# Psychological Effects of Phishing Email Exposure: A Review

**Haniza Nahar[1]*, Zulkiflee Muslim[2], Mohammad Radzi Motsidi[3], Siti Rahayu Selamat[4], Warusia Yassin[5] and Fauzi Adi Rafrastar[6]**

**[1,3]Faculty of Information & Communication Technology, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia**

**[2,4,5]Faculty of Artificial Intelligence & Cyber Security, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia**

**[6]Department of Informatic, Faculty of Computer Science, Universitas Dian Nuswantoro, Indonesia**

***Corresponding Author**

**University of Jember, Indonesia**

**DOI: https://dx.doi.org/10.47772/IJRISS.2025.91100611**

**Received: 12 December 2025; Accepted: 18 December 2025; Published: 26 December 2025**

## ABSTRACT

Phishing emails constitute a persistent and evolving cybersecurity threat, with growing evidence that psychological mechanisms critically shape user susceptibility. Yet, existing research remains fragmented, particularly in integrating emotional, cognitive, and contextual determinants with long-term intervention outcomes. This systematic review synthesizes empirical studies, theoretical models, and intervention evaluations published up to mid-2024 across cybersecurity, psychology, and behavioral science. The findings demonstrate that emotional responses fear, anxiety, and stress significantly increase vulnerability, while heuristic cognitive processing consistently predicts risk. Personality traits yield mixed associations, though anxiety-related cognitive styles emerge as more robust predictors than broad trait measures. Contextual factors, including message framing and targeted social engineering, further amplify susceptibility. Importantly, while training interventions enhance short-term detection, evidence for sustained behavioral change remains weak, exposing a critical research gap. By advancing an integrative perspective that combines emotional, cognitive, and contextual insights, this review contributes to theory development in human-centered cybersecurity and underscores the need for adaptive, psychologically informed interventions to mitigate the escalating risks of phishing at both individual and organizational levels.

**Keywords**: Phishing Attacks, Psychological Vulnerability, Cognitive Biases in Cybersecurity, Human-Centered Security, Behavioral Cybersecurity Interventions.

## INTRODUCTION

Phishing remains one of the most prevalent and damaging forms of cybercrime 56, accounting for a substantial proportion of security breaches worldwide. Beyond its technical implications, phishing leverages psychological manipulation to deceive individuals 7 into disclosing sensitive information or performing harmful actions. Over the past decade, phishing attacks have evolved from rudimentary scams to highly sophisticated social engineering tactics 89 that exploit emotional triggers such as fear, curiosity, urgency, and trust. This evolution reflects a strategic shift by attackers to exploit human vulnerabilities, making the psychological dimensions of phishing a critical area of scholarly inquiry.

While substantial research has focused on technical detection mechanisms and organizational defences, the psychological impact of phishing on recipients 10 remains comparatively underexplored. Phishing attacks do not merely deceive; they elicit emotional and cognitive responses that can impair judgment, erode trust, and contribute to long-term psychological distress. Victims often experience heightened anxiety, cognitive

overload, and diminished confidence 11 in digital communication. These effects are not limited to isolated incidents but can accumulate over time, affecting both individual well-being and organizational culture.

Existing studies often address phishing susceptibility in terms of user awareness or cognitive biases but lack a comprehensive understanding of the emotional and behavioural consequences of phishing exposure 12. Moreover, there is limited consensus on how individual differences such as personality traits, prior experiences, or contextual factors modulate users' psychological responses to phishing attempts. This knowledge gap hampers the development of effective, human-centred interventions and limits the applicability of cybersecurity strategies that do not fully consider the human element.

This review adopts an interdisciplinary perspective, drawing from empirical research in cybersecurity, psychology, and behavioural science to synthesize current knowledge on the psychological impact of phishing emails. It examines emotional and cognitive responses, evaluates psychological models of susceptibility and resilience, explores the influence of personality and contextual variables, and assesses the effectiveness of existing intervention strategies. By integrating insights across these domains, the review aims to inform the design of adaptive, psychologically grounded cybersecurity interventions that enhance user resilience and reduce the adverse effects of phishing on individuals and organizations.

## LITERATURE REVIEW

The psychological dimensions of phishing have garnered increasing attention in recent years, reflecting a shift in cybersecurity research toward more human-centered approaches. This literature review synthesizes key themes emerging from interdisciplinary studies, encompassing emotional and cognitive responses, personality traits, contextual factors, and the effectiveness of training interventions.

### Emotional and Cognitive Responses

Affective states such as fear, anxiety, stress, and curiosity play a central role in phishing susceptibility. Multiple studies have demonstrated that emotionally charged phishing messages impair recipients' ability to evaluate risks objectively, thereby increasing the likelihood of compliance with malicious requests. For instance, 13 applied the Affective Infusion Model (AIM) to show how emotional valence influences decision-making under uncertainty, while 14 highlighted the use of fear appeals and anticipation to drive impulsive user behaviour. Heuristic processing characterized by fast, intuitive judgments is consistently linked with higher susceptibility, particularly when users are under cognitive load or time pressure 15.

### Personality Traits and Individual Differences

The role of personality traits, particularly those within the Big Five framework, remains an area of both interest and debate. Traits such as neuroticism and extraversion have shown mixed correlations with phishing susceptibility. Some studies 171819 found that higher neuroticism is associated with greater vulnerability, while others report inconsistent results due to methodological differences, sample heterogeneity, and self-report biases 16. Emerging evidence suggests that anxiety-related cognitive styles may serve as stronger predictors than stable personality traits, emphasizing the need to consider dynamic emotional and behavioural patterns.

### Contextual and Message Framing Effects

Phishing attacks often rely on contextualized cues such as urgency, authority, and familiarity that exploit psychological heuristics. Tailored messages that mimic legitimate communication from trusted entities significantly increase success rates, particularly when aligned with users' environmental context or current concerns 15. Studies also indicate that demographic variables, including age, gender, and technical proficiency, influence how recipients interpret and react to contextual cues 2020.

### Training and Awareness Interventions

Educational interventions and phishing awareness programs have been widely deployed to enhance user

resilience. Evidence suggests that active learning approaches, particularly those incorporating immediate feedback and emotional engagement, outperform traditional, passive awareness campaigns 2122. However, most interventions demonstrate short-term effectiveness, with limited evidence supporting sustained behavioural change. Adaptive, stage-based training that accounts for individual psychological profiles has been proposed as a more effective alternative.

Stage-based training refers to a progressive and adaptive cybersecurity education approach in which learning is structured according to stages of user readiness and psychological development, allowing gradual, personalized reinforcement that supports long-term behavioral change.

**Broader Psychological Consequences**

Beyond immediate deception, phishing can have lasting psychological effects, including emotional exhaustion, diminished trust, and reduced work engagement 2526. Qualitative studies highlight the emotional toll of phishing victimization, drawing attention to the need for post-incident psychological support and organizational response protocols 27.

**Research Gaps**

Despite the growing body of literature, several gaps remain. There is a paucity of longitudinal studies 38 examining the enduring psychological impact of phishing. Theoretical integration across cognitive, emotional, and behavioural domains is still limited, and few studies 3436 rigorously evaluate the long-term efficacy of interventions. Moreover, the integration of psychological insights into technical cybersecurity measures remains underdeveloped 53, pointing to the need for more holistic, interdisciplinary approaches.

## METHODOLOGY

This study employs a qualitative systematic review approach to synthesize and interpret the psychological dimensions of phishing email exposure. Unlike meta-analytical reviews that aggregate statistical data, this method emphasizes the integration of theoretical insights, interpretive patterns, and thematic convergence across studies. It is particularly suitable for exploring complex psychosocial constructs such as emotion, cognition, trust, and behavioural vulnerability in the cybersecurity context.

**Review Objective and Research Question**

The central aim of this review is to understand how phishing emails affect the emotional, cognitive, and behavioural states of recipients. The over-arching research question guiding this inquiry is:

R1: What are the psychological effects of phishing email exposure?

R2: How do these effects manifest across emotional, cognitive, and contextual domains?

To support this inquiry, the review examines how individual characteristics, contextual factors, and user education interventions interact with susceptibility and victimization outcomes.

**Literature Search and Data Sources**

A purposive and iterative search was conducted across five (5) major academic databases: IEEE Xplore, ACM Digital Library, Scopus, SpringerLink, and Google Scholar. The review considered peer-reviewed journal articles, conference papers, and systematic literature reviews published up to June 2024.

Search terms were developed iteratively and combined using Boolean operators, including:

- “phishing email” AND “emotional impact”
- “phishing susceptibility” AND “cognitive bias”

- "social engineering" AND "psychological response"
- "personality traits" AND "phishing victimization"
- "anti-phishing training" AND "behavioural change"

The strategy ensured broad thematic coverage while remaining focused on psychological constructs. To maintain methodological transparency and focus, the following criteria were applied in Table 1**Error! Reference source not found.**:

**Table 1. Inclusion / Exclusion Criteria**

| Inclusion Criteria | Exclusion Criteria |
|---|---|
| • Studies examining psychological, emotional, cognitive, or behavioural aspects of phishing email exposure.<br>• Research involving human participants (end-users, employees, or organizational representatives)<br>• Studies offering qualitative findings, theoretical analysis, or interpretive discussions relevant to psychological impact.<br>• English language, peer-reviewed publications | • Studies focusing solely on technical or algorithmic phishing detection without psychological analysis.<br>• Non-peer-reviewed materials (blog posts, white papers, unpublished dissertations)<br>• Research unrelated to phishing email contexts (generic cybercrime or malware) |

**Study Selection and Quality Appraisal**

The initial search yielded 289 papers. Title and abstract screening reduced the pool to 103, followed by full-text review based on relevance and methodological rigor. A final set of 50 studies was selected for synthesis.

Each paper was appraised using qualitative quality indicators adapted from the Critical Appraisal Skills Programme (CASP), evaluating:

- Conceptual clarity
- Theoretical grounding
- Transparency of methods
- Relevance to psychological dimensions of phishing

Studies were retained regardless of discipline such as cybersecurity, psychology, organizational studies if they addressed human-centred responses to phishing.

**Data Extraction and Thematic Synthesis**

A framework synthesis approach was employed, combining deductive and inductive coding. Deductive themes were informed by established psychological models such as the Heuristic-Systematic Model and Affective Infusion Model, while inductive coding allowed emergent concepts to surface from the data.

Six (6) dominant themes emerged through iterative coding:

1. Emotional and cognitive responses to phishing
2. Personality and individual susceptibility
3. Contextual and framing effects

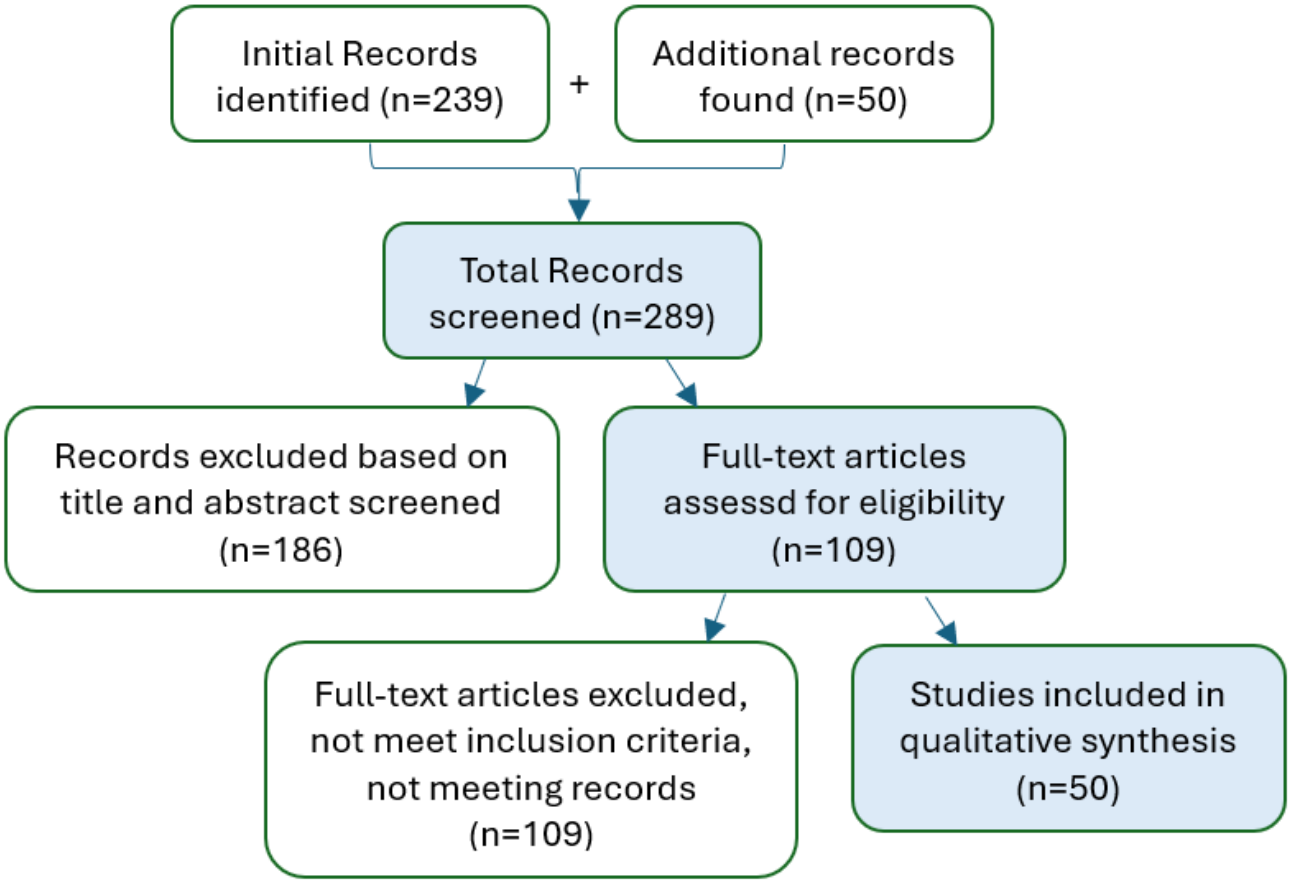
4. Effectiveness of user education and training
5. Social engineering and psychological manipulation
6. Broader psychosocial consequences

Thematic convergence and divergence were recorded, and interpretive patterns were discussed with reference to both established theory and practical implications.

**Methodological Limitations**

As a qualitative framework synthesis, this study prioritizes conceptual depth and thematic richness over statistical generalizability 50 . Recognized limitations include potential language bias (English-only sources), publication bias (exclusion of gray literature), and interpretive subjectivity inherent in qualitative integration 52. Although formal inter-coder reliability statistics were not computed, reliability was ensured through reflexive cross-checking, consensus validation, and iterative refinement of the codebook by multiple reviewers 49. This process upheld transparency and consistency across coding, while future iterations may incorporate quantitative reliability indices such as Cohen's Kappa or Krippendorff's Alpha 51 to further enhance methodological robustness and replicability.

**Figure 1. PRISMA Selection Process**




## RESULT

The final pool of 50 studies presents a rich interdisciplinary landscape spanning cybersecurity, psychology, behavioural science, and organizational research. Results are presented thematically across five (5) domains:

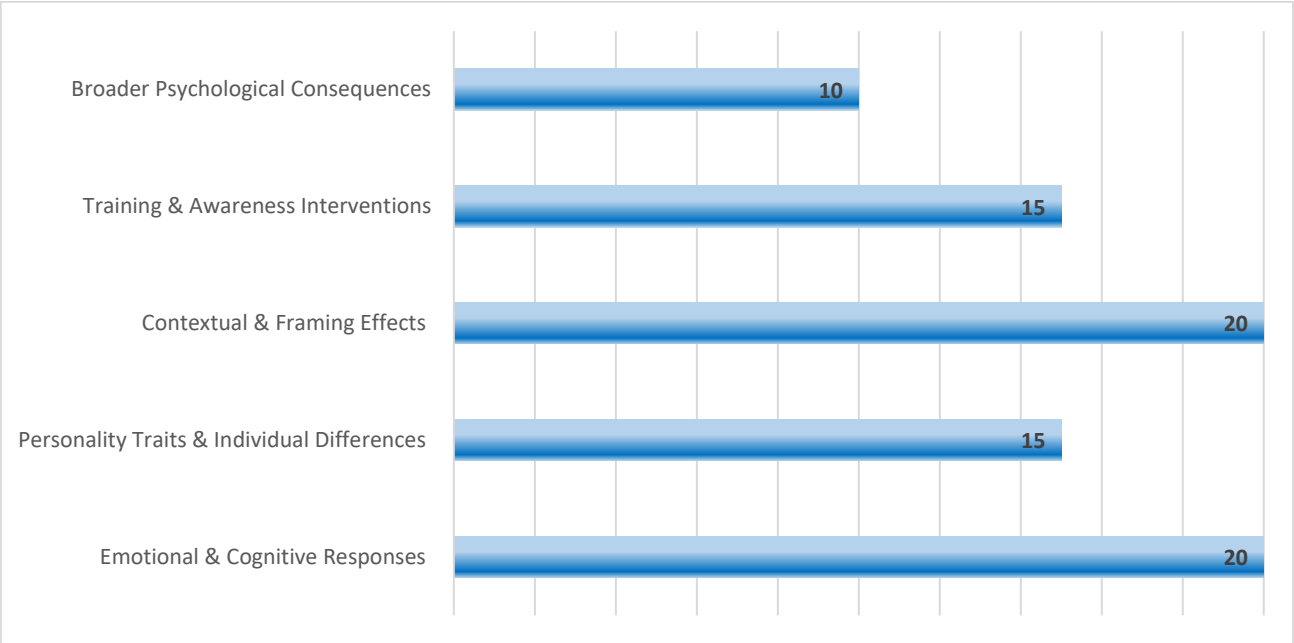
1) Emotional and cognitive responses
2) Personality traits and individual differences

3) Contextual and message framing influences

4) Training and awareness interventions

5) Broader psychological and social consequences of phishing exposure

**Figure 2. Thematic categorization of reviewed studies**




**Emotional and Cognitive Responses**

Most studies 11023 underscore the pivotal role of emotional triggers such as fear, anxiety, and curiosity in shaping user responses to phishing attempts. Emotional states were shown to lower recipients' cognitive defences, impair critical thinking, and increase susceptibility. The Affective Infusion Model (AIM) and Heuristic Systematic Model (HSM) emerged as the dominant frameworks explaining how affective conditions influence decision-making under deceptive conditions.

Cognitive overload, especially in time-constrained or high-pressure environments, was repeatedly associated with an overreliance on heuristic processing 2128. Behavioural indicators such as eye-tracking and mouse movement studies revealed that attentional focus and gaze duration positively correlated with accurate phishing detection 3031.

**Personality Traits and Individual Differences**

Approximately one-third of the studies examined the role of personality traits in phishing susceptibility, particularly within the Big Five model. Findings were mixed: neuroticism and extraversion were positively associated with phishing risk in some studies 24, while others reported no significant correlations 9. Variability in sample composition and measurement tools was identified as a source of inconsistency.

Beyond trait-level predictors, emotional styles such as generalized anxiety emerged as more consistent indicators of susceptibility 24. These findings support the notion that state-based psychological factors may be more predictive than stable personality profiles.

**Contextual and Message Framing Effects**

Twenty studies emphasized the importance of contextualization and message framing in influencing phishing outcomes. Emails that employed urgency, authority, familiarity, or scarcity were significantly more successful in eliciting user compliance 15. Personalization such as referencing user location, interests, or recent activity further increased engagement and clickthrough rates [3].

Demographic moderators such as age, gender, and digital literacy were also influential. Younger users and females were more vulnerable in certain contexts, while prior experience and training mitigated these effects 1415.

### Effectiveness of Training and Awareness Interventions

Fifteen studies assessed the impact of educational interventions on phishing awareness and response accuracy. Active learning techniques, particularly those incorporating feedback and behavioural engagement, demonstrated short-term effectiveness in improving detection 2122. However, the long-term efficacy of these programs remains limited.

Studies highlighted that one-size-fits-all training models often failed to account for individual cognitive and emotional variability. Tailored, stage-based training aligned with users' emotional profiles, personality traits, and prior experiences showed stronger potential in fostering sustained behavioural change 424.

### Broader Psychological and Social Consequences

While most studies focused on immediate susceptibility, a smaller subset explored the long-term psychological and social consequences of phishing victimization. Victims frequently reported trust erosion, emotional exhaustion, and increased anxiety in their digital interactions 262729. Work engagement and performance were negatively impacted in organizational settings, and some studies suggested the emergence of learned helplessness in chronically targeted individuals 25.

These broader impacts emphasize the need for phishing research and interventions to go beyond technical defences and address the human cost of cyber deception.

## DISCUSSION

The findings of this review underscore phishing as not merely a technical challenge but a psychologically complex phenomenon that exploits human affective, cognitive, and behavioural vulnerabilities. Drawing on interdisciplinary literature, the results reveal five interlinked domains that collectively shape individual susceptibility and psychological response to phishing emails: emotional reactivity, cognitive processing style, personality traits, contextual influences, and training efficacy.

### Emotional and Cognitive Mechanisms of Susceptibility

Consistent with dual-process theories such as the Heuristic-Systematic Model (HSM), this review confirms that phishing emails often succeed by prompting heuristic processing under emotionally charged conditions. Emotional states such as fear, anxiety, and urgency reduce critical thinking and increase compliance with malicious requests 114. These findings validate prior work on affective decision-making, particularly the Affective Infusion Model (AIM), which explains how mood and emotion permeate cognitive evaluation.

While much of the literature confirms the general vulnerability of emotionally aroused users, fewer studies examined the durability of these effects or their interactions with situational variables such as task pressure, information overload. This gap signals a need for more temporally sensitive models of phishing susceptibility that account for dynamic emotional-cognitive feedback loops during user-email interaction.

### The Conditional Role of Personality

The influence of personality traits on phishing susceptibility was found to be inconsistent, with neuroticism and extraversion emerging as both risk and neutral factors depending on context and methodology 1617. This variability suggests that trait-level predictors alone may be insufficient, and that they must be examined in conjunction with state-level psychological factors such as stress, attentional capacity, or generalized anxiety.

This reinforces calls in recent cybersecurity psychology research for trait-state interaction models, where

personality traits may moderate the effects of transient emotional or contextual variables rather than act as direct predictors of phishing behaviour.

**Contextual and Social Engineering Tactics**

The effectiveness of phishing is amplified when messages are tailored to exploit context-specific cues, including urgency, social proof, authority, and familiarity 15. Such messages trigger intuitive reasoning, often bypassing users' cognitive safeguards. Importantly, susceptibility was shown to vary based on demographic and environmental variables, highlighting the need for context-aware threat modelling and risk communication.

Despite these insights, relatively few studies have examined how organizational culture, interpersonal trust, or institutional design may mediate these contextual effects. This represents a meaningful area for future inquiry, particularly for enterprises seeking to operationalize phishing defence mechanisms beyond user training.

**Limitations of Existing Interventions**

Although training programs were generally effective in enhancing short-term phishing detection, their long-term impact remains questionable. Evidence suggests that without reinforcement, users tend to revert to baseline behavior over time 21. Moreover, many programs adopt generic formats that fail to account for individual psychological profiles, emotional vulnerabilities, or real-time environmental constraints.

Tailored, adaptive interventions that incorporate feedback, gamification, and user-specific cognitive-emotional traits were found to be more promising but remain underutilized in mainstream organizational practice. This highlights a critical gap between empirical research and implementation, suggesting that cybersecurity training must evolve toward personalized behavioral conditioning rather than static awareness modules.

**Broader Psychological Consequences**

Beyond the immediate threat of deception, phishing has profound psychological effects, including emotional exhaustion, diminished trust in digital platforms, and reduced workplace engagement. These downstream impacts though less frequently studied underscore phishing as a chronic psychological stressor, not just an episodic security risk 2529.

Importantly, few interventions explicitly address post-victimization recovery or incorporate organizational psychological support mechanisms. A more holistic approach to phishing defence must therefore include not only preventive strategies but also restorative frameworks that rebuild trust, confidence, and digital resilience among affected users.

**Table 2. Summary of Key Psychological Themes in Phishing Susceptibility: Insights and Research Gaps.**

| Theme | Key Insights | Gaps/Needs |
|---|---|---|
| Emotional and Cognitive Mechanisms<br>103233 3435 | Phishing exploits fear, anxiety, and urgency triggering heuristic processing, reducing critical evaluation. | More studies on emotional-cognitive feedback loops and the duration of emotional impact. |
| Role of Personality Traits<br>1929 3637 | Neuroticism and extraversion show mixed associations; emotional states are stronger predictors of susceptibility. | Integration of trait-state interaction models to explain variability in susceptibility. |

| | | |
|---|---|---|
| Contextual and Social Engineering Tactics<br>103238 3940 | Tailored messages exploiting authority, urgency, and social proof increase victimization; demographics modulate effects. | Greater focus on organizational and cultural mediators of contextual susceptibility. |
| Training and Awareness Interventions<br>214142 4344 | Generic training improves short-term detection but lacks sustainability; adaptive, personalized interventions are more promising. | Design of long-term, stage-based, and psychologically tailored training approaches. |
| Broader Psychological Consequences<br>4546 4748 | Phishing leads to emotional exhaustion and loss of digital trust; few interventions support psychological recovery. | Development of recovery-focused strategies addressing post-attack emotional harm. |

# CONCLUSION

This review synthesized interdisciplinary research on the psychological effects of phishing email exposure, emphasizing the emotional, cognitive, and contextual factors that shape user susceptibility. Phishing attacks are increasingly effective not because of technical sophistication alone, but because they strategically exploit human psychological vulnerabilities particularly fear, anxiety, cognitive overload, and heuristic reasoning. While individual personality traits such as neuroticism and extraversion have been studied extensively, findings remain inconclusive. Instead, situational and emotional states appear to exert stronger influence on users' decisions during phishing encounters.

Contextual factors including message framing, authority cues, and social engineering tactics significantly amplify risk, especially when tailored to individual characteristics. Although training interventions have demonstrated short-term effectiveness, their long-term sustainability is limited. Generic awareness programs often fail to account for the diversity of user traits, emotional states, and evolving phishing techniques. A more effective defence strategy requires adaptive, psychologically grounded approaches that integrate real-time risk detection with personalized user support.

Importantly, the review highlights that the impact of phishing extends beyond immediate deception, encompassing broader psychological consequences such as emotional exhaustion, trust erosion, and reduced engagement with digital systems. These effects demand a shift from purely technical defences to holistic, human-centred cybersecurity strategies.

Future work should prioritize longitudinal and mixed-methods research to explore the temporal dynamics of phishing susceptibility, develop integrative theoretical models, and validate adaptive intervention frameworks. Advancing digital resilience will require close collaboration across psychology, cybersecurity, and organizational behaviour to protect not only systems, but also the people who use them.

## ACKNOWLEDMENT

The authors would like to thank the Research Group of Information Security Forensics and Computer Networking (INSFORNET), Center for Advanced Computing Technology (C-ACT), Fakulti Teknologi Maklumat dan Komunikasi (FTMK), Universiti Teknikal Malaysia Melaka for the financial support through PJP/2024/FTMK/PERINTIS/SA0038. This work has been supported by Universiti Teknikal Malaysia Melaka.

# REFERENCES

1. Tian, C. A., Jensen, M. L., & Bott, G. J. "The influence of affective processing on phishing susceptibility". European Journal of Information Systems 2024.
2. Lopez-Aguilar, P., Patsakis, C., & Solanas, A. "The Role of Extraversion in Phishing Victimisation: A Systematic Literature Review". APWG Symposium on Electronic Crime Research 2022.

3. Distler, V. "The Influence of Context on Response to Spear-Phishing Attacks: An In-Situ Deception Study". International Conference on Human Factors in Computing Systems 2023.
4. Ebot, A. C. T. "Using stage theorizing to make anti-phishing recommendations more effective". 2018
5. A. K. Ghazi-Tehrani, H. N. Pontell. "Phishing Envolves: Analyzing the Enduring Cybercrime". Int. Journal of Evidence-based Research, Policy and Practice 2021, Vol. 16, No. 3, pp. 316–342
6. Z. Alkhalil, C. Hewage, L. Nawaf, I. Khan. "Phishing Attacks: A Recent Comprehensive Study and A New Anatomy". Frontiers in Computer Science. 2021, Vol. 3, pp. 1-23
7. R. Montanez, E. Golob, S. Xu. "Human Cognition Through the Lens of Social Engineering Cyberattacks". Frontier in Physchology 2020, Vol.
8. K. Khadka, A. B. Ullah, W. Ma, E. M. Marroquin. "A Survey on the Principles of Persuasion as a Social Engineering Strategy in Phishing". IEEE 22nd Int. Conf. on Trust, Security and Privacy in Computing and Communications 2023, pp. 1-8
9. T. Longtchi, R. M. Rodriquez, K. Gwartney, E. Ear, D. P. Azari, C. P. Kelly, S. Xu. "Quantifying Physchological Sophistication of Malicious Emails". IEEE Access 2024, pp. 1-22
10. M. Jari. "An Overview of Phishing Victimization: Human Factors, Training and the Role of Emotions". CCSIT 2022. pp. 217-228
11. F. P. E. Putra, Ubaidi, A. Zulfikri, G. Ariffin, R. M. Ilhamsyah. "Analysis of Phishing Attacks Trends, Impacts and Preventation Methods: Literature Study". Brilliance Research of Artificial Intelligent 2024, Vol. 4, pp. 413- 421
12. M. Bada, J. R. C. Nurse. "The Social aand Psychological Impact of Cyberattacks. Emerging Cyber Threats and Cognitive Vulnerabilities". Academic Press 2020
13. G. Norris, A. Brookes. "Personality, Emotion and Individual Differences in Response to Online Fraud". 2021
14. Goel, S., Williams, K. J., & Dincelli, E. "Got Phished ? Internet Security and Human Vulnerability". Journal of the Association for Information Systems 2017
15. Hassandoust, F., Singh, H., & Williams, J. E. "The Role of Contextualization in Individuals' Vulnerability to Phishing Attempts". Australasian Journal of Information Systems 2020.
16. Lopez-Aguilar, P., Patsakis, C., & Solanas, A. "The Role of Extraversion in Phishing Victimisation: A Systematic Literature Review". APWG Symposium on Electronic Crime Research 2022.
17. S. Eftimie, R. Moinescu, C. Racuciu. "Spear-Phishing Susceptibility Stemming from Personality Traits". IEEE Access 2022. Vol. 10
18. H. Lam, E. Azar, D. Batur, S. Gao, W. Xie, S. R. Hunter, M. D. Rossetti. "Design, Modeling and Simulation of Cybercriminal Personality-based Cyberattack Campaigns". Proceedings of the 2024 Winter Simulation Conference.
19. A. Islam, M. M. Rashid, F. Othman. M. G. Kaosar. "Identifying Personality Treat Associated with Phishing Susceptibility". Security Journal 2025.
20. Taib, R., Yu, K., Berkovsky, S., Wiggins, M. W., & Bayl-Smith, P. "Social engineering and organisational dependencies in phishing attacks". 2019
21. Marshall, N., Sturman, D., & Auton, J. C. "Exploring Evidence for Email Phishing Training: A Scoping Review". Computers & Security 2024
22. Pujari, S. R., & Hussain, M. "Human Factor in Cybersecurity: Behavioral Insights into Phishing and Social Engineering Attacks". Nanotechnology Perceptions 2024.
23. Ignatova, E. S. "Manipulation Of Emotional Security By Cybercriminals Using Social Engineering Technologies: A Case Study". 2024
24. Stalans, L. J., Chan-Tin, E., Moran, M. J., & Kennison, S. M. "Predicting Phishing Victimization: Comparing Prior Victimization, Cognitive, and Emotional Styles, and Vulnerable or Protective E-mail Strategies". Victims & Offenders 2023
25. Werner, M., & Njenga, K. "Phishing Attack Victims and the Effect on Work Engagement". 2023
26. Adejobi, J. A., Carroll, F., Nawaf, L., & Montasari, R. "Phishing, Trust And Human Wellbeing". Web Based Communities 2021.
27. Buse, J. H. M., Ee, J., & Tripathi, S. "Unveiling the Unseen Wounds—A Qualitative Exploration of the Psychological Impact and Effects of Cyber Scams in Singapore". Psychology 2023 Vol. 14.
28. Dwivedi, A. "A Comprehensive Review of Phishing in Cybersecurity: Risks, Impacts, and Defence Strategies". Indian Scientific Journal of Research in Engineering and Management 2024

29. Osman, Z., Alwi, N. H., & Khan, B. N. A. “Psychological Impact on the Public Susceptible to Online Scams”. International Journal of Academic Research in Business & Social Sciences 2024
30. Abdrabou, Y., Dietz, F., Shams, A. M., Knierim, P., Abdelrahman, Y., Pfeuffer, K., Hassib, M., & Alt, F. “Revealing the Hidden Effects of Phishing Emails: An Analysis of Eye and Mouse Movements in Email Sorting Tasks” 2023
31. Hussein, N. “Eye-Tracking In Association With Phishing Cyber Attacks: A Comprehensive Literature Review”. 2023
32. Wang, & Girma. “Psychological tactics of phishing emails: A review”. IACIS International Journal of Information Systems, 2, 71-83. 2020
33. Fall-on, C. K., Baweja, J. A., Yun, J. Y., Thompson, N. D., & Arendt, D. L. “Phishing in the wild: An ecologically valid study of the phishing tactics and human factors that predict susceptibility to a phishing attack.” Pacific Northwest National Laboratory.2021
34. Sarno, D. M. “Which phish is captured in the net? Understanding phishing susceptibility and individual differences.” Applied Cognitive Psychology. 2023
35. AnubisNetworks, “The psychology behind phishing attacks.” (online blog). 2024
36. Halevi, T., Lewis, J., & Memon, N. “Phishing, personality traits and Facebook” 2013
37. “Characteristics that Predict Phishing Susceptibility: A Review”. (2022). NSF Technical Report.
38. Butavicius, M., Parsons, K., Pattinson, M., & McCormac, A. “Breaching the human firewall: Social engineering in phishing and spear-phishing emails.” 2016
39. Jie Wang et al. “The dynamic emotional experience of online fraud victims during the process of being defrauded: A text-based analysis” Journal of Consumer Behaviour. 2024
40. Nurse, J. R. C. “Cybercrime and you: How criminals attack and the human factors that they seek to exploit.” 2018
41. Ho, G., Mirian, A., Luo, E., et al. “Understanding the efficacy of phishing training in practice.” IEEE Symposium on Security and Privacy 2025
42. Alluqmani, K., Elsharif Karrar, A., Alhaidari, M., Alharbi, R., & Alharbi, S. “Assessing the efficacy of security awareness training in mitigating phishing attacks: A review.” International Journal of Advanced Trends in Computer Science and Engineering, 14(3), 177-184. 2025
43. Lain, D., Jost, T., Matetic, S., Kostiainen, K., & Capkun, S.”Content, nudges and incentives: A study on the effectiveness and perception of embedded phishing training.” 2024
44. Abdulrahman A, Hussain A, Khalid A, Mounir F, “Phishing simulation as a proactive defense”. International Journal of Advanced Computer Science and Applications. 2025
45. Luke Balcombe, “The Mental Health Impacts of Internet Scams.” *PMC*. 2025
46. Button, M., et al. “The financial and psychological impact of identity theft among fraud victims.” *PMC* 2023
47. Vikki Davies, “The psychological impact of phishing attacks on your employees”. Cyber Magazine 2023
48. Moya Crockett, “The secret health hell of being scammed: ‘I felt as though my mind was disintegrating’”. The Guardian. 2024
49. Lombard, M., Snyder-Duch, J., & Bracken, C. C. “Content analysis in mass communication: Assessment and reporting of intercoder reliability.” Human Communication Research, 28(4), 587–604. 2002
50. Miles, M. B., Huberman, A. M., & Saldaña, J. “Qualitative data analysis: A methods sourcebook (3rd ed.)”. Sage. 2014
51. Neuendorf, K. A. “The content analysis guidebook (2nd ed.)”. Sage. 2017
52. O’Connor, C., & Joffe, H. “Intercoder reliability in qualitative research: Debates and practical guidelines.” International Journal of Qualitative Methods, 19, 1–13. 2020
53. Bada, M., & Sasse, M. A. “Cyber security awareness campaigns: Why do they fail to change behaviour?” Global Cyber Security Capacity Centre Technical Report, University of Oxford. 2015