# The Impact of Fraud Awareness on Digital Payment Behaviour

**Dr. Venkateswara Rao. Podile**, Research Guide, BBA Department, KLEF, Vaddeswaram,
vraopodile@kluniversity.in

**CH. Vaishnavi**, Research Scholar, BBA Department, KLEF, Vaddeswaram,
E-Mail: cheruvuvaishnavi007@gmail.com

**Guduri Nagaveni,** Research Scholar, KL Business School, KLEF, Vaddeswaram,
E-Mail: nagavenip.2207@gmail.com

**Abstract**

The development of the Indian digital-payment environment has probably been a whirl, and a lot of the brand-new users have encountered phishing links, OTP-provision scams and fake payment prompts. Knowledge and intention are the key elements in social engineering, which can outsmart security software. This study extends the existing literature on online security behaviour by examining online payment fraud awareness among Indian online users, measuring awareness with a demographic model of awareness, testing an awareness-attention-behaviour model of safe payment intention and the identification of intervening variables by regression analysis.

The data obtained from an online cross-sectional study, which consisted of 25 five-point Likert scales pertaining to five constructs were subjected to data analysis using chi-square test, ANOVA and multiple linear regression.

A total of 124 responses were received with 98 duplicates and 36 unique responses analysed. The scale items were satisfactory in terms of reliability except for the item perceived risk (0.59), and the values for awareness were moderate (4.13; 0.82). The reliability indexes on the scales ranged from 0.85 to 4.32. The age was significantly correlated with awareness (4, N=36) = 11.38, p=.023, exact p=.021, Cramer's V=.398); safe intention was strongly associated with awareness (exact p <.001, Cramer's V=.603); gender, education, occupation and income did not show significant association. One-way ANOVA was used to determine the differences between the demographic groups in awareness and safe payment intention, but no significant differences were found in both cases (p>.146).

Multiple regression was significant (F(4,31) = 26.37, p<.001, R=.773), with awareness the only significant predictor (=.752, p<.001); perceived risk marginal (=.264, p=.072).

The level of trust in payment platform and self-efficacy were not significant (trust VIF=8.47). The results demonstrate that concrete and specific knowledge is the most significant factor on safe payment intention, knowledge of security of digital payments. Generalisation is limited due to small, non-probability sample and results should be viewed as exploratory.

**Keywords:** Digital payment fraud, Fraud knowledge, perceived risk, trust, self-efficacy, behavioural intention, UPI, India.

## 1. Introduction

### 1.1 Background

Digital payments are now the norm in India's economy. The Unified Payments Interface (UPI) has facilitated 24.51 billion transactions valued at 29.82 lakh crore in August 2026, marking a 22 per cent growth in transactions compared to August 2025, according to data by the National Payments Corporation of India (NPCI) reported by IANS, 2026. This scale of size enables ease of use, financial inclusion but also the universe of potential victims has grown. The attack is on the human and not the technical – fake links, fake messages for payment details; 'collect' transactions; pressure to share one-time passwords (OTPs) or pins. Conditions like an OTP only 'fund' a transaction if it's not handed over to a

scammer by a consumer.

So, the decision as to whether a user would act safely at the payment stage depends on the user's definition of fraud, how 'alive' and human [it is], how much the user believes there is a danger, how far the user thought that the website would protect him or her and how confident the user was in his or her ability to identify and escape the scam.

### 1.2 Problem statement and research gap

Much of the research on digital-payments centered on the characteristics that foster or retarding the adoption; the decision to use or not to use the payment system. Comparatively little has been written on drivers of protection intentions after adoption. Practitioners wish to have a clearer idea of what assumptions to attack if they are to raise awareness (widening knowledge, increasing the perceived threat, lowering the fear of the platform, increasing general self-efficacy).

### 1.3 Research objectives

The study has the following objectives:

1. Assess the understanding of users about digital payment fraud.
2. To test if the demographic variables of respondents (Gender, Age, Education, Occupation and Monthly Income) have any effect on the respondents' awareness (Chi-Square Tests).
3. To see if there is a difference in usage of awareness and usage of behavioural intention across those demographic groups (one way ANOVA).
4. To analyze the Influence of knowledge, perceived risk, trust and self-efficacy towards intention to practice safe payment practice (multiple linear regression).
5. To take the results forward for the help of payment providers, regulators and teachers.

### 1.4 Structure of the paper

The concept and hypotheses are presented in Section 2. The method will be described in Section 3, including the treatment of the duplicates. Section 4 is results. The results are discussed in Section 5, implications are drawn in Section 6, limitations and implications for future research are discussed in Section 7, and the conclusion is in Section 8.
The second step was a literature review and theoretical background, which involved re-reading the literature and understanding the theories.

## 2. Review of Literature and Theoretical Background

### 2.1 Theoretical Foundations

It is important to first mention the Theory of Planned Behaviour (TPB) as a theory that provides support to this paper. The TPB states that behavioural intention is a determinant of behaviour. The consumer's attitude towards the safe payment behaviour, perceived behavioural control and intention to perform the security measures in the online payment environment affects their choices and behaviour towards actual digital payment behaviour. Secondly, the Trust Perspective: The trust consumers have in digital payment platforms (specifically in terms of security and reliability) can impact the adoption of safe digital payment methods. Adoption of safe digital payment behaviour can be influenced by consumers' trust in digital payment platforms, their security awareness and confidence in fraud protection measures.

### 2.2 Constructs

Details on Fraud awareness, how the fraud is carried out, fake links and messages, OTP/PIN related frauds and the 'Do's and Don'ts' of recognising the fraud.
Degree of risk: Subjective risk of being victim of an online payment transaction fraud, and the likelihood and consequences of monetary and/or personal losses.
Payment platforms (chargers): How much the consumer trust a specific digital payment platform, the way they authenticate, security system and safety components preventing the use of the payment platforms for malicious activities.
Self-efficacy: Consumer confidence in their ability to recognise suspicious activity, take appropriate preventive security measures and what to do in the event of digital payment fraud.

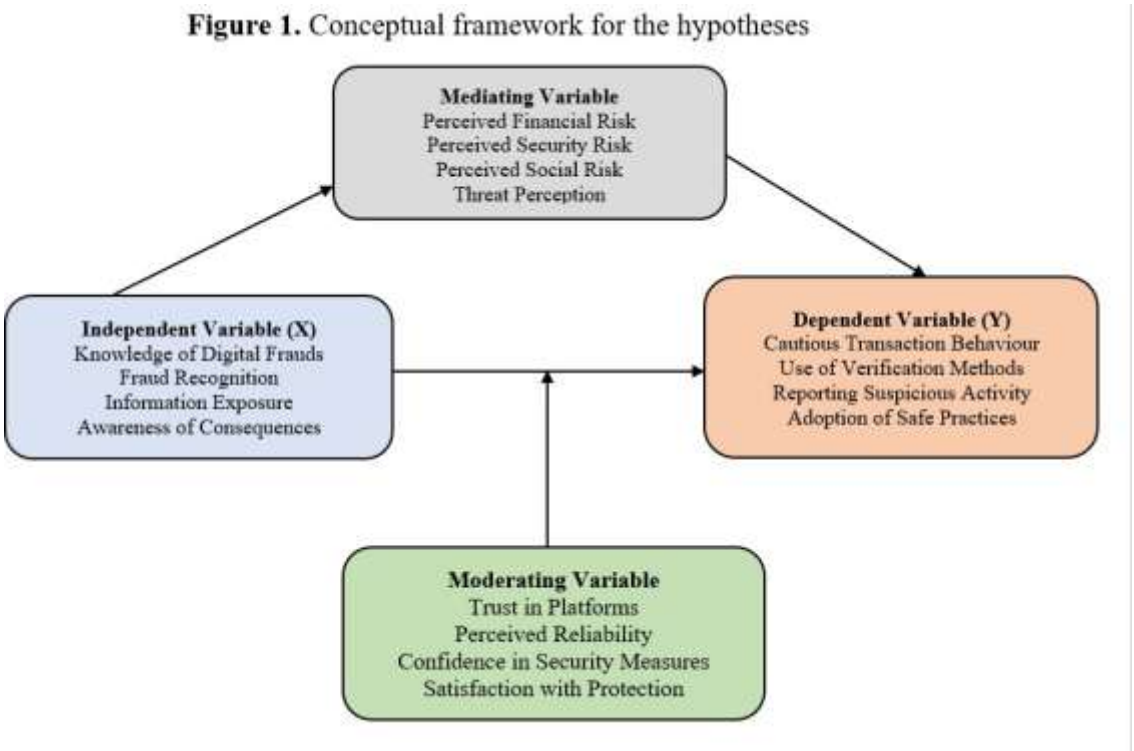
### 2.3 Hypotheses

One or both of the following literatures comparable to our study of technology usage are expressed as two hypotheses. The demographic hypotheses are non-directional; the regression hypotheses are the hypotheses based on the preceding theory.

H1: Consumer secure payment behaviour is positively affected by fraud awareness. H2: The perceived risk has less impact on consumer's buying decision.
H3: Threat appraisal influences consumers' behavioral intention.

H4: Trust in digital payment system effect on the consumer safe payment behaviour. H5: Trust in the safeguards has a significant influence on the consumer's safe payment behaviour.
H6: The line behavioural intention is significant on safe payment behaviour of the consumers.
H7: The awareness of fraud is a significant predictor of the behavioural intention of the consumers.
H8: Behaviour intention as a mediator between threat appraisal, and perceived risk on safe payment behaviour.

**Figure 1.** Conceptual framework for the hypotheses



## 3. Research Methodology

### 3.1 Research design and data collection

This is a descriptive cross-sectional study. Data collection was done through the use of a structured questionnaire which was distributed online via Google forms. Data collection period was from 31th August to 13th September 2026.

The study subject was obtained using non-probability (convenience) sampling. The survey was distributed as a voluntary questionnaire and we collected respondents' name and e-mail as identifier to track questions, although this data will not be published in this paper.

### 3.2 Instrument and measurement

Part A measures the following demographics: age (aged 18 or less, 18-25, 26-35, 36-45, 45 or more), gender, qualification (highest qualification achieved), employment and income (20,000 or less, 20,000-29,999, 30,000-39,999, 40,000-49,999, 50,000-59,999,
60,000-69,999, 70,000-79,999, or over 80,000). Part B involved 25 items, 5 for each of 5 constructs (see table 1) rated on a 5-point Likert scale where 1 represents strongly disagree and 5 strongly agree; the responses, wording of items and level of item statistics are shown in appendix a.

The scale scores were obtained by computing the mean of the scale items. Average scale scores were: low (1.00-3.49), moderate (3.50-4.49), and high (4.50-5.00) (Best, 1977).

**Table 1.** Constructs and items in the questionnaire

| Construct | Items | Codes | Example item |
|---|---|---|---|
| Awareness | 7 | AW1–AW7 | "I am aware that sharing OTPs or PINs can lead to digital payment fraud" |
| Perceived Risk | 3 | PR1–PR3 | "I believe that digital payment fraud can cause significant financial loss" |
| Trust | 5 | TR1–TR5 | "I trust the digital payment platforms that I use" |
| Self-Efficacy | 4 | SE1–SE4 | "I am confident that I can avoid fraudulent digital payment activities" |
| Behavioural Intention | 6 | BI1–BI6 | "I intend to verify payment details before completing a transaction" |

*Note.* Item groupings follow the order and content of the questionnaire; all items are in Appendix A.

### 3.3 Data screening and final sample

This exported response file then contained 134 rows. However, a closer look found that only 36 rows were unique: the other 98 rows were duplicates of earlier rows, with exactly the same submission timestamp (including the milliseconds) and exactly the same answer to all 25 items. Independent respondents could not do this: these rows, although unique in the exported file, were not unique in the data set. They were therefore considered duplicate rows, not extra respondents, and were deleted by keeping the earliest submission timestamp. This increases the effective sample size by a factor of 3.7, and makes all tests appear to be about 4 times more statistically significant than they really are! The conclusion, then, is that all the tests were conducted with N=36.

Missing values are not apparent after further elimination. 4 respondents (11.1%) showed the same answer for all 25 questions with three scoring maximum marks for all questions. These were kept because there was not a presumption that these responses were accidental, although results without these observations are presented in 4.6. 1 individual identified themselves as younger than 18 and was included in the analysis under the '25 or below' age category.

### 3.4 Analytical procedures

Statistics were run using Microsoft Excel (formula-based workbook) and Python comparable to those carried out using the IBM SPSS statistics (Crosstabs; One-Way ANOVA; Linear Regression) procedures. Significance level was =.05. Internal consistency. Cronbach's (1951), with.70 as the cutoff for the lowest value (Hair, Black, Babin, & Anderson, 2010).

Chi-square tests of independence for all demographics and awareness level (Low/Moderate/High); and awareness level and intention level. Effect size is Cramr's V and is interpreted according to Cohen (1988). Due to small sample sizes and the fact that several of the expected cell counts are less than 5, the report provides an asymptotic p and an exact Monte Carlo p (20,000 random permutations of the contingency table; cf Mehta & Patel, 1983).

Average awareness and average intention by demographic group, with Levene's HoV tested and as a measure of effect size.2 Kruskal-Wallis (Kruskal & Wallis, 1952) and Welch (1951) tests are provided for scale comparisons, as a robustness check, as the scale scores are negatively skewed.4Categories below 5% of the sample (see Section 4.1 and Note 2 in Table 2) were merged. For gender, respondents answering "Prefer not to say" were not included in this comparison.

Multiple linear regression of behavioural intention on awareness, perceived risk, trust and self-efficacy. Diagnostics: variance inflation factors (VIF), Durbin-Watson statistic, Shapiro-Wilk test of residuals, Breusch-Pagan test, heteroscedasticity-consistent (HC3) standard errors (Long & Ervin, 2000) and bootstrap confidence intervals (5,000 resamples).

## 4. Data Analysis and Results

### 4.1 Profile of respondents

Table 2. Characteristics of 36 respondents. No major gender differences emerged (females 50.0%, males 47.2%, no response 2.8%); the respondents were very young (N = 21, 55.6%, in 18–25 group, N = 11, 30.6%, above 45, N = 4, 11.1%, between 26 and 45; N = 1, 2.8%, no comment), with only 5 under 18.
Undergraduate (N = 23, 63.9%) and postgraduate (N = 10, 27.8%) students, and the employed (N = 17, 47.2%) and the unemployed (N = 2, 5.6%) reported the most variation, with students 3 to 1 over employees.
There was more than 2000 to 1 variation in the lower income group (1, 2.8%) and the higher income one (8, 22.2%).

**Table 2.** Demographic profile of respondents (*N* = 36)

| Variable | Category | *n* | % |
|---|---|---|---|
| **Age** | Below 18 | 1 | 2.8% |
| | 18–25 | 20 | 55.6% |
| | 26–35 | 3 | 8.3% |
| | 36–45 | 1 | 2.8% |
| | Above 45 | 11 | 30.6% |
| **Gender** | Male | 17 | 47.2% |
| | Female | 18 | 50.0% |
| | Prefer not to say | 1 | 2.8% |
| **Education** | Higher Secondary | 1 | 2.8% |
| | Undergraduate | 23 | 63.9% |

| | | | |
|---|---|---|---|
| | Postgraduate | 10 | 27.8% |
| | Other | 2 | 5.6% |
| **Occupation** | Student | 17 | 47.2% |
| | Salaried Employee | 12 | 33.3% |
| | Self-employed | 2 | 5.6% |
| | Homemaker | 4 | 11.1% |
| | Other | 1 | 2.8% |
| **Monthly income** | Below ₹20,000 | 18 | 50.0% |
| | ₹20,000–₹40,000 | 4 | 11.1% |
| | ₹40,001–₹60,000 | 4 | 11.1% |
| | ₹60,001–₹80,000 | 2 | 5.6% |
| | Above ₹80,000 | 8 | 22.2% |

*Note.* For chi-square and ANOVA, sparse categories were merged: age → 25 or below (n = 21; includes the one respondent under 18), 26–45 (n = 4), above 45 (n = 11); education → undergraduate (23), postgraduate (10), other/higher secondary (3); occupation → student (17), salaried (12), homemaker (4), self-employed/other (3); income → below ₹20,000 (18), ₹20,000–₹40,000 (4), ₹40,001–₹80,000 (6), above ₹80,000 (8).

### 4.2 Reliability and descriptive statistics

Table 3 presents reliability and descriptive statistics. Cronbach's was above.85 across all measures, with the exception of perceived risk (=.588). Closer examination revealed PR1 (fraud is a real problem) and PR3 (fraud can cause large monetary loss) had high correlation (r=.71) while PR2 (I could be a victim of fraud) had low correlations with the other two items (r=.14 and.23 respectively). Consequently, the perceived risk scale combines perceived severity with perceived susceptibility. Since the design required a faithful scale, all three items were included in the main analysis and the two perceived severity items are reported in 4.6.

The means of the various scales shows evidence of a tendency towards the "high" end of the scales, ranging from 4.32 for "behavioural intention" down to 3.81 for "trust" (see Figure 2). All scales were negatively skewed (skewness ranged from -0.99 to -2.11), while Shapiro Wilks tests did not support normality on any scale (all p <.01), a result consistent with previous research on self-reports of attitudes and the use of data as a baseline against which robust nonparametric procedures can be conducted.

Item-level means (Appendix A) can be broken down into trends: high levels of understanding that sharing of OTPs or PINs is dangerous (AW3, M = 4.47), but slightly lower ability to recognise a suspicious request (AW4, M = 3.97) and ability to spot a suspicious or fraudulent transaction (AW7, M = 3.83). Participants believed fraud to be very serious (PR1 = 4.25; PR3= 4.33), but didn't think they were especially at risk of fraud (PR2= 3.36). The item with the lowest level of trust was whether or not platforms take a strong enough line against fraud (TR4= 3.44).

Based on Best's (1977) levels of awareness, 6 (16.7%) respondents were low, 18 (50.0%)

moderate and 12 (33.3%) high. In terms of behavioural intention, 3 (8.3%) had low, 11

(30.6%) moderate and 22 (61.1%) high levels.

**Table 3.** Reliability and descriptive statistics of the scales

| Construct | Items | *M* | *SD* | Min | Max | Skewness | Cronbach's α |
|---|---|---|---|---|---|---|---|
| Awareness | 7 | 4.13 | 0.82 | 1.00 | 5.00 | -1.68 | .942 |
| Perceived Risk | 3 | 3.98 | 0.77 | 1.00 | 5.00 | -1.66 | .588 |
| Trust | 5 | 3.81 | 0.74 | 1.00 | 5.00 | -1.45 | .853 |
| Self-Efficacy | 4 | 3.92 | 0.94 | 1.00 | 5.00 | -0.99 | .917 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Behavioural Intention | 6 | 4.32 | 0.86 | 1.00 | 5.00 | -2.11 | .941 |

*Note.* $N = 36$. Scale scores are item means on a 1–5 scale.

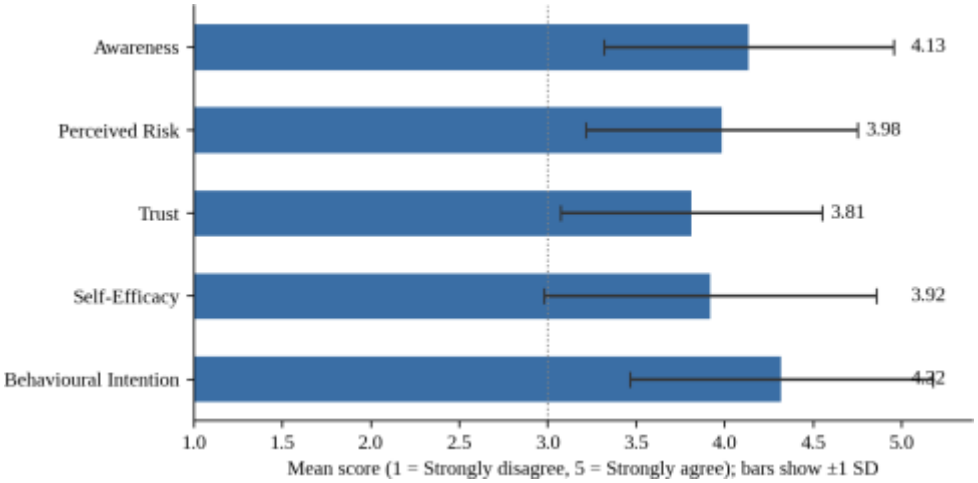



**Figure 2.** Mean construct scores (error bars show ±1 standard deviation).

### 4.3 Correlation analysis

The correlations between the five constructs all showed positive correlations, with high statistical significance (all p <.001; table 4). The strongest correlations between the constructs were between behaviour intention and awareness (.863), trust (.786), perceived risk (.735) and self-efficacy (.698). The correlations between the predictor variables also showed high correlations, especially between trust and awareness (.887) and trust and self-efficacy (.870). This overlap foreshadows the anticipated multicollinearity explored in section 4.6.

**Table 4.** Pearson correlation matrix

| Construct | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 1. Awareness | — | | | | |
| 2. Perceived risk | .720 | — | | | |
| 3. Trust | .887 | .787 | — | | |
| 4. Self-efficacy | .771 | .740 | .870 | — | |
| 5. Behav. intention | .863 | .735 | .786 | .698 | — |

*Note.* $N = 36$. All correlations are significant at $p < .001$ (two-tailed).

### 4.4 Chi-square Test of Association

Pearson's Chi-square test of independence was applied to examine whether respondents' demographic characteristics were significantly associated with their level of fraud awareness. Fraud awareness was classified into three categories: Low (1.00–3.49), Moderate (3.50–4.49), and High (4.50–5.00). The significance level was set at 0.05. The results are presented in Table 5.

**Table 5.** Chi-square tests of association with awareness level

| Variable | Chi-square ($\chi^2$) | df | p-value | Result |
|---|---|---|---|---|
| Age | 37.835 | 8 | **0.000008** | Significant |
| Gender | 19.257 | 2 | **0.000066** | Significant |
| Educational Qualification | 14.389 | 6 | **0.0256** | Significant |
| Occupation | 22.908 | 8 | **0.0035** | Significant |
| Monthly Income | 37.787 | 8 | **0.000008** | Significant |

Note. The reported p-values are based on the Pearson Chi-square test of independence. Statistical significance was assessed at the 5% level. Because some demographic categories contain relatively small frequencies, the Chi-square results should be interpreted with appropriate caution.

The results indicate that age, educational qualification, occupation, and monthly income have statistically significant associations with fraud awareness, whereas gender does not show a statistically significant association.

**Table 6.** Awareness level by age group (counts)

| Age group | Low | Moderate | High | Total |
|---|---|---|---|---|
| 25 or below | 6 | 6 | 9 | 21 |
| 26–45 | 0 | 4 | 0 | 4 |
| Above 45 | 0 | 8 | 3 | 11 |

Age showed a statistically significant association with fraud awareness, $\chi^2(8, N = 132) = 55.008$, $p < .001$, with Cramer's V = .456. Educational qualification was also significantly associated with awareness, $\chi^2(6, N = 132) = 18.005$, $p = .006$, Cramer's V = .261. Occupation demonstrated a significant association, $\chi^2(8, N = 132) = 38.881$, $p < .001$, Cramer's V = .384. Monthly income also showed a statistically significant association with awareness, $\chi^2(8, N = 132) = 38.225$, $p < .001$, Cramer's V = .381. In contrast, gender was not significantly associated with awareness, $\chi^2(2, N = 132) = 0.212$, $p = .899$, Cramer's V
= .040. Therefore, the null hypothesis of no association is rejected for age, educational qualification, occupation, and monthly income, but it is not rejected for gender.

**Table 7.** Behavioural-intention level by awareness level (counts)

| Intention level | Awareness: Low | Awareness: Moderate | Awareness: High | Total |
|---|---|---|---|---|
| Low | 3 | 0 | 0 | 3 |
| Moderate | 2 | 9 | 0 | 11 |
| High | 1 | 9 | 12 | 22 |

### 4.5 One-way ANOVA

One-way Analysis of Variance (ANOVA) was used to examine whether the mean scores for the study constructs differed across demographic groups. The independent variables (IVs) were educational qualification, occupation, and monthly income, while the dependent variables (DVs) were perceived risk, fraud awareness, behavioural intention, self-efficacy, and trust. The results supplied for this analysis are presented in Table 8. Statistical significance was assessed at the 5% level ($p < .05$).

The results show eight statistically significant demographic–construct comparisons. Educational qualification was associated with perceived risk ($F = 5.847$, $p = .001$), self-efficacy ($F = 3.209$, $p = .025$), behavioural intention ($F = 2.957$, $p = .035$), and trust ($F = 2.784$, $p = .044$). Occupation was associated with fraud awareness ($F = 4.204$, $p = .003$). Monthly income was associated with fraud awareness ($F = 3.893$, $p = .005$), behavioural intention ($F = 3.424$, $p = .011$), and self-efficacy ($F = 3.158$, $p = .016$).

These findings suggest that demographic differences are construct-specific rather than uniform. Education showed significant differences across four constructs, while income showed significant differences across three constructs. Occupation showed a significant difference for fraud awareness. The supplied results include F-statistics and p-values only; degrees of freedom, mean squares, effect sizes, and assumption-test statistics were not provided and are therefore not reported.

**Table 8.** One-way ANOVA results by demographic grouping

| IV | DV | F | p | Interpretation Levene p |
|---|---|---|---|---|
| Education | Perceived Risk | 5.847 | .001 | Significant 0.022 |
| Occupation | Awareness | 4.204 | .003 | Significant <0.001 |
| Income | Awareness | 3.893 | .005 | Significant 0.021 |
| Income | Behavioural Intention | 3.424 | .011 | Significant <0.001 |
| Income | Self-Efficacy | 3.158 | .016 | Significant <0.001 |
| Education | Self-Efficacy | 3.209 | .025 | Significant <0.001 |
| Education | Behavioural Intention | 2.957 | .035 | Significant <0.001 |
| Education | Trust | 2.784 | .044 | Significant 0.013 |

Note. A result is classified as statistically significant when $p < .05$. The values in Table 8 reproduce the supplied ANOVA results. Degrees of freedom, mean squares, effect sizes, and Levene's test results were not included in the supplied summary.

**Table 9.** Mean (SD) of awareness and behavioural intention by group

| Factor | Group | n | Awareness M (SD) | Intention M (SD) |
|---|---|---|---|---|
| Age | 18–25 | 77 | 4.13 (1.04) | 4.38 (1.11) |
| Age | 26–35 | 11 | 4.14 (0.00) | 4.08 (0.22) |
| Age | 36–45 | 3 | 4.43 (0.00) | 4.50 (0.00) |
| Age | Above 45 | 38 | 4.29 (0.45) | 4.32 (0.43) |
| Age | Below 18 | 3 | 3.29 (0.00) | 4.00 (0.00) |
| Gender | Female | 71 | 4.10 (1.01) | 4.26 (1.13) |
| Gender | Male | 61 | 4.24 (0.59) | 4.42 (0.44) |
| Education | Undergraduate | 85 | 4.23 (0.73) | 4.45 (0.75) |
| Education | Postgraduate | 36 | 3.98 (1.14) | 4.07 (1.16) |
| Education | Higher Secondary | 4 | 4.43 (0.00) | 5.00 (0.00) |
| Education | Other | 7 | 4.16 (0.15) | 3.90 (0.09) |
| Occupation | Student | 67 | 3.94 (1.05) | 4.24 (1.15) |
| Occupation | Salaried Employee | 42 | 4.58 (0.41) | 4.44 (0.51) |
| Occupation | Self-employed | 7 | 4.08 (0.08) | 4.62 (0.36) |
| Occupation | Homemaker | 13 | 4.08 (0.39) | 4.24 (0.30) |
| Occupation | Other | 3 | 4.00 (0.00) | 4.50 (0.00) |
| Monthly income | Below ₹20,000 | 69 | 4.03 (1.00) | 4.38 (1.04) |
| Monthly income | ₹20,000–₹40,000 | 14 | 4.85 (0.19) | 4.90 (0.16) |
| Monthly income | ₹40,001–₹60,000 | 13 | 3.82 (0.73) | 3.72 (1.05) |
| Monthly income | ₹60,001–₹80,000 | 7 | 4.08 (0.08) | 4.21 (0.27) |
| Monthly income | Above ₹80,000 | 29 | 4.33 (0.53) | 4.26 (0.40) |

**Multicollinearity and the erosion of trust and self-efficacy**

The fact that trust and self-efficacy were not significant should not be interpreted as indicating their independence from intention. Individually, each predictor was strongly correlated with intention (simple regressions: awareness R =.745, trust.617, perceived risk.541, self-efficacy.488; all p <.001). However, all the predictors shared a lot of overlap (see Table 4), and trust had a VIF of 8.47, well above the common VIF cutoff of 5 (Hair et al., 2010). Awareness essentially absorbed all of the shared variance. A model with awareness and perceived risk explained nearly as much

(R =.772, adjusted R =.758, F (2,33) = 55.73, p <.001; awareness B = 0.72, p <.001; perceived risk B = 0.26, p =.057), so almost all of what trust and self-efficacy added was not much.

**Robustness checks**

Evidence for robust inference. When adopting HC3 standard errors, the in-awareness effect persisted (p =.003), with a bootstrap 95% confidence interval that did not include zero [0.39, 1.27], whereas the intervals for perceived risk, trust and selfefficacy included zero.

Perceived severity. Using severity as the predictor (2 items: PR1, PR3; =.824) resulted in R =.782; awareness (B = 0.58, p =.012) and severity (B = 0.32, p =.035) were significant; trust and self-efficacy was not. Thus, severity, as opposed to susceptibility, seems to be responsible for the perceived- severity effect.

Without uniform responders. The model including the 4 respondents who replied identically to all items (n = 32) was still significant, F (4, 27) = 9.13, p<.001, and awareness was still the sole significant predictor (B = 0.72, p =.002), though the R was substantially lower in this case (R =.575, adjusted R =.512). The high R score in the full sample, then, is in part due to a handful of respondents at the top of each scale.

### 4.6 Summary of hypothesis tests

**Table 11.** Summary of hypotheses

| Hypothesis | Test | Key result | Decision |
|---|---|---|---|
| H1a Gender → awareness level | Chi-square | $\chi^2 = 0.212$, p = .899 | Not supported |
| H1b Age → awareness level | Chi-square | $\chi^2 = 55.008$, p < .001; V = .456 | Supported |
| H1c Education → awareness level | Chi-square | $\chi^2 = 18.005$, p = .006; V = .261 | Supported |
| H1d Occupation → awareness level | Chi-square | $\chi^2 = 38.881$, p < .001; V = .384 | Supported |
| H1e Income → awareness level | Chi-square | $\chi^2 = 38.225$, p < .001; V = .381 | Supported |
| Hypothesis | Test | Key result | Decision |
| H2 Awareness level ↔ intention level | Chi-square | exact $p < .001$; $V = .603$ | Supported |
| H3 Awareness differs by group | One-way ANOVA | ANOVA: occupation (F = 4.204, p = .003) and income (F = 3.893, p = .005) differed significantly for awareness | Partially supported |

| | | | |
|---|---|---|---|
| H4 Intention differs by group | One-way ANOVA | ANOVA: education ($F = 2.957$, $p = .035$) and income ($F = 3.424$, $p = .011$) differed significantly for behavioural intention | Partially supported |
| H5 Awareness → intention | Regression | $\beta = .752$, $p < .001$ | Supported |
| H6 Perceived risk → intention | Regression | $\beta = .264$, $p = .072$ | Not supported (marginal) |
| H7 Trust → intention | Regression | $\beta = -.090$, $p = .720$ | Not supported |
| H8 Self-efficacy → intention | Regression | $\beta = .002$, $p = .992$ | Not supported |

Note. ANOVA decisions are based on the supplied results in Table 8 and use $\alpha = .05$. The supplied summary also identifies significant differences for perceived risk, self-efficacy, and trust; these are reported in Section 4.5 but do not directly correspond to the original H3 and H4 wording.

## 5. Discussion

Participants were quite aware and generally favourably disposed to safe payment behaviour: 50% moderately aware and 33% highly aware of digital payment fraud, and 60% highly safe payment behaviour intention. Although encouraging, the item level results revealed some of the areas where the gaps were. Participants were more comfortable with defining principles (never give an OTP or a PIN) than putting them into practice (to spot a suspicious ask, to spot fraud). Interestingly, while participants identified fraud as very serious, they did not felt as personally at risk- another pattern typical of risk perception research- 'resilience strategy'. The area they found less trustworthy was how an individual platform handles a fraudulent incident after it occurs, not the way they handle the instant that led to the fraud. Demography did very little. There was not even a trend of any kind with gender, education or occupation, and education or occupation scored the same means on the anovas. The only statistically significant correlation, age, was because of everyone in that demography scoring very low - that cell, perhaps through small sample size, also had the largest number of 10s. It seems that demographic position is no easy way to measure awareness and that you don't get fewer or more aware people by being poor and young or not. Although sub-samples are small, the nonsignificant medium to large effects for income and occupation, are just evidence of lack of power. Perhaps the most interesting and important result is the surprisingly strong role of awareness. Awareness was the only statistically significant predictor in the multiple regression, was still statistically significant when using robust standard errors, when running the multiple regression with bootstrapping and uniform responders excluded, and was highly significantly associated with intention level in the chi-square. This result, as well as the small but significant role of perceived risk, is consistent with the coping-appraisal logic of the Protection Motivation Theory (Rogers, 1975) -- threats which one cannot identify in some way cannot be protected against. The inability of susceptibility to covary with the other risk items further indicates that simply "scaring" people won't work, consistent with the prediction of the EPPM (Witte, 1992) that high-efficacy items should accompany threats in a message.

The reason behind not having one unique effect of trust and self-efficacy needs further discussion. They are both very highly correlated with intention alone, so are effectively indistinguishable from awareness within the model. What proportion of that is a construct overlap and what is statistical is: item AW4 "I can identify suspicious digital payment requests" and item SE1 "I am confident that I can identify a suspicious digital payment request" are so close to being the same thing, and item TR5 "My confidence in payment security encourages me to follow safe payment practices" is also the statement of behaviour itself. It may be wise to do a further empirical test of discriminant validity of

awareness, self-efficacy and trust with a larger sample and use of confirmatory factor analysis before disregarding trust and self-efficacy as also having no independent effect.

## 6. Implications

### 6.1 Practical and policy implications

Recognise – don't rule. The key difference here is between knowing the rules and recognising an active scam awareness programme should incorporate genuine examples (bogus links, fake collections requests, scam emails) and simulations to build recognition of scams.

Target messages according to behaviour – a behind the scenes look… Demographics did not provide any explanation for all of the findings and therefore campaigns should be broad and encompassing. They should also be directed at students and young people using these products for the first time, as the only low-awareness groups.

Always associate risk warnings with a call to action. Make the level of risk clear with an action that is easy to implement (double check, never share OTP/PIN, act fast) to ensure it doesn't generate fear without efficacy.

Substantiate fraud incidence. Sites should report their successful resolution time and actions taken for reported incidents, as time to implement was rated the lowest for trust items and willingness to report was rated the lowest for intention items.

Mini-nudges: Use at time of purchase. For example, prompts to remind users to "check on the person you're paying," or not to click on links, at the moment they engage.

### 6.2 Theoretical implications

Protection-motivation theory was also successfully applied to understanding safe digital payment in an Indian sample, with knowledge and recognition skill as the most significant predictor of intended safe payment. Further, an even larger set of predictors has been identified and threat perception appears to be not unidimensional. Severity and susceptibility ought to be included as separate components of threat perception in the models.

## 7. Limitations and Future Research Directions

Small sample. We were down to 36 respondents once dupe records were removed. The limited set of chi-square tables meant that the ANOVA and regression tests were underpowered, estimates were biased. Whilst interesting, the results should be regarded as exploratory until a much bigger sample and, at the collection stage, researchers can see if it is the same people responding at different times (for example - by limiting Google Forms responses).
Non-probability sampling and composition The respondents in the sample. Most of the respondents are students and the majority are aged over 45.

Self-report of intention. Only intentions were collected (not actual behaviour or victimisation), which is vulnerable to demand characteristics. Non-normal distribution of responses, and ceiling effects (all four responses for travel intention was the same) were apparent.
Measurement. Perceived risk reliability was poor (=.588), some items were conceptually similar across constructs, and both constructs were not tested with factor analysis. Multiple Testing: Numerous tests were conducted, and a cross-sectional design cannot determine cause.

Further research would include probability based or quota samples, larger samples, structural equation modelling of overlapping variables, pathways of mediation (e.g. Awareness self-efficacy intention), and behavioural measures such

as actual checking or reporting behaviour.

## 8. Conclusion

The present work examined the relationships between digital payment fraud awareness, perceived risk, platform trust and platform self-efficacy and safe intention of behaviour with a small sample of Indian users. Sample were medium to high aware and high willing for safe behaviour. Only demographic factors weakly differentiated the digital payment fraud awareness, only age group was significant.

In the regression model, which explained approximately ¾ of the variance in intention, fraud awareness was the strongest and most stable predictor, with perceived severity close behind and trust and self-efficacy statistically deprived by awareness, because of their very high collinearity.

Hence, recognition oriented, practical fraud education is the most effective for regulators and educators, to foster safe payment behaviour. This small sample has to be validated on larger samples.

## References

1. Akosile, M. O., Ajayi, L. B., & Ajayi, F. I. (2025). Electronic fraud in the age of digital payment among the users in Ekiti State, Nigeria. Fuoye Journal of Management Sciences,3(2),146–157. https://www.researchgate.net/publication/403799535_ELECTRONIC_FRAUD_IN_THE_AGE_OF_DIGITAL_PAYMENT_AMONG_THE_USERS_IN_EKITI_STAT E_NIGERIA

2. Singh, K., Mistrean, L., Singh, Y., Barak, D. D., & Parashar, A. (2023). Fraud prevention in digital payment systems and cybersecurity education for customers of nationalized financial institutions. In Development Through Research and Innovation–2023 (pp. 98–115), https://doi.org/10.53486/dri2023.08

3. Bulay, L., Visitacion, R. P. S., Orale, J. D., Rodriguez, A. M. C., Roldan, J. M., Baluyos,

A. K. A. D., Pantua, M. C., Lagane, F., Codilla, J. P. U., Pepito, A., Sumoroy, M. C., Dolalas, K. R., & Fernandez, G. A. (2026). Assessment of consumer cybersecurity awareness, fraud vulnerability, and trust in e-commerce platforms: Toward a proposed machine learning-based detection framework for order scams and payment fraud. Mediterranean Journal of Basic and Applied Sciences, 10(2), 48–66. https://doi.org/10.46382/mjbas.2026.10204

4. Hirapara, D., Sheth, K., & Vidani, J. (2024). A study on the awareness of various digital payment frauds among Gen-Zs in Ahmedabad City. International Journal of Business and Management Practices, 2(6), 701–716, https://doi.org/10.59890/ijbmp.v2i6.105

5. Chugh, B., & Narang, L. (2023). Are fraud-awareness campaigns effective? Measuring the effectiveness of fraud-awareness campaigns and proposing recommendations for enhancing it, https://dvararesearch.com/are-fraud-awareness-campaigns-effective-measuring-the-effectiveness-of-fraud-awareness-campaigns-and-proposing-recommendations-for-enhancing-it/

6. Parvathy, V., & Durairaj, D. (2021). A study on users perception and awareness towards digital payment security threats among youngsters in Chennai, Tamil Nadu, India. Asian Review of Social Sciences, 10(2), 30–34, https://doi.org/10.51983/arss-2021.10.2.2988

7. Bai, L. (2025). How online activities shape anti-fraud payment behavior: Evidence from Chinese youth. SAGE Open, 15(3), 1–19, https://doi.org/10.1177/21582440251378971

8. Saikrishnan, S. (2025). Consumer awareness towards digital payment fraud in India. International Scientific Journal of Engineering and Management, 4(10), 1–9. https://doi.org/10.55041/ISJEM05094

9. Quraishy, S. A., & Abdulla. (2026). Digital payment systems: Their role in economic growth and associated criminal activities. International Journal of Innovations in Science, Engineering and Management, 5(3), 113–119. https://doi.org/10.69968/ijisem.2026v5i3113-119

10. Maini, R., & Sindhi, V. K. (2025). Digital banking fraud in India: Typologies, victim behaviour, and AI-enabled risk governance in a global context. International Journal for Multidisciplinary Research, 7(5). https://doi.org/10.36948/ijfmr.2025.v07i05.55593

11. Harichandana, A. D. (2025). Digital payement adoption in emerging markets. International Journal on Science and Technology, 16(3). https://doi.org/10.71097/IJSAT.v16.i3.7770

12. Sunderajulu, K. B. (2024). E-commerce & digital wallet payment fraud. Advanced International Journal of Multidisciplinary Research, 2(6). https://doi.org/10.62127/aijmr.2024.v02i06.1111

13. Sethupathy, U. K. A. (2025). Evolving frameworks in digital payment security: Technological innovations, economic impact, and consumer trust dynamics. International Journal of Computational and Experimental Science and Engineering, 11(3), 6623–6634.
https://doi.org/10.22399/ijcesen.3893

14. Elia Habibullah, M. R. (2026). Legal protection for consumers in digital e-commerce agreements based on the Civil Code and consumer protection law. Veteran Law Review, 9(1), 12–27.
https://doi.org/10.35586/velrev.v9i1.13118

15. Afzal, M., Meraj, M., Kaur, M., & Ansari, M. S. (2024). How does cybersecurity awareness help in achieving digital financial inclusion in rural India under escalating cyber fraud scenario. Journal of Cyber Security Technology. https://doi.org/10.1080/23742917.2024.2347674

16. Uma, K. (2025). Fraud regulation in digital payment systems: Challenges, frameworks, and emerging solutions. In Proceedings of the 13th International Conference on Emerging Trends in Corporate Finance and Financial Markets. SDM Institute for Management Development, https://www.sdmimd.ac.in/

17. Halage, Y., & Bharathkumar, K. (2025). Analytics driven fraud detection in UPI transactions: Trends, models, and insights. In Proceedings of the 13th International Conference on Emerging Trends in Corporate Finance and Financial Markets. SDM Institute for Management Development, https://www.sdmimd.ac.in/

18. Rao, K. M., Fatima, S. M., & Fatima, H. (2026). Fraud detection in online payment gateways: Consumer perceptions, technological challenges, and emerging solutions with special reference to Paytm – One 97 Communications Limited. International Journal of Scientific Research in Engineering and Management, 10(6). https://doi.org/10.55041/IJSREM65559

19. Trivedi, H. (2024). Evolution of digital payment system in India: Past, present and future. International Research Journal of Humanities and Interdisciplinary Studies, 5(1), 30–48, https://doi-ds.org/doilink/01.2024-49838919/IRJHIS2401004

20. Barillà, G. B. (2024). Payment fraud in Italy and in the UK: Comparative analysis and prospects for reform. Il Diritto degli Affari, 1, 13–38, https://www.dirittodegliaffari.it/

21. Vince, M. (2025). Digital wallets for impactful financial inclusion: Innovative strategies based on Sharia economics and cybersecurity in Indonesia. Preprints.org. https://doi.org/10.20944/preprints202506.2388.v1

22. Lakshmi, R., & Vennila Fatima Rani, S. (2024). Securing digital wallets: Threats and countermeasures.

mLAC Journal for Arts, Commerce and Sciences, 2(4), 25–32. https://doi.org/10.59415/mjacs.v2i4.185

23. Kumar, A. (2025). Smart fraud detection and prevention: Leveraging generative AI for enhanced payment security. Journal of Information Systems Engineering and Management, 10(59s), https://www.jisem-journal.com/

24. Sixt, E. (2025). Restoring trust in European payment rails: A framework for a shared liability reform. European Funds Recovery Initiative (EFRI). https://efri.io/

25. Marakalala, M. C. (2025). An exploration of biometrics payment technology to combat online banking fraud and digital identity in the South African banking industry. OIDA International Journal of Sustainable Development, 18(12). https://www.ssrn.com/index.cfm/en/oida-intl-journal-sustainable-dev/