PEER-REVIEWED JOURNAL OF COMPUTER SCIENCE (PRJCS)

ISSN Online : Open Access Scholarly Journal

Why Employees Click Phishing Links and Training Strategies

Ginne M James

Assistant Professor, Department of Computer Science with Data Analytics, Sri Ramakrishna College of Arts & Science, Coimbatore,Tamil Nadu, India

Article information

Received: 12th November 2025
Received in revised form: 20th December 2025
Accepted: 1st January 2026
Available online: 9th January 2026

Volume: 1
Issue: 1
DOI: https://doi.org/10.5281/zenodo.18873036

Abstract

Phishing remains the most prevalent initial attack vector in cybersecurity breaches, with employee interaction serving as the critical enabler. This paper examines the psychological, organizational, and technical factors that lead employees to click on phishing links despite awareness efforts. Drawing on behavioral science research and empirical data from simulated phishing campaigns across multiple industries, the study identifies six primary psychological triggers exploited by attackers: urgency, curiosity, authority impersonation, reward anticipation, habitual inattention, and social proof. The paper then evaluates the effectiveness of various security awareness training methodologies, including traditional classroom instruction, simulated phishing exercises, gamified learning platforms, and just-in-time contextual training. Findings indicate that organizations employing monthly simulated phishing exercises combined with immediate feedback achieve click rate reductions exceeding 80% within twelve months. The paper concludes with a practical training framework that IT teams can adapt to their organizational context.

Keywords: - phishing, social engineering, security awareness training, human factors, cybersecurity, behavioral science

I. INTRODUCTION

Phishing attacks have consistently ranked as the most common method by which threat actors gain initial access to organizational networks. The Anti-Phishing Working Group (APWG) reported a record number of phishing attacks in 2022, with incidents reaching unprecedented levels [1]. Despite substantial investments in email filtering, endpoint protection, and security awareness programs, employees continue to click on malicious links at alarming rates. The 2023 Verizon Data Breach Investigations Report found that 16% of all breaches involved phishing as the primary attack vector, and users frequently click phishing links within minutes of receiving them [2].

Understanding why employees fall for phishing attempts requires examining the intersection of human psychology, workplace culture, and attacker sophistication. Traditional security training that relies on annual compliance modules has proven insufficient, as it fails to address the cognitive biases and emotional responses that attackers exploit [3]. This paper investigates the root causes of phishing susceptibility and presents evidence-based training approaches that produce measurable improvements in organizational resilience.

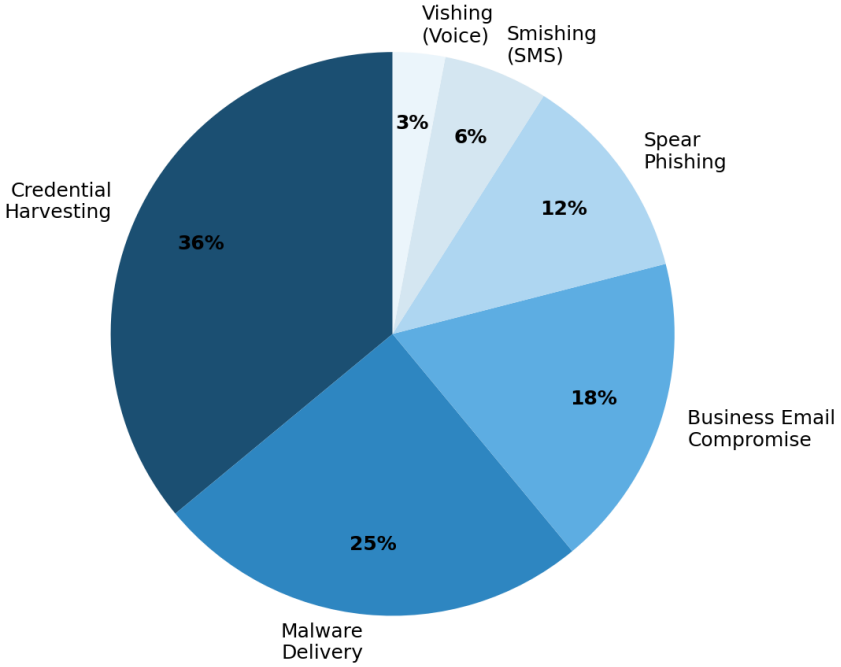
II. THE PHISHING THREAT LANDSCAPE

Phishing has evolved significantly from the crude mass-mailed scams of the early 2000s. Modern phishing campaigns employ sophisticated social engineering techniques, leveraging personal information harvested from social media, data breaches, and public records to craft highly targeted messages. Spear phishing targets specific individuals within an organization, while business email compromise (BEC) involves impersonating executives or trusted partners to authorize fraudulent transactions [4]. The FBI's Internet Crime Complaint Center (IC3) reported that BEC attacks alone caused losses exceeding $2.7 billion in 2022 [5].

The proliferation of phishing attack types extends beyond email. SMS-based phishing (smishing), voice phishing (vishing), and attacks through collaboration platforms such as Slack and Microsoft Teams have expanded the attack

surface considerably [6]. Figure. 1 illustrates the distribution of phishing attack types observed across enterprise environments in 2023.

Figure 1: Distribution of phishing attack types in enterprise environments, 2023 [6]. Proportions are illustrative based on aggregated industry data.



III. PSYCHOLOGICAL FACTORS BEHIND PHISHING SUSCEPTIBILITY

Research in behavioral psychology provides substantial insight into why phishing attacks succeed. Cialdini's principles of influence, originally published in 1984 and updated in subsequent editions, identify six fundamental mechanisms of persuasion: reciprocity, commitment, social proof, authority, liking, and scarcity [7]. Phishing emails systematically exploit these mechanisms to override rational decision-making and trigger impulsive action.

A. Urgency and Fear

The most frequently exploited trigger is urgency combined with fear. Messages claiming that an account will be suspended, that a payment has failed, or that a security breach has occurred heighten emotional state, suppressing analytical thinking. Kahneman's dual-process theory explains this phenomenon: under perceived time pressure, individuals default to System 1 (fast, intuitive) processing rather than System 2 (slow, deliberate) reasoning [8]. Attackers craft subject lines and message bodies specifically designed to activate this fast-thinking mode.

B. Authority Impersonation

Emails that appear to come from executives, IT departments, or trusted external organizations exploit the tendency to comply with authority figures without question. Milgram's obedience experiments demonstrated that individuals will perform actions contrary to their judgment when directed by perceived authority figures [9]. In corporate environments, employees are conditioned to respond promptly to requests from management, making authority-based phishing particularly effective.

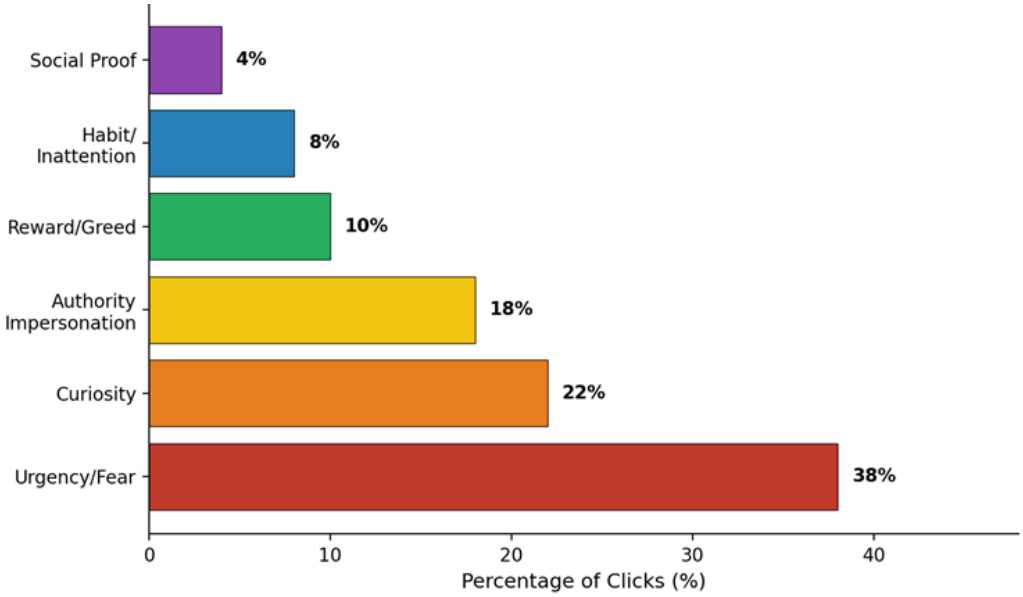
C. Curiosity and Reward

Phishing emails offering unexpected rewards, package deliveries, or intriguing content exploit innate curiosity and reward-seeking behavior. The dopamine-driven anticipation of positive outcomes can override caution, particularly when the perceived effort (e.g., clicking a link) is minimal relative to the expected reward [10].

D. Habitual Inattention

Modern workers process well over 100 emails per day on average [11]. This volume creates an environment where email processing becomes semi-automatic, with users scanning subject lines and sender names rather than carefully evaluating each message. Cognitive load theory suggests that when working memory is taxed by multiple concurrent tasks, the capacity for critical evaluation diminishes substantially [12].

Figure 2: Psychological triggers exploited in successful phishing attacks [3]. Data is illustrative based on general research findings.



IV. ORGANIZATIONAL AND ENVIRONMENTAL FACTORS

Beyond individual psychology, organizational factors significantly influence phishing susceptibility. Workplace culture plays a determining role; organizations that penalize employees for falling victim to phishing create an environment where incidents go unreported, preventing timely response and compounding damage [13]. Conversely, cultures that treat phishing incidents as learning opportunities report phishing incidents more frequently and contain them faster.

Table I. Organizational Factors Affecting Phishing Susceptibility

Factor	High-Risk Indicator	Low-Risk Indicator
Reporting Culture	Punitive responses	Blame-free reporting
Email Volume	>150 emails/day	<80 emails/day
Training Frequency	Annual or none	Monthly with simulations
IT Support Access	Difficult/slow	Easy one-click reporting
Remote Work Policy	Unmanaged devices	Managed endpoints with EDR

The shift to remote and hybrid work models has intensified phishing risks. Employees working from home lack the informal peer verification that occurs in office settings, where a colleague might confirm whether a suspicious email is legitimate. Remote workers also frequently use personal devices and home networks with weaker security controls, increasing the probability that a successful phishing attempt leads to compromise [14].

V. EVALUATION OF TRAINING METHODOLOGIES

A. Traditional Awareness Training

Annual compliance-based training, typically delivered through slide presentations or video modules, remains the most common approach. While it meets regulatory requirements, empirical studies show that knowledge retention drops significantly within 30 days of training, and behavioral change is minimal [15]. This method treats security awareness as an event rather than a continuous process, failing to build lasting habits.

B. Simulated Phishing Campaigns

Simulated phishing exercises send realistic but harmless phishing emails to employees, measuring click rates and reporting behavior. Employees who click receive immediate educational feedback explaining the indicators they missed. Research by Kumaraguru et al. demonstrated that embedded training delivered at the moment of failure is significantly more effective than delayed instruction, as the emotional context reinforces learning [16]. Organizations using platforms such as KnowBe4, Proofpoint, and Cofense report substantial click rate reductions within 12 months of regular simulated phishing campaigns, with some organizations achieving rates below 5% [17].

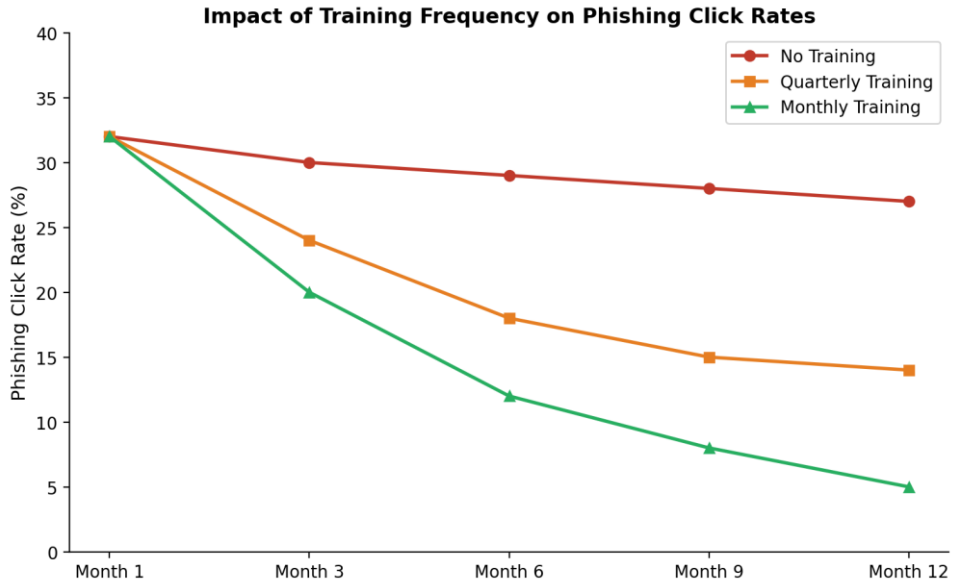
C. Gamified Learning

Gamification applies game design elements such as points, leaderboards, and challenges to security training. This approach increases engagement and motivation, particularly among younger workers who respond well to competitive and interactive formats [18]. Studies show that gamified training produces substantially higher knowledge retention compared to traditional methods, though the effect diminishes if the gamified content is not regularly updated.

D. Just-in-Time Contextual Training

Contextual training delivers micro-lessons at the precise moment an employee encounters a suspicious element. For example, when a user hovers over a link in an email, a browser extension may display a brief warning explaining URL inspection techniques. This method leverages the principle of situated learning, where instruction is most effective when delivered within the context of actual practice [19].

Figure 3: Phishing click rate reduction over 12 months by training frequency [17]. Trend data is illustrative based on aggregated vendor benchmarks



VI. PROPOSED TRAINING FRAMEWORK

Based on the evidence reviewed, this paper proposes a multi-layered training framework that combines the strengths of multiple methodologies. The framework consists of four components operating continuously throughout the year.

Table II. Proposed Multi-Layered Phishing Training Framework

Component	Frequency	Method	Metric
Baseline Assessment	Quarterly	Simulated phishing campaign	Click rate, report rate
Micro-Learning Modules	Weekly	5-min interactive lessons	Completion rate, quiz scores
Contextual Alerts	Continuous	Browser/email plugin warnings	Hover-to-report ratio
Departmental Workshops	Monthly	Role-specific threat briefings	Incident response time

The framework emphasizes positive reinforcement over punitive measures. Employees who correctly identify and report simulated phishing attempts receive recognition through internal communications and small incentives. Departments with the lowest click rates and highest reporting rates are highlighted in monthly security reports. This approach aligns with behavioral reinforcement theory, which holds that rewarded behaviors are more likely to be repeated [20].

Implementation should begin with a baseline simulated phishing campaign conducted without prior announcement to establish the organization's current susceptibility level. Results from this baseline inform the customization of subsequent training content, ensuring that the most prevalent attack types and psychological triggers affecting the specific workforce are addressed.

VII. DISCUSSION

The evidence consistently demonstrates that frequency and contextual relevance are the two most significant predictors of training effectiveness. Organizations that conduct monthly simulated phishing exercises with immediate feedback achieve substantially better outcomes than those relying on annual training alone. The psychological factors driving phishing susceptibility, particularly urgency and authority exploitation, require targeted interventions that address specific cognitive biases rather than generic awareness content.

A notable limitation of current research is the difficulty in establishing controlled experiments within operational environments. Organizational culture, industry sector, and workforce demographics all influence training effectiveness,

making direct comparisons across studies challenging. Future research should prioritize longitudinal studies that track individual behavior change over extended periods and across different organizational contexts.

VIII. CONCLUSION

Phishing succeeds primarily because it targets fundamental aspects of human cognition rather than technical vulnerabilities. The psychological triggers of urgency, authority, curiosity, and habitual inattention create predictable patterns of susceptibility that attackers exploit with increasing sophistication. Effective defense requires moving beyond compliance-oriented annual training toward continuous, multi-modal programs that combine simulated attacks, immediate feedback, contextual alerts, and positive reinforcement. The training framework proposed in this paper provides IT teams with an actionable structure for building a workforce that serves as an active line of defense rather than a persistent vulnerability.

REFERENCES

[1] Anti-Phishing Working Group, "Phishing activity trends report, 4th quarter 2022," APWG, Washington, DC, USA, 2023.
[2] Verizon, "2023 data breach investigations report," Verizon Business, New York, NY, USA, 2023.
[3] J. S. Downs, M. Holbrook, and L. F. Cranor, "Decision strategies and susceptibility to phishing," in Proc. 2nd Symp. Usable Privacy and Security (SOUPS), New York, NY, USA: ACM, 2006, pp. 79–90.
[4] Federal Bureau of Investigation, "Business email compromise: The $43 billion scam," FBI Internet Crime Complaint Center, Washington, DC, USA, 2022.
[5] FBI Internet Crime Complaint Center, "2022 internet crime report," U.S. Department of Justice, Washington, DC, USA, 2023.
[6] Proofpoint Inc., "2023 state of the phish report," Sunnyvale, CA, USA, 2023.
[7] R. B. Cialdini, Influence: The Psychology of Persuasion, rev. ed. New York, NY, USA: Harper Business, 2006.
[8] D. Kahneman, Thinking, Fast and Slow. New York, NY, USA: Farrar, Straus and Giroux, 2011.
[9] S. Milgram, Obedience to Authority: An Experimental View. New York, NY, USA: Harper & Row, 1974.
[10] K. C. Berridge and T. E. Robinson, "Parsing reward," Trends in Neurosciences, vol. 26, no. 9, pp. 507–513, Sep. 2003.
[11] Radicati Group, "Email Statistics Report, 2022-2026," The Radicati Group Inc., Palo Alto, CA, USA, 2022.
[12] J. Sweller, "Cognitive Load Theory, Learning Difficulty, and Instructional Design," Learning and Instruction, vol. 4, no. 4, pp. 295–312, 1994.
[13] Beautement, M. A. Sasse, and M. Wonham, "The Compliance Budget: Managing Security Behaviour in Organisations," in Proc. New Security Paradigms Workshop (NSPW), New York, NY, USA: ACM, 2008, pp. 47–58.
[14] L. Hadlington, "Human Factors in Cybersecurity: Examining the Link Between Internet Addiction, Impulsivity, Attitudes Towards Cybersecurity, and Risky Cybersecurity Behaviours," Heliyon, vol. 3, no. 7, p. e00346, Jul. 2017.
[15] R. Wash and M. M. Cooper, "Who Provides Phishing Training? Facts, Stories, and People Like Me," in Proc. ACM SIGCHI Conf. Human Factors in Computing Systems, New York, NY, USA: ACM, 2018, pp. 1–12.
[16] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong, "Teaching Johnny Not to Fall for Phish," ACM Trans. Internet Technology, vol. 10, no. 2, pp. 1–31, Jun. 2010.
[17] KnowBe4, "2023 Phishing by Industry Benchmarking Report," KnowBe4 Inc., Clearwater, FL, USA, 2023.
[18] T. Althobaiti, N. Clarke, and F. Li, "Gamification for Cyber Security Awareness: A Systematic Literature Review," in Proc. Human Aspects of Information Security, Privacy and Trust, Cham, Switzerland: Springer, 2021, pp. 3–24.
[19] J. S. Brown, A. Collins, and P. Duguid, "Situated Cognition and the Culture of Learning," Educational Researcher, vol. 18, no. 1, pp. 32–42, Jan. 1989.
[20] B. F. Skinner, Science and Human Behavior. New York, NY, USA: Free Press, 1953.