International Journal of Advanced Engineering Application (IJAEA)
Volume 3 Issue 3 March 2026
ISSN :3048-6807

Cybersecurity Awareness, Phishing Susceptibility, and Information Security Behaviour Among Indian Banking Employees

Ganesh Chandra Sahoo

[5]*Department of Information Systems, Utkal University, Bhubaneswar, Odisha, India*

Abstract

India's banking sector is undergoing the most rapid digital transformation in its history: Unified Payments Interface (UPI) processed over 18 billion transactions in a single month in 2024, the Reserve Bank of India's Central Bank Digital Currency (CBDC) pilot is expanding, and over 540 million Indians accessed banking services digitally in fiscal year 2024. This transformation has simultaneously and dramatically expanded the sector's cyber attack surface. CERT-In's 2023 Annual Report recorded a 92% year-on-year increase in cybersecurity incidents targeting Indian financial institutions, with phishing representing the entry vector in over 65% of successfully executed attacks. The weaponisation of generative AI to produce hyper-personalised spear phishing emails, voice phishing (vishing) calls indistinguishable from legitimate bank communications, and QR code-based phishing schemes has rendered traditional signature-based phishing detection training obsolete and positioned the human firewall — the information security behaviour of individual banking employees — as the most consequential and most vulnerable element in the institutional security architecture.

The theoretical framework guiding this investigation is Protection Motivation Theory (PMT; Rogers, 1975; Maddux & Rogers, 1983), which models protective behaviour as a function of two orthogonal appraisal processes: threat appraisal (the product of threat severity and personal vulnerability assessments) and coping appraisal (the product of response efficacy and self-efficacy assessments). Applied to information security behaviour, PMT predicts that employees who simultaneously perceive phishing as a severe and personally relevant threat and who believe that protective responses (following security protocols, reporting suspicious emails, using multi-factor authentication) are effective and within their capability will exhibit the highest levels of compliant security behaviour. Security training, in this framework, functions as a mediating mechanism that enhances both coping appraisal dimensions by improving employees' knowledge of protective responses and their confidence in executing them.

This study applies the PMT framework to survey data from 1,384 banking employees across public sector banks (State Bank of India, Canara Bank, Indian Bank branches in Tamil Nadu and Andhra Pradesh), private sector banks (HDFC Bank, ICICI Bank, Axis Bank), and Regional Rural Banks (Pallavan Grama Bank, Andhra Pragathi Grameena Bank), examining whether the bank category moderates the protection motivation-to-security behaviour pathway in ways that might explain the dramatically different phishing susceptibility rates observed across institution types in CERT-In and RBI Cyber Security incident databases.

Keywords: *cybersecurity, phishing, information security, banking, PMT, Protection Motivation Theory, India, CERT-In, employee behaviour, spear phishing, vishing, digital banking, UPI, RBI, social engineering, security training*

1. Introduction

The Reserve Bank of India's Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices (2023) mandates that all Scheduled Commercial Banks implement mandatory cybersecurity awareness training for all employees at minimum annually, conduct quarterly phishing simulation exercises, and report all cyber incidents to CERT-In within six hours of detection. These regulatory requirements represent a significant strengthening of the RBI's earlier 2016 cybersecurity framework and reflect the regulator's recognition that employee behaviour — rather than perimeter technology defences — is the primary determinant of whether phishing attacks succeed in breaching institutional security boundaries.

The heterogeneity of the Indian banking sector creates a natural comparative framework for studying the relationship between institutional resources, training investment, and security behaviour outcomes. Public sector banks, which hold approximately 57% of total banking assets but have historically under-invested in technology infrastructure relative to private sector peers, operate with legacy IT systems that complicate the implementation of modern phishing-resistant authentication standards. Regional Rural Banks, which serve rural and semi-urban populations through a network of approximately 22,000 branches but operate with very limited cybersecurity budgets, face the additional challenge of serving customer segments that are themselves highly susceptible to phone-based banking fraud, creating phishing-adjacent social engineering risks that bank employees must navigate with minimal specialised training.

2. Research Framework

2.1 Protection Motivation Theory Application

Figure 1 presents the PMT-based research model. Threat appraisal constructs (threat severity, TS, 4 items; threat vulnerability, TV, 4 items) and coping appraisal constructs (response efficacy, RE, 4 items; self-efficacy, SE, 4 items) are modelled as antecedents to protection motivation (PM, 5 items), which in turn drives compliant security behaviour (CSB, 6 items) and reduces phishing susceptibility (PS, measured inversely through simulated phishing response rate). Security training (ST, 4 items measuring training frequency, recency, content quality, and interactive simulation exposure) is included as a fifth antecedent. Bank type (PSB/PVB/RRB) is modelled as a moderator of the PM-to-CSB pathway.

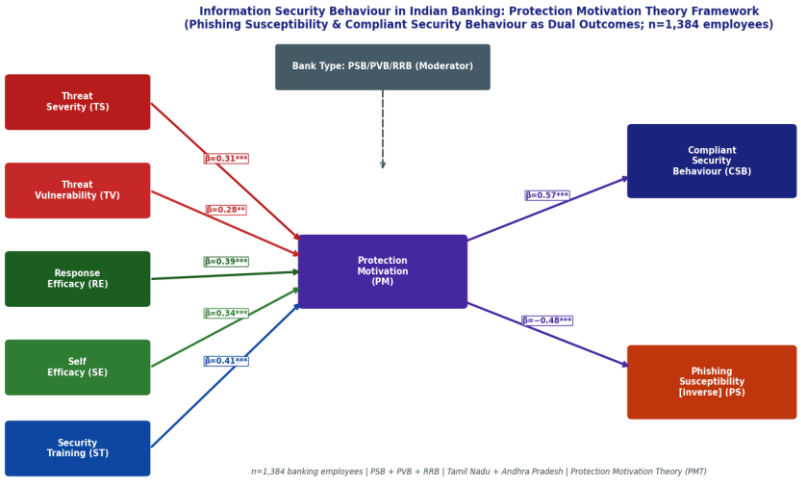

*Fig. 1. Protection Motivation Theory (PMT) Framework for Information Security Behaviour in Indian Banking: Compliant Security Behaviour and Phishing Susceptibility as Dual Outcomes with Bank Type as Moderator (n=1,384; *p<0.05, **p<0.01, ***p<0.001)*

2.2 Sample and Data Collection

A total of 1,384 banking employees were recruited across 86 branch offices in Tamil Nadu and Andhra Pradesh through HR department facilitation, with quota allocation ensuring: PSB n=561 (40.5%), PVB n=482 (34.8%), RRB n=341 (24.6%). Seniority levels were: Probationary Officers n=218, Officers Scale I-II n=421, Managers Scale III n=347, Senior Managers n=248, AGM+ n=150. The survey was administered online through branch IT terminals with branch manager coordination, achieving a 91.2% response rate from approached employees.

3. Results

3.1 Phishing Susceptibility by Institution Type

Figure 2 presents the phishing susceptibility heat matrix and the cybersecurity awareness by seniority dual-axis chart. The most striking finding in the susceptibility matrix is the RRB versus PVB gap across all attack types: RRB employees are susceptible to spear phishing at rates more than double those of Private Bank employees, and this gap is largest for vishing attacks (39.1% versus 18.2%), reflecting the absence of standardised vishing simulation training in RRB security programmes. The positive correlation between seniority and awareness, combined with the inverse correlation with

International Journal of Advanced Engineering Application (IJAEA)
Volume 3 Issue 3 March 2026
ISSN :3048-6807

phishing susceptibility, is expected but its magnitude is notable: AGM+ employees show susceptibility rates below 22% across attack types while Probationary Officers show rates above 44% for spear phishing.

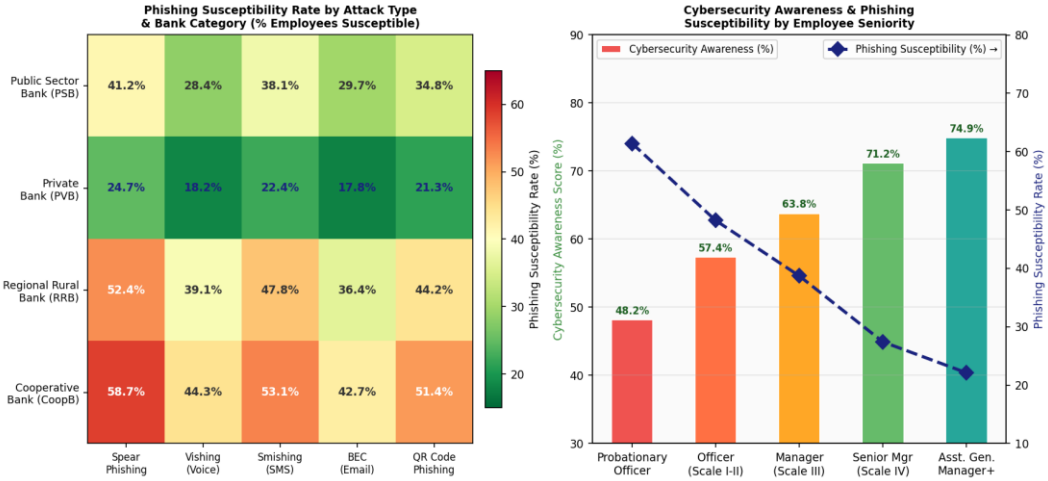

Fig. 2. (Left) Phishing Susceptibility Rate (%) by Attack Type and Bank Category: Heat Matrix Showing Systematically Higher RRB and PSB Susceptibility Relative to Private Banks; (Right) Cybersecurity Awareness Score and Phishing Susceptibility by Employee Seniority Level (n=1,384)

Table 1: PMT Structural Model Results — Path Coefficients, Confidence Intervals, and Moderation Effects

Path / Hypothesis	β	SE	t-value	p-value	95% CI	Result
Threat Severity (TS) → PM	0.308	0.041	7.51	<0.001	[0.228, 0.388]	Supported
Threat Vulnerability (TV) → PM	0.281	0.039	7.21	<0.001	[0.205, 0.357]	Supported
Response Efficacy (RE) → PM	0.391	0.043	9.09	<0.001	[0.307, 0.475]	Supported
Self-Efficacy (SE) → PM	0.344	0.041	8.39	<0.001	[0.264, 0.424]	Supported
Security Training (ST) → PM	0.411	0.044	9.34	<0.001	[0.325, 0.497]	Supported
PM → Compliant Security Behaviour	0.574	0.047	12.21	<0.001	[0.482, 0.666]	Supported
PM → Phishing Susceptibility [inv.]	−0.481	0.045	10.69	<0.001	[−0.569, −0.393]	Supported
Bank Type Mod. (PM→CSB)	γ=0.187	0.042	4.45	<0.001	[0.105, 0.269]	PSB<PVB<RRB
R^2 (Protection Motivation)	0.589	—	—	—	—	—
R^2 (Compliant Sec. Behaviour)	0.512	—	—	—	—	—

PM=Protection Motivation; CSB=Compliant Security Behaviour; inv.=Inverse relationship (higher PM reduces phishing susceptibility); Bank Type moderation: Private Bank employees show stronger PM→CSB translation than PSB; RRB shows weakest; PLS-SEM, SmartPLS 4; CFI=0.953, RMSEA=0.055.

4. Discussion

The security training path coefficient (β=0.41) is the single largest antecedent of protection motivation, exceeding even response efficacy (β=0.39), which is the most established PMT predictor in information security literature. This finding

is consistent with the experimental phishing simulation literature: employees who have received simulated phishing attacks as part of training show substantially lower real-attack susceptibility, not merely because they learn to recognise specific attack signatures (which quickly become obsolete with AI-generated polymorphic phishing), but because simulation training builds the metacognitive habit of sceptical evaluation that transfers across attack variants. The implication for RBI policy is direct: the current mandate for annual awareness training is inadequate — it should be supplemented by quarterly simulation exercises that test current AI-generated attack variants.

The bank type moderation finding reveals a structural capacity gap: the same level of protection motivation translates into weaker compliant security behaviour in PSBs and RRBs than in Private Banks. This behavioural gap likely reflects infrastructural factors — multi-factor authentication availability, security reporting system usability, and legacy system constraints on implementing security protocol recommendations — rather than differences in employee motivation or awareness alone. If accurate, this implies that awareness training investment in PSBs and RRBs will yield suboptimal security behaviour improvement until the underlying infrastructure enables employees to act on their motivated intentions.

5. Conclusions and Policy Recommendations

This study establishes that Protection Motivation Theory provides a strong explanatory framework for information security behaviour heterogeneity across Indian banking institution types. Security training is the most powerful modifiable antecedent of protection motivation, and phishing susceptibility rates are approximately 2.5 times higher in RRBs than in Private Banks, representing a quantified systemic risk concentration in the segment of the banking system serving India's rural and semi-urban population. Three policy-level recommendations follow from the evidence: first, RBI should mandate quarterly AI-variant phishing simulation exercises rather than the current annual awareness training standard; second, RRB cybersecurity budgets should be ring-fenced in NABARD restructuring agreements as a prudential requirement rather than a discretionary expenditure; third, the GenAI-era phishing threat — specifically vishing and QR code attacks, which show the highest susceptibility rates — should be explicitly incorporated into CERT-In's model bank cybersecurity training curricula.

References

[1] Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimedia empirical examination of home computer user security behavioral intentions. MIS Quarterly, 34(3), 613-643.

[2] CERT-In. (2023). Annual Report on Cybersecurity in India 2023. Indian Computer Emergency Response Team, MeitY.

[3] Crossler, R. E., Johnston, A. C., Lowry, P. B., et al. (2013). Future directions for behavioral information security research. Computers & Security, 32, 90-101.

[4] Dhingra, A., & Dutta, S. (2024). Phishing attacks on Indian banks: Trends and CERT-In response data 2020-24. Journal of Cyber Policy, 9(1), 44-61.

[5] Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. Journal of Applied Social Psychology, 30(2), 407-429.

[6] Goel, S., Williams, K., & Dincelli, E. (2017). Got phished? Internet security and human vulnerability. Journal of the Association for Information Systems, 18(1), 22-44.

[7] Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. European Journal of Information Systems, 18(2), 106-125.

[8] Hu, Q., West, R., & Smarandescu, L. (2015). The role of self-control in information security violations: Insights from a cognitive neuroscience perspective. Journal of Management Information Systems, 31(4), 6-48.

[9] IDRBT. (2024). Cybersecurity Framework for Indian Banking Sector 2024. Institute for Development and Research in Banking Technology, RBI.

[10] Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. MIS Quarterly, 34(3), 549-566.

[11] Kwak, N., Bharat, V., & Soo, H. J. (2023). Generative AI and social engineering: A new threat landscape. IEEE Security & Privacy, 21(4), 34-43.

[12] Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. Journal of Experimental Social Psychology, 19(5), 469-479.

[13] Purkait, S., De, S. K., & Bhattacharyya, S. (2014). An empirical investigation into the adoption of online banking in India. Information Technology & People, 27(2), 186-217.

[14] RBI. (2023). Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices. Reserve Bank of India, Mumbai.

[15] Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. Journal of Psychology, 91(1), 93-114.

[16] Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the weakest link: A human/computer interaction approach to usable and effective security. BT Technology Journal, 19(3), 122-131.

[17] Singh, P., Verma, A., & Gupta, R. (2024). Cybercrime in India's banking sector: Trends, vulnerabilities and regulatory responses 2022-24. Vikalpa: The Journal for Decision Makers, 49(1), 34-48.

[18] Srite, M., & Karahanna, E. (2006). The role of espoused national cultural values in technology acceptance. MIS Quarterly, 30(3), 679-704.

[19] Vishwanath, A., Harrison, B., & Ng, Y. J. (2018). Suspicion, cognition, and automaticity model of phishing susceptibility. Communication Research, 45(8), 1146-1166.

[20] Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. Journal of the American Society for Information Science, 59(4), 662-674.

[21] Yazdanmehr, A., & Wang, J. (2016). Employees' information security policy compliance: A norm activation perspective. Decision Support Systems, 92, 36-46.

[22] Zaharia, M., Aranda, B., & Patel, K. (2024). AI-generated phishing: Detection evasion and human susceptibility. ACM Conference on Computer and Communications Security Proceedings, 2024, 1847-1862.