SoK: Beyond One-Size-Fits All: A Culturally Informed Individual Framework for Phishing Awareness

M.S. Hiruni Peiris
University of Moratuwa
University of Ruhuna

C. Wijesiriwardana
University of Moratuwa

S.M. Vidanagamachchi
University of Ruhuna

Nalin A. G. Arachchilage
RMIT University

Abstract

Phishing attacks persist not only because users lack awareness, but because attackers exploit cultural and linguistic cues that shape everyday trust decisions. Much phishing research has been conducted with WEIRD (Western, Educated, Industrialised, Rich, and Democratic) populations and often assumes a uniform model of user behaviour. This limits the relevance of existing defences for non-native English speakers, users from high power distance or collectivist cultures, and employees in hierarchical organisations. We conducted a Systematic Literature Review (SLR) of 30 publications following Kitchenham's methodology and the PRISMA framework. The review identifies four dimensions of culturally shaped phishing susceptibility: social and linguistic cues, language and script, individual and organisational environment, and attacker adaptation. It also identifies three intervention categories: technical solutions, training and education, and organisational support. However, these interventions show limited cultural sensitivity and weak alignment with susceptibility factors. Based on these findings, we propose an evidence-based, culturally informed individual framework for phishing awareness with four steps: identify the cultural risk profile, apply culturally aware vigilance, verify and report suspicious messages, and seek culturally relevant awareness. The framework links cultural susceptibility to intervention design and supports culturally situated phishing defences.

1 Introduction

Phishing remains a persistent cybercrime despite continued research, technical defences, and awareness campaigns [6, 11, 15]. The Anti-Phishing Working Group reported more than one million phishing attacks in the first quarter of 2025 alone [1]. One reason for this persistence is that phishing susceptibility is not uniform: users interpret trust, authority, urgency, and legitimacy through their cultural, linguistic, and organisational contexts [17, 19].

Prior work shows that high power distance cultures, second-language use, and hierarchical workplaces can affect how users recognise, question, and report suspicious messages [4, 9, 12]. However, much phishing research remains shaped by WEIRD populations and often assumes a universal user model [7, 8]. This limits the relevance of existing defences for culturally and linguistically diverse users, particularly as attackers increasingly exploit local trust cues and cultural vulnerabilities [15].

This study addresses this gap through a Systematic Literature Review of 30 publications guided by two research questions:

RQ1: How are people susceptible to phishing attacks based on their culture, language, and organisational context?

RQ2: What human-centred interventions have been proposed or evaluated to help people from different cultural contexts recognise and respond to phishing attacks?

Based on the findings, we propose a culturally informed individual framework for phishing susceptibility awareness comprising four evidence-based steps [7, 17, 20].

2 Methodology

We conducted a Systematic Literature Review following Kitchenham's guidelines for structured evidence synthesis [13] and used the PRISMA framework to report the search and screening process transparently [16]. The review focused on phishing susceptibility, culture, language, human-centred interventions, and usable security. Search terms included phishing, susceptibility, awareness, intervention, culture, language, non-native speakers, organisation, and human factors. Studies were included if they examined cultural, linguistic, social, or organisational factors in phishing susceptibility or

USENIX Symposium on Usable Privacy and Security (SOUPS) 2024.
August 11–13, 2024, Philadelphia, PA, United States.

Table 1: How review findings inform the proposed framework

Finding	Gap	Framework step
Social and linguistic cues	Authority, politeness, urgency, and obligation shape trust decisions	Know the cultural risk profile
Language and script	Native language, second-language use, and scripts affect phishing recognition	Apply culturally aware vigilance
Organisational environment	Hierarchy and blame can reduce questioning and reporting	Verify and report suspicious messages
Weak cultural adaptation	Interventions rarely address or test cultural differences	Seek culturally relevant awareness

interventions, while purely technical detection studies without a human-centred or cultural component were excluded. A final set of 30 publications was analysed by extracting data on study context, participant groups, cultural and linguistic factors, intervention types, methods, and limitations. Thematic analysis was then used to code recurring concepts and group them into two main outputs: susceptibility dimensions and intervention categories [3].

3 Results and Framework Development

The review identified two connected findings: phishing susceptibility is shaped by cultural context (RQ1), and existing interventions show limited cultural sensitivity (RQ2). These findings informed the development of our culturally informed individual phishing awareness framework.

3.1 Cultural Susceptibility and Intervention Gaps

Four cultural susceptibility themes emerged. First, **social and linguistic cues**, such as authority, politeness, urgency, obligation, and institutional trust, influence phishing susceptibility. Attackers exploit these culturally familiar communication patterns to increase legitimacy and compliance [4, 19].

Second, **language and script** affect phishing recognition. Non-native English speakers may struggle to identify deceptive cues in English, while native-language phishing can appear more familiar and trustworthy [9, 18]. Detection systems trained mainly on English or Latin-script data may also remain limited in non-Latin script contexts [15].

Third, **organisational context** shapes user response behaviour. Workplace hierarchy, time pressure, role expectations, and blame culture may discourage users from questioning or reporting suspicious requests [10, 12, 20].

Fourth, attackers increasingly use **localised phishing strategies**, including local brands, familiar institutions, native-language writing styles, and culturally recognised trust signals [7, 15].

The review also identified three intervention categories: **technical solutions**, such as warnings and URL inspection tools; **training and education**, including simulations and game-based learning; and **organisational support mechanisms**, such as reporting pathways and escalation processes. However, these interventions often insufficiently align with the cultural factors shaping susceptibility. Technical tools are largely evaluated in English-language contexts [14, 15]; training often treats culture as translation rather than a design consideration [2, 5, 7]; and organisational support rarely addresses hierarchy, blame, or culturally shaped hesitation to report [15, 20]. These gaps show the need for an awareness framework that connects cultural susceptibility factors directly to intervention design.

3.2 Developing a Culturally Informed Awareness Framework

Based on these findings, we propose a culturally informed individual phishing awareness framework that can also support organisational-level interventions. The framework translates susceptibility factors and intervention gaps into four practical steps.

First, **know the cultural risk profile** responds to social and linguistic cues by helping users recognise how authority, politeness, obligation, institutional trust, and workplace hierarchy shape phishing risk. Second, **apply culturally aware vigilance** addresses language, script, and localised attacker strategies by encouraging users to examine messages that rely on native-language familiarity, local brands, urgency, or culturally expected communication styles. Third, **verify and report suspicious messages** responds to organisational barriers by promoting trusted, safe, and non-punitive reporting channels. Fourth, **seek culturally relevant awareness** extends the framework to organisational practice by encouraging training, warning messages, reporting pathways, and awareness materials that reflect local languages, scripts, institutions, hierarchy, and communication norms.

4 Conclusion

This paper presents a systematic review of 30 studies on phishing susceptibility from cross-cultural perspectives. The findings show that culture shapes susceptibility through social and linguistic cues, language and script, individual and organisational environment, and attacker adaptation, while existing interventions rarely address or evaluate these dimensions across cultures. We therefore propose an evidence-based, culturally informed individual framework for phishing awareness that begins with the user's cultural context and supports protective behaviours such as verification and reporting. Future work should validate the framework across diverse cultural groups and develop cross-cultural benchmarks for phishing defences.

Acknowledgments

The authors acknowledge the contributions of the researchers whose work formed the basis of this systematic review. No external funding was received for this study.

References

[1] Anti-Phishing Working Group (APWG). *Phishing Activity Trends Report: 1st Quarter 2025 (Activity January–March 2025)*. Anti-Phishing Working Group, Inc., 1st quarter 2025 edition, 2025. https://docs.apwg.org/reports/apwg_trends_report_q1_2025.pdf (published 2025-07-02).

[2] Nalin Asanka Gamagedara Arachchilage and Steve Love. A game design framework for avoiding phishing attacks. *Computers in Human Behavior*, 29(3):706–714, 2013.

[3] Virginia Braun and Victoria Clarke. Thematic analysis. american psychological association. 2012.

[4] Marcus A Butavicius, Kathryn Parsons, Malcolm R Pattinson, Agata McCormac, Dragana Calic, and Meredith Lillie. Understanding susceptibility to phishing emails: Assessing the impact of individual differences and culture. *HAISA*, 17:12–23, 2017.

[5] Giuseppe Desolda, Lauren S Ferro, Andrea Marrella, Tiziana Catarci, and Maria Francesca Costabile. Human factors in phishing attacks: a systematic literature review. *ACM Computing Surveys (CSUR)*, 54(8):1–35, 2021.

[6] Nguyet Quang Do, Ali Selamat, Ondrej Krejcar, Enrique Herrera-Viedma, and Hamido Fujita. Deep learning for phishing detection: Taxonomy, current challenges and future directions. *Ieee Access*, 10:36429–36463, 2022.

[7] Anjuli Franz, Verena Zimmermann, Gregor Albrecht, Katrin Hartwig, Christian Reuter, Alexander Benlian, and Joachim Vogt. {Sok}: Still plenty of phish in the sea—a taxonomy of {user-oriented} phishing interventions and avenues for future research. In *Seventeenth symposium on usable privacy and security (SOUPS 2021)*, pages 339–358, 2021.

[8] Ayako A Hasegawa, Daisuke Inoue, and Mitsuaki Akiyama. How {WEIRD} is usable privacy and security research? In *33rd USENIX Security Symposium (USENIX Security 24)*, pages 3241–3258, 2024.

[9] Ayako A Hasegawa, Naomi Yamashita, Mitsuaki Akiyama, and Tatsuya Mori. Why they ignore english emails: The challenges of {Non-Native} speakers in identifying phishing emails. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, pages 319–338, 2021.

[10] Asangi Jayatilaka, Nalin Asanka Gamagedara Arachchilage, and Muhammad Ali Babar. Falling for phishing: An empirical investigation into people's email response behaviors. *arXiv preprint arXiv:2108.04766*, 2021.

[11] Asangi Jayatilaka, Nalin Asanka Gamagedara Arachchilage, and Muhammad Ali Babar. Why people still fall for phishing emails: An empirical investigation into how users make email response decisions. *arXiv preprint arXiv:2401.13199*, 2024.

[12] Kalam Khadka and Abu Barkat Ullah. Human factors in cybersecurity: an interdisciplinary review and framework proposal. *International Journal of Information Security*, 24(3):1–13, 2025.

[13] Barbara Kitchenham et al. Procedures for performing systematic reviews. *Keele, UK, Keele University*, 33(2004):1–26, 2004.

[14] Daniele Lain, Yoshimichi Nakatsuka, Kari Kostiainen, Gene Tsudik, and Srdjan Capkun. Url inspection tasks: Helping users detect phishing links in emails. *arXiv preprint arXiv:2502.20234*, 2025.

[15] Bilal Naqvi, Kseniia Perova, Ali Farooq, Imran Makhdoom, Shola Oyedeji, and Jari Porras. Mitigation strategies against the phishing attacks: A systematic literature review. *Computers & Security*, 132:103387, 2023.

[16] Matthew J Page, Joanne E McKenzie, Patrick M Bossuyt, Isabelle Boutron, Tammy C Hoffmann, Cynthia D Mulrow, Larissa Shamseer, Jennifer M Tetzlaff, Elie A Akl, Sue E Brennan, et al. The prisma 2020 statement: an updated guideline for reporting systematic reviews. *bmj*, 372, 2021.

[17] Waldo Rocha Flores, Hannes Holm, Marcus Nohlberg, and Mathias Ekstedt. Investigating personal determinants of phishing and the effect of national culture. *Information & Computer Security*, 23(2):178–199, 2015.

[18] Eric Spero, Isa Seow, Lucas Betts, Eddie Fuatimau, Robert Biddle, Danielle Lottridge, and Giovanni Russello. Language as lure: A naturalistic study on pasifika phishing susceptibility. In *Twenty-First Symposium on Usable Privacy and Security (SOUPS 2025)*, pages 19–35, 2025.

[19] Rucha Tembe, Olga Zielinska, Yuqi Liu, Kyung Wha Hong, Emerson Murphy-Hill, Chris Mayhorn, and

Xi Ge. Phishing in international waters: exploring cross-national differences in phishing conceptualizations between chinese, indian and american samples. In *Proceedings of the 2014 Symposium and Bootcamp on the Science of Security*, pages 1–7, 2014.

[20] Rick Wash. How experts detect phishing scam emails. *Proceedings of the ACM on Human-Computer Interaction*, 4(CSCW2):1–28, 2020.

Ethics of the research This study used only published literature and did not involve human participants or personal data; therefore, formal human-subjects ethical clearance was not required.

AI Disclaimer. AI tools were used only for language refinement, including grammar and stylistic improvements.