A Human-Centric Review of Phishing Susceptibility Solutions and Literature

George Raywood-Burke[1,2,3] and Tiffany Campbell[1,4]

[1] Airbus Operations, The Quadrant, Celtic Springs Business Park, Newport, UK
[2] Human Factors Excellence Research Group, School of Psychology, Cardiff University, UK
[3] Centre for Artificial Intelligence, Robotics and Human Machine Systems, Cardiff University, UK
[4] School of Computing, Kennedy Building, University of Kent, UK
george.raywood-burke@airbus.com

Abstract. Recent advances in AI and technology have come with increased threats to cyber security. Social engineering attempts are being enhanced by cybercriminals utilising Generative AI (GenAI), making phishing attacks harder to detect. New phishing tactics designed to bypass automated systems and target end users are on the rise. Adopting a human-centric cyber security strategy is essential for organisations to bolster users' needs in relation to this threat. To achieve this, organisations need to keep up to date with the latest market solutions and identify which features may be best to incorporate. This paper presents a review of current market solutions designed to reduce phishing susceptibility, and compares their features with relevant academic literature. Comparisons are drawn between features and literature to identify similarities, differences, and gaps between feature themes and scientific research. From proactively monitoring support mechanisms, effective human-centric interventions can be incorporated to maintain the strongest links in the cyber security chain.

Keywords: Cyber Security · Human Factors · Cyberpsychology · Phishing.

1 Introduction

The threat of phishing is growing in volume and complexity. In 2025, phishing remains the most prevalent type of breach with 85% of UK businesses and 86% of UK charities experiencing phishing attacks in the last 12 months [26]. Social engineering in phishing is becoming more sophisticated, with 92% of polymorphic attacks (where the attacker uses constantly changing email structure or content)

utilise AI to bypass security filters and with some using invisible characters to "break" detection systems [17]. With the increased availability of GenAI, the threats phishing pose to humans in cyber security need to be closely monitored and supported with a human-centric approach. Often decision makers may be more likely to fall for GenAI phishing content compared to human-created content [27]. These attacks often succeed as they aim to exploit bias in human decision making rather than technical vulnerabilities, e.g. through adopting persuasion techniques instilling a sense of urgency or authenticity due to it coming from authority sources [25]. Contextual factors which limit users' information processing abilities such as high cognitive load and stress [30,35], or exploiting trust due to familiarity with colleagues [15] and online professional networks [3] can all increase the likelihood of phishing susceptibility. Cues previously used and promoted in phishing awareness campaigns, such as poor grammar and spelling, are significantly less reliable for phishing detection in recent years as these tactics are less utilised in Large Language Model (LLM)-generated emails [22]. These examples demonstrate perceived meaning from cues found in phishing and genuine messages can bias decision making through anchoring and adjustment. It is important, however, to not use these findings to operate on the assumption that humans are the weakest link. This has been challenged since Adams and Sasse [1] who emphasise that users are not the enemy to cyber security. Instead, users should be seen as vital assets who actively contribute to cyber resilience due to their ability to process contextual information intuitively in ways which technology cannot, which is essential to avoiding blame cultures [39]. Nevertheless, as highlighted in Bada, Sasse, and Nurse [2], the transfer of knowledge about good practices in security is far from enough to mitigate phishing risks. Going beyond awareness, and shifting towards a Human Risk Management (HRM) approach to supporting users has become a more recent trend [21] - indicating the growing interest in interventions which assume humans can become the strongest link in cyber security [20]. Many market solutions have been developed to help users and organisations manage threats from phishing attacks, though each takes different approaches - some of which may be more end user focused than others. With detecting phishing becoming increasingly difficult, there is a need for organisations to assess capabilities in mitigating these threats, and evaluate their effectiveness at supporting users when comparing solutions to known threats from academic research. This paper aims to support this requirement by providing a human-centric review of market solutions and literature. A comprehensive search was conducted for academic literature examples which explore factors influencing phishing susceptibility in human decision making, and evidence indicating how humans can be better supported. Current popular market solutions were identified and deconstructed to understand their features and how they deliver on reducing risk. Comparisons are then drawn between features and literature to identify similarities, differences, and gaps between market claims and scientific research.

2 Review Approach

For the academic literature search, database and journal searches were conducted using Google Scholar, IEEE Xplore, ACM Digital Library, ScienceDirect, and arXiv focusing on publications from the last five years. Search strings focused on key terms such as "phishing susceptibility", "security awareness", and "cyber security", combined with relevant psychological terms such as, but not limited to, "cognitive load", "stress", "gamification", and "decision making" to narrow the results to relevant literature. Citation searching was also adopted for relevant papers to further identify literature. Market solutions were identified through open-sourced industry reports such as Budge et al. [10] and Google search engine searches. Available reports and demonstrations were utilised to gain insights into the relevance of each market solution to supporting phishing resilience. Primary features of market solutions were identified and themed based upon their function. Similarities and differences between features were compared alongside relevant literature identified from the literature search.

3 Market Solutions and Literature Comparison

Eleven market solutions providers were identified with features which could help reduce phishing susceptibility (CybSafe, Fable Security, Hoxhunt, KnowBe4, Living Security, Mimecast, NINJIO, OutThink, RedFlags, SoSafe & Sublime Security). Key features are summarised and grouped by seven common themes across solutions (see Table 1). Below provides a summary of comparisons between market solution features and the academic literature.

Table 1: Summary of market solution features and number of solutions which adopted each feature. (x/11) indicates the number of adopting solutions.

Feature	Feature Description	Solutions
End User Data-Driven Automation (7/11)	Artificial Intelligence (AI) and Machine Learning (ML) used to build dynamic risk profiles from real-time observable user behaviours and psychological factors, which can be used to trigger automated interventions (e.g. behavioural nudging, change in conditional access)	CybSafe, Fable Security, KnowBe4, Living Security, Mimecast, OutThink, SoSafe
Predefined Rule-Based Automation (5/11)	Predefined sets of response conditions by platform users/managers using IF/THEN logic.	CybSafe, KnowBe4, Mimecast, RedFlags, Sublime Security

Feature	Feature Description	Solutions
Gamification (6/11)	Adding game design elements such as leaderboards, checklists, levels, and rewards into non-game contexts.	CybSafe, Hoxhunt, KnowBe4, Living Security, OutThink, SoSafe
Core Learning (10/11)	Informative training that is predefined and static covering broad principles which apply to everyone. Delivered through a range of methods (e.g., video, stories, games, quizzes).	CybSafe, Fable Security, Hoxhunt, KnowBe4, Living Security, Mimecast, NINJIO, OutThink, RedFlags, SoSafe
Adaptive Learning (9/11)	Informative training that tailors content based on an employee's attributes or historic performance, e.g., job role, location, phishing failures.	Cybsafe, Fable Security, Hoxhunt, KnowBe4, Living Security, Mimecast, NINJIO, OutThink, SoSafe
Phishing Simulations (9/11)	Cyber security exercise that assesses and trains user's ability to recognise and respond to phishing threats.	CybSafe, Fable Security, Hoxhunt, KnowBe4, Living Security, Mimecast, NINJIO, OutThink, SoSafe
Data Visualisation and Explainability (11/11)	Data visualisation consists of methods which track and display key metrics. Data explainability concerns the ability to interrogate underlying data in order to understand how a model's end result is reached.	CybSafe, Fable Security, Hoxhunt, KnowBe4, Living Security, Mimecast, NINJIO, OutThink, RedFlags, SoSafe, Sublime Security

3.1 End User Data-Driven Automation

The seven solutions adopting this feature provide unique methods for collecting, interpreting, and utilising behavioural data to inform nudging or tailored awareness campaigns. Living Security pulls data from an organisation's existing technology stack as well as publicly available Open-Source Intelligence (OSINT) data, using its AI to analyse over 250 risky and vigilant behaviours to inform a Human Risk Index (HRI) score used to identify user strengths and vulnerabilities across phishing contexts. Similarly, KnowBe4, Mimecast, Fable Security, OutThink, and SoSafe use AI Agents to continuously calculate a human risk score in

real-time by collecting end-user behavioural data to inform nudges for targeted interventions such as training or targeted awareness content. In contrast, SebDB - an AI-powered open-source database developed by CybSafe - maps over 150 cyber safe and risky behaviours and links these to specific risk outcomes, e.g., data compromise, financial loss. Risk for individuals can be inferred from shared characteristics with other employees even if complete datasets have not been gathered. Users are then nudged through notifications or prompted with advice. Literature on Just-In-Time (JIT) and feedback interventions based upon nudge theory [34] broadly support the efficacy of this type of user support when human-centric data is utilised. For example, Bender et al. [5] found from an experiment involving around 11,000 employees that those who received this post-decision feedback after falling for a simulated email were significantly less likely to fail a second test email sent two weeks later. By detecting specific behaviours and targeting feedback to those who need support rather than adopting a one-size-fits-all approach, lasting behaviour change may be more likely to occur. However, without adopting consistent nudges which are applicable to the individual the efficacy of nudge-based interventions may only be effective in the short term [38].

3.2 Predefined Rule-Based Automation

Five market solutions appeared to feature predefined rule-based automation. Sublime Security has a purpose-built language that allows security teams to write highly specific detection rules, such as combining digital malware signatures with sender attribute checks, to identify threats unique to their organisation. Sublime has AI assistance with making rules with its Autonomous Detection Engineer (ADÉ) and Autonomous Security Analyst (ASA), and platform managers using Mimecast can do this through their Human Risk Command Center (HRCC). ADÉ uses AI to automatically generate new MQL detection rules based on emerging attack patterns. ASA automates the triage process by analysing user-reported emails and instantly applying the appropriate rule-based remediation (e.g., quarantine). This user-driven approach not only allows end users to proactively strengthen their organisation's cyber posture, but also could potentially reduce the workload of network security teams providing further benefits for threat detection accuracy [13]. However, Bertiger et al. [6] evaluated the effectiveness of rules generated by Sublime Security's team and ADÉ, and found the LLM-generated rules were less likely to detect phishing events compared to human-generated rules. Similarly, CybSafe's no-code tool 'Workflows' and KnowBe4's 'SecurityCoach' tool could provide the same benefits to network administrators by automating training sign-ups and incident logging, or trigger automated responses based on specific event conditions. Nevertheless, the effectiveness of rule-based automated approaches can be dependent upon the quality of rules used - i.e. how specific they are for triggering responses [33]. Automated rules for JIT nudging interventions designed to prompt safe behaviours from end users can be observed in RedFlags. As previously discussed, nudge-based interventions can be effective if they are implemented consistently and tailored to individuals [5,38]. However, the implementation of tailoring content provided

by RedFlags requires rules to be set by managers, thus there is a dependency on these managers to accurately identify and implement rules which are effective for different individuals.

3.3 Gamification

Six market solutions incorporated game mechanics and design principles to non-game contexts with the purpose of engaging and motivating individuals. OutThink, Hoxhunt, Living Security, SoSafe, CybSafe, and KnowBe4 each included key gamification qualities such as award/reward incentivisation, leaderboards, difficulty levels, quizzes, score systems, interactive activities, and goal-setting. Whilst designed to incentivise and engage users to develop proactive habits, evidence suggests gamification needs to be varied over time in different environments using narratives and challenges to be effective [14]. A systematic review by Manzano-Leon et al. [18] found nearly all included papers implied gamification is a successful learning strategy, though indicated common elements such as score, badges, and leaderboards in isolation may be ineffective to motivate proactive engagement. Interactive, gamified content and activities can be significantly better for improving Information Security Awareness (ISA) compared to lecture-based learning [36], but how this translates into sustained behaviour change is unclear.

3.4 Core Learning and Adaptive Learning

The majority of market solutions (ten out of eleven) include core learning to maintain cyber security awareness for phishing. This is an essential function for organisations, not only for meeting compliance requirements under standards such as the GDPR, ISO 27001, and Cyber Essentials, but for maintaining awareness standards for all employees for current and future threats. This often consists of short, digestible formats of text or video designed to provide awareness applicable to everyone from each solution - also known as microlearning. How bite-sized awareness was presented differed between examples, with Mimecast and KnowBe4 adopting a focus on humour to encourage engagement, whereas NINJIO intentionally avoids comedy on the assumption humour could result in employees taking messages less seriously or interpreted differently across cultures [19]. When exploring academic literature, the effectiveness of microlearning can be mixed. For example, Rusmawati, Diantoro, and Firmansyah [28] indicated microlearning combined with core learning training modules can reduce phishing susceptibility, with phishing click rates dropping from 11.2% to 7.5% and report rates doubling over a 6-12 month period. On the other hand, Hull, Schuetz, and Lowry [16] indicated that despite more engaging content potentially encouraging more curiosity and phishing-detection self-efficacy, they note this type of material had no significant impact on users' ability to detect phishing emails. Most solutions (nine out of eleven) also try to go beyond core learning and incorporate adaptive learning to tailor phishing training to different users. Targeting training content would largely be implemented by AI agents (e.g., KnowBe4's

AIDA) to create fully personalised training paths. Whilst core learning may provide some utility to reducing phishing susceptibility, more targeted content and formatting could potentially provide more consistent support which accounts for individual differences in cyber security [7,24]. For example, matching phishing training content to users' current skill proficiency can enhance detection and broader phishing knowledge [29].

3.5 Phishing Simulations

Nearly all solutions (nine out of eleven) adopt some form of phishing simulation whereby imitation phishing emails are sent to employees, designed to mimic phishing tactics and increase users' ability to detect and report threats. Incorporating a variety of persuasion techniques, emotional triggers, and varying contexts, templates (e.g. phishing emails, QR codes, deepfake incorporation) can be generated with collaboration between solution providers and clients, providing the ability to modify templates to suit organisations. Including multiple factors which influence phishing susceptibility is important to incorporate into simulations given factors such as stress and contextual anchoring can increase risky behaviour [25,30,35]. However, the success of phishing simulations depends not just upon the authenticity of materials but the strategies to engage users in safe habits over time. The features discussed above can collectively impact the effectiveness of phishing simulations, with the need to tailor simulations to the needs of users, not just organisational motivations, being key [37]. Although, hidden costs due to time spent participating, and likelihood of high false positive rates (i.e., overly suspecting genuine requests as phishing) are worth considering in the cost-benefit analysis of simulation implementation [9].

3.6 Data Visualisation and Explainability

Beyond traditional behavioural metrics such as email clicks, and learning progress, all eleven market solutions provide alternative approaches to making risk more actionable through contextualising and quantifying risks and strengths. This could provide guidance over time for managers utilising visualisations such as index scores to monitor human risks and strength profiles, or provide users with feedback for self-reflective training to aid with goal setting. One of the challenges faced by adopting visualisation dashboards is ensuring data presented can be customised, interpreted and assessed appropriately by employees in different organisations [31]. However, incorporating User Experience (UX) feedback (e,g, evaluating self-reported or eye-tracking data - [4]) could enhance cyber security situation awareness by tailoring dashboards to ongoing user needs. Sublime Security's ADE allows for data explainability, though Fable Security goes a step further with its Human Behaviour Data Lakehouse and conversational AI agent. Through incorporating Explainable AI (XAI) into Human-Computer Interactions (HCIs), alert fatigue could be reduced and sensemaking supported for security analysts [12]. The utility from explainability, however, may be dependent upon the broader decision making conditions (i.e., time pressure and task

complexity may impact how well explainability measures can support decision making quality - [32]).

4 Conclusions and Recommendations

Each of the market solution providers contain features which demonstrate the shift away from a one-size-fits-all approach, and a progression towards more tailored human risk management [2,21]. Overall features tend to incorporate human-centric values, though how effective they can be may be dependent upon the users they are designed to support. The majority of solutions rely on their intervention timings being reactive, intervening only after a user makes a mistake - with the exception of nudging features (e.g. RedFlags). Proactive, JIT interventions such as nudging may be useful if used consistently with tailoring to individuals [5,38], though such interventions may not be appropriate for every job role. Whilst phishing simulations can offer a range of tailoring to individuals and organisations [37], there seems to be a lack of consensus regarding the design and execution between solutions. Complimentary psychological tools such as the Employee Cybersecurity Awareness Framework [7], the CybSafe Culture Awareness Tool (C-CAT - [8]), or phishing susceptibility frameworks which reflect alternative performance feedback to users (Chapter 4 in [23]) may be useful additions to tailor cyber security needs to different users to account for individual differences. Such tools could refine risk management profiles to support onboarding, monitor and demonstrate how users can be strong components to cyber security. Phishing detection could be supported further by encouraging habits which draw attention away from features which can appear in both genuine and phishing requests such as context and text content [25], and towards more concrete cues for detection (e.g., URLs - [11]). New and evolving market solutions are consistently being developed over time which may extend beyond those reviewed in this paper. It is therefore important to review future needs and cyber security requirements for solution applications on a regular basis. Future research could benefit from including users from more diverse backgrounds (e.g., culture, neurodivergence, skills and expertise) to gain further insights into what innovation is required for tailoring secure environments to complement naturalistic decision making. Direct evaluations of solution features across cyber settings would be a practical next step to identify required tailoring to meet individuals' cyber security needs.

Acknowledgments. This research was supported through the Airbus Cyber Innovation team in Airbus Operations where the second author works as a Cyber Security Research Intern with the first author, the Cyberpsychology Pillar Lead. Other support was provided by the Head of Airbus Cyber Innovation and the Airbus Cyber Awareness team.

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

References

1. Adams, A., Sasse, M.A.: Users are not the enemy. Communications of the ACM **42**(12), 40–46 (1999). https://doi.org/10.1145/322796.322806
2. Bada, M., Sasse, M.A., Nurse, J.R.C.: Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv, (2019). https://doi.org/10.48550/arXiv.1901.02672
3. Baki, S., Verma, R.M., Mukherjee, A., Gnawali, O.: Less is more: Exploiting social trust to increase the effectiveness of a deception attack. arXiv (2020). https://doi.org/10.48550/arXiv.2006.13499
4. Baltuttis, D., Teubner, T.: Effects of visual risk indicators on phishing detection behavior: An eye-tracking experiment. Computers & Security, **144**, 103940 (2024). https://doi.org/10.1016/j.cose.2024.103940
5. Bender, S., Horn, S., Loewenstein, G., Roberts, O.: Phishing feedback: just-in-time intervention improves online security. Behavioural Public Policy, pp. 1–13 (2024). https://doi.org/10.1017/bpp.2024.19
6. Bertiger, A., Filar, B., Luthra, A., Meschiari, S., Mitchell, A., Scholten, S., Sharath, V.: Evaluating llm generated detection rules in cybersecurity. arXiv, (2025). https://doi.org/10.48550/arXiv.2509.16749
7. Bishop, L.M., Asquith, P.M., Morgan, P.L.: The employee cybersecurity awareness framework. Human Behavior and Emerging Technologies, **1**, 1025045 (2025). https://doi.org/10.1155/hbe2/1025045
8. Blythe, J., Alashe, O.: Measuring cybersecurity culture - an intelligent and scientific approach to people-centric cybersecurity culture. Tech. rep., CybSafe (2019), https://www.cybsafe.com/whitepapers/cybsafe-culture-assessment-tool-whitepaper/
9. Brunken, L., Buckmann, A., Hielscher, J., Sasse, M.A.: "To do this properly, you need more resources": The hidden costs of introducing simulated phishing campaigns. In: Proceedings of the 32nd USENIX Security Symposium. pp. 4105–4122. USENIX Association (2023), https://www.usenix.org/conference/usenixsecurity23/presentation/brunken
10. Budge, J., Blankenship, J., Sjoblom, S., Nagel, B.: The forrester wave: Human risk management solutions, q3 2024. Tech. Rep. RES181374, Forrester (2024), https://www.forrester.com/report/the-forrester-wave-tm-human-risk-management-solutions-q3-2024/RES181374
11. Butavicius, M., Taib, R., Han, S.J.: Why people keep falling for phishing scams: The effects of time pressure and deception cues on the detection of phishing emails. Computers & Security, **123**, 102937 (2022). https://doi.org/10.1016/j.cose.2022.102937
12. Charmet, F., Tanuwidjaja, H.C., Ayoubi, S., Gimenez, P.F., Han, Y., Jmila, H., Blanc, G., Takahashi, T., Zhang, Z.: Explainable artificial intelligence for cybersecurity: a literature survey. Annals of Telecommunications, **77**, 789–812 (2022). https://doi.org/10.1007/s12243-022-00926-7
13. Chhetri, M.B., Tariq, S., Singh, R., Jalavand, F., Paris, C., Nepal, S.: Towards human-ai teaming to mitigate alert fatigue in security operations centres. ACM Transactions on Internet Technology, **24**(3), 1–22 (2024). https://doi.org/10.1145/3670009
14. Chou, Y.K.: Actionable Gamification: Beyond Points, Badges, and Leaderboards. Packt Publishing Ltd (2015). https://doi.org/10.17345/rio18.137-144

15. Fu, T., Brohman, K.: From familiarity to vulnerability: The role of social distance and information processing in spear phishing. In: AMCIS 2025 Proceedings (2025), https://aisel.aisnet.org/amcis2025/sig_sec/sig_sec/9/
16. Hull, D.M., Schuetz, S.W., Lowry, P.B.: Tell me a story: The effects that narratives exert on meaningful-engagement outcomes in antiphishing training. Computers & Security, **129**, 103252 (2023). https://doi.org/10.1016/j.cose.2023.103252
17. KnowBe4: 2025 phishing threat trends report. Tech. rep., KnowBe4 (2025), https://www.knowbe4.com/resources/whitepapers/phishing-threat-trends-report-6
18. Manzano-León, A., Camacho-Lazarraga, P., Guerrero, M.A., Guerrero-Puerta, L., Aguilar-Parra, J.M., Trigueros, R., Alias, A.: Between level up and game over: A systematic literature review of gamification in education. Sustainability, **13**(4), 2247 (2021). https://doi.org/10.3390/su13042247
19. Martin, G.N., Sullivan, E.: Sense of humor across cultures: A comparison of British, Australian and American respondents. North American Journal of Psychology, **15**(2), 375–384 (2013)
20. Morgan, P.L., Asquith, P.M., Bishop, L.M., Raywood-Burke, G., Wedgbury, A., Jones, K.: A new hope: Human-centric cybersecurity research embedded within organizations. In: Moallem, A. (ed.) HCI for Cybersecurity, Privacy and Trust. HCII 2020, Lecture Notes in Computer Science, vol. 12210. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-50309-3_14
21. Nurse, J.R.C., Milward, J., Alashe, O.: From security awareness and training to human risk management in cybersecurity. In: Moallem, A. (ed.) HCI for Cybersecurity, Privacy and Trust. HCII 2025, Lecture Notes in Computer Science, vol. 15814. Springer, Cham (2025). https://doi.org/10.1007/978-3-031-92833-8_19
22. Olea, C., Christensen, A., Fazio, L., Cutting, L., Lieb, M., Phelan, J., Wise, A., Tucker, H.: Evaluating phishing email efficacy. In: Proceedings of the 2025 Computers and People Research Conference. pp. 1–8. ACM (2025). https://doi.org/10.1145/3716489.3728437
23. Raywood-Burke, G.: Cognitive Load and Subjective Time Pressure: How Contextual Factors Impact the Quality of Cyber-Security Decision Making. Ph.D. thesis, Cardiff University (2023)
24. Raywood-Burke, G., Bishop, L., Asquith, P., Morgan, P.: Human individual difference predictors in cyber-security: Exploring an alternative scale method and data resolution to modelling cyber secure behavior. In: Moallem, A. (ed.) HCI for Cybersecurity, Privacy and Trust. HCII 2021, Lecture Notes in Computer Science, vol. 12788. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-77392-2_15
25. Raywood-Burke, G., Jones, D., Morgan, P.: Maladaptive behaviour in phishing susceptibility: How email context influences the impact of persuasion techniques. In: Moallem, A. (ed.) Human Factors in Cybersecurity. AHFE (2023) International Conference. AHFE Open Access, vol. 91. AHFE International, USA (2023). https://doi.org/10.54941/ahfe1003718
26. Rizvi, S., Fordham, E., Rizvi, S.: Cyber security breaches survey 2025. Official statistics, Department for Science, Innovation & Technology (DSIT) (2025). https://doi.org/10.5255/UKDA-SN-9404-1
27. Roy, S.S., Thota, P., Naragam, K.V., Nilizadeh, S.: From chatbots to phishing? - preventing phishing scams created using chatgpt, google bard, and claude. arXiv (2024). https://doi.org/10.48550/arXiv.2310.19181

28. Rusmawati, R.D., Diantoro, K., Firmansyah, B.: Improving organizational resilience to phishing: A cluster randomized field experiment with embedded microlearning. Journal of Information Systems and Management, **3**(1), 59–71 (2025). https://doi.org/10.61978/data.v3i1.948
29. Schöni, L., Carles, V., Stromeier, M., Mayer, P., Zimmerman, V.: You know what? - evaluation of a personalised phishing training based on users' phishing knowledge and detection skills. In: Proceedings of the 2024 European Symposium on Usable Security (EuroUSEC '24). pp. 1–14. ACM (2024). https://doi.org/10.1145/3688459.3688460
30. Schöps, M., Gutfleisch, M., Wolter, E., Sasse, M.A.: Simulated stress: A case study of the effects of a simulated phishing campaign on employees' perception, stress and self-efficacy. In: Balzarotti, D., Xu, W. (eds.) Proceedings of the 33rd USENIX Security Symposium. pp. 4589–4606. USENIX Association, Philadelphia, PA, USA (2024)
31. Shete, S.: Information visualization for a comprehensive cybersecurity risk quantification and measurement. Journal of Artificial Intelligence & Cloud Computing, **2**(2), 1–5 (2023). https://doi.org/10.47363/JAICC/2023(2)170
32. Skinner, G., Parrey, B.: A literature review on effects of time pressure on decision making in a cyber security context. Journal of Physics: Conference Series, **1195**, 012014 (2019). https://doi.org/10.1088/1742-6596/1195/1/012014
33. Sommestad, T., Holm, H., Steinvall, D.: Variables influencing the effectiveness of signature-based network intrusion detection. Information Security Journal: A Global Perspective, **31**, 711–728 (2022). https://doi.org/10.1080/19393555.2021.1975853
34. Thaler, R.H., Sunstein, C.R.: Nudge: Improving decisions about health, wealth, and happiness. Yale University Press (2008). https://doi.org/10.1016/j.soscij.2008.09.003
35. Wright, R., Johnson, S.L., Kitchens, B.: Phishing susceptibility in context: A multilevel information processing perspective on deception detection. MIS Quarterly, **47**(2), 803–832 (2023). https://doi.org/10.25300/MISQ/2022/16625
36. Wu, T., Tien, K.Y., Hsu, W.C., Wen, F.H.: Assessing the effects of gamification on enhancing information security awareness knowledge. Applied Sciences, **11**(19), 9266 (2021). https://doi.org/10.3390/app11199266
37. Yeoh, W., Huang, H., Lee, W.S., Jafari, F.A., Mansson, R.: Simulated phishing attack and embedded training campaign. Journal of Computer Information Systems, **62**(4), 802–821 (2022). https://doi.org/10.1080/08874417.2021.1919941
38. Zimmerman, V., Renaud, K.: The nudge puzzle: Matching nudge interventions to cybersecurity decisions. ACM Transactions on Computer-Human Interaction (TOCHI), **28**(1), 1–45 (2021). https://doi.org/10.1145/3429888
39. Zimmerman, V., Schöni, L., Schaltegger, T., Ambuehl, B., Knieps, M., Abert, N.: Human-centered cybersecurity revisited: From enemies to partners. Communications of the ACM, **67**(11), 72–81 (2024). https://doi.org/10.1145/3665665