# Not Just a Weak Link: Rethinking Aging, Cognition, and Cybersecurity in AI-Powered Workplaces

Research-in-progress

Andrea Brignone[1,†], Naomi Woods[2,*,†] and Ruilin Zhu[3,†]

[1] *Lancaster University, Bailrigg, Lancaster, LA1 4YW, UK*
[2] *University of Jyväskylä, Mattilanniemi 2, 40100 Jyväskylä, Finland*
[3] *Lancaster University, Bailrigg, Lancaster, LA1 4YW, UK*

**Abstract**

As artificial intelligence (AI) becomes increasingly important to organizational operations, cybersecurity risks are evolving. Aging employees, accounting for a growing percentage in the workforce, remain underrepresented in cybersecurity research despite their central role in organizational knowledge and continuity. This study investigates how age-related cognitive changes, digital self-efficacy, and socioemotional factors shape older workers' engagement with cybersecurity in AI-enabled workplaces. Drawing on interdisciplinary literature, we challenge the common portrayal of older workers as a monolithic, at-risk group and highlight the heterogeneity in their cybersecurity behaviors. Using a mixed-methods approach by combining cognitive assessments and interviews, this research aims to develop a conceptual framework that supports inclusive cybersecurity strategies. By foregrounding the human dimensions of digital transformation, the study contributes to both information systems theory and practical efforts to build secure, age-inclusive AI-empowered digital infrastructures.

**Keywords**

Artificial intelligence (AI), cybersecurity, aging employees, cognitive decline, digital transformation

## 1. Introduction

Organizations around the world are racing to integrate artificial intelligence (AI) into their operations. Less than three years since the launch of ChatGPT, 92% of companies report plans to increase investment in AI over the next three years [1]. These tools promise transformative benefits: enhanced efficiency and productivity, improved decision-making, and advanced capabilities like anomaly detection and automated risk scoring [2].

However, while organizations integrate AI into their activities, this new technology is radically changing the digital environment in which they operate. This transformation introduces new forms of complexity and risk, particularly in the realm of cybersecurity. Threats like phishing, ransomware, and social engineering attacks are not new, but AI has the potential to make them more sophisticated, scalable, and difficult to detect [3, 4].

Nevertheless, human involvement remains crucial in maintaining overall security. Without proactive guidance and continuous support in the fast-evolving digital environment, employees may become a potential weak link in the cybersecurity defenses of future organizations [5].

The human factor is especially critical as the workforce ages. From 2010 to 2023, the employment rate of individuals aged 55 and over in Europe increased by nearly 20%, and by 2030, one in three workers in advanced economies is projected to be over 55 [6]. These employees contribute vital

[1]The 11th International Workshop on Socio-Technical Perspectives in IS (STPIS'25) September 17-18 2025 Skopje, North Macedonia.
[*] Corresponding author.
[†] These authors contributed equally.
brignone.andrea@gmail.com (A. Brignone); naomi.woods@jyu.fi (N. Woods); ruilin.zhu@lancaster.ac.uk (R. Zhu)
0009-0005-0998-3351 (A. Brignone); 0000-0002-5692-5163 (N.Woods); 0000-0002-1074-0454 (R. Zhu)

institutional knowledge, technical expertise, and mentorship [7]. As life expectancy continues to rise [8], the well-being of aging employees is important for both public health and public finances, as continued work has been linked to better health outcomes and improved quality of life [6, 9]. Yet their integration into digital transformation efforts, particularly those concerning cybersecurity, remain uneven.

Studies have consistently shown that age plays a significant role in how individuals adopt and utilize technology. Previous research has examined how age affects technology acceptance, with older adults often report lower self-efficacy in using technology [10, 11, 12], which can impact their job performance and satisfaction if not addressed properly [9]. In addition, they appear to be more susceptible to deception, possibly due to changes in socioemotional factors related to aging, and are less likely to report fraud or use available security tools, even when they are aware of potential threats [13]. Cybersecurity threats powered by AI, such as deepfakes and voice impersonation, prey on older adults' trust and perceptual limitations [14].

These challenges underscore the need to understand how the distinct characteristics of aging workers shape their cybersecurity behaviors, especially as AI-driven systems become embedded in the modern workplace. Responding to growing calls for a more nuanced approach [13, 15], this study explores the intersection of technological innovation and demographic inclusion. Prior research has often treated aging employees as a homogeneous group, focusing on improving training practices without considering the diverse personal experiences, cognitive and socioemotional abilities, and learning preferences among them [16].

The proposed study argues that cybersecurity strategies in AI-enabled environments must be informed by a deeper understanding of how aging employees perceive, respond to, and engage with technology. While past studies have highlighted deficits in digital literacy (the ability to use digital tools) and digital awareness (understanding the broader implications of technology), there is still limited agreement on the role of age-related cognitive declines versus contextual or institutional factors in aggravating these challenges [12, 13, 17, 18, 19].

This study seeks to address that gap by establishing a foundational understanding of the underlying causes of barriers to digital engagement among older workers, by examining the impact of cognition factors on technology acceptance and cybersecurity perceptions. To this end, developing a robust framework will be essential for guiding future research in this area. The implications of this study are threefold. It will investigate older workers' perceptions of cybersecurity in AI-powered digital transformation for organizations. It will then identify and analyze the difficulties and challenges they encounter in adopting AI-mediated cybersecurity practices. The research will eventually develop a conceptual framework to support the integration of aging employees into the evolving digital environment. This integration is crucial for promoting both technological security and workforce inclusivity.

## 2. Literature Review

### 2.1. Human Risks in AI-powered Cybersecurity

The rapid integration of AI into organizational infrastructure has reshaped the cybersecurity landscape. AI-powered systems now play a pivotal role in risk detection and assessment, anomaly identification, and predictive threat analysis, allowing organizations to respond promptly to cybersecurity threats [2].

However, the same technologies that empower defenders are also being exploited by malicious actors. AI's capabilities—pattern recognition, natural language generation, and automated decision-making—have made cyberattacks more convincing, scalable, and difficult to detect. Deepfakes, voice cloning, and sophisticated phishing emails can now be generated at scale, mimicking trusted individuals or organizational communications with alarming precision [3, 4, 14].

In the evolving landscape of cybersecurity, the human factor remains critical: human mistakes, complacency, and lack of awareness can make employees one of the weakest links in even the most

sophisticated cybersecurity defenses [3, 15, 20]. As organizations become more digitally complex, aging employees are expected to navigate the changing cybersecurity risks, but face unique challenges that may require ad-hoc support and training [21].

Studies suggest that age-related socioemotional changes may make older workers more vulnerable to deception [13, 14, 22]. At the same time, research indicates that older workers often face barriers to digital engagement, including lower self-efficacy, reduced exposure to evolving technologies, and inconsistent access to relevant training [10, 12, 18, 19].

Nevertheless, the nuance of human factors in organizational cybersecurity strategies is rarely addressed accurately. Older employees are generically considered "at risk", overlooking the distinct psychological, experiential, and institutional factors that shape their behaviors [13, 15, 16]. As AI systems become more embedded in daily operations, it is essential to confront the social and cognitive dimensions of aging employees' perception of cybersecurity risks.

## 2.2. Understanding the Complexity of Older Employees' Cybersecurity Behavior

Age affects individuals' cognitive abilities in different ways and to varying degrees [23]. Furthermore, varying cognitive facets are impacted more than others, for example, autobiographical memories are not as susceptible to degradation (although some details will become more vague); whereas memories of newly learnt information can decline quite quickly [24]. Age-related cognitive decline can often affect abilities such as reasoning (specifically fluid reasoning), decision-making, learning, attention, speed of processing information, etc. [25]. Therefore, age-related cognitive changes can make certain individuals more susceptible to online deception, older workers do not necessarily have higher cybersecurity risks. Research reveals that, while age is an indicator of different technology-related behaviors, older adults are actually more likely than younger individuals to create strong passwords and engage in security practices such as regular software updates [12,20, 26, 27]. This contrast highlights the importance of recognizing the nuanced relationship between age and cybersecurity behaviors.

Moreover, older workers are far from homogeneous. Recent studies have shown substantial variations within this demographic in terms of their digital skills, exposure to technology, age, and education [16, 26]. For instance, individuals aged 50-59 are generally more open to technology compared to those over 60, and higher levels of education are associated with greater comfort and adaptability to technological development. Nevertheless, while there has been some research on the rapid digital transformation of business following the COVID pandemic, the specific impacts of the ongoing integration of AI remain underexplored.

Personal characteristics and professional experience also play a role in how aging individuals engage with digital transformation. Traits such as openness to technology and flexibility in goal-setting can influence one's ability to adapt to digital changes, and these traits can vary widely even among individuals in the same age group [26]. Furthermore, access to digital resources and training is not consistent across different countries and contexts. Komp-Leukkunen [28] emphasizes that access to digital training and cybersecurity support is not consistent across national and organizational contexts, reinforcing existing disparities and limiting the effectiveness of one-size-fits-all strategies.

Despite the growing attention to digital transformation in recent years, research on how the integration of AI specifically affects older workers' experience, behaviors, and inclusion in cybersecurity practices remains limited. As digital transformation continues to evolve, understanding this intersection is crucial for both technological innovation and workforce equity.

## 2.3. The Value and Vulnerability of Aging Workers in a Digitalized Workplace

Aging employees are central to the continued success of organizations by providing valuable institutional knowledge, maintaining operational consistency, offering expertise, and serving as mentors [7, 9]. With their growing presence in the workforce, their continued involvement also

brings broader societal benefits: working in later years is linked to enhanced quality of life, reduced reliance on healthcare services, and the sustainability of pension systems in the long run [6, 9].

Nevertheless, the ongoing digital transformation driven by AI in organizations and the increasing complexity of cybersecurity infrastructures present significant obstacles to the inclusion of aging workers. Previous research has highlighted the impact that age can have on technology acceptance and studies consistently indicate that older employees tend to exhibit lower confidence in using new technologies, leading to lower engagement with digital platforms and reduced participation in cybersecurity training [10, 12, 18]. This can be attributed to age-related cognitive decline and limited prior exposure to digital systems [22, 28].

Moreover, training programs are frequently not tailored to the needs of older learners, failing to accommodate varying levels of digital literacy and diverse learning preferences. As a result, many older workers may not be adequately prepared for the digital demands of the workplace [19, 20, 29]. If organizations are to fully benefit from the skills and knowledge of their aging workforce, they must design cybersecurity strategies and learning interventions that are not only technologically advanced but also socially inclusive.

## 2.4. Summary

The literature consistently highlights that older workers encounter significant challenges in adapting to AI-driven digital transformation and cybersecurity systems. These difficulties are often linked to age-related cognitive changes, lower technological acceptance and self-efficacy, and persistent gaps in digital literacy and awareness [10, 12, 13]. As cyber threats become more psychologically manipulative, particularly through tools such as deepfakes and voice impersonation that require increased abilities to identify deception, older adults may be especially vulnerable [14, 30].

However, a closer look at the research reveals a more complex situation. Contrary to common beliefs, older adults display heterogeneous cybersecurity skills: many are receptive to technological changes and generally follow recommended cybersecurity practices [12, 20]. The consensus across the literature is that aging employees are not a homogeneous group. Variability in education, professional exposure, digital skills, and even personality traits means that their engagement with cybersecurity is shaped by far more than age alone [16, 26].

Instead, factors like socioemotional aspects, context, and especially the quality of cybersecurity training play a crucial role in determining the cybersecurity readiness of older employees in AI-powered workplaces [15, 19, 29]. Inclusive training, tailored to personal learning styles, cognitive capacities, and motivational needs, has the potential to not only bridge skill gaps but also enhance self-confidence and long-term digital participation. In general, however, a more inclusive approach, able to empower and support older employees to participate in AI-driven digital transformation is essential for cybersecurity readiness.

## 2.5. Research Gaps

Despite growing scholarly attention to older workers in AI-driven digital environments, critical gaps remain in our understanding of their cybersecurity engagement. One major limitation is that research often groups aging employees together as a single demographic, which overlooks the diverse cognitive, socioemotional, and experiential factors that influence their interactions with AI systems [16].

Cybersecurity strategies should consider broader structural and cultural dimensions, including design inclusivity, learning requirements, organizational culture, and adaptability [13, 15, 31]. Furthermore, while studies demonstrate digital literacy gaps in older adults, it is unclear whether these are primarily due to age or other barriers such as lack of institutional support [17, 18]. In this regard, there is a need for research to examine older workers and their cognitive abilities, to get more precise understanding of how and at what point age-related cognitive decline impacts the way older workers engage with AI systems and cybersecurity.

These gaps reveal a great need for inclusive, context-sensitive, and psychologically informed

research. Understanding how to best help aging employees navigate cybersecurity challenges in AI-enhanced organizations is not just a technological or economic issue but a social one also. Addressing this complexity is crucial for designing effective policies and supporting security and inclusivity in the digital workplace.

## 3. Proposed Research Methods: Mixed-methods Study

A mixed method approach will examine cognitive abilities, cyber security perceptions, and knowledge, technology acceptance, and use of AI supportive technology. Participants will be recruited from a variety of organizations within Finland who have an AI initiative. The sample will include employees who have direct access to using AI to support their organizational roles. The participants will be of the age of 45+ as cognitive decline usually starts after the age of 40 years old [24]. We will aim to recruit 15-25 employees (or more until saturation has been reached) as, although this study will be mixed-methods, it will have a stronger qualitative approach.

Ethical considerations will be taken into account, and ethical clearance from the institution's ethical committee will be sought. Participants' consent will be obtained, information including privacy policies are provided to the participants, and data collected is kept confidential and coded.

### 3.1. Cognitive Ability

Different cognitive facets decline as people get older and at different speeds due to the aging process [23]. With the retirement age being around 65 years old for many countries globally, we propose to examine middle-aged adults (from 45-50 years old), and older adults (from 60-65 years of age) [32, 36].

Cognitive abilities can include several different aspects, such as memory, attention, comprehension, processing speed, and fluid intelligence/reasoning [25]. Not all cognitive facets decline with age, and some are not as strongly impacted. However, there are some cognitive abilities that are affected more strongly, for example, fluid intelligence which includes reasoning and problem-solving applied to processing new and novel information, that is less dependent on familiar experiences, has been noted to start declining in early 40's. With regard to memory, forming new memories declines with age, while autobiographical memories formed in the past tend to be stable. However, the accuracy for details declines. With regards to divided attention, learning new tasks while simultaneously performing other tasks also declines with age. This is an important skill that mainly affects productivity [24].

There are many tools to measure cognitive abilities and cognitive decline. Many instruments that measure cognitive decline, are often not sensitive enough to "normal" functioning, and are more sensitive to those experiencing the onset of dementia. Therefore, for the purpose of the proposed study, we will measure the cognitive abilities (rather than decline), using the Wechsler Adult Intelligence Scale (WAIS) fifth edition, to measure: fluid reasoning, working memory (including learning and attention), and processing speed [25]. Wechsler Adult Intelligence Scale (WAIS) is a prominent standardized test for measuring cognitive abilities within adults and older adolescents [33] that was originally developed in the 1950's and has been revised many times since. The tests can be administered in paper form or digitally, but for consistency, within the study, the test will be provided digitally.

### 3.2. Interviews

We propose to conduct semi-structured interviews using questions developed from the literature, and established guidelines [34]. Collecting qualitative data via conducting interviews are often chosen "since they enable researchers to step back and examine the interpretations of their fellow participants in some detail" [35, p. 78]. Interview questions will center around cybersecurity perceptions, technology acceptance, and ease of use in terms of AI supportive technology within organizations. Half of the interviews will be conducted before their cognitive abilities are evaluated,

and half of the participants will have their cognitive abilities evaluated before the interviews to eliminate any participant bias from evaluating their cognitive abilities first. Furthermore, the interviews will take place on a different day to that of the cognitive tests to reduce fatigue. The interview data will be transcribed and coded by at least two coders who will be guided and use verified data analysis methods [34]. All interview data will be analyzed using content analysis because of the prior background knowledge and understanding of the topic being explored.

## 4. Conclusion

Artificial intelligence is becoming integral to organizational operations, with many organizations introducing AI initiatives into work practice. With a growing global aging population, it is important to investigate how age-related cognitive changes, digital self-efficacy, and socioemotional factors shape older workers' engagement with cybersecurity in AI-enabled workplaces. Within the proposed study, we will not only consider age, but examine cognitive decline, as age-related cognitive change is different for every person and is varied in the abilities that are declining. These results will allow us to challenge the common portrayal of older workers as an at-risk group, generalized specifically on their age alone, and highlight the heterogeneity in their cybersecurity behaviors. Our findings will result in the development of a conceptual framework and could yield concreate suggestions that support inclusive cybersecurity strategies. Our findings could also advance IS literature through contributing and extending factors of technology acceptance models. Through highlighting human factors of digital transformation, this study will have implications for both information systems theory and practical efforts to build secure, age-inclusive AI-empowered digital infrastructures.

## Declaration on Generative AI

The authors have not employed any Generative AI tools.

## 5. References


[1]. McKinsey & Company, Superagency in the workplace: Empowering people to unlock AI's full potential at work, 2024. URL: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/superagency-in-the-workplace-empowering-people-to-unlock-ais-full-potential-at-work.

[2]. R. Amaresam. "AI-powered identity theft prevention: Revolutionizing online security." International Journal of Advanced Research in Science Communication and Technology, 5.3 (2025): 429–441.

[3]. O. Chimezie, O. Akagha, S. Dawodu, et al. "Comprehensive review on cybersecurity: Modern threats and advanced defense strategies." Computer Science & IT Research Journal, 5.1 (2024): 293–310.

[4]. S. Armoogum, V. Armoogum, A. Chandra, et al. "A comprehensive review of cyber hygiene practices in the workplace for enhanced digital security." JOIV: International Journal on Informatics Visualization, 9.1 (2025): 137–137.

[5]. J. J. Jeong, J. Mihelcic, G. C. Oliver, C. Rudolph, Towards an improved understanding of human factors in cybersecurity, in: Proceedings of the IEEE Humans and Cyber Security Workshop, IEEE, December 2019.

[6]. Eurofound, Keeping older workers in the labour force. Publications Office of the European Union. 2025, March 31. URL: https://www.eurofound.europa.eu/en/publications/2025/keeping-older-workers-labour-force.

[7]. J. Nyanjom, Mentoring and the older worker in contemporary organisations: The Australian case, in: S. Nachmias, V. Caven (Eds.), Inequality and Organizational Practice: Volume I: Work and Welfare, Palgrave Macmillan, 2019, pp. 65–85.

[8]. United Nations, Department of Economic and Social Affairs, Population Division, World population ageing: 1950–2050, 2017. URL: World Population Ageing 2017.

[9]. K. Komp-Leukkunen. “A life-course perspective on older workers in workplaces undergoing transformative digitalization.” The Gerontologist, 63.9 (2023): 1413–1418.
[10]. G. Wilson, J. R. Gates, S. Vijaykumar, D. J. Morgan. “Understanding older adults’ use of social technology and the factors influencing use.” Ageing & Society, 43.1 (2023): 222–245.
[11]. M. G. Morris, V. Venkatesh, P. L. Ackerman. “Gender and age differences in employee decisions about new technology: An extension to the theory of planned behavior.” IEEE Transactions on Engineering Management, 52.1 (2005): 69–84.
[12]. D. Branley-Bell, P. Briggs, L. Coventry, M. Dixon, A. Joinson. “Exploring age and gender differences in ICT cybersecurity behaviour.” Human Behavior and Emerging Technologies, 2693080 (2022).
[13]. E. Pacheco. “Older adults’ safety and security online: A post-pandemic exploration of attitudes and behaviors.” Journal of Digital Media & Interaction, 7.17 (2024): 107–126.
[14]. L. D. Herrera, L. Van Sickle, A. Podhradsky, Bridging the protection gap: Innovative approaches to shield older adults from AI-enhanced scams, 2024. URL: https://arxiv.org/abs/2409.18249.
[15]. S. G. Naqvi, A. Alishba, M. A. Mughal, K. Shehzad, R. T. Noor. “Organizational environment, protection motives, adoption of machine learning, and cybersecurity behavior.” Journal of Excellence in Social Sciences, 3.4 (2024): 11–25.
[16]. A. Poli, A. Heuer, A. Motel-Klingebiel. “Differential older workers’ experience with technology-related changes during the COVID-19 pandemic.” Nordic Journal of Working Life Studies, 14.S12 (2024): 1–19.
[17]. I. Durakova, D. Endovitsky. “Older workers and the supply and demand for digital technology jobs.” In: Proceedings of the CSIT Conference 2023, Yerevan, Armenia, September 25–30, 2023 (Paper No. 62).
[18]. I. Hecker, S. Spaulding, D. Kuehn. Digital skills and older workers: Supporting success in training and employment in a digital world, Urban Institute Report, Urban Institute, Washington, DC, September 2021.
[19]. H. Xie, Y. Fang, M. Wang, J. Liu, A. Lv. “Providing digital technology training as a way to retain older workers: The importance of perceived usefulness and growth need.” Work, Aging and Retirement, 9.4 (2023): 376–392.
[20]. D. Baltuttis, T. Teubner, M. T. P. Adam. “A typology of cybersecurity behavior among knowledge workers.” Computers & Security, 140 (2024): 103741.
[21]. E. Soja, P. Soja. “Fostering ICT use by older workers.” Journal of Enterprise Information Management, 33.2 (2020): 407–434.
[22]. N. C. Ebner, D. Pehlivanoglu, R. Polk, G. R. Turner, R. N. Spreng. Aging online: Rethinking the aging decision-maker in a digital era, in: Y. Hanoch, S. Wood (Eds.), A Fresh Look at Fraud: Theoretical and Applied Perspectives, Routledge, 2022, pp. 58–87.
[23]. O. Hatahet, M. L. Seghier. “The validity of studying healthy aging with cognitive tests measuring different constructs.” Scientific Reports, 14.1 (2024): 23880.
[24]. D. V. C. Brito, F. Esteves, A. T. Rajado, N. Silva, I. Araújo, J. Bragança, et al. “Assessing cognitive decline in the aging brain: Lessons from rodent and human studies.” npj Aging, 9.1 (2023): 23.
[25]. J, Jacobson & E. L. George, Wechsler Adult Intelligence Scale (WAIS), 2024. URL: Wechsler Adult Intelligence Scale (WAIS).
[26]. I. M. S. Haunschild, B. Leipold. “The use of digital media and security precautions in adulthood.” Human Behavior and Emerging Technologies, 5.1 (2023): 1436710. doi:10.1155/2023/1436710.
[27]. D. R. Avery, P. F. McKay, D. C. Wilson. “Engaging the aging workforce: The relationship between perceived age similarity, satisfaction with coworkers, and employee engagement.” Journal of Applied Psychology, 92.6 (2007): 1542–1556.
[28]. K. Komp-Leukkunen, J. Sarasma. “Social sustainability in aging populations: A systematic literature review.” The Gerontologist, 64.5 (2024): gnad097.
[29]. M. Djotaroeno, E. Beulen. “Information security awareness in the insurance sector: Cognitive and internal factors and combined recommendations.” Information, 15.8 (2024): 505.

[30]. U.S. Senate Special Committee on Aging. Aging Committee hearing on how scammers are using artificial intelligence & how we can fight back, Video, 2023. URL: https://www.youtube.com/watch?v=7CMhzgQdz_I.
[31]. I. Marcelino, J. Góis, R. Laza, A. Pereira. "Using ICT for tacit knowledge preservation in old age." In: J. M. Corchado, J. Bajo, P. Escobedo, A. F. De la Prieta (Eds.), Ambient Intelligence—Software and Applications: 6th International Symposium on Ambient Intelligence (ISAmI 2015), Springer International Publishing, 2015, pp. 75–83.
[32]. Oxford Dictionary, Middle age: Definition of middle age in Oxford Dictionary (American English), (n.d.), URL: middle age: definition of middle age in Oxford dictionary (American English) (US).
[33]. A. S. Kaufman, E. Lichtenberger, Assessing Adolescent and Adult Intelligence, 3rd ed., Wiley, Hoboken, NJ, 2006. ISBN: 978-0-471-73553-3.
[34]. M. D. Myers, Qualitative Research in Business and Management, Sage Publications, London, 2013.
[35]. G. Walsham. "Interpretive case studies in IS research: Nature and method." European Journal of Information Systems, 4 (1995): 74–81.
[36]. United Nations, Department of Economic and Social Affairs, Population Division, World population ageing: 1950–2050, 2017. URL: World Population Ageing 2019.