

A Systematic Review of Residual Risk in Cybersecurity Awareness Training

Venkat Laxmi Sateesh Nutulapati
Aldie, VA, USA
0009-0003-2914-7401

Abstract—Cybersecurity awareness training improves knowledge, yet human error continues to drive breaches. AI-enabled attacks such as deepfakes, voice-cloned vishing, and automated spear phishing magnify these risks. This review of 26 studies (2008–2025) introduces a residual-risk framework that measures outcomes beyond average effectiveness. Residual Insecure Behavior (RIB) captures risky practices that persist after training, while Residual Knowledge Gap (RKG) reflects remaining deficits. Across studies, residual risks were substantial—phishing susceptibility often above 10% and knowledge gaps over 30%. By applying RIB and RKG, future cybersecurity researchers can shift focus from statistical gains to reducing real-world exposure in an AI-driven landscape.

Keywords—*cybersecurity awareness, residual risk, insecure behavior, training effectiveness*

I. INTRODUCTION

With the advent of AI-driven threats such as deepfakes, voice-cloned vishing, and automated spear phishing, focusing on human risk is more critical than ever [1]. While organizations continue to invest heavily in cybersecurity awareness and training [2], [3], [4], research shows that training generally improves outcomes but remains highly context dependent [5], [6], [7]. Within information security, this gap is compounded by neutralization strategies that allow employees to rationalize noncompliance despite awareness [8]. Many awareness programs rely primarily on information provision that often fails to specify concrete behaviors or embed reinforcement mechanisms [9]. Furthermore, reviews that study student populations cannot reflect real-world circumstances.

The concept of residual risk is presented in this review not as a novel theoretical construct, but rather as synthesis of empirically documented phenomena that recur across the cybersecurity awareness training literature. Prior research has consistently shown limits in knowledge retention, incomplete transfer of training to real-world behavior, and reversion to habitual practices despite awareness interventions [8], [9], [10], [20], [29], [36]. These effects, variously discussed as training decay, behavioral non-compliance, neutralization, or intention-behavior gaps collectively describe a persistent risk surface that remains after formal training concludes, even

when average effectiveness is reported [10], [35]. The term residual risk is therefore used here as an integrative lens to unify these established findings and enable cross-study comparison of how much risk remains following training, rather than focusing solely on whether training produces immediate improvements. Within this context, we introduce residual insecure behavior (RIB) and residual knowledge gap (RKG) as measures of residual risk; the proportion of employees who still display insecure behaviors or retain knowledge gaps after training rather than relying solely on average improvements. This perspective aims to address significant operational risks left by check-the-box training [10]. By synthesizing RIB and RKG across delivery modes, domains, and follow-up designs, we aim to demonstrate that all types of cybersecurity awareness training programs leave residual risk even when the research shows statistical effectiveness, and hence the need to incorporate these in measuring effectiveness. By presenting residual risk as a lens, this review encourages future researchers and educators to design interventions that explicitly measure residual risk. We also present evidence-based recommendations for training to decrease residual risk.

II. METHODS

A. Search strategy

We performed a systematic review following the best practices outlined by Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines [11] as shown in Figure 1. This approach originated in clinical medicine and is now prominent [5], [12]. On April 15, 2025, we searched ACM Digital Library, Scopus, Web of Science, and APA PsycINFO using below search strategy validated in prior reviews [5], yielding 6,160 articles.

(cyber security OR cybersecurity OR information security OR IT security OR computer security OR digital security OR security awareness) AND (training OR intervention OR cybersecurity awareness OR education) AND (employ OR workforce OR workplace OR organization* OR organization*)*

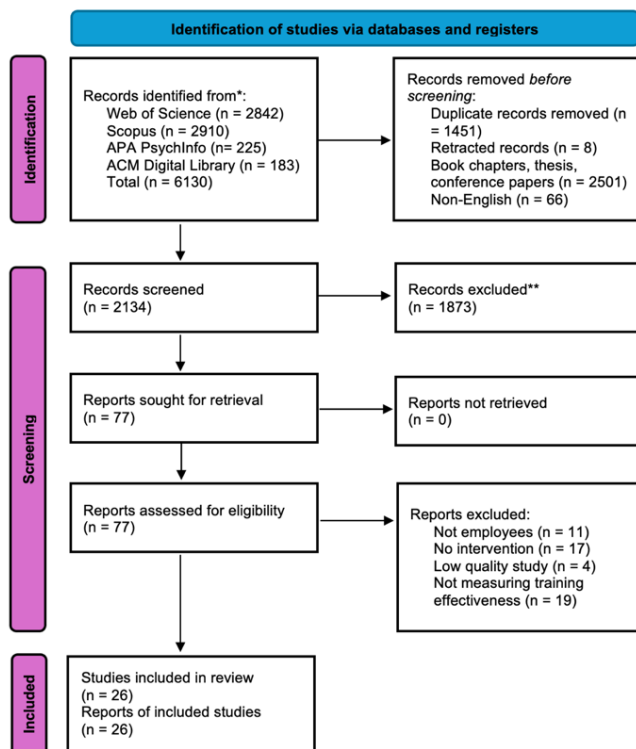


Fig. 1. PRISMA diagram. Adapted from Page *et al.*, [11].

B. Inclusion/Exclusion Criteria

We included studies that were peer-reviewed, in English, evaluated employees in organizational settings, assessed cybersecurity awareness training effectiveness, measured outcomes (behavior, knowledge, attitudes, or related indicators), and used an empirical design. We excluded studies lacking training interventions or effectiveness measures, involving non-organizational populations, not peer-reviewed, not in English, or classified as reviews, theoretical works, or book chapters. Conference proceedings were excluded a priori to maintain methodological comparability and to reduce the risk of double-counting preliminary findings that are often later replicated or extended in journal publications. Given the study's objective to determine whether residual risk persists following cybersecurity awareness training, the review was deliberately scoped to peer-reviewed journal articles, which were anticipated to provide sufficient evidence to address this research question without introducing additional heterogeneity.

C. Data Extraction

Given the methodological and contextual heterogeneity of the studies including intervention types, outcomes, and designs, a narrative synthesis approach was used to analyze and report findings. This approach involved organizing studies into conceptual categories such as training delivery modes, content focus, behavioral outcomes, and residual risks. The emphasis was on summarizing patterns and describing trends

across studies rather than estimating pooled effect sizes. As a result, no meta-analysis was conducted, and publication bias or risk of bias was not formally assessed.

D. Data Analysis

To address variation in study design, setting, and measures, we used a rule-based framework to classify training effectiveness as strong, moderate, or weak. Behavioral and knowledge outcomes were assessed separately using only field data, excluding lab or intention measures. Outcomes were rated strong if $\geq 90\%$ of participants demonstrated secure behavior/knowledge, moderate if 51–89%, and weak if $\leq 50\%$. For phishing or failure outcomes, thresholds were reversed ($\leq 10\%$ failures = strong). When only comparative or narrative results were reported, we estimated or inferred effectiveness using the same thresholds. The quantification scheme and cutoff thresholds used to classify residual risk were selected to support consistent cross-study comparison rather than to assert normative risk benchmarks.

Because the reviewed studies varied widely in outcome measures, reporting granularity, and follow-up timing, a rule-based framework was applied to translate heterogeneous results into comparable proportions of residual insecure behavior (RIB) and residual knowledge gap (RKG). Thresholds distinguishing lower versus higher residual risk were therefore set pragmatically, drawing on common reporting conventions in the training literature (e.g., proportions achieving secure behavior or avoiding failure outcomes) and on operational relevance, such that non-trivial minority exposure remained visible rather than obscured by average effects. This approach prioritizes interpretability and comparability across studies while acknowledging that alternative thresholds could shift categorical labels without altering the underlying pattern: across delivery modes and domains, substantial residual risk persisted even under conservative classification assumptions.

Importantly, we quantified residual insecure behavior (RIB) and residual knowledge gap (RKG) to estimate the proportion of cybersecurity risk or knowledge deficiency that remained after training. For behavioral outcomes, we used the percentage of participants who continued to exhibit insecure behavior. In one study, for example, 17.6% of participants in the deterrence group clicked a phishing link during a simulation after training; we reported this directly as residual insecure behavior. For knowledge outcomes, we subtracted participants' post-training test scores from 100%. In the same study, participants averaged 5.66 out of 9 on a self-reported knowledge test ($\approx 62.9\%$), yielding an RKG of 37.1%. When studies reported multiple behavioral outcomes, we selected the one aligned with the study's primary objective; for instance, prioritizing phishing click rate over reporting rate when click rate was the main focus. By focusing on residual risk, we expose how training that appears effective on paper may still leave a substantial portion of employees vulnerable to cybersecurity threats.

TABLE I. Study Characteristics and Summary of Findings

Study	Region	Sample	Design	Delivery	Behavior	Knowledge	RIB	RKG
Abu-Amara <i>et al.</i> , [13]	ME	10	QE	GAMIFY	Strong	NA	NC	0.25
Alahmari <i>et al.</i> , [14]	ME	128	QE	GAMIFY	Strong	Moderate	NC	NC
Albrechtsen & Hovden, [15]	EU	197	EXP	PEER	Weak	NA	0.175	NA
Alkhazi <i>et al.</i> , [16]	ME	128	EXP	E-LEARN	Moderate	NA	0.273	NA
Arain <i>et al.</i> , [17]	NA	586	OBS	E-LEARN	Moderate	Moderate	0.176	0.37
Back & Guerette, [18]	NA	2000	QE	E-LEARN	Negative	NA	0.33	0.21
Baxter <i>et al.</i> , [19]	NA	856	QE	GAMIFY	Strong	NA	0.07	NA
Bélanger <i>et al.</i> , [20]	EU	826	QE	NUDGE	Moderate	Moderate	0.3	NA
Ben Salamah <i>et al.</i> , [21]	ME	38	QE	BLEND	Moderate	Moderate	0.2	0.47
Bitrian <i>et al.</i> , [22]	EU	13,452	QE	GAMIFY	Strong	NA	NC	NC
Bullee <i>et al.</i> , [23]	EU	119	RCT	BLEND	Moderate	NA	NC	NC
Charoen <i>et al.</i> , [24]	NA	27	AR	F2F-IL, E-LEARN	NA	Moderate	NA	0
Daengsi <i>et al.</i> , [25]	ME	20134	QE	F2F-IL, E-LEARN	NA	Moderate	NA	0.584
Dincelli & Chengalur-Smith, [26]	NA	838	RCT	GAMIFY	Strong	NA	0.067	NA
Ghazvini & Shukur, [27]	AP	5	QE	GAMIFY	NA	Moderate	NC	NC
Gordon <i>et al.</i> , [28]	NA	772	QE	SIM-PHISH	Weak	NA	0.062	0.235
Grill <i>et al.</i> , [29]	EU	108	RCT	BLEND	Moderate	Moderate	0.2	0.134
He <i>et al.</i> , [30]	NA	119	EXP	E-LEARN	Moderate	NA	0.61	NA
Hillman <i>et al.</i> , [31]	ME	5000	QE	SIM-PHISH	Weak	Moderate	0.193	0.354
Nastjuk <i>et al.</i> , [32]	EU	363	RCT	F2F-IL	NA	Moderate	NA	0.095
Puhakainen & Siponen, [33]	EU	16	AR	F2F-IL	Moderate	Moderate	NC	NC
Silic & Lowry, [34]	EU	384	EXP	GAMIFY	Strong	NA	NC	NA
Siponen <i>et al.</i> , [35]	ME	87	QE	F2F-IL	Moderate	NA	0.37	NA
Stefaniuk, [36]	EU	98	QE	BLEND	Moderate	Strong	NC	NC
Weir <i>et al.</i> , [37]	EU	25	AR	F2F-IL	Moderate	Strong	0.31	0.14
Williams <i>et al.</i> , [38]	NA	307	QE	F2F-IL	NA	Weak	NA	0.525

Note: ME = Middle East; EU = Europe; NA = North America; AP = Asia Pacific. Study designs: QE = Quasi-experimental; RCT = Randomized controlled trial; OBS = Observational; AR = Action research; EXP = Experimental. Delivery methods: GAMIFY = gamified training; E-LEARN = e-learning; PEER = peer-based learning; BLEND = blended delivery; NUDGE = behavioral nudge; SIM-PHISH = simulated phishing; F2F-IL = face-to-face instructor-led. Outcomes: Behavior and Knowledge are coded as Strong, Moderate, Weak, NA = Not available. RIB = Residual Insecure Behavior; RKG = Residual Knowledge Gap. NC = Not computable (insufficient data)

III. RESULTS

A. Study Characteristics

As shown in Table I, we identified 26 studies from 2008 to 2025 composed of 4 randomized controlled trials, 14 quasi-experiments, 4 lab experiments, 3 action research projects, and 1 observational study. Samples ranged from 5 to 20,134 participants. Eight training modes were represented: gamified learning ($n=7$), face-to-face instruction ($n=5$), blended ($n=4$), e-learning ($n=4$), combined formats and simulated phishing ($n=2$ each), and peer learning and nudges ($n=1$ each). Outcomes varied where 9 studies assessed both behavior and knowledge, 11 focused only on behavior, and 6 on knowledge. Behavioral measures included phishing clicks, reporting, password hygiene, coding practices, and device security. Most ($n=15$) used both objective logs and self-reports, while 5 relied solely on self-reports. Knowledge outcomes, assessed through quizzes or surveys, covered password policies, data protection, malware, email, general cybersecurity, and smartphone safety.

B. Behavioral Outcomes

Across 21 eligible studies, delivery mode emerged as the strongest predictor of behavioral effectiveness. All six studies that implemented gamified interventions reported strong behavioral improvements (e.g., [13], [22]), demonstrating consistent success for game-based approaches. By contrast, conventional instructional formats such as face-to-face instruction [35], [37], blended delivery [23], nudges [20], and most e-learning programs [16], [30] tended to yield only moderate effects. One e-learning study even reported a negative outcome [18], highlighting the variability of knowledge-based modules. Simulated-phishing interventions and peer-led formats (e.g., [15], [31]) achieved only weak improvements.

Overall, more than half of the studies demonstrated merely moderate behavioral change, regardless of sample size or thematic focus. Strong results were concentrated in the gamification subgroup, whereas moderate outcomes dominated across face-to-face, blended, e-learning, and nudge formats. The distribution across small, medium, and large studies showed no systematic variation, suggesting that study scale did not account for differences in behavioral outcomes.

C. Knowledge Outcomes

Of the 14 studies that measured knowledge outcomes, most reported only moderate gains. Eleven studies (79%) achieved moderate improvements, two studies (14%) demonstrated strong knowledge effects, and one study (7%) reported weak results. Strong outcomes were observed in both blended and face-to-face programs (e.g., [36], [37]), suggesting that these traditional instructional formats can sometimes support substantive knowledge acquisition.

However, gamified interventions (e.g., [14]) that produced strong behavioral outcomes were associated only with moderate knowledge improvements. Similarly, nudges,

simulations, and combined face-to-face plus e-learning formats generated moderate effects. E-learning was modest as well, with available studies showing only moderate gains. Unlike the clear behavioral advantage observed for gamification, no delivery mode consistently predicted strong knowledge outcomes. The overall pattern suggests that cybersecurity awareness training enhances declarative knowledge incrementally but rarely produces substantial knowledge retention.

D. Residual Insecure Behavior

When studies were sorted by RIB, six stood out with the largest proportion of insecure actions remaining after training (see Table II). These studies were most often delivered through e-learning (3), with the remainder involving face-to-face instruction (2) or nudges (1). A clear pattern emerged in which general awareness modules were heavily represented, including topics such as malware, password policies, and device settings.

TABLE II. Top Studies by RIB

Study (Year)	Delivery	Topic	RIB
He <i>et al.</i> , [30]	E-LEARN	GC	0.61
Siponen <i>et al.</i> , [35]	F2F-IL	PH	0.37
Back & Guerette, [18]	E-LEARN	PA	0.33
Weir <i>et al.</i> , [37]	F2F-IL	GC	0.31
Bélanger <i>et al.</i> , [20]	NUDGE	GC	0.3
Alkhazi <i>et al.</i> , [16]	E-LEARN	GC	0.273

Note. RIB (Residual Insecure Behavior) represents the proportion of participants who continued to exhibit insecure behaviors after training. Higher RIB values indicate greater residual behavioral risk, while lower values indicate stronger behavioral adoption and lower residual risk. GC = General cybersecurity; PH = Password hygiene; PA = Phishing awareness.

The persistence of high RIB in both immediate and delayed assessments suggests that residual behavior is not solely attributable to decay over time but may also reflect limitations of information-heavy approaches that lack reinforcement within workplace practices.

E. Residual Knowledge Gap

Sorting by RKG identified another six studies with the largest remaining deficits in knowledge (see Table III). Unlike the RIB set, these high-RKG studies spanned a wide range of modalities, including face-to-face, blended, e-learning, simulation, and gamification. This variation indicates that knowledge retention challenges persist across delivery modes rather than being confined to any single format. Follow-up timing also varied, with some studies assessing immediately after training, others leaving timing unspecified, and several measuring knowledge months later, yet high RKG was observed across all.

TABLE III. Top Studies by RKG

Study (Year)	Delivery	Topic	RKG
Daengsi <i>et al.</i> , 2022	F2F-IL, E-LEARN	PA	0.584
Williams <i>et al.</i> , 2024	F2F-IL	PA	0.525
Ben Salamah <i>et al.</i> , 2023	BLEND	GC	0.47
Arain <i>et al.</i> , 2019	E-LEARN	GC	0.37
Hillman <i>et al.</i> , 2023	SIM-PHISH	PA	0.354
Abu-Amara <i>et al.</i> , 2021	GAMIFY	GC	0.25

Note. RKG (Residual Knowledge Gap) represents the proportion of participants who retained knowledge deficits following training. Higher RKG values indicate weaker knowledge retention and greater residual cognitive risk, while lower values indicate stronger knowledge retention. GC = General Cybersecurity, PA = Phishing awareness.

F. Other Patterns

Comparison of RIB and RKG patterns highlights some knowledge–behavior asymmetry. In multiple high-RKG cases, residual behavior was comparatively low [21]: RIB = 0.200 vs. RKG = 0.470; [17]: RIB = 0.176 vs. RKG = 0.370; [31]: RIB = 0.193 vs. RKG = 0.354. This suggests that employees can adopt secure behaviors even when unable to explicitly recall training content. This finding points to the influence of environmental prompts, habits, and structural supports in guiding behavior. Conversely, several high-RIB cases occurred in training that improved knowledge but left significant insecure actions in place. For example, e-learning modules covering malware, general awareness, or device configuration produced measurable knowledge outcomes but left large proportions of participants continuing insecure practices. Phishing appeared prominently across both sets, with some [18] identified in the high-RIB group and some in [25], [31], [38] in the high-RKG group.

IV. DISCUSSION

Despite many reports of statistical effectiveness, these studies repeatedly show that training often leaves a sizable portion of employees continuing to act insecurely or failing to retain critical knowledge. For example, phishing interventions reduced click-throughs but still left high-risk groups consistently more vulnerable, even after mandatory training [28], [31]. Similarly, social engineering experiments found that more than one-third of staff handed over keys to strangers despite awareness interventions, illustrating dangerous residual insecure behaviors [23]. Knowledge-focused gains often masked persisting gaps where employees reported better knowledge yet failed in routine practices such as password rotation or proper authorization [36], while others documented steep declines in protective knowledge and behavior over time, leaving residual vulnerabilities [20], [29].

Even gamified and engaging methods that improved motivation did not fully eliminate insecure practices, with significant heterogeneity across individuals and units [26], [34]. The stronger effect of gamification on behavior (lower RIB) compared to knowledge (higher RKG) likely reflects differences in how these outcomes are acquired and retained. Gamified interventions frequently embed cues, repetition, and feedback loops that promote action at the point of decision, enabling participants to adopt secure behaviors even when explicit recall of training content is incomplete [15], [26], [34]. This aligns with observed cases in which participants demonstrated improved behavioral compliance despite only moderate or weak knowledge retention. In contrast, durable knowledge acquisition requires structured encoding, reinforcement, and retrieval practice, which gamified formats do not consistently provide. As a result, gamification appears more effective at shaping habits and responses, reducing residual insecure behavior, while leaving residual knowledge gaps that persist over time. These findings show that average improvements obscure risk; what matters is how many employees remain unprotected. Measuring RIB and RKG better reflects residual risk and exposes persisting exploitable threats.

Knowledge and behavior often improve immediately post-intervention but decay without reinforcement, as seen in longitudinal studies where protective behaviors diminished within months [20], [29]. This suggests that declines in secure behavior over time are not solely a function of forgetting or diminished motivation but are strongly shaped by organizational context. Several studies showed that behavioral gains eroded within months when training was not reinforced through leadership engagement, peer norms, or shared practices [20], [29]. In environments where managers modeled secure behavior, reinforced expectations, and enabled informal knowledge sharing, behavioral improvements were more likely to persist beyond the immediate post-training period. Conversely, where security norms remained implicit or unsupported, employees reverted to habitual practices despite prior training, contributing to elevated residual insecure behavior over time. These patterns indicate that behavioral decay reflects the absence of sustained social and structural reinforcement, underscoring that residual risk is as much an organizational phenomenon as an individual one. Another concern is the heavy reliance on knowledge metrics while neglecting behavior. Employees frequently demonstrate higher self-reported awareness yet continue risky practices, such as failing to rotate passwords or mishandling data [36]. Even where policies exist, neutralization allows employees to justify insecure practices, leaving persistent risk [35]. The format of delivery further contributes to residual risks. One-off, perfunctory sessions often disengage participants and fail to produce lasting change [34], [36]. Without engaging formats or real-world relevance, employees struggle to internalize training. Employees often view compliance modules as tedious, leading to poor retention and weak translation to secure

actions [19], [34]. Despite training, many individuals complied with social engineering requests, demonstrating the limits of abstract knowledge when facing persuasive real-world tactics [23]. Leadership engagement and group norms also determine whether training translates into behavior [29]. Without supportive systems for sharing and reinforcing security knowledge, individual gains are not sustained or disseminated [14].

To address these shortcomings, practical improvements are needed. Reinforcement through longitudinal and cyclical approaches is essential to maintain behaviors over time [20], [36]. Interactive methods such as gamification, dialogue, and serious games can increase engagement and improve outcomes compared to static, one-directional formats [15], [27], [34]. Embedding training within organizational culture particularly by equipping managers to model, reinforce, and prioritize secure behavior appears especially effective [14], [29]. Addressing rationalizations directly also reduces insecure password practices [35]. Finally, interventions should expose employees to realistic, scenario-based threats to ensure knowledge translates under pressure [14], [23].

These design considerations are particularly salient in the context of AI-enabled threats such as generative phishing, deepfake-based phishing, and adaptive social engineering. These attacks do not introduce fundamentally new failure modes; rather, they exploit the same residual insecure behaviors, habitual responses, and incomplete knowledge retention documented across the reviewed studies. Training approaches that improve average outcomes may still leave a minority of employees vulnerable, but AI-driven attacks increase the realism, personalization, and scale with which these residual weaknesses can be targeted. As a result, residual risk becomes more consequential in AI-mediated threat environments, where persistent gaps in behavior or knowledge represent a scalable and repeatable attack surface rather than isolated lapses.

This study has limitations. Residual-risk thresholds were set pragmatically (e.g., $\leq 10\%$ phishing click rate as “low risk”) rather than validated against benchmarks, which may limit generalizability. We did not apply a formal risk-of-bias tool, as our goal was to map residual risk rather than conduct a meta-analysis. Heterogeneity in outcomes also precluded pooled analyses, so findings rest on descriptive synthesis and subgroup patterns. Future research should refine residual-risk thresholds, apply standardized bias assessments, and rate evidence certainty.

In conclusion, cybersecurity awareness training improves average outcomes but consistently leaves substantial gaps in knowledge and behavior. These residual vulnerabilities are amplified by motivational limits, organizational context, and increasingly by AI-driven threats. Looking ahead, we argue that the residual risk approach offers a pathway for researchers and educators to design better cybersecurity training programs. By systematically assessing RIB and RKG, future interventions can be built to reduce not only immediate

vulnerabilities but also the long-term risks that persist after training.

ACKNOWLEDGEMENT

ChatGPT (OpenAI) was used for grammar and condensation; all content, analysis, and conclusions are the authors' own.

REFERENCES

- [1] K. Khadka and A. B. Ullah, “Human factors in cybersecurity: an interdisciplinary review and framework proposal,” *Int J Inf Secur*, vol. 24, no. 3, p. 119, Jun. 2025, doi: 10.1007/s10207-025-01032-0.
- [2] Verizon, “Verizon 2025 Data Breach Investigations Report,” 2025.
- [3] Fortinet, “Fortinet 2024 Security Awareness and Training,” 2024.
- [4] KnowBe4, “KnowBe4 - 2023 SECURITY AWARENESS TRAINING REPORT,” 2023.
- [5] J. Prümmer, T. van Steen, and B. van den Berg, “A systematic review of current cybersecurity training methods,” *Comput Secur*, vol. 136, p. 103585, Jan. 2024, doi: 10.1016/j.cose.2023.103585.
- [6] J. Prümmer, T. van Steen, and B. van den Berg, “Assessing the effect of cybersecurity training on End-users: A Meta-analysis,” *Comput Secur*, vol. 150, p. 104206, Mar. 2025, doi: 10.1016/j.cose.2024.104206.
- [7] S. A.-D. Qawasmeh, A. A. S. AlQahtani, and M. K. Khan, “Navigating cybersecurity training: A comprehensive review,” *Computers and Electrical Engineering*, vol. 123, p. 110097, Apr. 2025, doi: 10.1016/j.compeleceng.2025.110097.
- [8] Siponen and Vance, “Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations,” *MIS Quarterly*, vol. 34, no. 3, p. 487, 2010, doi: 10.2307/25750688.
- [9] T. van Steen, E. Norris, K. Atha, and A. Joinson, “What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use?,” *J Cybersec*, vol. 6, no. 1, Jan. 2020, doi: 10.1093/cybsec/tyaa019.
- [10] J. Haney and W. Lutters, “Security Awareness Training for the Workforce: Moving Beyond ‘Check-the-Box’ Compliance,” *Computer (Long Beach Calif)*, vol. 53, no. 10, pp. 91–95, Oct. 2020, doi: 10.1109/MC.2020.3001959.
- [11] M. J. Page *et al.*, “The PRISMA 2020 statement: an updated guideline for reporting systematic reviews,” *BMJ*, p. n71, Mar. 2021, doi: 10.1136/bmj.n71.
- [12] B. Naqvi, K. Perova, A. Farooq, I. Makhdoom, S. Oyedeji, and J. Porras, “Mitigation strategies against the phishing attacks: A systematic literature review,” *Comput Secur*, vol. 132, p. 103387, Sep. 2023, doi: 10.1016/j.cose.2023.103387.
- [13] F. Abu-Amara, R. Almansoori, S. Alharbi, M. Alharbi, and A. Alshehhi, “A novel SETA-based gamification framework to raise cybersecurity awareness,” *International Journal of Information Technology (Singapore)*, vol. 13, no. 6, pp. 2371–2380, 2021, doi: 10.1007/s41870-021-00760-5.
- [14] S. Alahmari, K. Renaud, and I. Omoronyia, “Moving beyond cyber security awareness and training to engendering security knowledge sharing,” *INFORMATION SYSTEMS AND E-BUSINESS MANAGEMENT*, vol. 21, no. 1, pp. 123–158, 2023, doi: 10.1007/s10257-022-00575-2.
- [15] E. Albrechtsen and J. Hovden, “Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study,” *Comput Secur*, vol. 29, no. 4, pp. 432–445, 2010, doi: 10.1016/j.cose.2009.12.005.
- [16] B. Alkhazi, M. Alshaiikh, S. Alkhezi, and H. Labbaci, “Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior,” *IEEE ACCESS*, vol. 10, pp. 132132–132143, 2022, doi: 10.1109/ACCESS.2022.3230286.

- [17] M. A. Arain, R. Tarraf, and A. Ahmad, "Assessing staff awareness and effectiveness of educational training on IT security and privacy in a large healthcare organization," *J Multidiscip Healthc*, vol. 12, pp. 73–81, 2019, doi: 10.2147/JMDH.S183275.
- [18] S. Back and R. T. Guerette, "Cyber Place Management and Crime Prevention: The Effectiveness of Cybersecurity Awareness Training Against Phishing Attacks," *J Contemp Crim Justice*, vol. 37, no. 3, pp. 427–451, 2021, doi: 10.1177/10439862211001628.
- [19] R. J. Baxter, D. K. Holderness, and D. A. Wood, "Applying Basic Gamification Techniques to IT Compliance Training: Evidence from the Lab and Field," *Journal of Information Systems*, vol. 30, no. 3, pp. 119–133, Sep. 2016, doi: 10.2308/isys-51341.
- [20] F. Bélanger, J. Maier, and M. Maier, "A longitudinal study on improving employee information protective knowledge and behaviors," *Comput Secur*, vol. 116, p. 102641, 2022, doi: 10.1016/j.cose.2022.102641.
- [21] F. Ben Salamah *et al.*, "An Adaptive Cybersecurity Training Framework for the Education of Social Media Users at Work," *APPLIED SCIENCES-BASEL*, vol. 13, no. 17, 2023, doi: 10.3390/app13179595.
- [22] P. Bitrián, I. Buil, S. Catalán, and D. Merli, "Gamification in workforce training: Improving employees' self-efficacy and information security and data protection behaviours," *J Bus Res*, vol. 179, p. 114685, 2024, doi: 10.1016/j.jbusres.2024.114685.
- [23] J. W. H. Bullée, L. Montoya, W. Pieters, M. Junger, and P. H. Hartel, "The persuasion and security awareness experiment: reducing the success of social engineering attacks," *J Exp Criminol*, vol. 11, no. 1, pp. 97–115, 2015, doi: 10.1007/s11292-014-9222-7.
- [24] D. Charoen, M. Raman, and L. Olfman, "Improving end user behaviour in password utilization: An action research initiative," *Syst Pract Action Res*, vol. 21, no. 1, pp. 55–72, 2008, doi: 10.1007/s11213-007-9082-4.
- [25] T. Daengsi, P. Pornpongtechavanich, and P. Wuttidittachotti, "Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attacks," *Educ Inf Technol (Dordr)*, vol. 27, no. 4, pp. 4729–4752, 2022, doi: 10.1007/s10639-021-10806-7.
- [26] E. Dincelli and I. Chengalur-Smith, "Choose your own training adventure: designing a gamified SETA artefact for improving information security and privacy through interactive storytelling," *EUROPEAN JOURNAL OF INFORMATION SYSTEMS*, vol. 29, no. 6, pp. 669–687, 2020, doi: 10.1080/0960085X.2020.1797546.
- [27] A. Ghazvini and Z. Shukur, "A Serious Game for Healthcare Industry: Information Security Awareness Training Program for Hospital Universiti Kebangsaan Malaysia," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 9, 2018, doi: 10.14569/IJACSA.2018.090932.
- [28] W. J. Gordon *et al.*, "Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system," *JOURNAL OF THE AMERICAN MEDICAL INFORMATICS ASSOCIATION*, vol. 26, no. 6, pp. 547–552, 2019, doi: 10.1093/jamia/ocz005.
- [29] M. Grill, T. Sommestad, H. Karlzén, and A. Pousette, "Training for improved information security culture: a longitudinal randomized controlled trial," *INFORMATION AND COMPUTER SECURITY*, 2025, doi: 10.1108/ICS-08-2024-0189.
- [30] W. He *et al.*, "Improving employees' intellectual capacity for cybersecurity through evidence-based malware training," *JOURNAL OF INTELLECTUAL CAPITAL*, vol. 21, no. 2, pp. 203–213, 2020, doi: 10.1108/JIC-05-2019-0112.
- [31] D. Hillman, Y. Harel, and E. Toch, "Evaluating organizational phishing awareness training on an enterprise scale," *Comput Secur*, vol. 132, p. 103364, 2023, doi: 10.1016/j.cose.2023.103364.
- [32] I. Nastjuk, R. Florian, T. Simon, and J. and Benitez, "A field experiment on ISP training designs for enhancing employee information security compliance," *European Journal of Information Systems*, vol. 0, no. 0, pp. 1–24, May 2025, doi: 10.1080/0960085X.2024.2359460.
- [33] P. Puhakainen and M. Siponen, "IMPROVING EMPLOYEES' COMPLIANCE THROUGH INFORMATION SYSTEMS SECURITY TRAINING: AN ACTION RESEARCH STUDY," *MIS QUARTERLY*, vol. 34, no. 4, pp. 757–778, 2010.
- [34] M. Silic and P. B. Lowry, "Using Design-Science Based Gamification to Improve Organizational Security Training and Compliance," *JOURNAL OF MANAGEMENT INFORMATION SYSTEMS*, vol. 37, no. 1, pp. 129–161, 2020, doi: 10.1080/07421222.2019.1705512.
- [35] M. Siponen, P. Puhakainen, and A. Vance, "Can individuals' neutralization techniques be overcome? A field experiment on password policy," *Comput Secur*, vol. 88, p. 101617, Jan. 2020, doi: 10.1016/j.cose.2019.101617.
- [36] T. Stefaniuk, "TRAINING IN SHAPING EMPLOYEE INFORMATION SECURITY AWARENESS," *ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES*, vol. 7, no. 3, pp. 1832–1846, 2020, doi: 10.9770/jesi.2020.7.3(26).
- [37] C. Weir, I. Becker, J. Noble, L. Blair, M. A. Sasse, and A. Rashid, "Interventions for long-term software security creating a lightweight program of assurance techniques for developers," *SOFTWARE-PRACTICE & EXPERIENCE*, vol. 50, no. 3, pp. 275–298, 2020, doi: 10.1002/spe.2774.
- [38] J. A. Williams, H. Zafar, and S. Gupta, "Fortifying healthcare: An action research approach to developing an effective SETA program," *Comput Secur*, vol. 138, p. 103655, 2024, doi: 10.1016/j.cose.2023.103655.