

Development and Validation of a Healthcare Workers Phishing Risk Exposure (HWPRE) Taxonomy for Mobile Email

Christopher P. Collins
College of Computing, AI, and
Cybersecurity (CCAC)
Nova Southeastern University
Ft. Lauderdale, FL, USA
cc2409@mynsu.nova.edu
0009-0009-2088-6359

Yair Levy
College of Computing, AI, and
Cybersecurity (CCAC)
Nova Southeastern University
Ft. Lauderdale, FL, USA
levyy@nova.edu
0000-0002-8994-6497

Gregory Simco
College of Computing, AI, and
Cybersecurity (CCAC)
Nova Southeastern University
Ft. Lauderdale, FL, USA
greg@nova.edu
0000-0001-5760-6933

Ling Wang
College of Computing, AI, and
Cybersecurity (CCAC)
Nova Southeastern University
Ft. Lauderdale, FL, USA
lingwang@nova.edu
0000-0002-9202-6501

Abstract—Email on mobile has become a dominant communication channel for healthcare professionals, yet its constrained interface and context of use amplify vulnerability to social engineering attacks, especially phishing. This paper reports the development and empirical validation of the Healthcare Workers Phishing Risk Exposure (HWPRE) taxonomy, a 2x2 framework that positions individuals by (i) general email phishing susceptibility; and (ii) ability to detect mobile-specific phishing cues. We followed a sequential three-phase design: (1) a Delphi study with cybersecurity subject matter experts to validate mobile-relevant phishing indicators and components of a susceptibility index; (2) a pilot to refine instruments and procedures; as well as (3) a large-scale study ($N=300$ healthcare workers) using scenario-based assessments on smartphone-generated email stimuli. We present the construction of the Healthcare Workers Email Phishing Susceptibility Index (HWEPSI), reliability/validity evidence, and statistical analyses relating HWPRE placement to role, experience, medical departments, prior training, and demographic indicators. The results show significant heterogeneity across departments and experience bands; in addition, the ability to recognize mobile cues does not follow uniformly with general susceptibility. We discuss implications for targeted Security Education, Training, and Awareness (SETA) programs and measurement driven program evaluation. We conclude with practical guidance for integrating HWPRE into organizational phishing defense and directions for future research.

Keywords—Phishing, social engineering, healthcare cybersecurity, mobile device cybersecurity, human factors in cybersecurity, SETA in healthcare

I. INTRODUCTION

Email phishing is a persistent enabler of data breaches and fraud across sectors, with healthcare organizations being uniquely targeted due to high data value, time pressure, and distributed mobile work practices [1], [2]. Mobile devices concentrate communication, workflow approvals, and patient-

related coordination in contexts rife with interruptions, limited screen real estate, and ambiguous identity signals [3], [4], [5]. Compared to desktop environments, mobile user interfaces complicate link inspection and provenance checks, while notifications and on-the-go usage increase cognitive load and response urgency [6]. These characteristics contribute to error-prone judgments in security-critical moments [7], [8], [9], [10]. Security leaders commonly measure “phishing resilience” by click rates in simulated campaigns or by aggregate reporting statistics. Although useful, those measures blur the distinct underlying causes: Some workers click because they do not perceive cues on small screens; others perceive risk but comply due to workload, authority gradients, or operational urgency [11], [12]. Treating these paths as interchangeable undermines precision in training and control design [13]. A sharper model should separate perceptual capacity from behavioral susceptibility and do so in the modality where most triage occurs: smartphones.

This paper addresses a practical gap in phishing risk management for healthcare organizations. Beyond generic click rate metrics, organizations need a defensible, role-sensitive way to measure individual exposure that accounts for mobile-specific perceptual and cognitive constraints. We introduce and validate the **Healthcare Workers Phishing Risk Exposure (HWPRE)** taxonomy, which classifies users along two orthogonal dimensions: (1) general susceptibility to email phishing (captured by a composite index, **Healthcare Workers Email Phishing Susceptibility Index (HWEPSI)**) and (2) ability to detect validated phishing signs in mobile email displays. By positioning workers in HWPRE quadrants, security leaders can prioritize tailored training, just-in-time prompts, and compensating controls (e.g., attachment / link detonation, DMARC enforcement, or adaptive step-up authentication) where they matter most. We set this study with the following four Research Questions (RQs) in mind:

RQ1. Which susceptibility components identified in prior literature are applicable to the *HWEPSI*?

- RQ2. Which mobile email phishing indicators do subject matter experts (SMEs) validate as diagnostic for healthcare workers, and how do these indicators differ from those for nonhealthcare workers?
- RQ3. Which *HWEPSI* components are validated by SMEs through the Delphi process?
- RQ4. How are approximately 300 healthcare workers distributed across the *HWPRE taxonomy* based on *HWEPSI* and mobile phishing detection ability?

II. BACKGROUND AND RELATED WORKS

A. Phishing and the Human Element

Email phishing is a persistent enabler of data breaches and fraud across sectors, with healthcare organizations being uniquely targeted due to high data value and distributed mobile work practices [14]. Decades of research show that social engineering success is based on cognitive shortcuts under uncertainty and time pressure. Surveys emphasize the growth of targeted email, text (“smishing”), voice (“vishing”), and cross-channel deception, especially on smartphones [15], [16]. In healthcare specifically, repeated studies show significant susceptibility to simulated phishing and measurable benefits from well-designed awareness programs, although effect sizes depend on lure difficulty, training format, and engagement quality [17], [18], [19]. Industry breach reports also attribute a substantial fraction of healthcare organization incidents to social engineering and credential compromise, underscoring the human element in breach pathways [20], [21]. Beyond generic influence tactics, organizational culture shapes risk [22], [23], [24]. For example, norms that elevate responsiveness over verification can create systematic response biases. Rotating on-call duties, high patient volumes, and time-sensitive Electronic Health Records (EHR) notifications can further increase the likelihood of snap decisions that bypass verification. In this sense, the risk of phishing is a property of sociotechnical systems rather than a property of individuals alone [25], [26].

B. Mobile Detection Ability

Smartphones alter threat detection salience: truncated sender fields, collapsed headers, short Uniform Resource Locators (URLs), disabled hover, and non-standard certificate indicators attenuate users' ability to verify authenticity [27]. The context of use matters: interruptions, multitasking, commuting, and physical mobility degrade scrutiny and increase reliance on heuristics. Notifications invite glanceable interactions in which a single tap can initiate unsafe actions [28], [29]. Platform-specific security features (e.g., long-press URL previews, header expansion) are underutilized or inconsistently implemented. Therefore, evaluating mobile device risk requires instruments and scenarios that reflect actual small screen renderings, constrained interactions, and notification-driven triage. Specifically, phone numbers and messaging identities enable adversaries to correlate between applications, facilitating targeted pretexts. Attackers can

combine breached credential dumps with employment rosters and public social signals to craft lures that blend personal and institutional context. Healthcare-themed pretexts (e.g., Health Insurance Portability and Accountability Act (HIPAA) policy updates, benefits enrollment, vaccine clinics, Electronic Health Record access) exploit authority and duty of care [6].

C. Theoretical Lens

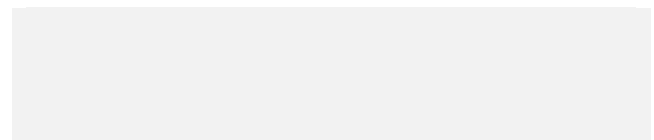
Signal Detection Theory (SDT) provides a basic framework for modeling detection performance under uncertainty, separating sensitivity (ability to distinguish phishing from benign) from response bias (propensity to flag or trust) [30]. In phishing detection, sensitivity maps to cue recognition and knowledge, whereas bias reflects organizational norms (e.g., “reply-fast” cultures), workload, and individual preferences. Persuasion frameworks (e.g., the Elaboration Likelihood Model; Cialdini’s principles) describe how authority, scarcity/urgency, and social proof shape compliance, especially when cognitive resources are thin. Behavioral economics adds information on default effects, present bias, and loss of aversion, which adversaries exploit with time-limited threats or rewards. *HWPRE* operationalizes these ideas by disentangling general susceptibility from mobile-cue detection ability and making both dimensions observable at the level of individual workers and teams.

III. THE HEALTHCARE WORKERS PHISHING-RISK EXPOSURE (HWPRE) TAXONOMY OVERVIEW

HWPRE is a two-dimensional taxonomy situating a worker along the following axes:

- **X-axis: Ability to Detect Signs of Phishing on Mobile Device:** Accuracy in recognizing expert-validated mobile phishing indicators within smartphone-rendered email stimuli (e.g., unfamiliar sender, technical urgency, suspicious links, unsolicited attachments, fake login pages, generic greetings, unusual requests).
- **Y-axis Email Phishing Susceptibility.** A composite scale derived from validated components that makes up the Healthcare Workers Email Phishing Susceptibility Index (*HWEPSI*) (e.g., cyber curiosity, situational awareness, email load, impulsivity, hygiene habits) and behavioral responses in scenario tasks.

Figure 1 highlights the four quadrants of the *HWPRE* Taxonomy, which include: Q1 (Low susceptibility, High detection): low cyber risk exposure; Q2 (Low susceptibility, Low detection): moderate cyber risk exposure; Q3 (High susceptibility, High detection): high cyber risk exposure (bias mitigation, workflow redesign); and Q4 (High susceptibility, Low detection): extremely high cyber risk exposure.



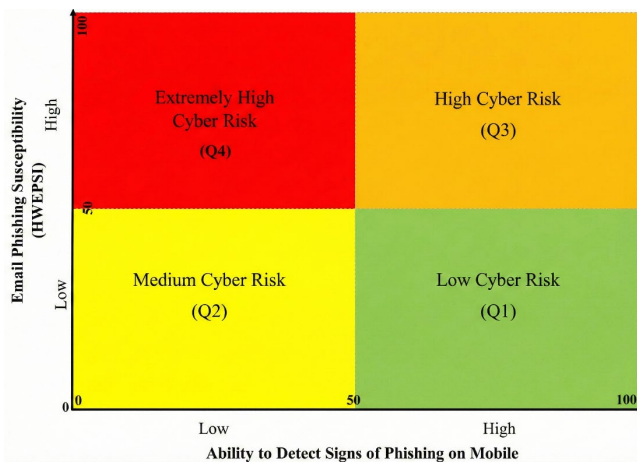


Fig. 1. HWPRE quadrant model with axes scaled from 0-100.

IV. METHODOLOGY

A. Study Design

We used a sequential mixed methods design in three phases.

Phase I (Delphi). We recruited a diverse panel of cybersecurity Subject Matter Experts (SMEs) with healthcare experience, including cybersecurity engineers, incident responders, Chief Information Security Officers (CISOs), red-team operators, and penetration testers. During this phase, the cybersecurity SMEs rated and refined mobile email phishing cues and HWEPSI components.

Phase II (Pilot). We piloted the instrument to measure both the *Ability to Detect Signs of Phishing on Mobile Device* (x-axis of the taxonomy) and *Email Phishing Susceptibility* (HWEPSI, the y-axis) with healthcare workers ($n = 40$) to assess the properties of clarity, burden and measurement, improving the wording and the realism of the scenarios. We confirmed scoring procedures and examined reliability and item-total correlations.

Phase III (Large-scale Study). We surveyed 300 healthcare workers from a United States (U.S.) hospital system in the northeast. Medical departments included nursing, pharmacy, laboratory, radiology, administration, and others. Data included demographics indicators such as role, department, tenure, recent cybersecurity training, email usage patterns (daily volume), and responses to smartphone rendered email scenarios that were balanced between benign and phishing. Research participants judged legitimacy and identified present signs of phishing; confidence ratings were captured on a 7-point Likert scale.

B. Measures

Ability to Detect Signs of Phishing on Mobile Device Score (x-axis). For each phishing scenario, participants selected applicable signs of phishing in emails from the Delphi-validated list. Scores were gathered and normalized to yield a final x-axis value between 0 and 100. Higher scores

indicate greater ability to detect signs of phishing on mobile devices.

HWEPSI (y-axis). Items captured constructs hypothesized in prior work to influence susceptibility (e.g., impulsivity, cyber curiosity, situational awareness, cybersecurity hygiene, email load, self-efficacy, prior victimization). Overall scores were aggregated and then normalized with a normalization coefficient, resulting in a final y-axis score ranging from 0 to 100. Higher scores indicate greater susceptibility.

Outcomes and Covariates. Primary outcome was HWPRE quadrant assignment. Secondary outcomes included Analysis of Variance (ANOVA) across demographic indicators (e.g., role, medical department, tenure bands, cybersecurity training recency).

C. Data Quality and Ethics

Mandatory responses were required, reducing any missing survey responses data. Mahalanobis Distance was used to assess multivariate outliers. Institutional Review Board (IRB) approval and informed consent procedures were in place; personal identifiers were not collected. Scenario stimuli were clear and did not rely on significant deception.

V. RESULTS

A. Subject Matter Experts (SMEs) Consensus and HWPRE Validation

The validation process for the HWPRE and HWEPSI was conducted through the Delphi method to establish a formal consensus among the cybersecurity SMEs. We had 22 cybersecurity professionals participating in the SMEs panel, many with over 18 years of experience, who participated in a multi-round systematic feedback process [31]. These experts utilized a 7-point Likert scale to evaluate and validate specific phishing indicators and susceptibility components derived from existing literature. To ensure rigorous validation, a minimum consensus threshold of 70% agreement was required for any sign or component to be included in the final index. Quadrants of the HWPRE taxonomy were also validated by the experts. Overall, the SMEs feedback from Phase I yielded agreement on the top signs of phishing for healthcare workers including key factors such as email load, impulsivity, and attention span as validated measures of a healthcare worker's risk level.

B. Pilot and Study Participants

Our pilot included 40 healthcare participants that helped refine the linguistic clarity and authentic nature of the scenarios. A few words were adjusted following the pilot study, but the essence of the scenarios and instructions remained the same. The main data was collected from healthcare professionals at a large hospital in the northeastern U.S. The initial sample consisted of 302 participants. Upon review, two records displayed identical scores for all responses, indicating a response set; these were excluded before subsequent analysis. Table I provides the descriptive statistics of the 300 records collected. There were 33 different departments represented.

TABLE I. Descriptive Statistics of Study Participants (N=300).

Age Group	Frequency	Approx. Percentage
18-20	27	9.00%
21-29	31	10.30%
30-39	41	13.70%
40-49	77	25.70%
50-59	68	22.70%
60-67	54	18.00%
Above 67	2	0.60%

Medical Department	Frequency	Approx. Percentage
Acute Pain Management	1	0.33%
Adult Urology	2	0.67%
Anesthesiology	15	5.00%
Anesthesiology	1	0.33%
Behavioral Health	1	0.33%
Bioethics and Humanities	19	6.33%
Cancer Center	26	8.67%
Cardiac Anesthesia	3	1.00%
Cardiology	12	4.00%
Clinical Research Unit	5	1.67%
Emergency Medicine	13	4.33%
Family Medicine	27	9.00%
Global Health	2	0.67%
Infertility	1	0.33%
Medicine	1	0.33%

Medical Department	Frequency	Approx. Percentage
Microbiology	5	1.67%
Neuroanesthesia	1	0.33%
Neurology	12	4.00%
Neurosurgery	12	4.00%
Obstetrics	8	2.67%
Orthopedics	9	3.00%
Pain Management	1	0.33%
Pathology	21	7.00%
Pediatrics	2	0.67%
Pediatric Urology	10	3.33%
Psychiatry	13	4.33%
Radiology	17	5.67%
Radiology Oncology	12	4.00%
Rehab	12	4.00%
Research	1	0.33%
Surgery	13	4.33%
Thoracic Anesthesia	10	3.33%
Urology	12	4.00%

Years in Healthcare Role	Frequency	Approx. Percentage
1-5 years	65	21.67%
6-10 years	52	17.33%
11-20 years	91	30.33%
20+ years	92	30.67%

C. HWPRE Taxonomy Distribution of 300 Healthcare Workers

By mapping each participant's scores onto the HWPRE taxonomy quadrants, we were able to identify patterns of susceptibility and detection ability, as shown in Figure 2.

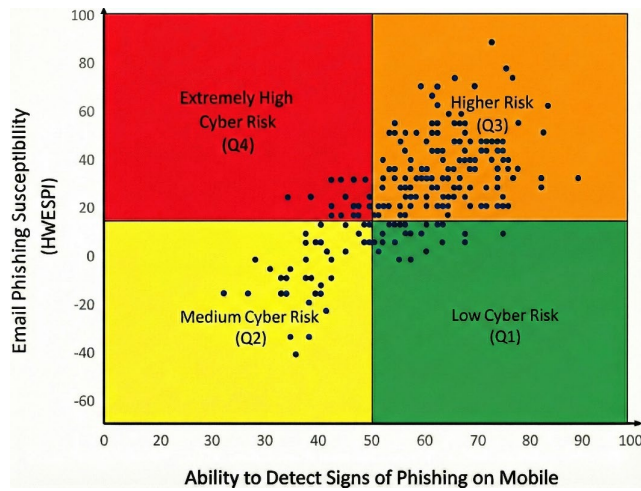


Fig. 2. HWPRE Position of the 300 Healthcare Workers ($N=300$).

The results of our research showed that 6.67% (20 of the 300) healthcare participants were classified into the Extremely High Cyber Risk exposure quadrant (Q4) of the HWPRE, 73.3% (220 out of 300) were classified into the High Cyber Risk exposure quadrant (Q3), 12.67% (38 out of 300) were classified into the Medium Cyber Risk exposure quadrant (Q2), while only 7.34% (22 out of 300) participants were classified into the Low Cyber Risk exposure quadrant (Q1). Moreover, Data analysis for Phase III of this research study utilized ANOVA to determine whether there were any significant differences between the means of each demographic indicator measured (i.e., (a) department, (b) age, (c) years on the job, (d) if the user participated in SETA programs within the last 12 months, (e) gender, and (f) years of using a mobile device) against the ability to detect phishing in mobile emails and their overall email phishing susceptibility. The analysis indicated that when it comes to *Ability to Detect Phishing in Emails on Mobile Devices*, years on the job, recent participation in SETA programs, and years of using a mobile device were statistically significant ($p=0.03$, 0.05 , and 0.01 respectively), while when it comes to healthcare workers email phishing susceptibility (as measured by HWESPI), only age was significant at $p < 0.001$.

VI. DISCUSSION

By systematically being able to identify critical or high-risk groups, healthcare organizations should be able to effectively allocate further resources and implement targeted training initiatives to strengthen their overall security posture. Our findings empirically support the high degree of email phishing susceptibility within the healthcare workforce, as the HWESPI scores revealed that much of the sample exhibited behavioral and cognitive traits—such as high email load and impulsivity—

that increase risk exposure. Furthermore, the statistical significance of age in relation to HWESPI scores ($p < 0.001$) provides quantitative evidence that susceptibility is a distinct, measurable human factor that remains prevalent regardless of a worker's technical ability to detect mobile phishing cues.

A. Limitations

This research had several limitations. One limitation of this study was that it was only conducted at a single healthcare institution in the U.S. It is possible that different results would be produced if using other hospitals located across the U.S. in addition to outside of the U.S. Another limitation was the number of SMEs that participated. Unfortunately, a few SMEs did not participate because their email system may have identified the request to participate as spam; thus, they never received our request to participate. Finally, the use of scenario-based simulations may not fully capture real-world pressures, especially in very stressful healthcare situations such as rotating on-call duties, high patient volumes, and during time-sensitive EHR notifications or in the emergency and trauma rooms, or the Intensive Care Unit (ICU), Labor and Delivery Unit, or Maternal Critical Care Unit.

B. Implications

This research study highlighted the need for role specific cybersecurity training. Proper training is important to reduce overall mobile phishing susceptibility in healthcare organizations. Organizations can benefit from utilizing microlearning techniques to ensure that their employees are receiving content that is not only relevant, but impactful.

VII. CONCLUSIONS AND FUTURE RESEARCH

Our study established a strong empirical foundation that can be expanded in various domains and user groups. The HWPRE taxonomy and HWESPI both provide scalable frameworks that can also aid future researchers validate broader cybersecurity constructs. Future work can explore how separate roles in other industries compare in their susceptibility to mobile phishing threats. Doing such can provide organizations with enhanced cybersecurity risk mitigation approaches and focus their cybersecurity training to those who appear to be needing it the most. Moreover, as our study focused on 300 healthcare workers from a single hospital system, we recommend that future work may assess the taxonomy using healthcare professionals from multiple organizations, and even preferably from different regions in the world in order to further increase the generalizability of the findings. Our scenario-based simulations could not capture the added real-world pressures, especially in very stressful healthcare situations as noted previously in the Limitations. Thus, additional avenues to expand on the findings of this research may include replacing the use of scenario-based simulations with experimental or quasi-experimental procedures in very stressful healthcare situations.

REFERENCES

- [1] A. H. Seh *et al.*, "Healthcare data breaches: Insights and implications," *Healthcare (Basel)*, vol. 8, no. 2, Art. no. 133, 2020.
- [2] B. Hewitt, D. Dolezel, and A. McLeod Jr., "Mobile device security: Perspectives of future healthcare workers," *Perspect. Health Inf. Manag.*, vol. 14, Winter, Art. no. 1c, 2017.
- [3] R. Bitton, A. Finkelshtein, L. Sidi, R. Puzis, L. Rokach, and A. Shabtai, "Taxonomy of mobile users' security awareness," *Comput. Secur.*, vol. 73, pp. 266–293, 2018.
- [4] A. Jayatilaka, N. A. G. Arachchilage, and M. A. Babar, "Why people still fall for phishing emails: An empirical investigation into how users make email response decisions," in *Symp. Usable Secur. Privacy (USEC)*, San Diego, CA, Feb. 2024. [Online]. Available: <https://arxiv.org/abs/2401.13199>
- [5] R. Bitton, K. Boymgold, R. Puzis, and A. Shabtai, "Evaluating the information security awareness of smartphone users," in *Proc. 2020 CHI Conf. Human Factors Comput. Syst.*, Apr. 2020, pp. 1–13.
- [6] S. Baadel, F. Thabtah, and A. Majeed, "Avoiding the phishing bait: The need for conventional countermeasures for mobile users," in *Proc. 9th Annu. Inf. Technol., Electron. Mobile Commun. Conf. (IEMCON)*, pp. 421–425, 2018. doi: 10.1109/IEMCON.2018.8615095
- [7] M. Yadav, "A study of the effects of an individual's personality and characteristics on job behavior using the Myers-Briggs Type Indicator," *Int. J. Innov. Res. Eng. Manag.*, vol. 10, pp. 49–52, 2023.
- [8] P. K. Yeng, M. A. Fauzi, B. Yang, and P. Nimbe, "Investigation into phishing risk behaviour among healthcare staff," *Information*, vol. 13, no. 8, Article 392, 2022.
- [9] E. O. Yeboah-Boateng and P. M. Amanor, "Phishing, SMiShing & vishing: An assessment of threats against mobile devices," *Int. J. Comput. Netw. Commun. Secur.*, vol. 2, no. 6, pp. 165–176, 2014.
- [10] M. Waddell, "Human factors in cybersecurity: Designing an effective cybersecurity education program for healthcare staff," *Healthc. Manag. Forum*, vol. 37, no. 1, pp. 13–16, 2024.
- [11] S. L. K. Stewart, C. Wright, and C. Atherton, "Deception detection and truth detection are dependent on different cognitive and emotional traits: An investigation of emotional intelligence, theory of mind, and attention," *Pers. Soc. Psychol. Bull.*, vol. 45, no. 5, pp. 794–807, 2019.
- [12] K. F. Steinmetz, A. Pimentel, and W. R. Goe, "Performing social engineering: A qualitative study of information security deceptions," *Comput. Human Behav.*, vol. 124, Art. no. 106930, 2021. doi: 10.1016/j.chb.2021.106930
- [13] N. Sebescen and J. Vitak, "Securing the human: Employee security vulnerability risk in organizational settings," *J. Assoc. Inf. Sci. Technol.*, vol. 68, no. 9, pp. 2237–2247, 2017.
- [14] Proofpoint, "State of the Phish: An in-depth look at user awareness," 2022. [Online]. Available: <https://go.proofpoint.com/2023-State-of-the-Phish-Report.html>
- [15] Anti-Phishing Working Group, "Phishing activity trends report," 2021. [Online]. Available: https://docs.apwg.org/reports/apwg_trends_report_q3_2021.pdf
- [16] Scaife, N., Carter, H., Traynor, P., & Butler, K. R.B. (2016). CryptoLock (and Drop It): Stopping ransomware attacks on user data. *Proceedings of the 2016 International Conference on Distributed Computing Systems (ICDCS)*, 2016, 303–312.
- [17] A. Alyami, D. Sammon, K. Neville, and C. Mahony, "Critical success factors for security education, training, and awareness (SETA) programme effectiveness: An empirical comparison of practitioner perspectives," *Inf. Comput. Secur.*, vol. 32, no. 1, pp. 53–73, 2023.
- [18] R. Rohan *et al.*, "A systematic literature review of cybersecurity scales assessing information security awareness," *Heliyon*, vol. 9, no. 3, Art. no. e14234, 2023. [Online]. Available: <https://doi.org/10.1016/j.heliyon.2023.e14234>
- [19] O. Tinubu, O. Falana, E. Oluwumi, A. Sodiya, and S. Rufai, "PHISHGEM: A mobile game-based learning for phishing awareness," *J. Cyber Secur. Technol.*, vol. 7, pp. 1–20, 2023. doi: 10.1080/23742917.2023.2167276
- [20] W. Yeoh, H. Huang, W. S. Lee, F. Al Jafari, and R. Mansson, "Simulated phishing attack and embedded training campaign," *J. Comput. Inf. Syst.*, vol. 62, no. 4, pp. 802–821, 2021.
- [21] D. Hillman, Y. Harel, and E. Toch, "Evaluating organizational phishing awareness training on an enterprise scale," *Comput. Secur.*, vol. 132, Art. no. 103364, 2023. [Online]. Available: <https://doi.org/10.1016/j.cose.2023.103364>
- [22] M. Jalali, M. Bruckes, D. Westmattmann, and G. Schewe, "Why employees (still) click on phishing links: Investigation in hospitals," *J. Med. Internet Res.*, vol. 22, no. 1, Art. no. e16775, 2020.
- [23] O. Sarker, A. Jayatilaka, S. Haggag, C. Liu, and M. A. Babar, "A multi-vocal literature review on challenges and critical success factors of phishing education, training, and awareness," *J. Syst. Softw.*, vol. 208, Art. no. 111899, 2024.
- [24] J. Scott, Y. Levy, W. Li, and A. Kumar, "Comparing phishing training and campaign methods for mitigating malicious emails in organizations," Nova Southeastern Univ., College of Computing and Engineering, 2024.
- [25] M. Althobaiti, "Assessing users' susceptibility and awareness of cybersecurity threats," *Intell. Autom. Soft Comput.*, vol. 28, no. 1, pp. 167–177, 2021.
- [26] KnowBe4, "Phishing by industry benchmarking," 2021. [Online]. Available: <https://info.knowbe4.com/2021-phishing-by-industry-benchmarking>
- [27] Butavicius, M., Taib., R., Han, S. J. (2022). Why people keep falling for phishing scams: The effects of time pressure and deception cues on the detection of phishing emails. *Computers & Security*, 123, Article 102937, <https://doi.org/10.1016/j.cose.2022.102937>
- [28] T. Lin *et al.*, "Susceptibility to spear-phishing emails," *ACM Trans. Comput.-Hum. Interact.*, vol. 26, pp. 1–28, 2019.
- [29] R. Ahmad, S. Terzis, and K. Renaud, "Content analysis of persuasion principles in mobile instant message phishing," in *Proc. Int. Symp. Human Aspects Inf. Secur. Assurance*, vol. 674, pp. 324–336, Jul. 2023.
- [30] M. Alsharif, S. Mishra, and M. AlShehri, "Impact of human vulnerabilities on cybersecurity," *Comput. Syst. Sci. Eng.*, vol. 40, no. 3, pp. 1153–1166, 2022.
- [31] C. P. Collins, Y. Levy, G. Simco, and L. Wang, "Expert panel validation of a phishing susceptibility risk index on mobile devices in the healthcare industry," in *Refereed Paper Proceedings - KM Conference 2025 - Siena, Italy: A Publication of the International Institute for Applied Knowledge Management, Siena, Italy, 2025*, pp. 53–62.