29, 6, 1017–1045 (2000).
34. OECD: *Hows Life in the Digital Age?* (2019).
35. Page, M.J. et al.: The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *International journal of surgery*. 88, 105906 (2021).
36. Pais, R. et al.: Global cognitive impairment prevalence and incidence in community dwelling older adults—a systematic review. *Geriatrics*. 5, 4, 84 (2020).
37. Palmer, L.: The relationship between stress, fatigue, and cognitive functioning. *College Student Journal*. 47, 2, 312–325 (2013).
38. Paré, G., Kitsiou, S.: *Methods for Literature Reviews*. In: *Handbook of eHealth Evaluation: An Evidence-based Approach* [Internet]. University of Victoria (2017).
39. Reeves, A. et al.: “Get a red-hot poker and open up my eyes, it’s so boring” 1: Employee perceptions of cybersecurity training. *Computers & Security*. (2021).
40. Sarkis-Onofre, R. et al.: How to properly use the PRISMA Statement. *Systematic Reviews*. 10, 1, 1–3 (2021).
41. Soare, B.: Vectors of attack, <https://heimdalsecurity.com/blog/vectors-of-attack/>.
42. Stankovska, A.: Cyber Threat Actors And Cyber Threat Management. *Entrepreneurship*. 4, 1, 174–185 (2016).
43. Ur, B. et al.: I added ‘!’ at the end to make it secure”: Observing password creation in the lab. Presented at the Proc. SOUPS (2015).

44. Verhagen, S.J. et al.: Measuring within-day cognitive performance using the experience sampling method: A pilot study in a healthy population. *PloS one*. 14, 12, e0226409 (2019).
45. Vishwanath, A. et al.: Suspicion, cognition, and automaticity model of phishing susceptibility. *Communication Research*. 45, 8, 1146–1166 (2018).