A Study on Cybersecurity Awareness and Authentication Usability in Secure Digital Banking

1. **Dr Ajay Kumar**, Department of BBA, KLEF (Koneru Lakshmaiah Education Foundation).
Email: varshneyak@rediff.com

2. **Ms Katakam Pujitha Gayatri**, Research Scholar, Department of BBA, KLEFVaddeswaram.
Email: 2400560038bba@gmail.com

Abstract
While digital banking has made the day-to-day financial transactions faster and convenient, it's opened the floodgates for customers to fall prey to phishing, OTP fraud, identity theft and unauthorised transactions. In this study, the link between the cybersecurity awareness of customers and the usability of authentication methods to digital banking is discussed. The structured questionnaire with five-point likert scale was used to respondents (digital banking users) in Andhra Pradesh, India. Data screening resulted in 19 unique respondents being included in analysis. The analysis applied to the data was chi-square test, one-way ANOVA and linear regression. Cybersecurity awareness and authentication usability were both positively and significantly related to secure banking behaviour with strong level of association ($r = .788$, $p < .001$; $r = .690$, $p = .001$, respectively). When combined, they accounted for 71.5% of the variance (adjusted $R2 = .679$), with awareness being the better predictor ($\beta = .586$) than usability ($\beta = .366$). Gender, age group, frequency of use and years of use were not significantly associated with secure behaviour, while high awareness and high usability were significantly associated with high secure behaviours. Generalisation was limited by the small sample and the effect of the usability was less consistent when applying bootstrap resampling. The results indicate that the banks should "marry" the easy, convenient authentication methods with ongoing customer awareness campaigns, especially regarding reporting suspicious activity.
The keywords for this research are cybersecurity awareness, the usability of authentication, secure digital banking behaviour, phishing, OTP fraud, and India.

1. Introduction

Digital banking has become a part of the banking business in the modern era. Internet banking and mobile banking and digital payment services enable customers to transfer funds, pay bills, check account statements and perform other banking functions without having to go to a branch. As mentioned by Shehab et al. (2024), technology has reshaped the banking industry and electronic financial services are much more convenient.

As digital banking becomes more prevalent, however, so do cybersecurity risks. Phishing, malware, identity theft and other cyber attacks can result in monetary loss, data breaches and loss of customer trust for banks and customers. Shehab et al. (2024) state that technology usage brings cyber security risks and financial risks and digital banking has provided new avenues for cyber-attacks.

Customer knowledge of cybersecurity is thus essential. Users should be aware of the risks encountered online and be careful to protect their passwords, pin number and OTP, and to avoid suspicious links and messages. Banking risk can be amplified if user mistakes or lack of awareness occurs in a small way (Shehab et al., 2024).

Awareness is not the only component of digital banking security, however—so is the usability of authentication. Bank identification is done using passwords, PINs, one-time passwords (OTPs), fingerprints or facial recognition. Security measures should, however, be convenient and easy to use. When security makes banking more difficult and complex, customers can sometimes bypass or bypass it, as Skelton (2017) notes. The authentication systems must therefore be secure and easy to use and understand.

However, customer behaviour is also a crucial factor in technological protection, as financial institutions are constantly and continuously threatened by cybercrime. Skelton (2017) highlights the need to be aware of the vulnerabilities of humans and the way that they may be exploited, including by phishing. This study, then, explores the customer side of

the issue: what customers know, and how user friendly they consider authentication to be, and how this affects their security behaviours.

2. Research Gap

Most literature suggests that the focus has been on technical and regulatory aspects of banking cybersecurity, while the customer side is slightly underrepresented.
There are few studies that look at this triple combination of cybersecurity awareness, ease of use of authentication and the actual security measures a customer takes in digital banking.
This relation with the measurable and secure customer behaviour has been given little attention in India so far.
Therefore, an empirical study with primary data, which views the customer from the perspective of secure digital banking, is necessary to identify the factors that affect the behaviour of secure digital banking.

3. Problem Statement

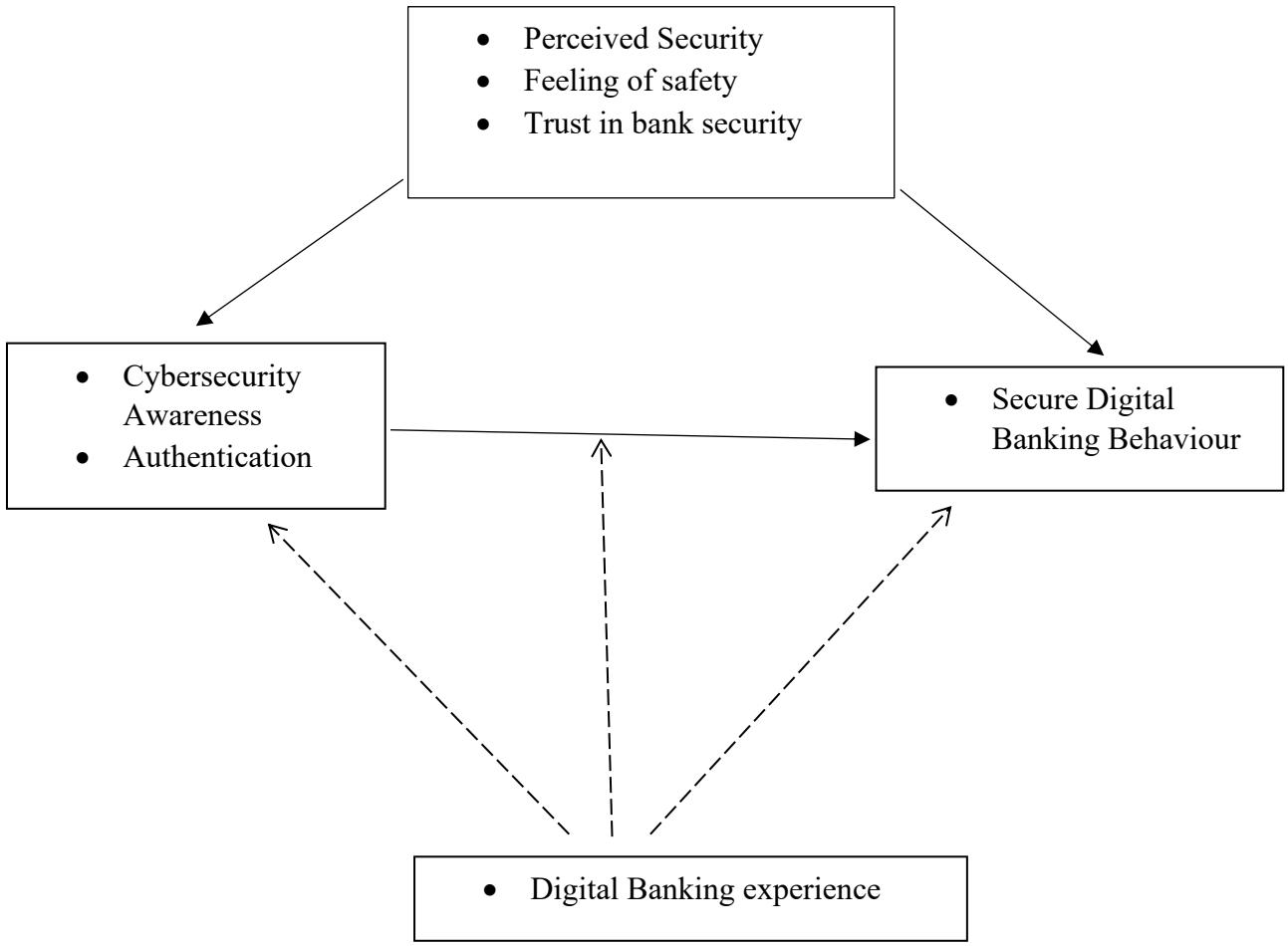
With the digital banking industry booming, customers are more vulnerable to phishing, OTP fraud, ID theft and unauthorised transactions. Banks have a sophisticated authentication suite, but the extent to which these are effective relies on consumer knowledge of cyber risks and ease of use of the tools. The current research is mainly technical/regulatory in nature and empirical evidence on the level of security behaviour of customers in India is scarce. This study thus explores the relationship between cybersecurity awareness, cybersecurity authentication usability and secure digital banking behaviour of the Indian customers.

4. Research Questions

Background: What is the awareness level of customers regarding cyber-related frauds including phishing, OTP fraud and unauthorised digital banking transactions?
RQ2: How is the awareness of cybersecurity linked to the behaviours of secure digital banking?
RQ3: How is the usability of the authentication related to the secure digital banking behaviour?
RQ4: Does the interaction of the usability of awareness and authentication predict secure banking behaviour better than either of them individually and is there differences in behaviour between customer groups (frequency and duration of use, gender, age)?

5. Conceptual Framework

Cybersecurity Awareness and Cybersecurity Authentication Usability are independent variables and Secure Digital Banking Behaviour is the dependent variable. Customer characteristics (frequency of use, duration of use, gender, age and education) are used to compare groups. Perceived security, feeling of safety and trust in bank security were considered at the conceptualisation stage as possible mediators, and digital banking experience as a possible moderator. Mediators were not measured with specific scales in the questionnaire, and therefore are not tested here, and are recommended for future studies (Section 13).



6. Research Objectives

1. To gauge the extent of cyber security awareness of the digital banking customers.
2. To evaluate the usability of the authentication techniques adopted in digital banking.
3. To analyze the impact of cybersecurity awareness on safe digital banking behaviour.
4. To measure the relationship between authentication usability and secure digital banking behaviour.
5. To explore the joint effect of awareness and authentication usability on secure banking behaviour.

To determine if there are differences in secure banking behaviour based on customer group by usage frequency and duration of use.

7. Hypotheses

H1: Cybersecurity awareness has a significant positive relationship with secure digital banking behaviour.

This is because there is a significant positive relationship between authentication usability and secure digital banking behaviour.

There is a joint contribution between awareness and authentication usability to secure digital banking behaviour, with each contributing uniquely.

H4: There is a significant difference between the digital banking behaviours of the three levels of awareness, the three levels of usability, the three frequencies of use and the three durations of use.

H5: There is a significant association between the levels of awareness and secure behaviour, between the levels of awareness and customer profile (gender, age, frequency and duration of use).

Each hypothesis is tested against its null statement (no significant relationship, difference or association) at the 5% significance level.

8. Review of Literature

1. Waliullah et al. (2025)

The research sheds light on the impact of cyber security risks on digital banking adoption and customer trust, including from a phishing, malware and data breach perspective.

But little empirical literature has been published on FinTech security problems, usability of MFA, the cost of compliance and real-time adaptive cybersecurity.

2. Mehta (2024)

The study explores the impact of technological advancements on banking frauds in India and highlights the role of AI, biometrics, and digital payments in ensuring security.

It does not, however, have primary empirical data and lacks focus on cybersecurity literacy, blockchain, and quantum-resistant technologies in India.

3. Mahdi (2024)

The paper also focuses on the concept of shared responsibility in the field of cybersecurity between banks and their customers and emphasizes the significance of AI, MFA, biometrics, and customer awareness.

The study, however, is based on a small sample and primarily focuses on perceived rather than actual secure banking practices or security incidents.

4. Haruna et al. (2023)

The study highlights key cyber threats to the payments and banking sector and adopts a layered defence and surveillance approach through the use of AI.

But it is mostly descriptive without any empirical testing of OTP, device identification, transaction monitoring or a real-time defence mechanism.

5. Zahoor et al. (2016)

The paper addresses key issues of privacy and security in banking and various countermeasures towards Cyber security threats.

But there is not a single comprehensive solution validated in real banking environments and newer AI- and blockchain-based solutions are not included.

6. Kuzmenko et al. (2020)

The study will focus on the trend trends and strategies in banking fraud and the evaluation of cyber security risks in banking.

The proposed cybersecurity assessment framework, however, is not empirically tested and fails to sufficiently cover customers' perceptions.

7. Chandra Sekhar & Kumar (2023)

This study aims to offer an overview of cyber security threats in digital banking and highlight some of the different cyber security measures that can be undertaken to secure banking systems.

The effectiveness of the suggested security measures, however, is not empirically tested from customer / banking data.

8. Skelton (2017)

The study examines the significant cyber threats prevailing in the financial sector and their significance of cybersecurity protection.

But it's not very empirical and lacks in detail on the implementation of cybersecurity solutions.

9. Anjum & Naseem (2015)

The study analyzes the cyber laws pertaining to e-banking and the role of legal protection in fighting cyber threats.

It does, however, concentrate primarily on the law and offers a limited amount of technical and empirical examination of cybersecurity.

10. Asgarimehr & Maghsoodlou (2023)

To this end, a study on the implementation of a cybersecurity risk management model for a digital transformation in the context of an Iranian bank is presented as a case study.

However, the results are only applicable to the banking sector in Iran because of the limited scope of the study.

11. Lavanya & Mangayarkarasi (2024)

The research examines the artificial intelligence application and risk assessment in the field of cybersecurity threats in banking.

It does not, however, offer experimental proof or comparisons of the performance of the various AI models.

12. Darem et al. (2023)

The study identifies the most significant cyber threats in banking and talks about the measures that can be taken to safeguard financial institutions against these cyber threats.

The proposed classification, however, is not empirically tested in real banking environments, nor are the countermeasures to these classifications.

13. Ghelani et al. (2022)

The study concludes by identifying cybersecurity threats and vulnerabilities, and suggests biometric authentication and digital signatures as solutions to security.

But the proposed model does not have an implementation and validation in the real world in various banking environments.

9. Research Methodology

9.1 Research design

The study used literature review and quantitative, Cross-sectional survey design. Primary data was collected by using of convenience sampling techniques from 100 digital banking users in Andhra Pradesh, India, by structured, self-administered online questionnaire.

9.2 Data screening and final sample

The 133 records were exported to a response file. When checked, 114 records were duplicates (identical submission time and all the answers to the 30 items were identical) and each of the remaining respondents had appeared 7 times. To eliminate duplication, 19 separate respondents were used for the analyses following the removal of duplicate records. The duplicated file would have given approximately 7 times the number of cases and have exaggerated statistical significance. There were no missing values.

9.3 Sample profile

Table 1. Profile of respondents (N = 19)

Characteristic	Category	n (%)
Age	Below 18	2 (10.5%)
	18–25	16 (84.2%)
	26–35	1 (5.3%)
Gender	Female	11 (57.9%)
	Male	7 (36.8%)
	Prefer not to say	1 (5.3%)
Education	Intermediate/12th	3 (15.8%)
	Undergraduate	15 (78.9%)
	Other	1 (5.3%)
Frequency of use	Daily	9 (47.4%)
	Several times a week	6 (31.6%)
	Once a week	1 (5.3%)
	Occasionally	2 (10.5%)
	Rarely	1 (5.3%)
Duration of use	Less than 1 year	3 (15.8%)

Characteristic	Category	n (%)
	1–3 years	13 (68.4%)
	4–6 years	2 (10.5%)
	More than 6 years	1 (5.3%)

Source: Primary survey data.

The sample is young and largely student-based: 16 of 19 respondents (84.2%) were aged 18–25 and 15 (78.9%) were undergraduates. Nearly half (47.4%) used digital banking daily.

9.4 Instrument and variables

The questionnaire had a demographic and usage section followed by 25 statements rated on a five-point Likert scale (1 = strongly disagree, 5 = strongly agree). Scale scores are the mean of their items.

Construct	Items	Role	Example item
Cybersecurity Awareness (AWR)	Q1–Q5	Independent	I can identify suspicious banking messages, emails, or links.
Authentication Usability (AUT)	Q6–Q10	Independent	The authentication process in my digital banking app is easy to use.
Secure Digital Banking Behaviour (SBB)	Q11–Q15	Dependent	I never share my OTP, PIN, or password with others.
Perceived influence of usability on behaviour (AUI)	Q16–Q20	Supplementary	Easy-to-use authentication encourages me to follow secure banking practices.
Perceived combined effect (CMB)	Q21–Q25	Supplementary	Cybersecurity awareness and easy authentication together improve my digital banking security.

9.5 Statistical techniques

The reliability of the scales is reported as Cronbach's alpha.

Descriptive statistics, Pearson correlation (Spearman rank correlation as a robustness check).

- Chi-square test of independence. Scale scores were classified as Low (< 3.0), Moderate (3.0–3.99) or High (≥ 4.0). Due to the small number of cases, most tests are based on 2 × 2 tables (High vs Not high) and results are presented as Fisher's exact p-values; 3 × 3 tables are used, but presented as Monte Carlo exact p-values (20,000 permutations). Effect sizes are either phi or Cramér's V.

A one-way ANOVA test of scale scores between groups, Levene's test, Tukey HSD test as post hoc comparisons, η^2 as an effect size, and a Kruskal–Wallis test as a non-parametric comparison check.

Linear regression (OLS) using secure banking behaviour as the dependent variable, two OLS simple regression and one multiple regression. Assumptions were assessed by using the Shapiro–Wilk test (residual normality), Durbin–Watson test (independence of errors), Breusch–Pagan test (constancy of variance), VIF test (multicollinearity) and Cook's distance; bootstrap (5,000 resamples) confidence intervals were calculated for the multiple regression.

Results were obtained in Python (SciPy, statsmodels) and checked in real formulas in Microsoft Excel, which gave the same results. These tests can be replicated using SPSS Analyze → Descriptive Statistics → Crosstabs (chi-square), Analyze → Compare Means → One-Way ANOVA, and Analyze → Regression → Linear.

9.6 Statistical power

A two-tailed correlation test, with $\alpha = .05$ and 80% power, can reliably detect only large effects ($r \geq |r| \geq .60$) for $N = 19$. If a result is not significant, particularly for group comparisons where the cells are very small, it should be considered inconclusive and not reported as evidence that there is no effect.

10 . Data analysis

10.1 Reliability and descriptive statistics

Table 2. Reliability and descriptive statistics (N = 19)

Scale	Items	α	Mean	SD	Min	Max
Cybersecurity Awareness	5	0.795	3.45	1.07	1.20	4.80
Authentication Usability	5	0.832	3.92	0.86	2.20	5.00
Secure Banking Behaviour	5	0.836	3.97	0.85	2.40	5.00
Influence of usability on behaviour	5	0.929	3.85	1.06	2.00	5.00
Combined effect perception	5	0.950	3.94	1.05	2.00	5.00

Note: 5-point scale. α = Cronbach's alpha.

The internal consistencies of all scales were satisfactory ($\alpha = 0.795 – 0.950$). The scores for usability ($M = 3.92$), secure behaviour ($M = 3.97$) were higher than for awareness ($M = 3.45$) which also exhibited the greatest spread ($SD = 1.07$). Awareness: 10 (52.6%) were high; 3 were moderate, and 6 were low; Usability: 11 were high; 5 were moderate and 3 were low; Secure behaviour: 11 were high, 5 were moderate and 3 were low.

The most confident responses were for maintaining confidentiality of passwords (Q3, $M = 4.21$) and the least confident were that they knew how to report suspicious or fraudulent activity (Q5, $M = 2.84$) at the item level (RQ1). Awareness of common threats (Q1) and recognising suspicious messages and links (Q2) were both moderate ($M = 3.26$). The strongest practices were not sharing OTP, PIN or password ($M = 4.26$), avoiding unknown links ($M = 4.11$) when it comes to behaviour. Public Wi-Fi risks (Q4) were at $M = 3.68$.

10.2 Correlation analysis

Table 3. Correlations between scale scores (N = 19)

Pair	Pearson r	p	Spearman ρ	p
Awareness – Usability	.552	.014	.470	.042
Awareness – Behaviour	.788	< .001	.729	< .001
Usability – Behaviour	.690	.001	.537	.018

Awareness was strongly and positively correlated with secure behaviour ($r = .788$, $p < .001$), and usability was also strongly correlated with behaviour ($r = .690$, $p = .001$). Awareness and usability were moderately related to each other ($r = .552$, $p = .014$). Spearman coefficients gave the same conclusions.

10.3 Chi-square tests of independence

Table 4. Chi-square tests of independence

Test	n	χ^2	df	p	Exact p	φ / V	Min E
C1 Awareness level × Gender[1]	18	1.17	1	.280	.367	.255	3.11
C2 Awareness level × Age group	19	2.48	1	.115	.211	.362	0.95
C3 Awareness level × Frequency of use	19	0.46	1	.498	.656	.156	4.26
C4 Awareness level × Duration of use	19	0.53	1	.466	.582	.167	1.42
C5 Behaviour level × Awareness level	19	8.93	1	.003	.005	.685	3.79
C6 Behaviour level × Usability level	19	6.13	1	.013	.024	.568	3.37
C7 Awareness (3 levels) × Behaviour (3 levels)	19	13.33	4	.010	.005	.592	0.47
C8 Usability (3 levels) × Behaviour (3 levels)	19	10.50	4	.033	.036	.526	0.47

Note: Exact p = Fisher's exact test (2 × 2) or Monte Carlo exact test (3 × 3). Min E = smallest expected cell count. [1] Female and Male respondents only (n = 18). Age: below 18 vs 18 and above; frequency: daily vs less than daily; duration: up to 3 years vs more than 3 years.

Customer profile and awareness (C1-C4). No demographic or usage variable was significantly associated with high awareness: gender ($\chi^2(1, N = 18) = 1.17$, p = .280, Fisher's exact p = .367), age group ($\chi^2(1, N = 19) = 2.48$, p = .115, Fisher's exact p = .211), frequency of use ($\chi^2(1, N = 19) = 0.46$, p = .498, Fisher's exact p = .656) and duration of use ($\chi^2(1, N = 19) = 0.53$, p = .466, Fisher's exact p = .582). The 18-under-18 group and the not-high group were not statistically significant with such few respondents, but all 10 respondents high in awareness were 18 or older.

C5–C8: Awareness, usability and behaviour. In the 2 × 2 analysis ($\chi^2(1, N = 19) = 8.93$, p = .003, Fisher's exact p = .005, φ = .685), nine of 10 (high awareness) also had high secure behaviour, and two of nine (rest) had high secure behaviour. Usability level was likewise significantly associated with behaviour level ($\chi^2(1, N = 19) = 6.13$, p = .013, Fisher's exact p = .024, φ = .568). The full 3 × 3 tables agreed (awareness × behaviour: $\chi^2(4, N = 19) = 13.33$, p = .010, Monte Carlo exact p = .005, V = .592; usability × behaviour: $\chi^2(4, N = 19) = 10.50$, p = .033, Monte Carlo exact p = .036, V = .526). Several counts were below 5 so the exact rather than the asymptotic p-values should be used.

10.4 One-way ANOVA

Table 5. One-way ANOVA results

Test	F	df	p	η^2	Levene p	K–W p
A1 Behaviour by awareness level	7.91	2, 16	.004	0.497	.497	.022
A2 Behaviour by usability level	9.92	2, 16	.002	0.554	.057	.024
A3 Behaviour by frequency of use	0.17	2, 16	.846	0.021	.491	.953
A4 Behaviour by duration of use	0.03	2, 16	.974	0.003	.601	.955
A5 Awareness by frequency of use	1.81	2, 16	.196	0.184	.041	.195
A6 Awareness by duration of use	0.46	2, 16	.638	0.055	.854	.395

Note: K–W = Kruskal–Wallis test. Frequency groups: Daily / Several times a week / Weekly or less. Duration groups: Less than 1 year / 1–3 years / 4 years or more. Behaviour differed significantly by awareness level ($F(2, 16) = 7.91$, $p = .004$, $\eta^2 = 0.497$): Low ($n = 6$, $M = 3.20$, $SD = 0.84$); Moderate ($n = 3$, $M = 3.73$, $SD = 0.81$); High ($n = 10$, $M = 4.50$, $SD = 0.44$). The high-awareness group had a significantly higher score than the low-awareness group (mean difference = 1.30, $p = .003$), while the other differences were not statistically significant. Tukey comparisons were used to determine which groups differed significantly. This was confirmed by the Kruskal–Wallis test ($p = .022$).

Behaviour also differed by usability level ($F(2, 16) = 9.92$, $p = .002$, $\eta^2 = 0.554$): Low ($n = 3$, $M = 2.67$, $SD = 0.31$); Moderate ($n = 5$, $M = 3.80$, $SD = 0.97$); High ($n = 11$, $M = 4.40$, $SD = 0.44$). The high-usability group was significantly higher than the low-usability group (mean difference = 1.73, $p = .001$) and the low–moderate contrast was nearly significant ($p = .052$). The Kruskal–Wallis result confirmed the finding with a border line result of Levene's test ($p = .057$, $p = .024$).

Secure behaviour did not differ significantly by frequency of use ($F(2, 16) = 0.17$, $p = .846$, $\eta^2 = 0.021$) or by duration of use ($F(2, 16) = 0.03$, $p = .974$, $\eta^2 = 0.003$). Awareness likewise did not differ by frequency ($F(2, 16) = 1.81$, $p = .196$, $\eta^2 = 0.184$) or duration ($F(2, 16) = 0.46$, $p = .638$, $\eta^2 = 0.055$); for A5, Levene's test indicated unequal variances ($p = .041$) but the Kruskal–Wallis test gave the same conclusion. Some groups had a small number of participants (3 or 4) and thus the tests were of limited power.

10.5 Linear regression

Table 6. Regression of secure banking behaviour on awareness and usability (N = 19)

Model / predictor	B	SE	β	t	p	95% CI
Model 1: $R^2 = .622$, adj. $R^2 = .599$, $F(1, 17) = 27.94$, $p < .001$						
Constant	1.804	0.428	—	4.22	< .001	[0.90, 2.71]
Awareness (AWR)	0.627	0.119	.788	5.29	< .001	[0.38, 0.88]
Model 2: $R^2 = .476$, adj. $R^2 = .445$, $F(1, 17) = 15.44$, $p = .001$						
Constant	1.292	0.697	—	1.85	.081	[-0.18, 2.76]
Usability (AUT)	0.684	0.174	.690	3.93	.001	[0.32, 1.05]
Model 3: $R^2 = .715$, adj. $R^2 = .679$, $F(2, 16) = 20.07$, $p < .001$						
Constant	0.938	0.538	—	1.74	.101	[-0.20, 2.08]
Awareness (AWR)	0.466	0.127	.586	3.66	.002	[0.20, 0.74]
Usability (AUT)	0.363	0.159	.366	2.29	.036	[0.03, 0.70]

Note: B = unstandardised coefficient; β = standardised coefficient. Model 1 and Model 2 are simple regressions; Model 3 is the multiple regression.

In Model 1, awareness was significantly correlated with secure behaviour and accounted for 62.2% of the variance, with every one-point increase in awareness resulting in a 0.63-point increase in behaviour. Model 2 showed that usability alone explained 47.6% of the variance ($B = 0.68$, $p = .001$).

The two predictors in the multiple regression (Model 3) accounted for 71.5% of the variance in secure behaviour, $F(2, 16) = 20.07$, $p < .001$. The equation that is fitted is as follows: Secure Behaviour = 0.94 + 0.47 × Awareness + 0.36 × Usability. Awareness ($\beta = .586$, $p = .002$) was the more powerful unique predictor, but usability ($\beta = .366$, $p = .036$) also contributed uniquely. The 95% confidence interval for the usability coefficient was however, [0.23, 0.84] for awareness, and [0.64, -0.18] for usability which contained zero. The specific contribution of usability should thus be considered as a suggestion, rather than a conclusion.

Assumptions of the checks were satisfactory: there were no unduly influential observations (maximum Cook's D = 0.39), low variance (VIF = 1.44), and errors were not correlated (Durbin–Watson = 2.36) or deviated from normality (Shapiro–Wilk p = .644), and no observation was unusually large (Breusch–Pagan p = .404).

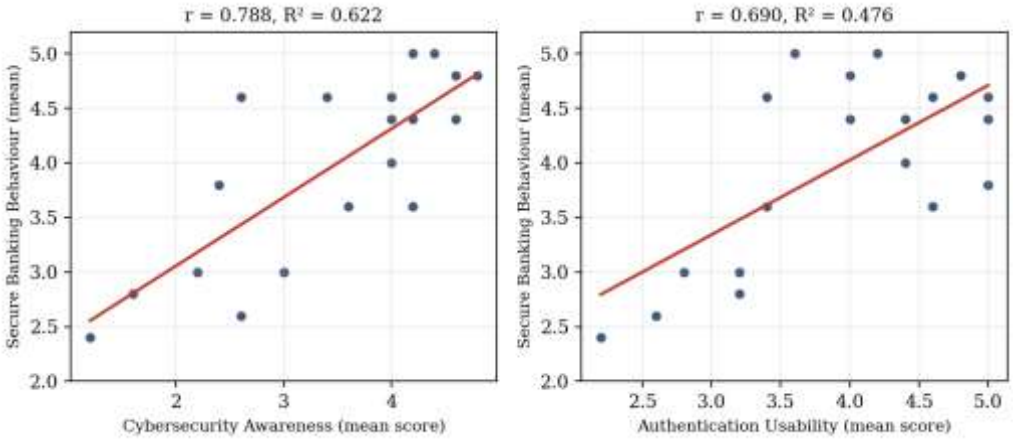


Figure 2. Scatter plots and fitted regression lines: awareness and usability against secure banking behaviour

10.6 Summary of hypothesis testing

Hypothesis	Test	Result	Decision
H1 Awareness → behaviour	Correlation, Model 1	r = .788, R^2 = .622, p < .001	Supported
H2 Usability → behaviour	Correlation, Model 2	r = .690, R^2 = .476, p = .001	Supported
H3 Joint prediction	Model 3	R^2 = .715; awareness p = .002; usability p = .036 (bootstrap CI includes 0)	Supported for awareness; tentative for usability
H4 Behaviour differs across groups	ANOVA A1–A4	Significant by awareness and usability levels; not by frequency or duration of use	Partly supported
H5 Level associations	Chi-square C1–C8	Awareness and usability levels associated with behaviour level; awareness level not associated with gender, age, frequency or duration	Partly supported

11. Discussion

The correlation, chi-square and ANOVA and regression all concur on the main finding: customers who are more educated about cyber threats and those who find authentication easier to use report safer banking behaviors. Awareness proved to be the greater influence. This echoes Shehab et al.'s (2024) and Mehta's (2024) concerns with customer awareness being a primary barrier to security and that security needs to be usable to be used as a barrier to security.It can be said to support the concern raised by Shehab et al. (2024) and Mehta (2024) that customer awareness is a primary barrier to security and that security needs to be usable to be used as a barrier to security.

Awareness and usability are moderately correlated (r = .55), and both still explain the multiple regression, meaning that they act as complements and do not substitute each other. The outcome is consistent with the expectation set in the framework, as neither technology nor knowledge is enough to get the customer. That being said, there was a weak

contribution of usability in the bootstrap resampling, and it will require a larger sample size to be certain that usability contributes to the explanatory power beyond awareness.

It is important to note that the item-level results indicate where the weakest link is. Most of the respondents recognised the value of confidentiality, and the least common understanding of how to report suspicious activity (M = 2.84), while they were only moderately able to identify suspicious messages or links (M = 3.26). It's more often you'll know not to do something if it looks bad, than it is that it's private.

There were no links between frequency or duration of use and awareness or secure behaviour, and no link between gender and awareness. This means it's not enough for customers to use digital banking services frequently or for extended periods of time to become more security conscious; it needs to be taught. These null results do not mean that there are no differences, given that the tests were underpowered.

12. Implications

For banks: (i) ensure authentication is simple, quick and easy to understand – usable security is more likely to be followed; (ii) keep awareness campaigns running – particularly awareness campaigns on how to identify phishing messages and links as such; (iii) target awareness campaigns towards younger, and newer users; and (iv) do not assume that the more frequently someone uses the app, the more they will know about security. For regulators and education providers: include awareness programmes in financial education programmes for students and first-time digital banking users. For customers: security aware behaviour (tight security on OTP, not clicking on unknown links, checking transactions) is the practical equivalent of good authentication on the bank.

13. Limitations and Future Research.

- Small sample. There were only 19 unique respondents, which reduces statistical power, imprecision of effect estimates, and small chi-square and ANOVA cells for the demographic groups. The results are not representative of all Indian digital banking consumers.

- Sampling. Convenience sampling from Andhra Pradesh yielded young and student dominated sample. Document consent procedure for minors if applicable because two people were under the age of 18.

- Self-reported, cross-sectional data. Responses might be socially desirable and design does not infer causality – direction of influence between awareness and behaviour is not determinable.

- Measurement. Actual exposure to phishing, OTP fraud and unauthorised transactions were not measured and self-reported secure behaviour was not observed. Conservation of security, security feeling and trust on the security of the bank were not measured.

Future research should include a larger and more representative multi-city sample; include actual fraud incidents; test mediation by perceived security and trust and moderation by digital banking experience with structural equation modelling or PROCESS; and directly compare authentication methods (OTP, biometrics, PIN).

14. Conclusion

This research study focuses on the relationship between cybersecurity awareness and authentication usability to secure the digital banking behaviour. The secure behaviour was strongly and positively related to both and together accounted for approximately 72% of the variance in secure behaviour, with awareness being the stronger of the two. Practices were significantly higher for customers who had a high awareness or high usability perceptions, and there was no significant relationship between frequency of use, duration of use, and gender for this small sample. Technical security and customer understanding must both progress to ensure secure digital banking, banks must ensure authentication is easy to use and invest in awareness, particularly for recognising and reporting suspicious activity. These findings need to be replicated with more diverse and larger sample sizes to validate and extend the findings

References

1. **Waliullah, M., George, M. Z. H., Hasan, M. T., Alam, M. K., Munira, M. S. K., & Siddiqui, N. A. (2025).** Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: A systematic literature review. *American Journal of Advanced Technology and Engineering Solutions, 1*(1), 226–257. https://arxiv.org/abs/2503.22710
2. **Mehta, A. (2024).** Impact of technological advancements on banking frauds: A case study of Indian banks. *International Journal of Research in Finance and Management, 7*(1), 261–266. https://doi.org/10.33545/26175754.2024.v7.i1c.308
3. **Mahdi, M. F. (2024).** Shared cybersecurity responsibilities in the banking sector: A case study of the Republic of Iraq. *Journal of Education for Pure Science, 14*(4), 130–149. https://doi.org/10.32792/jeps.v14i4.420
4. **Haruna, W., Aremu, T. A., & Modupe, A. Y. (2022).** Defending against cybersecurity threats to the payments and banking system. *arXiv*. https://arxiv.org/abs/2212.12307
5. **Zahoor, Z., Ud-din, M., & Sunami, K. (2016).** Challenges in privacy and security in banking sector and related countermeasures. *International Journal of Computer Applications, 144*(3), 24–35. https://doi.org/10.5120/ijca2016910173
6. **Kuzmenko, O., Pilina, N., & Pilin, R. (2020).** Trends of fraud operations on the banking market and approaches of cybersecurity assessment. *Efektyvna Ekonomika*, (5). https://doi.org/10.32702/2307-2105-2020.5.11
7. **Chandra Sekhar, S., & Kumar, M. (2023).** An overview of cyber security in digital banking sector. *East Asian Journal of Multidisciplinary Research, 2*(1), 43–52. https://doi.org/10.55927/eajmr.v2i1.1671
8. **Skelton, A. (2017).** *Analyzing cyber threats affecting the financial industry* [Undergraduate research]. Embry-Riddle Aeronautical University. https://commons.erau.edu/student-works/60/
9. **Anjum, R., & Naseem, F. (2015).** An appraisal of cyber laws with reference to e-banking in Pakistan. *Computer Engineering and Intelligent Systems, 6*(10), 1–5. https://www.iiste.org/Journals/index.php/CEIS/article/view/26215
10. **Asgarimehr, M., & Maghsoodlou, Z. (2023).** A model for cybersecurity risk management in digital transformation: Case study of an Iranian bank. *Multicultural Education, 9*(7). https://doi.org/10.5281/zenodo.8179189
11. **Lavanya, M., & Mangayarkarasi, S. (2024).** A review on detection of cybersecurity threats in banking sectors using AI-based risk assessment. *Journal of Electrical Systems, 20*(6s), 1359–1365. https://journal.esrgroups.org/jes/article/download/2909/2307/5239
12. **Darem, A. A., Alhashmi, A. A., Alkhaldi, T. M., Alashjaee, A. M., Alanazi, S. M., & Ebad, S. A. (2023).** Cyber threats classifications and countermeasures in banking and financial sector. *IEEE Access, 11*, 125138–125158. https://doi.org/10.1109/ACCESS.2023.3327016
13. **Ghelani, D., Hua, T. K., & Koduru, S. K. R. (2022).** *Cyber security threats, vulnerabilities, and security solutions models in banking* [Preprint]. Authorea. https://doi.org/10.22541/au.166385206.63311335/v1
14. **Shehab, R., Alismail, A. S., Almaiah, M. A., Alkhdour, T., AlWadi, B. M., & Alrawad, M. (2024).** Assessment of cybersecurity risks and threats on banking and financial services. *Journal of Internet Services and Information Security, 14*(3), 167–190. https://doi.org/10.58346/JISIS.2024.I3.010
15. **Mazumder, M. M. M., & Hossain, D. M. (2023).** Voluntary cybersecurity disclosure in the banking industry of Bangladesh: Does board composition matter? *Journal of Accounting in Emerging Economies, 13*(2), 217–239. https://doi.org/10.1108/JAEE-07-2021-0237

16. **Keränen, A.-M. (2022).** *Rising cyber threats targeting the banking sector* [Bachelor's thesis, University of Jyväskylä].
https://jyx.jyu.fi/bitstream/handle/123456789/81740/1/URN%3ANBN%3Afi%3Ajyu-202206153350.pdf
17. **Stanikzai, A. Q., & Shah, M. A. (2021).** Evaluation of cyber security threats in banking systems. In *2021 IEEE Symposium Series on Computational Intelligence (SSCI)* (pp. 1–4). IEEE.
https://doi.org/10.1109/SSCI50451.2021.9659862
18. **Ojeka, S. A., Ben-Caleb, E., & Ekpe, E.-O. I. (2017).** Cyber security in the Nigerian banking sector: An appraisal of audit committee effectiveness. *International Review of Management and Marketing, 7*(2), 340–346.
https://www.econjournals.com/index.php/irmm/article/view/4124
19. **Oyewole, A. T., Okoye, C. C., Ofodile, O. C., & Ugochukwu, C. E. (2024).** Cybersecurity risks in online banking: A detailed review and preventive strategies application. *World Journal of Advanced Research and Reviews, 21*(3), 625–643.
https://doi.org/10.30574/wjarr.2024.21.3.0707