ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 5| May 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

PHISHGUARD: A WEB-BASED PHISHING SIMULATION AND AWARENESS TRAINING PLATFORM FOR ORGANIZATIONAL CYBERSECURITY

Yamuna J, Subha M, Yogeshwari J, Vishwa Pooja V
Department of Information Technology, PSNA College of Engineering and Technology, Dindigul, India

ABSTRACT

Phishing remains the leading vector of organizational data breaches globally, with over 36% of reported incidents attributable to deceptive email tactics targeting human behavior rather than technical system vulnerabilities. Existing countermeasures – firewalls, spam filters, and endpoint antivirus tools – are fundamentally ill-suited to address the social engineering dimension of phishing attacks. This paper presents PhishGuard, a web-based Phishing Simulation and Awareness Training Platform designed to systematically evaluate and enhance employee phishing resilience within organizations. PhishGuard enables administrators to orchestrate realistic, customizable phishing simulation campaigns spanning delivery notification scams, HR policy impersonation, password reset directives, and account verification lures. A token-based behavioral tracking engine captures three critical interaction events – email open, link click, and credential submission – and a weighted risk scoring model aggregates these signals into a per-employee composite susceptibility score. An administrative analytics dashboard delivers real-time visual reports, department-level vulnerability heat maps, and campaign effectiveness metrics, enabling precision-targeted training interventions. Upon credential submission, the platform triggers an immediate context-sensitive awareness feedback mechanism that presents phishing indicators and links the employee to a structured training module. A role-based difficulty assignment algorithm calibrates simulation complexity to organizational hierarchy, ensuring equitable and meaningful assessment across all staff tiers. Experimental evaluation across four campaign types and three difficulty levels demonstrates that PhishGuard accurately differentiates phishing susceptibility, measurably reduces click and submission rates following training, and provides actionable intelligence for organizational security posture improvement. The modular RESTful architecture ensures scalability and compatibility with enterprise security ecosystems.

INDEX TERMS – *Phishing Simulation, Cybersecurity Awareness Training, Social Engineering, Behavioral Tracking, Risk Scoring, Security Analytics, Employee Vulnerability Assessment, Spear Phishing.*

I. INTRODUCTION

The digital transformation of organizational operations has dramatically expanded the attack surface available to adversarial actors. Among the full spectrum of contemporary cyber threats, phishing consistently ranks as the most operationally effective and widely deployed attack modality [6][8]. Phishing leverages deceptive electronic communications to impersonate trusted entities—financial institutions, logistics providers, government agencies, and internal departments—with the intent of inducing recipients to disclose credentials, transfer funds, or install malicious payloads [8]. The 2023 Verizon Data Breach Investigations Report identified phishing as the primary initial access vector in 36% of all recorded breaches, underscoring its persistent operational relevance.

What distinguishes phishing from technically sophisticated attack vectors is its deliberate exploitation of cognitive vulnerabilities rather than software weaknesses. Adversaries apply well-documented psychological principles—authority, urgency, scarcity, and social proof—to override employees' critical judgment and compel impulsive action [1][2]. This human-centric attack surface cannot be neutralized through perimeter defenses alone. Even organizations maintaining mature technical security infrastructure—intrusion detection systems, next-generation firewalls, and email gateway filters—routinely fall victim to phishing campaigns that exploit the predictable behavioral patterns of their personnel [1].

The inadequacy of passive, technical-only defenses has catalyzed widespread adoption of security awareness training as a complementary mitigation strategy [7]. Empirical research demonstrates that employees who participate in structured, simulation-based phishing awareness programs exhibit statistically significant reductions in click rates and credential submission rates over time [7]. Despite this evidence, the majority of organizations lack access to dedicated, configurable platforms capable of designing operationally realistic simulations, capturing granular behavioral data, and translating that data into actionable training interventions.

Existing commercial solutions—while functionally capable—frequently impose prohibitive licensing costs, restrict template customization, and fail to integrate campaign management, behavioral analytics, and adaptive training within a unified system. Open-source alternatives typically lack enterprise-grade analytics and role-aware difficulty calibration. This capability gap creates an unmet need for an affordable, flexible, and analytically

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 5| May 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

rigorous phishing simulation platform suited to organizations of varying sizes and security maturity levels.

This paper presents PhishGuard, a web-based Phishing Simulation and Awareness Training Platform that addresses this gap through four core capabilities: (1) configurable, role-aware phishing campaign management; (2) token-based behavioral event tracking with millisecond-precision logging; (3) weighted composite risk scoring with department-level granularity; and (4) immediate, context-sensitive awareness feedback integrated at the point of simulated compromise. The system architecture follows REST principles across four modular layers, ensuring horizontal scalability and integration compatibility with enterprise SIEM and identity management tools.

The remainder of this paper is organized as follows. Section II reviews related work in phishing detection and awareness training. Section III presents the proposed methodology and system architecture. Section IV details the core algorithms underpinning the platform. Section V reports experimental evaluation results and discussion. Section VI concludes with directions for future work.

II. RELATED WORKS

Research addressing phishing as a security challenge bifurcates into two complementary streams: automated technical detection and human behavioral intervention. Understanding the limitations of each stream motivates the integrated approach adopted in this work.

A. Technical Detection Approaches

Early phishing mitigation research concentrated on automated URL and webpage analysis. Jain and Gupta [3] demonstrated that visual similarity metrics between phishing pages and their legitimate counterparts could be exploited to achieve high-accuracy detection, though their approach requires substantial computational resources for real-time deployment. Verma and Dyer [4] established that statistical analysis of lexical and structural URL features could classify phishing domains with precision exceeding 95%, establishing a foundation for lightweight browser-side filters. Subsequent work expanded these approaches through ensemble learning and deep neural architectures [13][15]. Ibrahim and Elhafiz [11] applied BERT and RoBERTa transformer models to phishing email body classification, achieving F1 scores above 0.97 on benchmark datasets. Ming et al. [12] combined BERT embeddings with TF-IDF features in a hybrid architecture that improved robustness against adversarial obfuscation.

Despite these advances, technical detection systems share a structural limitation: they intercept phishing artifacts rather than modifying the human behaviors that determine campaign success. A detection rate of 98% still exposes one in fifty employees to unfiltered phishing content in high-volume email environments. Furthermore, spear-phishing emails—crafted with individualized contextual detail—frequently evade automated classifiers because their content is indistinguishable from legitimate correspondence [16][17][18].

B. Behavioral Awareness and Training Research

Recognizing the irreducible human dimension of phishing susceptibility, Vishwanath et al. [1] conducted a controlled study identifying cognitive elaboration and email habit strength as significant predictors of phishing vulnerability, establishing a psychological basis for training intervention design. Sheng et al. [2] complemented this with demographic susceptibility analysis, finding that younger and older age cohorts exhibited disproportionate vulnerability, informing targeted training program design. Kirlappos and Sasse [7] argued persuasively that conventional security awareness training—characterized by passive lecture-style instruction—produces negligible durable behavior change, and proposed experiential simulation as the theoretically grounded alternative. Hong [6] provided a comprehensive epidemiological survey of phishing attack evolution, documenting the shift from generic mass-phishing to highly personalized spear-phishing as adversaries adapted to improving technical defenses.

C. Existing Simulation Platforms and Gaps

Murhej and Nallasivan [9] proposed a multimodal phishing detection framework combining EM-BERT with LSTM for sequential analysis of email threads, achieving strong results but focusing exclusively on detection rather than awareness training. Al-qasmi et al. [10] evaluated machine learning classifiers for phishing detection, highlighting the generalization limitations of models trained on static datasets against evolving adversarial templates. Commercial phishing simulation platforms such as KnowBe4 and Proofpoint Security Awareness Training offer mature simulation capabilities but are prohibitively expensive for small and medium enterprises and do not expose their behavioral analytics or risk scoring methodologies for academic scrutiny. Sasirekha et al. [14] and Abraham and George [15] surveyed machine learning approaches to email phishing detection, confirming the research community's predominant focus on detection over training. The platform proposed in this paper addresses the identified gaps by delivering: configurable simulation campaigns with role-aware difficulty; granular behavioral event logging; an interpretable weighted risk scoring model; and integrated, immediate awareness feedback—all within an open, extensible web-based architecture.

III. PROPOSED METHODOLOGY

PhishGuard is architected as a modular, four-layer web-based system. The methodology is organized across five functional stages: data acquisition, campaign simulation, behavioral tracking, risk analytics, and awareness intervention. Each stage is designed to operate independently while contributing to a coherent end-to-end phishing resilience assessment workflow.

A. System Architecture

The platform adopts a four-layer architecture: (1) the User Layer, encompassing both the administrator portal and the employee-

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 5| May 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

facing simulation interface; (2) the Application Layer, housing the campaign engine, tracking module, risk scoring service, and feedback system; (3) the Data Layer, comprising the relational event database and campaign configuration store; and (4) the Reporting Layer, delivering the analytics dashboard with real-time visualization. All inter-layer communication is mediated through RESTful APIs using JSON payloads, enabling horizontal scalability and straightforward integration with external security information and event management (SIEM) platforms, identity providers, and Learning Management Systems (LMS). Figure 1 illustrates the complete system architecture.

B. Data Acquisition and User Onboarding

The initial stage establishes the organizational context required for meaningful simulation. Administrators onboard employees via CSV bulk import or manual entry, supplying name, institutional email address, department, and role classification. The platform maps each role to a predefined seniority tier—Executive, Senior Staff, or General Staff—which governs difficulty assignment in subsequent stages. All employee records are encrypted at rest using AES-256 and isolated per organizational tenant to ensure data privacy compliance with applicable data protection regulations. The onboarding module also supports Active Directory and LDAP integration for seamless synchronization with enterprise user directories.

C. Phishing Campaign Simulation Engine

The campaign simulation engine enables administrators to configure and dispatch phishing simulation campaigns through a guided interface. Four template categories are supported, each reflecting statistically prevalent real-world attack patterns: delivery notification scams; HR policy and compliance impersonation; password reset and account security alerts; and financial account verification requests. Templates are parameterized with recipient-specific fields including name, department, and role, ensuring each simulation email is personalized to maximize ecological validity.

Each email is embedded with a unique per-recipient UUID-based tracking token, encoded within a hyperlink that redirects through the PhishGuard tracking endpoint to a simulated phishing landing page. The landing page is visually designed to resemble a legitimate organizational login portal, calibrated to the selected difficulty level. This design permits precise behavioral attribution per recipient and campaign while eliminating exposure to genuine malicious infrastructure.

D. Behavioral Tracking and Event Logging

The tracking module intercepts HTTP requests bearing embedded tokens and classifies interactions into three behavioral event categories: Email Open—detected via an invisible tracking pixel loaded upon email rendering; Link Click—captured when the recipient activates the embedded hyperlink; and Credential Submission—logged when the recipient completes and submits the simulated login form. Each event is persisted with a high-resolution timestamp, campaign identifier, employee identifier, and session metadata. The tracking architecture is designed to function correctly across common email clients including Microsoft Outlook, Gmail, and mobile mail applications. Upon detection of a credential submission event, the system immediately transitions the recipient to an awareness notification page, interrupting the simulated phishing flow and initiating the educational intervention.

E. Analytics Dashboard and Risk Assessment

The analytics module aggregates event logs to produce multi-dimensional susceptibility profiles. At the individual level, a composite risk score is computed per employee per campaign. At the organizational level, department-level vulnerability heat maps and campaign comparison charts are rendered on the administrative dashboard. The dashboard supports drill-down from organizational overview to department, team, and individual employee levels, enabling administrators to identify and prioritize training resources with precision. Figure 2 illustrates the system data flow from campaign creation through analytics generation.

IV. ALGORITHMS USED IN THE PROPOSED SYSTEM

PhishGuard incorporates five purpose-designed algorithms governing campaign delivery, behavioral event capture, risk quantification, awareness delivery, and adaptive difficulty assignment. Each algorithm is presented below with its formal specification.

A. Algorithm 1: Phishing Campaign Scheduling and Email Delivery

This algorithm governs the preparation, personalization, and SMTP dispatch of simulation emails. Unique UUID-based tracking tokens are generated per recipient-campaign pair to enable precise behavioral attribution. Token generation incorporates employee identifier, campaign identifier, and epoch timestamp to guarantee collision-free uniqueness across concurrent campaigns.

```
Algorithm 1: Campaign Email Delivery
Input:  Campaign config C, Employee list
E, Template T
Output: Delivered emails with unique
tracking tokens
BEGIN
  Load C (template type, difficulty
level D, schedule S)
  FOR each employee e in E DO
    token = SHA256(e.id || C.id ||
epoch_timestamp)
    Personalize T with {e.name,
e.department, e.role}
    trackURL = baseURL + "/track?t=" +
token
    pixelURL = baseURL + "/open?t=" +
token
    Embed trackURL and pixelURL into
personalized T
```

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 5| May 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

```
    Store (token, e.id, C.id,
status=SENT, sentAt) in DB
    Dispatch personalized email to
e.email via SMTP
  END FOR
END
```

B. Algorithm 2: Behavioral Event Logging and Awareness Trigger

The tracking server intercepts all incoming HTTP requests bearing valid tokens. Event classification is determined from the request endpoint. All events are timestamped and persisted. Credential submission events additionally trigger an asynchronous awareness notification to the employee, ensuring zero latency between simulated compromise and educational feedback delivery.

```
Algorithm 2: Behavioral Event Logging
Input:  HTTP request R containing
tracking token t
Output: Persisted event log entry;
awareness trigger if SUBMIT
BEGIN
  Validate token t; retrieve (e.id,
C.id) from DB
  IF endpoint == "/open"   THEN event =
OPEN
  IF endpoint == "/track"  THEN event =
CLICK
  IF endpoint == "/submit" THEN event =
SUBMIT
  Log(e.id, C.id, event, UTC_timestamp,
IP, userAgent)
  IF event == SUBMIT THEN
    Trigger AwarenessNotification(e,
C.templateType)
    Redirect browser to
/awareness?t=token
  END IF
END
```

C. Algorithm 3: Weighted Composite Risk Score Computation

The risk scoring algorithm derives a normalized susceptibility score from the three behavioral event rates. Differential weights reflect the increasing severity of each action: email opening (W_1=0.20) indicates exposure; link clicking (W_2=0.30) indicates susceptibility; and credential submission (W_3=0.50) indicates critical compromise. The resulting score supports categorical risk assignment and training prioritization as defined in Table IV.

```
Algorithm 3: Risk Score Computation
Input:  Event log L for employee e over
campaign C
Output: RiskScore [0.0, 1.0], Category
{Low, Medium, High}
BEGIN
  W1=0.20; W2=0.30; W3=0.50
  N = total emails sent to e in campaign
C
  OR = COUNT(OPEN events for e in C) / N
  CR = COUNT(CLICK events for e in C) /
N
  SR = COUNT(SUBMIT events for e in C) /
N
  RiskScore = W1*OR + W2*CR + W3*SR
  IF RiskScore >= 0.60 THEN category =
"High"
  ELSE IF RiskScore >= 0.30 THEN
category = "Medium"
  ELSE category = "Low"
  RETURN (RiskScore, category)
END
```

TABLE IV: Risk Category Thresholds and Recommended Interventions

Risk Category	Score Range	Recommended Action
Low	0.00 – 0.29	Periodic refresher awareness module
Medium	0.30 – 0.59	Targeted phishing awareness workshop
High	0.60 – 1.00	Mandatory retraining and supervisor alert

D. Algorithm 4: Context-Sensitive Awareness Feedback Delivery

Upon credential submission detection, this algorithm retrieves a template-specific set of observable phishing indicators and constructs a personalized awareness page displayed to the employee immediately. The algorithm applies pedagogical principles of immediate corrective feedback and contextual anchoring, presenting the specific warning signs present in the email the employee just interacted with rather than generic phishing guidance.

```
Algorithm 4: Awareness Feedback Delivery
Input:  Employee e, Template type T,
Event = SUBMIT
Output: Personalized awareness page;
training module link
BEGIN
  I = RetrievePhishingIndicators(T)
  // I contains template-specific red
flags
  Render awareness page to e containing:
    - Notification: "This was a
PhishGuard simulation."
    - Highlighted phishing indicators I
from this email
    - Explanation of why each indicator
is suspicious
    - Link to targeted cybersecurity
training module
  Log(e.id, C.id, AWARENESS_DELIVERED,
UTC_timestamp)
END
```

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 5| May 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

E. Algorithm 5: Role-Based Adaptive Difficulty Assignment

To ensure that simulation complexity is proportionate to each employee's organizational role and corresponding threat exposure, the platform maps role tiers to difficulty levels. Senior executives and IT administrators—who are prime targets for spear-phishing campaigns—receive sophisticated, highly personalized templates. General staff receive baseline scenarios representative of mass-phishing attacks. This adaptive approach produces meaningful and differentiated susceptibility measurements across all organizational levels.

```
Algorithm 5: Role-Based Difficulty
Assignment
Input:  Employee e with attribute e.role
Output: Difficulty level D, Filtered
template set TS
BEGIN
  IF e.role IN {CEO, CTO, CFO, Senior
Manager, IT Admin}
    THEN D = Hard   // Spear-phishing,
BEC-style templates
  ELSE IF e.role IN {Team Lead,
Supervisor, Finance Staff}
    THEN D = Medium // Hybrid
generic/targeted templates
  ELSE
    THEN D = Easy   // Generic mass-
phishing templates
  TS = FilterTemplates(TemplateLibrary,
D)
  RETURN (D, TS)
END
```

V. PERFORMANCE EVALUATION AND DISCUSSION

Platform performance was evaluated through a controlled experimental study simulating phishing campaigns against a representative dataset of 480 users drawn from five departments across a mid-sized technology organization. Four campaign types were deployed at three difficulty levels, generating 5,760 individual simulation email interactions. All experiments were conducted within an isolated test environment with IRB-equivalent approval from the participating institution's ethics committee.

A. Evaluation Metrics

The metrics employed to assess platform performance and campaign effectiveness are defined in Table I. The composite Risk Score formula is included as a derived metric.

TABLE I: Evaluation Metrics and Definitions

Metric	Description
Email Delivery Rate	Percentage of simulation emails successfully delivered to target inboxes
Open Rate (OR)	Percentage of recipients who opened the simulated phishing email
Click Rate (CR)	Percentage of recipients who activated the embedded tracking link
Submission Rate (SR)	Percentage of recipients who entered credentials on the simulated page
Awareness Improvement	Reduction in click/submission rates following targeted training intervention
Risk Score	Weighted composite score: RiskScore = 0.20·OR + 0.30·CR + 0.50·SR

B. Experimental Results by Campaign Type

Table II presents aggregate behavioral outcomes across the four campaign types at mixed difficulty settings. Delivery scam campaigns elicited the highest link activation rate (42%), consistent with prior research establishing the potency of logistics-themed lures, which exploit the high base rate of online parcel deliveries and associated recipient expectation [2]. HR policy alert campaigns produced the highest email open rate (81%), attributable to the perceived institutional authority of human resources communications. Password reset campaigns generated the lowest credential submission rate (33%), suggesting employees exercise elevated scrutiny toward security-themed notifications—a finding consistent with the increasing prevalence of multi-factor authentication awareness training in enterprise environments.

TABLE II: Phishing Campaign Performance Metrics by Template Type

Campaign Type	Sent	Delivered	Open (%)	Click (%)	Report (%)
Delivery Scam	120	115	78	42	18
HR Policy Alert	120	118	81	36	15
Password Reset	120	117	75	33	12
Account Verification	120	116	70	29	20

C. Difficulty Level Impact Analysis

Table III presents the effect of difficulty configuration on user behavioral outcomes across all campaign types. A pronounced inverse relationship exists between difficulty level and susceptibility indicators: transitioning from Easy to Hard difficulty reduces the click rate from 48% to 22% and the credential submission rate from 21% to 8%, while the reporting rate increases from 15% to 38%. This pattern demonstrates two

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 5| May 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

important findings: first, the role-based difficulty assignment algorithm successfully differentiates simulation complexity in ways that produce meaningfully distinct behavioral responses; second, employees at higher difficulty tiers—predominantly senior staff targeted with spear-phishing templates—demonstrate superior baseline vigilance, validating the construct validity of the difficulty calibration approach.

TABLE III: Difficulty Level Impact on Employee Behavioral Outcomes

Difficulty Level	Click Rate (%)	Submission Rate (%)	Reporting Rate (%)
Easy	48	21	15
Medium	36	14	24
Hard	22	8	38

D. Awareness Training Effectiveness

A longitudinal sub-study tracked 120 employees classified as High risk (RiskScore ≥ 0.60) following initial campaign exposure. After completing the platform-assigned targeted training module, the same cohort was re-exposed to an equivalent campaign one month later. Mean click rate for the cohort declined from 61% to 28%, and credential submission rate declined from 34% to 11%—reductions of 54% and 68% respectively. These outcomes provide empirical support for the effectiveness of the platform's context-sensitive, point-of-failure awareness delivery mechanism in producing durable behavioral change.

E. Comparative Discussion

Relative to existing commercial phishing simulation platforms, PhishGuard distinguishes itself through three contributions. First, the weighted risk scoring model provides an interpretable, mathematically grounded susceptibility quantification that commercial platforms typically obscure behind proprietary algorithms. Second, role-based adaptive difficulty ensures that simulation realism is calibrated to the specific threat landscape faced by each organizational tier, producing more ecologically valid measurements than uniform difficulty deployments. Third, the immediate context-sensitive awareness feedback mechanism—triggered at the precise moment of simulated compromise—aligns with established principles of effective behavioral correction, contrasting with the deferred, generic training modules typical of existing solutions. Collectively, these features position PhishGuard as a rigorous, transparent, and practically deployable organizational phishing resilience tool.

VI. CONCLUSION

Phishing attacks persist as the dominant initial access vector in organizational cyber incidents, succeeding through the systematic exploitation of human cognitive vulnerabilities rather than technical system weaknesses [6][8]. The absence of dedicated, analytically rigorous, and cost-accessible simulation platforms represents a critical capability gap for organizations seeking to build phishing-resistant workforces.

This paper presented PhishGuard, a web-based Phishing Simulation and Awareness Training Platform that addresses this gap through a four-layer modular architecture integrating configurable campaign management, token-based behavioral tracking, weighted composite risk scoring, role-adaptive difficulty assignment, and context-sensitive awareness feedback. Experimental evaluation across 480 participants and 5,760 simulated interactions demonstrated that the platform accurately quantifies phishing susceptibility at individual and departmental levels, that the role-based difficulty algorithm produces ecologically valid and differentiated behavioral measurements, and that the integrated awareness feedback mechanism drives substantial and durable reductions in click and credential submission rates.

The platform makes three principal contributions to the field: a transparent, interpretable weighted risk scoring model; an adaptive difficulty calibration framework grounded in organizational role hierarchy; and an integrated point-of-failure awareness intervention that applies established behavioral correction principles. These contributions collectively advance both the scientific understanding of organizational phishing susceptibility and the practical toolkit available to security administrators.

Future work will extend PhishGuard in three directions. First, integration of transformer-based NLP models—specifically fine-tuned BERT variants [11][12]—will enable automated generation of personalized, contextually coherent spear-phishing templates, substantially expanding simulation realism. Second, longitudinal risk trajectory modeling using recurrent neural networks will enable the platform to predict future susceptibility and proactively prescribe training interventions before compromise occurs. Third, integration with enterprise SIEM platforms will enable correlation of simulation-derived risk scores with real-world security incident data, enabling validation of the platform's predictive validity in operational environments.

ACKNOWLEDGMENT

The authors express sincere gratitude to the Department of Information Technology, PSNA College of Engineering and Technology, Dindigul, for providing the computational infrastructure and institutional support that facilitated this research. The authors also acknowledge the constructive feedback received from peer reviewers and faculty mentors during the development of the PhishGuard platform.

REFERENCES

1. *A. Vishwanath, T. Herath, R. Chen, J. Wang, and H. Rao, "Why do people get phished? Testing individual differences in phishing vulnerability," Decision Support Systems, vol. 51, no. 3, pp. 576–586, Jun. 2011. doi: 10.1016/j.dss.2011.01.002*

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 5| May 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

2. *S. Sheng, M. Holbrook, P. Kumaraguru, L. Cranor, and J. Downs, "Who falls for phish? A demographic analysis of phishing susceptibility," in Proc. SIGCHI Conf. Human Factors Comput. Syst. (CHI), Atlanta, GA, USA, Apr. 2010, pp. 373–382. doi: 10.1145/1753326.1753383*
3. *A. K. Jain and B. B. Gupta, "Phishing detection: Analysis of visual similarity-based approaches," Security and Communication Networks, vol. 10, no. 13, pp. 1–14, Sep. 2017. doi: 10.1002/sec.1864*
4. *R. Verma and K. Dyer, "On the character of phishing URLs: Accurate and robust statistical learning classifiers," in Proc. 5th ACM Conf. Data and Application Security and Privacy (CODASPY), San Antonio, TX, USA, Mar. 2015, pp. 111–122. doi: 10.1145/2699026.2699115*
5. *Anti-Phishing Working Group (APWG), "Phishing Activity Trends Report, Q4 2023," APWG, Tech. Rep., 2024. [Online]. Available: https://apwg.org/trendsreports/*
6. *J. Hong, "The state of phishing attacks," Communications of the ACM, vol. 55, no. 1, pp. 74–81, Jan. 2012. doi: 10.1145/2063176.2063197*
7. *I. Kirlappos and M. A. Sasse, "Security education against phishing: A modest proposal for a major rethink," IEEE Security & Privacy, vol. 10, no. 2, pp. 24–32, Mar. 2012. doi: 10.1109/MSP.2011.179*
8. *N. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, "Phishing attacks: A recent comprehensive study and a new anatomy," Frontiers in Computer Science, vol. 3, Mar. 2021. doi: 10.3389/fcomp.2021.563060*
9. *M. Murhej and G. Nallasivan, "Multimodal Framework for Phishing Attack Detection and Mitigation Using EM-BERT and LSTM," Frontiers in Communication Networks, 2025.*
10. *A. Al-qasmi et al., "Machine Learning-Based Phishing Detection System," International Journal of Intelligent Systems and Applications in Engineering, 2024.*
11. *M. Ibrahim and R. Elhafiz, "Phishing Email Detection Using BERT and RoBERTa," Computation, vol. 14, no. 2, p. 46, 2026.*
12. *C. C. Ming, M. N. Al-Andoli, and C. Zheng, "Hybrid Phishing Detection Model: Integrating BERT with TF-IDF for Enhanced Email Security," International Journal on Robotics, Automation and Sciences, 2025.*
13. *"Comparative Analysis of Machine Learning Algorithms for Email Phishing Detection Using TF-IDF, Word2Vec, and BERT," Computers, Materials & Continua, 2024.*
14. *C. Sasirekha, R. Nandhini et al., "Email Phishing Detection Using Machine Learning," International Journal of Engineering Research & Technology (IJERT), 2023.*
15. *S. Abraham and S. George, "A Review of Phishing Email Detection based on Different Machine Learning Methods," IJERT Conference Paper, 2022.*
16. *Y. Lee, J. Saxe, and R. Harang, "CATBERT: Context-Aware Tiny BERT for Detecting Social Engineering Emails," arXiv preprint arXiv:2012.10947, 2020.*
17. *S. Mahendru and T. Pandit, "SecureNet: A Comparative Study of DeBERTa and Large Language Models for Phishing Detection," 2024.*
18. *I. Altan, A. Bachir et al., "Dual-Path Phishing Detection: Integrating Transformer-Based NLP with Structural URL Analysis," 2025.*