

Optimism-Bias-Oriented Fraud-Risk Appraisal in Mobile Banking: Measurement Evidence and Demographic Patterns among Users in Chennai

S. Jayaprakash Narayanan¹ and V. Shanmugasundaram^{2*}

¹Ph.D Scholar, Department of Commerce, Madras Christian College, Chennai, Tamil Nadu, India

²Assistant Professor, Department of Commerce, Madras Christian College, Chennai, Tamil Nadu, India

*Corresponding Author E-mail: shanmugasundaram@mcc.edu.in

Abstract

Purpose: This study evaluates an optimism-bias-oriented fraud-risk appraisal measure and examines whether demographic, socioeconomic, and usage characteristics differentiate such appraisal among mobile-banking users in Chennai.

Design/methodology/approach: A bilingual English-Tamil questionnaire was completed by 114 users in May 2026. Reliability, minimum-residual factor analysis, 5,000-replication parallel analysis, Welch tests, effect sizes, Spearman correlation, hierarchical regression, HC3 robust standard errors, and response-pattern sensitivity analysis were used.

Findings: The six-item measure showed good internal consistency ($\alpha = .856$; $\omega = .860$) and one-factor evidence (Kaiser-Meyer-Olkin = .821; loadings = .591–.822). The mean score was 3.10 (SD = 0.94). Age, reported gender, education, occupation, income, application type, and usage-frequency groups were not reliably differentiated (all $p > .10$). Usage intensity showed a weak positive tendency, $\rho = .166$, 95% bootstrap CI $[-.031, .359]$, $p = .078$. Demographic and socioeconomic predictors explained 2.3% of variance; adding usage intensity increased R^2 to .041, while application type added little (final $R^2 = .043$).

Originality: The study distinguishes classical comparative optimism from a broader fraud-risk appraisal composite and shows that direct threat-appraisal assessment is more defensible than demographic profiling for mobile-banking risk communication.

Keywords: optimism bias; mobile banking; behavioral cybersecurity; fraud-risk appraisal; Protection Motivation Theory; threat appraisal

Introduction

India's mobile-payment ecosystem has moved from occasional digital use to routine financial dependence. The Reserve Bank of India reported that retail digital payments increased from 162 crore transactions in 2012–2013 to more than 16,416 Crore in 2023–2024, alongside continuing investment in authentication, tokenization, customer protection, and payment-system resilience (Reserve Bank of India, 2025a). The expansion of Unified Payments Interface use has made mobile transactions ordinary across diverse user groups, increasing the importance of how individuals interpret fraud warnings and personal exposure (Reserve Bank of India, 2025b).

Technical protection does not remove the need for personal judgment. A user still decides whether a payment request is legitimate, whether a public network is safe, whether a small unauthorized debit deserves attention, and whether institutional security makes personal verification unnecessary. These decisions can be distorted by optimism bias, the tendency to expect that personal outcomes will be more favorable than an appropriate comparative or objective standard (Shepperd et al., 2015; Weinstein, 1980).

In cybersecurity, optimism bias matters because perceived personal invulnerability can weaken threat appraisal. Owen et al. (2024) found that optimism bias was associated with insecure phishing-related behavior in a financial-services setting. Yet optimism bias has rarely been examined as a mobile-banking fraud appraisal pattern in India, and demographic categories are often used in awareness campaigns without sufficient evidence that they reliably identify users who underestimate threat.

The study addresses this gap through four objectives:

- O1. Evaluate the dimensionality and internal consistency of the six-item fraud-risk appraisal measure.
- O2. Explore variation across age, reported gender, education, occupation, and income.
- O3. Examine associations with usage intensity and preferred application category.
- O4. Assess the joint explanatory contribution of demographic, socioeconomic, and usage characteristics through Protection Motivation Theory.

The contribution is deliberately focused. The study offers context-specific measurement evidence, tests the empirical value of broad demographic profiling, and interprets

optimism-oriented appraisal as a possible attenuation of perceived vulnerability and severity. It does not equate demographic membership with security weakness.

Literature Review

Optimism Bias and Risk Appraisal

Classical optimism bias is comparative: people judge their own likelihood of an adverse outcome as lower than that of comparable others or lower than warranted by an external benchmark (Weinstein, 1980). It differs from dispositional optimism, trust, positive attitude, risk tolerance, and self-efficacy (Shepperd et al., 2015). Comparative formulations also require careful interpretation because respondents do not always process relative-risk questions as intended (Cho et al., 2020).

The present measure contains one direct comparative item and five context-specific beliefs involving confidence, public Wi-Fi, institutional reliance, severity minimization, and low perceived daily risk. Accordingly, the operational construct is termed optimism-bias-oriented fraud-risk appraisal. This qualified label preserves conceptual accuracy while recognizing the coherent common dimension observed in the data.

Optimism Bias in Cybersecurity

Behavioral cybersecurity research shows that security action depends on more than technical knowledge. A systematic review identified Protection Motivation Theory as a prominent explanation of cybersecurity behavior and called for more evidence from individual and non-Western contexts (Almansoori et al., 2023). Evidence from phishing research further suggests that optimism bias can accompany insecure intentions and behavior (Owen et al., 2024). However, organizational employees and voluntary mobile-banking consumers operate under different incentives, routines, and institutional protections.

Demographic and Socioeconomic Heterogeneity

Age, gender, education, occupation, and income may shape exposure, access to advice, perceived control, and the consequences attached to financial loss. Their effects are not universal. Age-related optimism varies across cultural contexts, and apparent differences can depend on response format (Comerford, 2021; You et al., 2009). Gender differences likewise depend on scenario valence and social context rather than following a stable general pattern (Dricu et al., 2022). Indian research has shown that culture and socioeconomic circumstances

can shape comparative optimism, reinforcing the need for context-specific analysis (Joshi & Carter, 2013).

Mobile-Banking Use and Risk Normalization

Frequent mobile-banking use can operate in opposing directions. Experience may improve competence and recognition of suspicious events, while repetition may normalize risk and reduce scrutiny. Application categories also supply different institutional cues, but a category label alone does not determine warning quality, authentication practice, or user behavior. These competing mechanisms justify exploratory analysis rather than rigid directional assumptions.

Theoretical Framework

Protection Motivation Theory separates threat appraisal from coping appraisal. Threat appraisal evaluates perceived severity, perceived vulnerability, and maladaptive rewards; coping appraisal evaluates response efficacy, self-efficacy, and response costs (Rogers, 1975, 1983). Meta-analytic evidence indicates that the theory is influential in information security, but relationships vary by context and are strongest when threats and protective responses are personally relevant and behavior specific (Mou et al., 2022; Sommestad et al., 2015).

Item content	PMT interpretation
Fraud is more likely to affect others	Reduced perceived vulnerability
Confidence in avoiding loss	Confidence-related belief; not identical to validated self-efficacy
Public Wi-Fi adds little risk	Threat minimization
Reliance on bank security instead of checking	Institutional delegation and possible maladaptive reward
Small unauthorized transactions are not serious	Reduced perceived severity
Little risk in daily mobile banking	Reduced vulnerability and severity

The measure is therefore interpreted as an appraisal pattern that may attenuate the threat pathway. It is not presented as a full empirical test of Protection Motivation Theory.

Research Expectations and Questions

Measurement expectation 1: The six items form one interpretable fraud-risk appraisal dimension.

Measurement expectation 2: The composite demonstrates adequate internal consistency.

H1: Greater usage intensity is positively associated with optimism-bias-oriented fraud-risk appraisal.

- RQ1. How does the appraisal score vary across demographic and socioeconomic groups?
- RQ2. Does appraisal differ across preferred application categories?
- RQ3. How much variance is explained jointly by demographic, socioeconomic, and usage characteristics?

Methodology

Design, Setting, and Participants

A cross-sectional questionnaire was administered in May 2026 to active mobile-banking users residing across all zones of Chennai, Tamil Nadu, India. Convenience sampling produced 114 complete responses. The questionnaire was available in English and Tamil and captured age, reported gender, preferred application category, education, occupation, monthly personal income, usage frequency, and six appraisal items.

Table 2: Measurement and Coding

Code	Item	Content
OB1	Financial fraud is more likely to affect others than me.	Comparative invulnerability
OB2	I trust my judgment to avoid financial loss from fraud.	Personal confidence
OB3	Public Wi-Fi does not greatly increase my fraud risk.	Risk minimization

Code	Item	Content
OB4	I rely on bank security systems instead of checking every transaction.	Institutional reliance
OB5	Small unauthorized transactions are not a big risk.	Severity minimization
OB6	There is very little fraud risk in my daily mobile-banking activities.	Low vulnerability

Items were rated from 1 (strongly disagree) to 5 (strongly agree). The composite was the arithmetic mean of OB1–OB6; higher scores represented stronger optimism-oriented appraisal. Application responses were harmonized into third-party UPI, institutional banking, and dual-channel use. Occupations were consolidated into five conceptually coherent groups.

Analytical Strategy

Reliability was assessed using Cronbach's alpha, McDonald's omega, corrected item-total correlations, and item-deletion diagnostics. Construct structure was evaluated using the Kaiser-Meyer-Olkin measure, Bartlett's test, minimum-residual factor analysis, and 5,000-replication parallel analysis (Horn, 1965). Welch tests compared unequal groups, with Cohen's d and eta squared describing effect magnitude. Spearman correlation assessed ordered usage intensity. Hierarchical ordinary least squares regression estimated demographic and socioeconomic predictors in Model 1, added usage intensity in Model 2, and added application type in Model 3. HC3 robust standard errors addressed heteroskedasticity. A response-pattern sensitivity analysis repeated principal estimates after excluding 22 constant-response profiles; this analysis was treated as a robustness check rather than a superior specification.

The analysis used de-identified responses and reports results in aggregate form. Data handling emphasized confidentiality and research integrity.

Results

Table 2: Respondent Profile

Characteristic	Category	n	%
Age	18–24	29	25.4
	25–35	27	23.7
	36–45	31	27.2
	46–60	18	15.8
	Above 60	9	7.9
Reported gender	Female	63	55.3
	Male	51	44.7
Education	Postgraduate/professional	74	64.9
	Undergraduate	23	20.2
	Other/unspecified	17	14.9
Application	Third-party UPI	87	76.3
	Dual-channel	16	14.0
	Institutional	11	9.6

Measurement Evidence

The composite mean was 3.10 (SD = 0.94; median = 3.17; range = 1.00–5.00). Internal consistency was good, $\alpha = .856$ and $\omega = .860$. Corrected item-total correlations ranged from .543 to .745, and deletion of any item did not improve alpha materially.

Table 3: Measurement Evidence

Item	M	SD	Corrected item-total r	α if deleted
OB1	3.07	1.23	.655	.829

Item	M	SD	Corrected item-total r	α if deleted
OB2	3.35	1.17	.570	.844
OB3	2.89	1.33	.645	.831
OB4	3.26	1.17	.745	.813
OB5	2.94	1.33	.543	.852
OB6	3.10	1.17	.722	.818

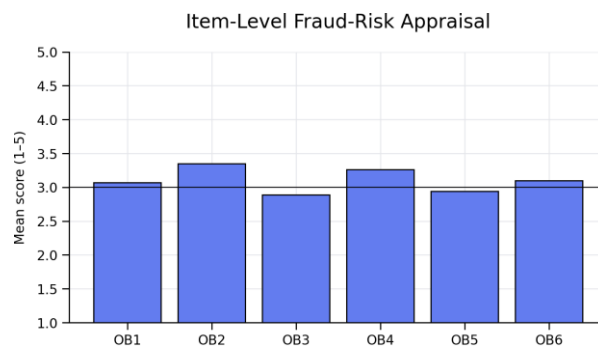


Figure 1. Item-level fraud-risk appraisal

The item matrix was suitable for factor analysis, Kaiser-Meyer-Olkin = .821, Bartlett's $\chi^2(15) = 289.71$, $p < .001$. Parallel analysis retained one factor: the first observed eigenvalue was 3.527 compared with a random benchmark of 1.455, while the second observed eigenvalue was 0.827 compared with 1.251. Minimum-residual loadings ranged from .591 to .822 and explained 51.0% of common variance. Both measurement expectations were met.

Demographic, Socioeconomic, and Usage Patterns

Grouping	Welch statistic	p	Effect size	Interpretation
Age	$F(4, 36.79) = 1.04$	.400	$\eta^2 = .039$; 95% boot CI [.013, .192]	Small, imprecise heterogeneity

Grouping	Welch statistic	p	Effect size	Interpretation
Reported gender	$t \approx 0.00$	.997	$d = .001$; mean-difference CI [-.354, .356]	Negligible observed difference
Education	$F(2, 36.04) = 1.85$	.172	$\eta^2 = .032$; CI [.003, .129]	Small, imprecise heterogeneity
Occupation	$F(4, 40.22) = 2.05$	.105	$\eta^2 = .065$; CI [.023, .205]	Largest descriptive heterogeneity
Income	$F(4, 29.20) = 1.24$	.315	$\eta^2 = .049$; CI [.018, .216]	Small-to-modest, imprecise pattern
Usage frequency	$F(5, 29.21) = 0.90$	.494	$\eta^2 = .054$; CI [.023, .227]	Group pattern inconclusive
Application type	$F(2, 19.39) = 0.07$	.936	$\eta^2 = .001$; CI [.001, .077]	Negligible differentiation

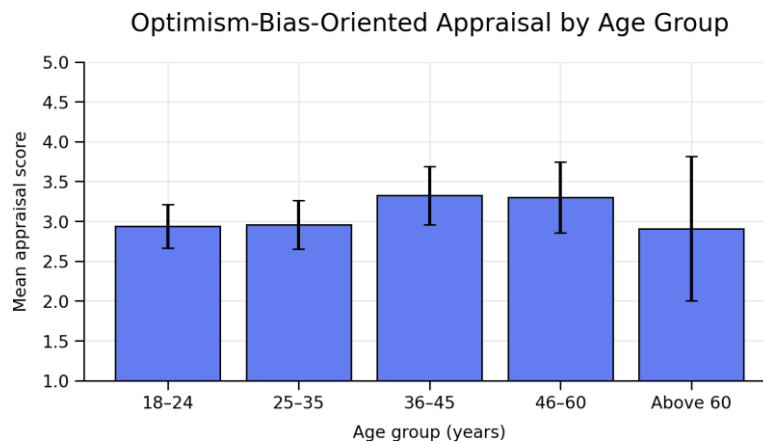


Figure 2. Appraisal scores by age group with approximate 95% confidence intervals

Usage intensity showed a weak positive association, $\rho = .166$, 95% bootstrap CI [-.031, .359], $p = .078$. The direction was consistent with H1, but the interval included zero and the prespecified significance threshold was not reached; H1 was not supported.

Hierarchical Regression

Model	Predictors added	R ²	Adjusted R ²	Robust model p
1	Age, reported gender, postgraduate education, income	.023	-.013	.699
2	Model 1 + usage intensity	.041	-.003	.577
3	Model 2 + application category	.043	-.020	.751

Usage intensity increased R² by .018, whereas application category added only .002. In the final model, age had the largest standardized coefficient ($\beta = .208$, $p = .199$), followed by usage intensity ($\beta = .143$, $p = .251$); neither estimate was statistically precise. Variance-inflation factors ranged from 1.11 to 2.07. The Breusch-Pagan test supported HC3 inference, $p = .016$; residual normality was acceptable, Jarque-Bera = 3.06, $p = .217$, and Durbin-Watson = 1.94.

Response-Pattern Sensitivity Analysis

Excluding the 22 constant-response profiles reduced the analytical sample to 92. Alpha remained acceptable at .766, and all six one-component loadings remained positive (.557–.793). The final-model R² increased to .084, adjusted R² = .008, robust model $p = .291$. Age became positive and statistically detectable ($B = 0.226$, $p = .037$), whereas usage intensity remained nonsignificant ($p = .496$). Because the age result appeared only under a post hoc exclusion rule and the full-sample estimate was imprecise, it was treated as sensitivity evidence requiring independent confirmation rather than as a primary finding.

Discussion

The study's strongest result is measurement based. The six items formed a coherent common dimension with good reliability, but their content extends beyond classical comparative optimism. The qualified label optimism-bias-oriented fraud-risk appraisal is therefore both theoretically and empirically appropriate. It captures comparative invulnerability, minimization of threat, confidence-related belief, and institutional reliance

without treating these components as interchangeable with a pure comparative probability judgment.

Broad demographic and socioeconomic categories offered limited differentiation. Reported gender and application type were especially negligible, while occupation, usage frequency, and income produced larger descriptive effects that remained imprecise. These findings do not establish population equality. Rather, they show that demographic labels were weak classifiers of fraud-risk appraisal in this convenience sample. This interpretation is consistent with evidence that optimism differences vary with culture, scenario, and measurement format (Dricu et al., 2022; Joshi & Carter, 2013; You et al., 2009).

Usage intensity showed a small positive tendency. Repeated use may normalize transactions and reduce scrutiny, but experience may also improve recognition and coping competence. The hierarchical model suggests that usage adds more explanatory value than application category, although the increment remained modest. Longitudinal research is required to determine whether increasing use changes vulnerability beliefs or whether pre-existing optimism encourages more intensive use.

The sensitivity analysis reinforces the need for restraint. Removing uniform response profiles changed reliability and produced an age coefficient not observed in the full sample. This instability demonstrates why post hoc exclusions should not be used to manufacture support. The appropriate conclusion is that age may deserve targeted replication, not that age has been established as a determinant.

Theoretical Implication

Protection Motivation Theory clarifies why demographic profiling underperforms. Age, gender, education, and income are distal characteristics; threat appraisal is proximal. Comparative invulnerability weakens perceived vulnerability, while minimization of small unauthorized transactions weakens perceived severity. Confidence and institutional reliance may intersect with coping appraisal, but they require dedicated response-efficacy and self-efficacy measures before those constructs can be claimed. Future models should position optimism-oriented appraisal as a distortion of threat appraisal and retain severity, vulnerability, maladaptive rewards, response efficacy, self-efficacy, response costs, protection motivation, and actual safety behavior as distinct paths.

Practical Implications

Banks, payment-system operators, and public agencies should avoid assuming that one age, gender, income, or application group inherently underestimates fraud. Universal baseline communication should be supplemented by behaviorally triggered support around new recipients, unfamiliar devices, public networks, unusual transaction values, warning dismissal, and small unauthorized debits. Messages should make personal vulnerability concrete, explain why apparently minor incidents matter, demonstrate effective protective actions, and keep verification costs manageable. This approach follows Protection Motivation Theory more closely than demographic targeting alone.

Limitations and Future Research

- Convenience sampling limits population generalization beyond the observed Chennai sample.
- Smaller occupational, income, and application groups produced wide effect-size intervals.
- The construct combines comparative invulnerability with other risk-normalizing beliefs; future scale development should separate these dimensions through expert review, cognitive interviewing, and confirmatory validation.
- Cross-sectional self-report data support association rather than causal ordering.
- Constant-response sensitivity changed one demographic result, highlighting the importance of preregistered response-quality rules.
- Future studies should use stratified zone-level recruitment, larger balanced samples, complete Protection Motivation Theory scales, longitudinal designs, and behaviorally grounded security outcomes.

Conclusion

The six-item instrument produced reliable one-factor evidence for optimism-bias-oriented fraud-risk appraisal among 114 mobile-banking users in Chennai. Broad demographic, socioeconomic, and application characteristics explained little variance, while usage intensity showed a weak positive tendency that remained statistically uncertain. The evidence therefore supports direct assessment of perceived vulnerability and severity rather than demographic profiling. Within Protection Motivation Theory, fraud prevention should focus on how users

appraise personal threat and protective options, not on assumptions derived from group membership.

Reference

- Almansoori, A., Al-Emran, M., & Shaalan, K. (2023). Exploring the frontiers of cybersecurity behavior: A systematic review of studies and theories. *Applied Sciences*, 13(9), 5700.
- Cho, H. L., Miller, D. G., & Kim, S. Y. H. (2020). Understanding people's unrealistic optimism about clinical research participation. *Journal of Medical Ethics*, 46(3), 172–176.
- Comerford, D. A. (2021). Apparent age and gender differences in survival optimism: To what extent are they a bias in the translation of beliefs onto a percentage scale? *Judgment and Decision Making*, 16(4), 1072–1096.
- Dricu, M., Moser, D. A., & Aue, T. (2022). Optimism bias and its relation to scenario valence, gender, sociality, and insecure attachment. *Scientific Reports*, 12, 18534.
- Horn, J. L. (1965). A rationale and test for the number of factors in factor analysis. *Psychometrika*, 30(2), 179–185.
- Joshi, M. S., & Carter, W. (2013). Unrealistic optimism: East and West? *Frontiers in Psychology*, 4, 6.
- Kumar, R., Singh, R., Kumar, K., Khan, S., & Corvello, V. (2023). How does perceived risk and trust affect mobile banking adoption? Empirical evidence from India. *Sustainability*, 15(5), 4053.
- Mou, J., Cohen, J. F., Bhattacharjee, A., & Kim, J. (2022). A test of Protection Motivation Theory in the information security literature: A meta-analytic structural equation modeling approach. *Journal of the Association for Information Systems*, 23(1), 196–236.
- Owen, M., Flowerday, S. V., & van der Schyff, K. (2024). Optimism bias in susceptibility to phishing attacks: An empirical study. *Information & Computer Security*, 32(5), 656–675.
- Reserve Bank of India. (2025a, January 27). Payment System Report, December 2024.
- Reserve Bank of India. (2025b, October 23). Payment Systems Report, June 2025.
- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1), 93–114.

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. T. Cacioppo & R. E. Petty (Eds.), *Social psychophysiology: A sourcebook* (pp. 153–176). Guilford Press.

Shepperd, J. A., Waters, E. A., Weinstein, N. D., & Klein, W. M. P. (2015). A primer on unrealistic optimism. *Current Directions in Psychological Science*, 24(3), 232–237.

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). A meta-analysis of studies on Protection Motivation Theory and information security behaviour. *International Journal of Information Security and Privacy*, 9(1), 26–46.

Weinstein, N. D. (1980). Unrealistic optimism about future life events. *Journal of Personality and Social Psychology*, 39(5), 806–820.

You, J., Fung, H. H., & Isaacowitz, D. M. (2009). Age differences in dispositional optimism: A cross-cultural study. *European Journal of Ageing*, 6(4), 247–252.



Citation:

S. Jayaprakash Narayanan and V. Shanmugasundaram, *Optimism-Bias-Oriented Fraud-Risk Appraisal in Mobile Banking: Measurement Evidence and Demographic Patterns among Users in Chennai*, [International Journal of Business and Economics Research \(IJBER\)](#) e-ISSN: 2455-3921; 12.3 (2026): 7-20. Published by [Dr. BGR Publications](#).