Transformation Learning Theory for Cyber Security

Monica T Whitty

Monash University, Melbourne 3800, Australia
monica.whitty@monash.edu

Abstract. This paper builds on Sasse's significant work in cyber security, with a focus on adult cyber security education. In line with Sasse, the paper critiques traditional compliance-driven, one-size-fits-all cybersecurity training methods. It introduces the Transformative Learning Theory as a framework for rethinking cybersecurity education, focusing on how adults might critically reassess assumptions, develop judgement under uncertainty, and integrate safer behaviours into everyday practice. The paper discusses the inadequacies of information-deficient models of behaviour change and the failure of fear-based motivational strategies. It emphasises the importance of understanding users' mental models of risk, responsibility, and accountability, and the need for supportive, human-centred intervention design. By applying Transformative Learning Theory, the paper proposes a shift from rule-based awareness and compliance towards critical reflection, sensemaking, and perspective change. This approach aims to foster durable, internally motivated behaviour change, thereby creating a more secure digital environment by empowering users to make informed decisions and integrate safer behaviours into their everyday lives.

Keywords: Human Factors in Cyber Security, Transformation Learning Theory, Cyber Security education

1 Introduction

For decades, humans have been blamed for being the 'weakest link' in cyber security. This paper advances an alternative perspective, arguing that humans are better understood as the last line of defence. Over more than 25 years, Sasse's influential body of work has challenged scholars and practitioners to recognise that 'users are not the enemy' and that responsibility lies with cybersecurity professionals to design usable security that supports and protects users, rather than expecting users to adapt to systems that are opaque, counterintuitive, or

unnecessarily complex. Her work has further demonstrated the limitations of attempting to 'train away' noncompliance with security policies. It is this latter insight, concerning the inadequacy of compliance-driven training, that this paper explicitly builds upon. This paper argues that improving cyber security behaviour among adults requires a fundamental shift in how education is conceptualised. Beyond the excellent and substantial contributions of Sasse and her colleagues, this paper contends that cyber security research and practice should explicitly incorporate adult education theory to improve cyber security learning and behaviour.

2 Background of Sasse's and her Contemporaries' Research

Adams and Sasse's seminal 'Users are not the enemy' paper reframed organisational information security failures as predictable outcomes of misaligned design and governance, rather than as user irrationality or laziness [2]. Drawing on empirical observation of workplace practice, they argued that security controls often impose disproportionate cognitive and time costs (e.g., frequent password changes, multiple credentials, confusing terminology, brittle procedures), which predictably drives workarounds as employees prioritise primary job tasks and productivity over abstract security goals. Their central contribution was to treat 'non-compliance' as a usability and organisational fit problem: users circumvent controls when mechanisms are hard to execute correctly, when policies conflict with real workflows, and when security teams communicate poorly (or punitively), undermining understanding, trust, and sustained engagement.

Follow-up work by Sasse and colleagues extended this argument into a broader 'usable security' programme: rather than treating humans as the weakest link to be constrained, security should be engineered as a socio-technical system that supports task completion and makes secure behaviour the easiest, most reliable path. In their paper, 'Transforming the weakest link', Sasse et al. challenged cyber security designers, arguing that they need to "identify the causes of undesirable user behaviour, and address these in design effective security systems" [26, p. 122]. Subsequent research further elaborated the organisational dimension of this problem by showing that security behaviour is shaped not only by interface design but also by users' mental models of risk, responsibility, and accountability. Sasse and Flechais argued that users' security decisions are embedded within complex social and organisational contexts, where responsibility for security is often ambiguous and risks are poorly communicated [27].

In their influential 'compliance budget' model, Beautement et al. showed that employees have a finite capacity to comply with security demands, and that excessive or poorly prioritised requirements lead to disengagement, routinised box-ticking, or deliberate circumvention rather than genuine security improvement [6]. From this perspective, awareness programmes that emphasise rule adherence without addressing competing task demands, incentives, and usability constraints risk exhausting users' limited compliance resources without

improving security outcomes. More recent work reinforced this critique by showing that compliance-driven approaches implicitly frame users as liabilities rather than competent agents, undermining trust and discouraging proactive security behaviour [13].

In later work in cyber security compliance, 'stealth approaches' have been designed by researchers. In this approach, security controls are designed to improve security without requiring users to consciously change their behaviour or feel burdened by security demands. According to this approach, rather than attempting to 'train away' noncompliance, organisations should select and justify security controls using models that explicitly incorporate user productivity impacts and willingness to comply, thereby identifying controls that are workable in context [22]. In Parkin et al.'s research, security managers were invited to discuss with the researchers' mock-up tool prototypes that embodied the 'stealth' approach. Their work developed a tool to help visualise the mechanisms and their trade-offs. In complementary work that also took the same stance [14], it is argued that usability is necessary but not sufficient. Kirlappos and Sasse (2014) contend that compliance is also shaped by whether organisations trust and engage employees as competent agents. This work emphasised shifting from restrictive, distrust-based security to approaches that support informed judgement, shared responsibility and meaningful involvement, because mechanisms that users experience as illegitimate, obstructive or unfair invite avoidance.

As a final and non-trivial point, Sasse later critiqued fear- and shame-based awareness approaches, arguing that 'scaring and bullying' does not reliably produce secure behaviour and can degrade trust, motivation, and reporting [25]. This, in part, explains why victims of cyber scams feel shamed and blamed for the crime [33]. This perspective also reinforces the need for supportive, human-centred intervention design rather than adversarial compliance campaigns.

3 Cyber Security Education and Awareness Campaigns

Cyber security awareness campaigns and educational initiatives are widely adopted as primary mechanisms to improve users' security behaviour. Governments, organisations, and industry bodies invest heavily in training programmes, public messaging, and awareness materials to reduce cyber risk. However, despite decades of effort, evidence suggests that such interventions often fail to produce sustained behavioural change [38,5,20]. While campaigns may improve knowledge or awareness, they rarely translate into consistent, secure practices [35].

3.1 Information-deficient Models of Behaviour Change

The main criticism of cyber security campaigns is their continued reliance on information-deficient models of behaviour change. Many campaigns assume that insecure behaviour stems from a lack of knowledge and that providing information about threats and protective actions will naturally lead to safer behaviour. Yet research in psychology and risk communication shows that knowledge alone

is a poor predictor of action [10,3]. As Bada et al. note, awareness campaigns frequently conflate knowing with doing, overlooking the structural and contextual constraints that shape everyday security decisions [5].

3.2 Decision-making

Another reason for failure lies in how cyber security education frames decision-making. Many campaigns emphasise rule compliance and static 'best practices' rather than fostering understanding and judgement. Prescriptive guidance, such as blanket warnings against clicking links or sharing information, fails to account for the complexity of contemporary digital environments, where malicious and legitimate communications are often indistinguishable [24,34]. Research shows that users rely on heuristics, trust cues, and contextual signals when making decisions under uncertainty and time pressure [23], and this also applies to cyber security decision-making [35,34,39]. When education fails to engage these cognitive processes or to explain the underlying logic of threats, users are poorly equipped to adapt to novel attacks, including sophisticated phishing and social engineering.

3.3 Motivation

Cyber security campaigns also frequently fail because of how motivation is addressed. Many rely on fear appeals that emphasise worst-case outcomes, such as financial loss or identity theft [25]. While fear can increase attention, extensive evidence from protection motivation and risk communication research shows that fear appeals are ineffective when individuals lack perceived control or self-efficacy [9,12]. In cyber security contexts, users often perceive threats as unavoidable or beyond their personal influence, which can lead fear-based messaging to produce avoidance, disengagement, or fatalism rather than protective action.

3.4 Optimism Bias/Illusion of Vulnerability

Further complicating the effectiveness of cyber security training is the well-documented optimism bias, often referred to as an 'illusion of vulnerability', whereby individuals systematically underestimate their own likelihood of experiencing harm relative to others [16,36]. Research in cognitive and social psychology shows that individuals consistently believe they are less likely than others to experience negative events, even when they acknowledge the general prevalence of risk [31]. In cyber security contexts, this bias manifests as a belief that cyber-attacks, scams, or data breaches are problems that happen to 'other people' [37]. As a result, training messages that emphasise the general prevalence of threats may increase abstract awareness but fail to motivate personal protective action.

3.5 One Size Fits All

As a final point, a persistent weakness in cyber security training and awareness programmes is the assumption that users are a homogeneous group. Cyber security education is often delivered through one-size-fits-all campaigns that fail to account for differences in digital literacy, experience, cognitive capacity, cultural context, and exposure to exposure. Campaigns that ignore this diversity risk being irrelevant, inaccessible, or mistrusted, particularly among groups that are disproportionately targeted by cybercrime.

4 Educating humans in Cyber Security – Drawing from Theories and Research in Adult Education

Although cyber security researchers increasingly acknowledge the existence of a digital divide [1], comparatively little attention has been paid to how cyber security education should be designed differently for children and adults. This gap is particularly striking given that most cyber security training and awareness initiatives target adult populations in workplaces and communities. In response, this paper argues for the utility of Mezirow's Transformative Learning Theory [19] as a theoretically grounded framework for adult cyber security education, offering a pathway to move beyond compliance-based training toward approaches that foster critical reflection, meaning-making and durable behavioural change.

4.1 Adult Education and Transformational Learning Theory

Until the 1970s, adult learning was considered equivalent to educating children. Knowles' work on 'andragogy' shifted scholarly thinking about adult learning, distinguishing it from child-focused education. Andragogy has six assumptions: (a) self-directedness, (b) need to know, (c) use of experience in learning, (d) readiness to learn, (e) orientation to learning, and (f) internal motivation [15,7]. According to Knowles, adults are self-directed learners who bring a wealth of life experiences to the learning process, which serve as valuable resources for building new knowledge. Knowles defined the art and science of adult learning, emphasising the importance of autonomy, practical application, and experiential learning [15,8]. Despite its utility, andragogy has been criticised for oversimplifying the diversity of adult learners and failing to account for cultural, content, and individual differences [28].

Since Knowles' time, scholars have reworked his principles to develop the 'Transformative Learning Theory' (Mezirow, 2018). This theory posits that adults learn by critically reflecting on their experiences, challenging their assumptions, and ultimately transforming their perspectives and understanding of the world. The theory departs from behaviourist and cognitive models by conceptualising adult learning as a process of meaning transformation rather than knowledge acquisition alone [19,17,18]. At its core, transformative learning involves revising deeply held assumptions, beliefs, and perspectives, which Mezirow termed

meaning perspectives, that shape how individuals interpret the world and guide their actions.

Transformative Learning Theory assumes that adults learn in fundamentally different ways from children. Unlike children, whose learning is often guided by developmental readiness and structured around the gradual accumulation of foundational knowledge, adults do not approach education as blank slates. Instead, they bring accumulated life experiences, established belief systems, and socially embedded assumptions that actively shape how new information is interpreted and evaluated. Whereas dominant child learning theories, such as behaviourist and constructivist approaches, typically emphasise knowledge acquisition, skill formation, and guided scaffolding, adult learning is less about absorbing new information and more about revising existing frames of reference in response to experience.

4.2 Disorienting Dilemma

In his earlier version of the Transformative Learning Theory, Mezirow argued that central to learning is the concept of a disorienting dilemma: an experience that disrupts frames of reference by exposing their inadequacy in explaining a new situation [19,17,18]. Such dilemmas may arise from personal crises, social change, or encounters with contradictory information. In response, learners engage in critical reflection, examining the origins, validity, and consequences of their assumptions. This reflective process is not merely introspective but evaluative, requiring individuals to question taken-for-granted norms, power relations, and habitual ways of thinking.

4.3 Transformation - Non-Linear Phases

A distinctive contribution of Mezirow's Transformative Learning Theory is its articulation of transformation as a phased, though non-linear process through which adults revise their frames of reference. Mezirow originally identified ten phases of perspective transformation beginning with a disorienting dilemma, as described above, which exposes a mismatch between existing assumptions and lived reality. This is followed by self-examination, often accompanied by emotional responses such as guilt, fear, or anxiety, and a critical assessment of previously unquestioned assumptions. As learners recognise that their difficulties are not solely personal but shared by others, they engage in discourse that validates alternative viewpoints and supports the reconstruction of meaning.

Subsequent phases involve exploring new roles, relationships, or actions; acquiring the knowledge and skills to enact these alternatives; and experimenting with provisional new behaviours. Over time, learners build competence and confidence in these new ways of acting, ultimately reintegrating their transformed perspectives into their lives. Importantly, Mezirow emphasised that these phases are not strictly sequential, as learners may move back and forth among reflection, dialogue, and action, and not all transformations involve all phases in a clearly delineated manner [18].

Later developments of this theory highlighted that transformative learning does not always require dramatic or singular disorienting dilemmas [19]. These developments refined the phased model by emphasising that transformative learning does not always require such dramatic or singular disorienting dilemmas. Mezirow acknowledged that transformation can also emerge from incremental or cumulative experiences, where repeated inconsistencies between expectations and outcomes gradually prompt critical reflection [19]. This refinement broadened the applicability of the theory to professional and workplace learning contexts, where transformation often unfolds over time rather than through acute crises. Additionally, scholars have emphasised that the emotional and relational dimensions of these phases are as significant as the cognitive ones, with trust, dialogue, and social support playing a critical role in sustaining reflection and change [29].

5 Applying Transformational Learning Theory to Cyber Security

Mezirow's theory has been mainly applied in healthcare education, where computer simulations have been developed to simulate complex patient scenarios. According to the theory, reflective debriefing sessions integrated into these simulations are essential for fostering perspective transformation among participants. For instance, Almomani et al. demonstrated that reflective learning conversations in healthcare simulations enhanced clinical reasoning and empathy among participants [4]. Similarly, Gum et al. (2010) found these training techniques helpful for the midwives, doctors and nurses who participated in their study [11].

To date, Mezirow's Transformation Learning Theory has received limited application in the cyber security education and training literature. At the time of writing, the few studies that explicitly draw on this theoretical framework are largely confined to computer-based simulation training. For example, Ncube et al. explored the potential of Transformative Learning Theory to inform the design of gamified cyber security education, highlighting its suitability for supporting reflection and perspective change in adult learners [21]. Similarly, Whitty et al. (2025) applied Mezirow's theory to develop a hybrid computer simulation to educate employees about insider threats [35]. Drawing explicitly on the principles of disorienting dilemmas, critical reflection, and reflective action, their study demonstrated that learners engage with transformative processes in different ways. While some participants were more inclined towards self-reflection on their own assumptions and behaviours, others were more likely to adopt the perspective of 'the other', underscoring the importance of incorporating multiple reflective pathways into learning design.

This paper argues that Transformative Learning Theory is relevant to adult cyber security education beyond the use of computer simulations. Specifically, it proposes that applying this theory enables a shift from rule-based awareness and compliance towards critical reflection, sensemaking, and perspective change. The theory suggests unsafe behaviour is driven by ingrained views on risk, trust, re-

sponsibility, and vulnerability, not ignorance. Cyber security education informed by transformative learning may aim to challenge and revise these assumptions so that safer behaviour becomes internally motivated and durable rather than externally enforced.

In cyber security, a disorienting dilemma may arise when an adult encounters information or experiences that contradict their existing beliefs; for example, realising that highly educated, cautious people are frequently victimised by sophisticated phishing or investment scams [32,30]. Many adults hold implicit assumptions such as "I would notice a scam" or "only naïve users get hacked". Transformative learning interventions could deliberately challenge these assumptions by presenting credible evidence, narratives, or simulations that expose misjudgements. Crucially, this should not be done through fear or blame, but through structured reflection that invites learners to examine why they believed they were personally safe and how those beliefs were formed. Following this disruption, learners could be guided to reflect critically on their decision-making processes. In cyber security training, this might involve analysing past near-miss experiences (e.g., emails almost clicked, passwords reused), identifying heuristics such as trust in authority cues or overconfidence, and discussing how time pressure or workplace norms influence behaviour. Dialogue with peers could play a central role at this stage, as adults come to recognise that their assumptions are socially shared rather than idiosyncratic, reducing shame and defensiveness while enabling collective sensemaking. Subsequent phases could focus on exploring and experimenting with new understandings and behaviours. This type of training may help users make slower decisions under uncertainty, verify requests through secondary channels, or recognise cues of emotional manipulation. Learners could then practice these strategies in realistic scenarios, gradually building confidence and competence. Over time, safer behaviour may be reintegrated into everyday routines, supported by a transformed understanding of cybersecurity as an ongoing judgement task rather than a checklist of rules.

Notably, Mezirow's Transformational Learning Theory addresses the 'one size fits all' problem highlighted earlier in this paper by recognising that adults interpret risk and learning through diverse experiences, beliefs, and social contexts. Rather than assuming uniform responses to rules or awareness messages, the theory focuses on how individuals critically reflect on their own assumptions about cybersecurity and reconstruct meaning in ways that are personally relevant. Transformative Learning Theory can enable cybersecurity education that accommodates user diversity.

5.1 Hypothetical Example

A hypothetical example may help to illustrate the potential of Mezirow's Transformational Learning Theory to cyber security training. Consider an adult workplace training program addressing phishing. Instead of beginning with "do not click suspicious links", the programme starts with anonymised case studies showing experienced professionals falling victim to well-crafted spear-phishing emails. This creates a disorienting dilemma by challenging the belief that competence

alone confers safety. Participants then reflect on how they personally assess email legitimacy, discussing factors such as trust in internal branding, urgency cues, or workload pressures. Through facilitated discussion, they recognise shared vulnerabilities and critically reassess their assumptions about personal risk. The training then introduces adaptive strategies, such as deliberate pause techniques and verification norms, allowing users to practice these in simulated environments. Over time, participants report not only improved detection, but a fundamental shift in how they conceptualise cyber security risk: from something that happens to 'others' to an ongoing, reflective practice embedded in everyday work.

6 Conclusions

In conclusion, this paper builds on the excellent work of Sasse and her colleagues to argue that improving cybersecurity behaviour among adults requires a fundamental shift in educational approaches. In line with Sasse, it is argued that traditional compliance-driven training methods are inadequate and that a more holistic, human-centred approach is needed. It is proposed that the Transformative Learning Theory offers a promising framework for rethinking cyber security education, focusing on critical reflection, sensemaking, and perspective change. By challenging deeply embedded assumptions and fostering a deeper understanding of cybersecurity risks, this approach can lead to more durable and internally motivated behaviour change. Ultimately, the goal should be to create a more secure digital environment by empowering users to make informed decisions and integrate safer behaviours into their everyday lives.

References

1. Acheampong, D., Meso, P., Agyemang, I.O., Cudjoe, J.: Bridging the digital divide: Securing information and computer systems in an unequal world. In: Chigona, W., Kabanda, S., Seymour, L.F. (eds.) Implications of Information and Digital Technologies for Development. pp. 77–90. Springer Nature Switzerland, Cham (2024)
2. Adams, A., Sasse, M.A.: Users are not the enemy. Commun. ACM **42**(12), 40–46 (1999). https://doi.org/10.1145/322796.322806
3. Ajzen, I.: The theory of planned behavior. Organizational Behavior and Human Decision Processes **50**(2), 179–211 (1991). https://doi.org/10.1016/0749-5978(91)90020-T
4. Almomani, E., Sullivan, J., Saadeh, O., Mustafa, E., Pattison, N., Alinier, G.: Reflective learning conversations model for simulation debriefing: a co-design process and development innovation. BMC Medical Education **23**(1), 837 (2023). https://doi.org/10.1186/s12909-023-04778-0
5. Bada, M., Sasse, A.M., Nurse, J.R.: Cyber security awareness campaigns: Why do they fail to change behaviour? (2019), arXiv:1901.02672
6. Beautement, A., Sasse, M.A., Wonham, M.: The compliance budget: managing security behaviour in organisations. In: Proceedings of the 2008 New Security Paradigms Workshop. pp. 47–58. Association for Computing Machinery, Lake Tahoe, California, USA (2008). https://doi.org/10.1145/1595676.1595684

7. Chan, S.: Applications of andragogy in multi-disciplined teaching and learning. Journal of adult education **39**(2), 25–35 (2010)
8. Clair, R.S.: Andragogy: Past and present potential. New Directions for Adult and Continuing Education **2024**(184), 7–13 (2024). https://doi.org/10.1002/ace.20546
9. Dodge, C., Fisk, N., Burruss, G., Moule Jr, R., Jaynes, C.: What motivates users to adopt cybersecurity practices? a survey experiment assessing protection motivation theory. Criminology & Public Policy **22**, 849–868 (2023)
10. Fischhoff, B.: The sciences of science communication. Proceedings of the National Academy of Sciences **110**(supplement_3), 14033–14039 (2013). https://doi.org/10.1073/pnas.1213273110
11. Gum, L., Greenhill, J., Dix, K.: Clinical simulation in maternity (csim): interprofessional learning through simulation team training. Quality and Safety in Health Care **19**(5), e19 (2010). https://doi.org/10.1136/qshc.2008.030767
12. Jamil, H., Zia, T., Nayeem, T., Whitty, M., D'Alessandro, S.: Human-centric cyber security: Applying protection motivation theory to analyse micro business owners' security behaviours. Information and Computer Security **33**, 49–76 (2024)
13. Kirlappos, I., Beautement, A., Sasse, M.A.: "comply or die" is dead: Long live security-aware principal agents. In: Adams, A.A., Brenner, M., Smith, M. (eds.) Financial Cryptography and Data Security. pp. 70–82. Springer Berlin Heidelberg, Berlin, Heidelberg (2013)
14. Kirlappos, I., Sasse, M.A.: What usable security really means: Trusting and engaging users. In: Tryfonas, T., Askoxylakis, I. (eds.) Human Aspects of Information Security, Privacy, and Trust. pp. 69–78. Springer International Publishing, Cham (2014)
15. Knowles, M.S.: Andragogy: Adult learning theory in perspective. Community College Review **5**(3), 9–20 (1978). https://doi.org/10.1177/009155217800500302
16. Kononovich, V., Kononovych, I., Shvets, O.: Vulnerabilities of cyber security of technical intelligentsia in relation to social engineering. In: CEUR Workshop Proceedings. pp. 127–136 (2021)
17. Mezirow, J.: Transformative dimensions of adult learning. ERIC (1991)
18. Mezirow, J.: Learning to think like an adult. In: Learning as transformation: Critical perspectives on a theory in progress, pp. 3–33 (2000)
19. Mezirow, J.: Transformative learning theory. In: Contemporary theories of learning, pp. 114–128. Routledge (2018)
20. Nagyfejeo, E., Von Solms, B.: Why do national cybersecurity awareness programmes often fail. International Journal of Information Security and Cybercrime **9**, 18–27 (2020)
21. Ncube, Z.P., Mpofu, N., Nxumalo, M.A.: Transformative pedagogies: Educational innovations in cybersecurity. In: 2024 4th International Multidisciplinary Information Technology and Engineering Conference (IMITEC). pp. 442–445 (2024). https://doi.org/10.1109/IMITEC60221.2024.10851040
22. Parkin, S., Moorsel, A.v., Inglesant, P., Sasse, M.A.: A stealth approach to usable security: helping it security managers to identify workable security solutions. In: Proceedings of the 2010 New Security Paradigms Workshop. pp. 33–50. Association for Computing Machinery, Concord, Massachusetts, USA (2010). https://doi.org/10.1145/1900546.1900553
23. Petty, R.E., Cacioppo, J.T.: Communication and persuasion: Central and peripheral routes to attitude change. Springer-Verlag, New York (1986)

24. Redmiles, E.M., Malone, A.R., Mazurek, M.L.: I think they're trying to tell me something: Advice sources and selection for digital security. In: 2016 IEEE Symposium on Security and Privacy (SP). pp. 272–288 (2016). https://doi.org/10.1109/SP.2016.24
25. Sasse, A.: Scaring and bullying people into security won't work. IEEE Security & Privacy **13**(3), 80–83 (2015). https://doi.org/10.1109/MSP.2015.65
26. Sasse, M.A., Brostoff, S., Weirich, D.: Transforming the 'weakest link' — a human/computer interaction approach to usable and effective security. BT Technology Journal **19**(3), 122–131 (2001). https://doi.org/10.1023/A:1011902718709
27. Sasse, M.A., Flechais, I.: Usable security: Why do we need it? how do we get it? In: Cranor, L., Garfinkel, S. (eds.) Security and Usability: Designing secure systems that people can use. O'Reilly (2005)
28. Stancil, C.: So, do reusable assignments really benefit students? Journal of Open Educational Resources in Higher Education **3**(1) (2025). https://doi.org/10.31274/joerhe.17911
29. Taylor, E.W., Cranton, P.: The handbook of transformative learning: Theory, research, and practice. John Wiley & Sons (2012)
30. Taylor, J., Whitty, M.: Exploration of the awareness and attitudes of psychology students regarding their psychological literacy for working in the cybersecurity industry. Psychology Learning & Teaching **23**(2), 298–314 (2024). https://doi.org/10.1177/14757257231214612
31. Weinstein, N.D.: Unrealistic optimism about future life events. Journal of Personality and Social Psychology **39**(5), 806–820 (1980). https://doi.org/10.1037/0022-3514.39.5.806
32. Whitty, M.T.: Predicting susceptibility to cyber-fraud victimhood. Journal of Financial Crime **26**(1), 277–292 (2019). https://doi.org/10.1108/JFC-10-2017-0095
33. Whitty, M.T., Buchanan, T.: The online dating romance scam: The psychological impact on victims – both financial and non-financial. Criminology & Criminal Justice **16**(2), 176–194 (2016). https://doi.org/10.1177/1748895815603773
34. Whitty, M.T.: Drug mule for love. Journal of Financial Crime **30**(3), 795–812 (2023). https://doi.org/10.1108/JFC-11-2019-0149
35. Whitty, M.T., Abdulgalimov, D., Oliver, P., Ruddy, C., Seguin, J., Young, G.: Inside the threat matrix: Using hybrid computer simulations to educate adults on malicious insider threat and technology misuse. In: Moallem, A. (ed.) HCI for Cybersecurity, Privacy and Trust. pp. 298–312. Springer Nature Switzerland, Cham (2025). https://doi.org/10.1007/978-3-031-92833-8_18
36. Whitty, M.T., Moustafa, N., Grobler, M.: Cybersecurity when working from home during covid-19: considering the human factors. Journal of Cybersecurity **10**(1), tyae001 (2024). https://doi.org/10.1093/cybsec/tyae001
37. Whitty, M.: The scammers persuasive technique model: Development of a stage model to explain the online dating romance scam. British Journal of Criminology **53**, 665–684 (2013). https://doi.org/10.1093/bjc/azt009
38. Whitty, M.: Who can spot an online romance scam? Journal of Financial Crime **26**, 623–633 (2019). https://doi.org/10.1108/JFC-06-2018-0053
39. Whitty, M., Ruddy, C., Jamil, H.: Words matter: Applying the elaboration likelihood model to examine the persuasive cues evident in true and fake news about the 'indigenous voice to parliament'. In: Furnell, S., Clarke, N. (eds.) International Symposium on Human Aspects of Information Security and Assurance. Springer Nature Switzerland, Mytilene, Greece (2025). https://doi.org/10.1007/978-3-032-02504-3_24