Human-Centred Initiatives for Inclusive Cyber Security in a Medium-Sized UK Organisation

Elzbieta Titis[1] & Andrew Burd[2]

[1]University of Warwick, [2]Skewb Ltd

SUMMARY

This study builds on our prior research identifying key barriers to cyber security engagement, such as techno-invasion stress, demographic disparities in training uptake, and frustration with rigid protocols. Through a mixed-methods approach, it proposes targeted, human-centred initiatives with micro actions to improve engagement, reduce stress, and promote shared responsibility across age and gender groups in a mid-sized UK organisation, moving beyond purely technical considerations. We outline these initiatives and reflect on their long-term impact. The study recommends that organisations leverage these insights as a model of good practice and, along with other available data, use them to refine and strengthen their cyber security strategies.

KEYWORDS

Human factors, usability, cyber security culture, barriers, human-centred interventions

Introduction

Our prior research into cyber security engagement within a mid-sized UK organisation identified several key barriers (Burd, 2025). These included techno-invasion stress caused by constant digital connectivity and monitoring, demographic disparities in training uptake, and widespread frustration with rigid or unclear security protocols. Employees stated they did have a sense of personal responsibility (because of working in a positive culture environment), however what that meant was unclear. They indicated later that they needed guidance on how to be cyber responsible. The findings highlighted the need for more inclusive, empathetic, and user-centred approaches to cyber security practice, and targeted recommendations were developed to address these challenges.

In this study, we operationalise these recommendations through inclusive initiatives that incorporate targeted micro-actions designed to support the needs of specific demographic groups; for example, in previous study we found that techno-invasion stress disproportionately affects women. The actions were co-created with stakeholders and grounded in Self-Determination Theory (SDT), drawing on the core psychological needs of autonomy, competence, and relatedness to foster deeper engagement and intrinsic motivation in secure behaviour (Gangire, 2019).

Background

Digital innovation in Information and Communication Technology (ICT) has been driving datafication, virtual collaboration, and new communication ecosystems, redefining organisational structures and work practices alongside accelerating flexible, boundaryless work. In today's highly digitalised world, five major trends in contemporary work are reshaping how individuals navigate this complex landscape (Kossek, 2016). Work now permeates virtually any space and time, progressively eroding the traditional temporal and spatial boundaries that once separated professional responsibilities from personal life. At the same time, employees increasingly tailor their schedules, environments, and role boundaries to fit individual preferences, resulting in highly

personalized but more complex work–life arrangements. They are placed under growing pressure to manage their own working time, balancing availability, focus, and rest, which can exacerbate strain when organisational safeguards are lacking. The fragmentation of work and non-work interactions further complicates role transitions and can increase cognitive load. Finally, boundary experiences are not uniform, as different groups face distinct constraints, expectations, and cultural norms that shape how effectively they can manage work–life challenges (Kossek, 2016). These trends directly contribute to techno-stressors (e.g., complexity, insecurity, interruptions, invasion, overload, etc.), heightening ICT-related work demands (La Torre, 2019) and requiring ongoing self-regulation to avoid burnout (Yener, 2021).

Boundary theory holds that individuals may be engaged in work and non-work domains at the same time, enabling strain from one domain to spill over and affect the other (Amstad, 2011); caution is therefore warranted due to the risk of heighten interdomain conflict (Farivar, 2021). Boundary blurring intensifies job demands, such as constant connectivity and difficulty disengaging from work, which, in turn, heightens cognitive load and emotional strain (La Torre, 2019, Lițan, 2025). Organisational approaches to reducing techno-stressors include improving employees' digital literacy, setting clear communication norms, and fostering a supportive culture that promotes healthier technology use (Joy, 2024). The negative effects of digital-tool use can be mitigated by setting clear boundaries between work and personal time (Uslu, 2025) and limiting digital interruptions that disrupt concentration (Ohly, 2023). Segmentation (e.g., separating work and personal accounts), prioritisation (determining which messages or tasks warrant attention), and distancing (e.g., turning off notifications) help self-regulate after-hours connectivity (Aljabr, 2022), while controlling alerts and pop-ups reduces cognitive load and supports sustained focus (Berger, 2024). Finally, supporting staff in managing notifications and interruptions, for example, through effective mentoring (Riforgiate, 2025), can promote healthier digital habits, helping to reduce stress while improving overall well-being and productivity (Berger, 2024).

Methodology

This study builds on our earlier work, which identified four demographic groups based on evidence that techno-stress factors differ by age and sex (Hsieh, 2020, Hauk, 2019): females aged 18–39 years, males aged 18–39 years, females aged 40 years and above, and males aged 40 years and above. Sex-based and age-related differences in neurological processes - particularly the gradual reduction of dopamine receptor availability over time and associated risk–reward mechanisms, as well as the transition from fluid to crystallised intelligence (Kankam, 2025) - contribute to differential patterns of security behaviour and decision-making. Cognitive divergence typically occurs around 35–40 years of age (Horn, 1967, 1982), with stress levels peaking during late adolescence and early adulthood (around 18 years) before declining near the age of 40 (Newport, 2009). Participants were recruited from a UK-based organisation specialising in project management consultancy and digital solutions within the critical infrastructure sector. Pregnant women were excluded from participation.

In this study, the demographic structure remains consistent with the prior work; however, age categories have been refined to 18–29 years, 30–39 years, and 40 years and above. This adjustment reflects evidence from the initial study indicating notable cognitive and behavioural differences within the 30–39 age range, potentially associated with the emergence of crystallised intelligence, as well as observable contrasts between the 18–29 cohort and older participants. In the older group, risk aversion appeared to stem from accumulated prior experience, which led to reduced engagement in risky behaviours when tasks involved domains participants were familiar with. In earlier work, this was tested using an AI-related question that intentionally removed prior knowledge of AI-mediated breaches, revealing how participants caution changed when experience could no longer guide judgement. However, a corresponding drawback was a noticeable reduction

in agility, namely older participants tended to "think before they jump", which is a pattern consistent with age-related neurobiological changes, including the gradual decline in dopamine receptor density. In addition to age and sex, we used an additional demographic variable of job type classified as either occupying digital/IT roles or non-digital/IT roles. This was also informed by previous findings showing that occupational expertise bias responses in the AI-related tasks.

The current study employed a mixed-methods approach to both designing and evaluating proposed actions to improve cyber security engagement within the participating company. These are directly aligned with the barriers identified previously and co-developed with organizational stakeholders through participatory workshops, leveraging several design approaches as outlined in Table 1. The rollout follows a randomized design and will be assessed using pre- and post-surveys, behavioural audits (e.g., login hygiene, phishing response), and focus groups, allowing for comprehensive understanding of behavioural, emotional, and cognitive responses and outcomes across age and sex groups.

Table 1: Design approaches used in the study with justification grounded in SDT

Approach	**Justification**
Design Thinking Empathy-driven design	Users are central to the empathy and testing phases, which ensures the final product is usable, relevant, and trusted. Designing with empathy enhances users' sense of self-efficacy. When users feel understood and supported, they are more likely to engage with and trust cyber security systems.
Inclusive design	Addressing emotional barriers can improve autonomy and competence. Tailoring strategies to demographic differences supports competence and relatedness. Meeting these needs foster deeper engagement and long-term motivation to adopt and maintain secure behaviours.
User-centred design	Systems should be designed to align with users' capabilities, constraints, and real-world contexts, enhancing both usability and accessibility.
Participatory design	Involving stakeholders early through co-design ensures interventions are relevant and accepted. This approach supports autonomy, competence, and relatedness.

Results

Our initial study (Burd, 2025) revealed that:

- Employees lacked clarity about their personal cyber-security responsibilities.
- Techno-invasion concerns were especially pronounced among women.
- Training engagement varied significantly by age and sex.
- Frustration with updates and lack of support hindered compliance.

These findings informed a set of practical recommendations, including tailored training, empathetic feedback, and privacy-respecting monitoring policies. Following from this, we co-created human-centred actions/interventions, as outlined and categorised in Table 2. Specific impacts to date include reset/re-onboard iPhones, deployment of Teams via Mobile Device Management (MDM), peer mentoring networks, digital boundary agreements, work-life separation kits, and accessible performance dashboard, to name a few.

Excessive cognitive demands divert limited mental resources away from essential tasks, impairing users' ability to follow security procedures effectively; therefore, security controls should not exceed users' mental processing capacities (Pfleeger, 2012). Simplifying interfaces and instructions

to match users' cognitive capacities, such as reducing unnecessary steps, minimising ambiguity, and designing clear, low-effort workflows, can significantly improve security outcomes and adherence to protective behaviours (Pfleeger, 2012). Resetting and re-onboarding devices reduces digital clutter and lowers hypervigilant stress responses triggered by constant connectivity, improving cognitive recovery (Bondanini, 2025). Digital boundary agreements and structured tools help reinforce clear distinctions between work and home, which enhances productivity (Park, 2011), helps detach and recover from work demands (Berger, 2023), and reduces strain-based spillover (Berger, 2023, Chen, 2009). Moreover, work-family practices reduce work-family conflict but only *if* employees feel they can control their boundaries (Geraldes, 2025). Standardised deployments of communication tools reduce overload and support predictable workflows, which are linked to lower psychological strain and fewer boundary intrusions (Arnold, 2023). Meanwhile, supportive interpersonal relationships and trusting interactions, such as those fostered within peer-mentoring networks, promotes adaptive coping by enhancing psychological meaningfulness, safety, and availability (Barber, 2023). Finally, managers can provide relational support that buffers the negative effects of *work role overload, ambiguity* and *conflict,* including those of blurred boundaries (Kahn, 1990).

Table 2: Example interventions categorised by themes

Theme	**Action/Intervention**
Shared Responsibility	Cyber security Role Cards + "Security Champions"
Techno-Invasion	Digital Boundary Agreements + Privacy Workshops
Demographic Training	Age/Gender-Specific Microlearning Modules
Supportive Culture	Peer Mentoring + Empathetic Helpdesk Scripts
Positive Reinforcement	Gamified Dashboards + Anonymous Audit Reports
UX Balance	Frustration Logging Tool + Feature-Enhanced Updates
Support Resources	Rapid IT Hotline + Self-Service Portal

The following sections describe two key initiatives implemented within this study alongside a case study illustrating the successful prevention of a Business Email Compromise (BEC) attack. The two initiatives include the phishing-competition to improve security awareness and engagement, and the mobile-device redesign to support work–life balance. Each initiative integrates multiple actions/interventions, while the case study demonstrates early benefits of adopted approaches. As this is an ongoing study, evaluation results were not yet available at the time this research was published.

The phishing competition

The phishing competition initiative included a series of interconnected activities designed to enhance user engagement, strengthen security awareness, and embed a more collaborative and empowered organisational cyber-security culture as follows.

- **Responsibility and Engagement:** To promote shared responsibility and engagement in organisational security, users were actively involved as contributors to the training process. This was achieved by introducing a competition in which participants proposed realistic phishing email scenarios. The secondary aim was to make the training more authentic, relatable, and grounded in everyday organisational experience, alongside strengthening employees' ability to recognise and think critically about social-engineering tactics.

- **Tailored Training:** Users who failed the phishing exercise were provided with targeted, non-technical training intended to build confidence and reduce feelings of stigma. Training was delivered in several formats to accommodate diverse preferences and learning needs. Options included one-to-one discussions with cyber security staff in a private, supportive environment; group "lunch and learn" sessions that enabled collaborative inquiry; and short instructional videos supplemented with references for further independent study. Opportunities to engage with cyber security personnel for follow-up questions were made available across all formats.
- **Anonymised Feedback and Collective Learning:** Anonymised results from the exercise were presented to employees through team briefings or lunch-and-learn sessions. These feedback sessions explained the structure of the phishing test, analysed common reasons for user error, demonstrated effective methods for identifying similar attacks in the future, and included Q&A to support learning.
- **Security Champion:** To reinforce positive engagement, the participant who proposed the winning phishing scenario was recognised as a "Security Champion." This individual received a small reward and was invited to present their idea during the anonymised feedback session. Additionally, they participated in the production of an in-house phishing awareness video based on their scenario. The exercise will be repeated in future programme cycles. The aim is to empower selected employees to act as local advocates, role models, and communication bridges for cyber-security within their teams.
- **Performance Dashboard:** A publicly accessible dashboard displaying anonymised results of the latest phishing exercise alongside historical data was provided to allow employees to track the effectiveness of phishing awareness interventions over time. This transparency aimed to encourage continued improvement and normalise participation in organisational cyber security practices.

The process flow for the phishing competition is shown in Figure 1.

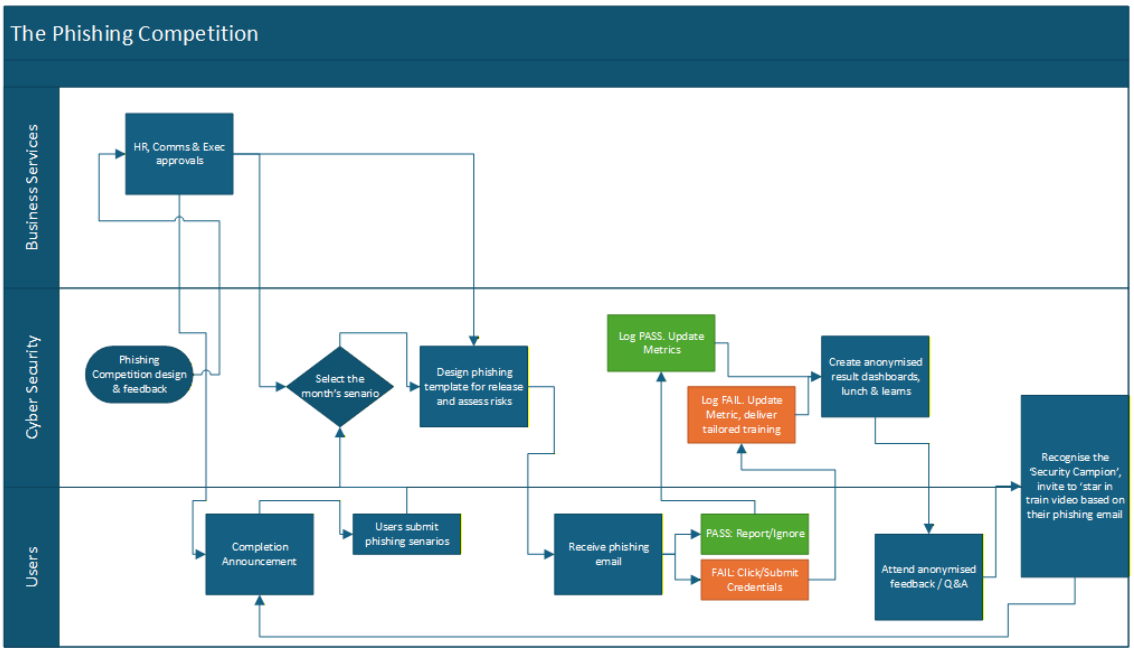

Figure 1: Phishing competition

Mobile device redesign

One of the stressors identified in the original study concerned the use of personal mobile phones for work-related communication. Participants reported a sense of being unable to disconnect from their professional responsibilities, as they remained contactable outside of working hours. Several participants expressed that this blurred boundary between work and personal time contributed significantly to their perceived inability to "switch off" after work. One participant stated:

> *"I have a work phone and a personal phone. I think they should be separate for mental health reasons. So, you can switch off."*

In practice, organisational budget constraints mean that not all employees can be issued a dedicated work mobile phone. Furthermore, several employees indicated that they did not wish to carry multiple devices, chargers, and associated accessories. To address these challenges, a redesigned approach to mobile-device management was implemented. An overview of this approach and its user-controlled features is shown in Figure 2.

Under the new model, existing configurations on users' devices were removed, and updated licences and profiles were deployed via the organisation's MDM system. The revised configuration provides each user with a separate work telephone number delivered through Microsoft Teams. This number can be assigned a distinct ringtone, enabling users to differentiate easily between personal and work-related calls on a Bring-Your-Own-Device (BYOD) handset. In addition, Teams, email, and other work-related applications can be configured to display the user as "offline" outside contracted working hours or during periods of leave. During these times, work calls are automatically directed to voicemail, and email notifications are silenced, while the device's personal number remains fully active. Consequently, users can continue to receive personal calls or, where they have chosen to share their primary number, be contacted in emergencies without compromising boundaries between work and personal life. The redesign also differentiates between Apple's Volume Purchase Programme (VPP), which applies to corporate-owned devices, and the use of publicly available application licences for BYOD environments. In the latter case, users are provided with guidance on how to configure the required applications securely.

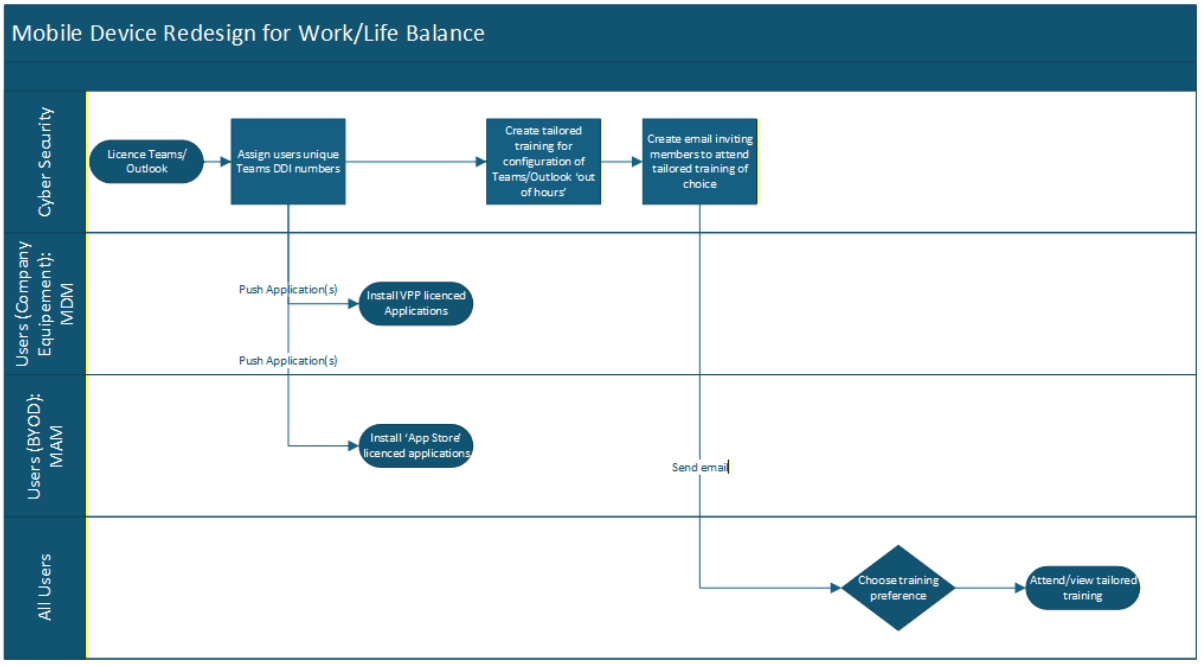

Figure 2: Mobile device redesign

BEC case study: Humans as the solution

To deliver a more personalised and responsive cyber security service, the organisation internalised its service desk function and staffed it with security personnel. This restructuring enabled users to directly contact cyber security professionals quickly and without intermediaries, while also providing a supportive environment in which employees could discuss potential security concerns without apprehension. The arrangement further allowed security staff to become recognised, trusted experts within the organisation who could respond to user queries promptly and in accessible, non-technical language. This initiative has already demonstrated tangible benefits, particularly in the early identification of security incidents that might otherwise evade technical detection mechanisms. Namely, users receive routine training on recognising phishing attempts, including indicators such as emails from unfamiliar senders, suspicious domains, or unverified embedded links. However, in BEC attacks, adversaries commonly gain access to legitimate email accounts and issue messages that appear entirely genuine, including accurate signatures and established communication styles. Such an incident occurred in 2025, when several employees received an email containing a link to a quotation originating from an external supplier. The attacker likely used a distribution list held at the originating company that had the compromised email account.

When attempting to access the quote, the user's login attempt failed. Reflecting on the incident, one user noted that the credentials should not have failed and that the invoice appeared earlier than expected. Experiencing a sense of unease, the user immediately contacted the service desk to report the issue. Subsequent security analysis of the email indicated no characteristics typically associated with phishing, and the message originated from the legitimate sender and expected company domain. The only anomaly identified was that the hyperlink directing the user to the quotation appeared suspicious. Consequently, the user's sign-in logs were examined and the organisation's geo-location blocking controls showed that attempted logins from a non-approved country had been successfully blocked. Early reporting enabled a rapid response, while existing technical safeguards provided additional time to prevent a potential security breach. Approximately one hour passed between the first click and the security response, during which the attack was successfully contained and remediated.

This case illustrates the critical role of human judgment as the first line of cyber defence. This includes recognising that not all phishing emails display obvious phishing indicators, as well as the importance of users' intuitive "gut-feeling" in detecting malicious activity. The BEC example was shared across the organisation to reinforce that employee vigilance is a critical component of the organisation's cyber defences, and to reaffirm that employees' proactive contributions to collective resilience are openly appreciated and acknowledged by the security team.

Closing remarks

This research contributes towards empathy-driven, inclusive, and co-created cyber-security strategies that recognise users' capabilities, limitations, and lived experiences, while acknowledging the complexity of real-world organisational dynamics. Across the implemented actions, the overarching outcomes centre on the re-establishment of digital boundaries and the enhancement of perceived autonomy and emotional resilience in navigating technological demands. Creating healthier technology-related working conditions helps reduce techno-stressors, while simplifying interfaces and instructions can strengthen overall security outcomes. Effective cyber-security strategies must also address the emotional and demographic factors that shape user engagement, tailoring approaches to differences in age, gender, and digital literacy to strengthen users' sense of competence and encourage secure behaviour.

References

Aljabr, N., Chamakiotis, P., Petrakaki, D. and Newell, S., 2022. After-hours connectivity management strategies in academic work. *New Technology, Work and Employment*, *37*(2), pp.185-205. https://doi:10.1111/ntwe.12217

Amstad, F.T., Meier, L.L., Fasel, U., Elfering, A. and Semmer, N.K., 2011. A meta-analysis of work–family conflict and various outcomes with a special emphasis on cross-domain versus matching-domain relations. *Journal of Occupational Health Psychology*, *16*(2), pp.151-169. https://doi:10.1037/a0022170

Arnold, M., Goldschmitt, M. and Rigotti, T., 2023. Dealing with information overload: a comprehensive review. *Frontiers in Psychology*, *14*, p.1122200. https://doi.org/10.3389/fpsyg.2023.1122200

Barber, L.K., Kuykendall, L.E. and Santuzzi, A.M., 2023. How managers can reduce "always on" work stress in teams: An optimal work availability framework. *Organizational Dynamics*, *52*(3), p.100992. https://doi:10.1016/j.orgdyn.2023.100992

Berger, D.L., 2023. Does work-life boundary management improve work-life balance for remote workers: A critically appraised topic. *Engaged Management Review*, *7*(1), p.2. https://doi.org/10.28953/2375-8643.1128

Berger, M., Schäfer, R., Schmidt, M., Regal, C. and Gimpel, H., 2024. How to prevent technostress at the digital workplace: a Delphi study. *Journal of Business Economics*, *94*(7), pp.1051-1113. https://doi:10.1007/s11573-023-01159-3

Bondanini, G., Giovanelli, C., Mucci, N. and Giorgi, G., 2025. The Dual Impact of Digital Connectivity: Balancing Productivity and Well-Being in the Modern Workplace. *International Journal of Environmental Research and Public Health*, *22*(6), p.845. https://doi:10.3390/ijerph22060845

Burd, A, and Titis, E., 2025. From Boomers to Zoomers: Cyber Security Behaviours in an AI Era. In *International Conference on Artificial Intelligence, Computer, Data Sciences and Applications (ACDSA)*, (pp.1-6). IEEE. https://doi/10.1109/ACDSA65407.2025.11166114

Chen, Z., Powell, G.N. and Greenhaus, J.H., 2009. Work-to-family conflict, positive spillover, and boundary management: A person-environment fit approach. *Journal of Vocational Behavior*, *74*(1), pp.82-93. https://doi:10.1016/j.jvb.2008.10.009

Farivar, F. and Richardson, J., 2021. Workplace digitalisation and work-nonwork satisfaction: the role of spillover social media. *Behaviour & Information Technology*, *40*(8), pp.747–758. https://doi.org/10.1080/0144929X.2020.1723702

Gangire, Y., Da Veiga, A. and Herselman, M., 2019. A conceptual model of information security compliant behaviour based on the self-determination theory. In: *2019 Conference on Information Communications Technology and Society (ICTAS)*, (pp.1–6). IEEE https://doi:10.1109/ICTAS.2019.8703629

Geraldes, D.T., Chambel, M.J. and Carvalho, V.S., 2025. Work-family practices and work-family relationship: the role of boundary management. *BMC Public Health*, *25*(1), pp.1-14. https://doi.org/10.1186/s12889-025-22512-x

Hauk N, Göritz A.S. and Krumm S., 2019. The mediating role of coping behavior on the age-technostress relationship: A longitudinal multilevel mediation model. PLoS ONE 14(3): e0213349. https://doi.org/10.1371/journal.pone.0213349

Horn, J.L. and Cattell, R.B., 1967. Age differences in fluid and crystallized intelligence. *Acta Psychologica, 26*, pp.1–23.

Horn, J.L., 1982. The Theory of Fluid and Crystallized Intelligence in Relation to Concepts of Cognitive Psychology and Aging in Adulthood. In: Craik, F.I.M., Trehub, S. (eds) Aging and Cognitive Processes. Advances in the Study of Communication and Affect, vol 8. Springer, Boston, MA. https://doi.org/10.1007/978-1-4684-4178-9_14

Hsieh, Y.C., Tsai, W.C. and Hsia, Y.C., 2020. A Study on Technology Anxiety Among Different Ages and Genders. In: Gao, Q., Zhou, J. (eds) Human Aspects of IT for the Aged Population. Technology and Society. HCII 2020. Lecture Notes in Computer Science, vol 12209. Springer, Cham. https://doi.org/10.1007/978-3-030-50232-4_17

Joy, S. and Arun Kumar, A., 2024, December. Evaluating Technostress: Work-Life Balance and Well-Being in Varied Work Contexts. In *International Conference on Leveraging Emerging Technologies and Analytics for Development* (pp. 83-101). Singapore: Springer Nature Singapore. https://doi:10.1007/978-981-96-8582-0_5

Kahn, W.A., 1990. Psychological conditions of personal engagement and disengagement at work. *Academy of Management Journal, 33*(4), pp.692–724. https://doi.org/10.2307/256287

Kankam, H., 2025. Cognitive Development and Aging. In: A Brief Excursion into Human Cognition. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-89752-8_12

Kossek, E.E., 2016. Managing work-life boundaries in the digital age. *Organizational Dynamics*, *45*(3), pp.258-270. https://doi.org/10.1016/j.orgdyn.2016.07.010

La Torre, G., Esposito, A., Sciarra, I. and Chiappetta, M., 2019. Definition, symptoms and risk of techno-stress: a systematic review. *International Archives of Occupational and Environmental Health*, 92(1), pp.13–35. https://doi.org/10.1007/s00420-018-1352-1

Liţan, D.E., 2025. Psychological "effects" of digital technology: a meta-analysis. *Frontiers in Psychology*, *16*, p.1560516. https://doi:10.3389/fpsyg.2025.1560516

Newport, F. and Pelham, B.W., 2009. *Don't worry, be 80: Worry and stress decline with age*. Retrieved at http://www.gallup.com/poll/124655/dont-worry-be-80-worry-stress-decline-age.aspx

Ohly, S. and Bastin, L., 2023. Effects of task interruptions caused by notifications from communication applications on strain and performance. *Journal of Occupational Health*, *65*(1), p.e12408. https://doi.org/10.1002/1348-9585.12408

Park, Y., Fritz, C. and Jex, S.M., 2011. Relationships between work-home segmentation and psychological detachment from work: The role of communication technology use at home. *Journal of Occupational Health Psychology, 16*(4), pp.457-467. https://doi.org/10.1037/a0023594

Pfleeger, S.L. and Caputo, D.D., 2012. Leveraging behavioral science to mitigate cyber security risk. *Computers & Security*, *31*(4), pp.597-611. https://doi:10.1016/j.cose.2011.12.010

Riforgiate, S.E., Ruh, C., Ibiwoye, C., Zinia, J.F. and Nartey, G.M., 2025. Mentoring in and Across Work Organizations. *Encyclopedia*, *5*(4), p.169.

Uslu, O., 2025. Understanding digital wellbeing: impacts, strategies, and the path to healthier technology practices. *Discov Soc Sci Health* 5, 145. https://doi.org/10.1007/s44155-025-00259-5

Yener, S., Arslan, A. and Kilinç, S., 2021. The moderating roles of technological self-efficacy and time management in the technostress and employee performance relationship through

burnout. *Information Technology & People*, *34*(7), pp.1890–1919. https://doi.org/10.1108/ITP-09-2019-0462