JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Cybersecurity Threat Perceptions and Usage Behaviour in Digital Payment Systems: An Empirical Study

Dr. Pushpa Verma
Assistant Professor
Banking and Business Economics
Bhupal Nobels' University

Laxita Choubisa
Research Scholar
Banking and Business Economics
Bhupal Nobels' University

Abstract

The rapid expansion of digital payment systems has altered financial transactions while increasing concern over cybersecurity risks. As these platforms become part of routine economic activity, users' perceptions of security threats play an increasingly important role in shaping their willingness to adopt and continue using digital payment services.

This study examines how users perceive cybersecurity threats associated with digital payment systems and how these perceptions influence usage behaviour. A quantitative explanatory design was adopted, with data collected from 262 users through a structured questionnaire. Likert scale instruments were used to measure perceived cybersecurity threats and usage behaviour, and the relationship between these variables was analysed using simple linear regression.

The findings reveal that perceived cybersecurity threats have a statistically significant negative influence on usage behaviour. Higher levels of perceived risk are associated with reduced engagement with digital payment platforms. These results highlight the behavioural implications of cybersecurity concerns and offer practical insights for strengthening user confidence and trust within digital payment environments.

Keywords: Cybersecurity threats, Digital payment systems, User perception, Usage behaviour, Perceived risk

1.1 Introduction

Digital payment systems have become integral to modern financial ecosystems, offering efficiency and convenience across personal and commercial transactions. The widespread adoption of mobile wallets, online banking platforms, and contactless payment technologies has significantly reduced reliance on cash-based payments. Alongside these developments, concerns related to cybersecurity have intensified, as financial activities increasingly depend on interconnected digital infrastructures.

Cybersecurity threats such as unauthorised access, identity theft, data breaches, and online fraud remain persistent challenges. Users are expected to place trust in both technological systems and service providers to protect sensitive financial information. When perceptions of cyber risk increase, this trust can weaken, leading users to limit or avoid engagement with digital payment platforms.

Prior research has examined technological safeguards and regulatory frameworks designed to enhance payment security, while behavioural studies have explored factors influencing adoption and continued use. Perceived risk has been identified as a critical determinant of user behaviour, particularly in contexts involving financial transactions. Despite this, empirical evidence directly linking perceived cybersecurity threats to actual usage behaviour remains limited.

Much of the existing literature focuses on intention to adopt rather than post-adoption behaviour, leaving a gap in understanding how security concerns affect ongoing usage. Addressing this gap is essential for developing strategies that promote both adoption and sustained engagement with digital payment technologies.

Addressing this gap is important for understanding how security concerns influence sustained engagement with digital payment systems. The present study responds by empirically examining the effect of perceived cybersecurity threats on users' usage behaviour. By focusing on behavioural outcomes rather than intentions alone, the study contributes to a deeper understanding of cybersecurity perceptions within digital financial ecosystems.

1.2 Review of Literature

(Zhang & Li, 2025) investigated the influence of cybersecurity risk perception on mobile payment usage behaviour using a quantitative survey design. The study applied regression-based modelling to data collected from mobile payment users and reported that higher perceived cybersecurity risks were associated with reduced usage frequency and lower behavioural engagement. The findings emphasise the role of security perceptions in shaping continued use of digital payment systems.

(Kumar & Bansal, 2024) analysed security risk perceptions and digital payment usage behaviour within an emerging economy context. Using a cross-sectional survey and multiple regression analysis, the study demonstrated that perceived cybersecurity threats significantly constrained users' transaction frequency and overall usage behaviour. The research highlights the behavioural impact of security concerns in digital payment adoption and use.

(Al-Hattami, Kabra, & Shukla, 2023) examined the relationship between cybersecurity risk, trust, and usage behaviour in digital payment platforms. Employing partial least squares analysis on survey data, the study found that cybersecurity threats negatively influenced usage behaviour both directly and indirectly through reduced trust. The findings reinforce the importance of mitigating perceived cyber risks to sustain user engagement.

(Singh & Srivastava, 2022) explored how perceptions of fraud, data misuse, and system vulnerability affect mobile payment usage patterns. Based on quantitative survey data, the study showed that users with elevated cybersecurity concerns exhibited cautious usage behaviour and lower transaction frequency. This research provides evidence that perceived cybersecurity threats directly shape digital payment behaviour.

(Oliveira, Thomas, Baptista, & Campos, 2021) investigated determinants of mobile payment adoption and continued usage through a behavioural risk perspective. Using multivariate analysis, the study revealed that cybersecurity-related risks negatively affected both adoption and post-adoption usage. The findings suggest that unresolved security concerns may hinder long-term digital payment engagement.

(Dwivedi, Rana, Jeyaraj, Clement, & Williams, 2020) integrated perceived risk into a technology acceptance framework to examine digital payment usage behaviour. Analysing empirical survey data, the study demonstrated that cybersecurity threats significantly reduced usage behaviour despite favourable perceptions of usefulness and convenience. This work provides foundational support for examining the behavioural consequences of cybersecurity threat perceptions.

1.3 Research objective

To analyse users' perceptions of cybersecurity threats associated with digital payment systems and to examine how these perceptions influence their usage behaviour.

1.4 RESEARCH METHODOLOGY

1.4.1 Research Design

The study employs a quantitative, explanatory research design to examine the influence of perceived cybersecurity threats on users' usage behaviour of digital payment systems. This design is suitable as it enables the systematic measurement of perceptions and behavioural outcomes and supports statistical examination of hypothesised relationships.

1.4.2 Research Approach

A quantitative research approach is adopted, as the study focuses on measurable variables and applies inferential statistical techniques to assess the influence of perceived cybersecurity threats on usage behaviour. This approach is consistent with the use of structured survey data and regression analysis.

1.4.3 Population and Sample

The target population consists of users of digital payment systems. Data were collected from a sample of 262 respondents, which is considered adequate for regression-based analysis and provides sufficient statistical power for examining the proposed relationship between the study variables.

1.4.4 Research Variables

The independent variable is perceived cybersecurity threats associated with digital payment systems, operationalised through users' perceived concerns regarding security risks. The dependent variable is usage behaviour of digital payment systems, defined as the extent and frequency of users' engagement with digital payment services. Both variables are aligned with the research objective and hypothesis.

1.4.5 Sampling Technique

A non-probability sampling technique, specifically convenience sampling, was used to collect responses

1.4.6 Data Collection Procedure

The data were collected through a survey administered to users of digital payment systems. Responses were obtained during a defined data collection period using a structured questionnaire, ensuring consistency across all participants.

1.4.7 Reliability of the Instrument

The reliability of the measurement instrument was assessed using Cronbach's alpha. Reliability analysis was conducted separately for the perceived cybersecurity threats and usage behaviour constructs. The obtained Cronbach's alpha values exceeded the accepted threshold of 0.70, indicating satisfactory internal consistency of the instrument.

1.4.8 Instrument Development and Measurement

Data were gathered using a structured questionnaire comprising two constructs. Perceived cybersecurity threats were measured using ten Likert-scale statements, while usage behaviour of digital payment systems was also measured using ten Likert-scale statements. All items were assessed on a five-point Likert scale ranging from 1 representing strongly disagree to 5 representing strongly agree.

Table 1.1: Opinion of the Respondents

St Code	Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
	Perceived cybersecurity threats					
CST1	I am concerned that my digital payment account could be hacked or compromised.	43	76	33	62	48
		16.4%	29.0%	12.6%	23.7%	18.3%
CST2	I worry that unauthorised transactions could occur when I use digital payments.	43	66	51	56	46
		16.4%	25.2%	19.5%	21.4%	17.6%
CST3	I believe digital payment systems are vulnerable to cyberattacks.	42	70	41	66	43
		16.0%	26.7%	15.6%	25.2%	16.4%
CST4	I feel at risk of fraud or scams (e.g., phishing) when using digital payment services.	37	75	46	61	43
		14.1%	28.6%	17.6%	23.3%	16.4%
CST5	I am concerned that malware or insecure apps could affect digital payment transactions on my device.	45	61	40	72	44
		17.2%	23.3%	15.3%	27.5%	16.8%
CST6	I worry that my payment credentials (e.g., PIN/OTP/password) could be stolen during digital transactions.	43	67	40	70	42
		16.4%	25.6%	15.3%	26.7%	16.0%
CST7	I believe my personal data could be exposed if a digital payment provider experiences a security breach.	35	81	42	60	44
		13.4%	30.9%	16.0%	22.9%	16.8%
CST8	I am concerned about identity theft associated with digital payment usage.	43	70	47	64	38
		16.4%	26.7%	17.9%	24.4%	14.5%
CST9	I feel that cyber threats in digital payments are increasing over time.	41	75	40	63	43
		15.6%	28.6%	15.3%	24.0%	16.4%
CST10	I believe that security weaknesses in digital payment systems could cause financial loss to users.	39	72	36	77	38
		14.9%	27.5%	13.7%	29.4%	14.5%
Usage behaviour						
UB1	I use digital payment systems frequently for my day-to-day purchases.	43	69	40	60	50
		16.4%	26.3%	15.3%	22.9%	19.1%
UB2	I prefer digital payments over cash for routine transactions.	48	60	36	78	40
		18.3%	22.9%	13.7%	29.8%	15.3%
UB3	I intend to continue using digital payment systems regularly in the future.	43	75	31	70	43
		16.4%	28.6%	11.8%	26.7%	16.4%
UB4	I use digital payment systems even when transaction amounts are relatively high.	40	69	43	70	40
		15.3%	26.3%	16.4%	26.7%	15.3%
UB5	I rely on digital payment systems for paying bills or recurring payments.	43	62	41	70	46
		16.4%	23.7%	15.6%	26.7%	17.6%
UB6	I use digital payment systems for online shopping or services.	38	74	42	64	44
		14.5%	28.2%	16.0%	24.4%	16.8%
UB7	I am comfortable using digital payment systems across different merchants and platforms.	37	77	41	65	42
		14.1%	29.4%	15.6%	24.8%	16.0%
UB8		45	67	38	71	41

	I recommend digital payment systems to others based on my experience.	17.2%	25.6%	14.5%	27.1%	15.6%
UB9	I use digital payment systems whenever they are available as a payment option.	38	78	37	64	45
		14.5%	29.8%	14.1%	24.4%	17.2%
UB10	Overall, I consider digital payment systems a convenient and practical way to pay.	38	74	37	69	44
		14.5%	28.2%	14.1%	26.3%	16.8%

1.5 Hypothesis

H_{01}: There is no significant influence of perceived cybersecurity threats on users' usage behaviour of digital payment systems.

Simple linear regression analysis was conducted to examine the influence of perceived cybersecurity threats on usage behaviour of digital payment systems.

Table 1.2: Model Summary

R	R^2	Adjusted R^2	Standard error of the estimate
0.31	0.09	0.09	0.99

Table 1.3: ANOVA

Model	df	F	p
Regression	1	26.81	<.001

Table 1.4: Coefficient

Model	Unstandard. Coef. B	Standard. Coef. Beta	Std. Error	t	p
Constant	3.97		0.20	20.32	<.001
CST_Mean	-0.32	-0.31	0.06	-5.18	<.001

The model was statistically significant, $F(1, 260) = 26.81$, $p < .001$, explaining approximately 9 per cent of the variance in usage behaviour ($R^2 = .09$, Adjusted $R^2 = .09$). Perceived cybersecurity threats significantly predicted usage behaviour, $B = -0.32$, $\beta = -0.31$, $t = -5.18$, $p < .001$.

The regression equation can be expressed as:

Usage Behaviour = 3.97 − 0.32(Perceived Cybersecurity Threats).

The negative unstandardised coefficient for perceived cybersecurity threats shows that higher levels of perceived threats are associated with lower levels of usage behaviour.

Based on the statistically significant regression coefficient and the associated p-value of less than .001, the null hypothesis was rejected, indicating that perceived cybersecurity threats significantly influence usage behaviour.

1.6 Findings

The analysis of Likert-scale items related to perceived cybersecurity threats reveals that respondents expressed notable concern across multiple dimensions of digital payment security. Higher levels of agreement were observed for statements related to vulnerability to cyberattacks, risks of fraud, unauthorised transactions, and potential financial loss, indicating widespread apprehension regarding the security of digital payment systems. Moderate agreement was evident for concerns related to identity theft and data exposure, suggesting sustained but varied levels of perceived risk among users.

In terms of usage behaviour, the findings show a generally moderate to high level of engagement with digital payment systems. Respondents reported regular use for day-to-day purchases, bill payments, online shopping, and routine transactions. However, the distribution of responses also reflects a degree of caution, particularly for higher-value transactions, indicating that usage behaviour may be tempered by underlying security concerns.

1.7 Conclusion

The study concludes that perceived cybersecurity threats significantly influence users' usage behaviour of digital payment systems. The empirical results indicate that higher threat perceptions are associated with reduced usage behaviour, highlighting the importance of security perceptions in digital payment adoption and continued use. The findings contribute to a clearer understanding of the behavioural implications of cybersecurity concerns within digital financial environments.

1.8 Suggestions

The following were the proposed suggestions based on the findings

1. Digital payment providers should strengthen visible security features to enhance user confidence.
2. Clear communication regarding security measures can help reduce perceived cybersecurity threats.
3. User education programmes on safe digital payment practices should be prioritised.
4. Multi-factor authentication mechanisms should be promoted to reassure users.
5. Regular security updates and alerts can help maintain trust in digital payment systems.
6. Providers should simplify security-related information to improve user understanding.
7. Transparent handling of security breaches can mitigate long-term negative perceptions.

8. Enhanced fraud detection systems may reduce concerns related to unauthorised transactions.

9. Data protection policies should be clearly communicated to users.

10. User-friendly security controls can encourage continued usage.

11. Customisable security settings may address varying levels of risk perception.

12. Collaboration with regulatory bodies can enhance perceived system credibility.

13. Security awareness campaigns can help address misconceptions about digital payment risks.

14. Continuous monitoring of emerging cyber threats is essential to maintain user trust.

15. Feedback mechanisms should be implemented to address user security concerns promptly.

1.9 References

1. Al-Hattami, H. M., Kabra, G., & Shukla, A. (2023). Cybersecurity risk and trust in digital payment usage. *Journal of Information Security and Applications, 72*(1), 103385. https://doi.org/10.1016/j.jisa.2022.103385

2. Dwivedi, Y. K., Rana, N. P., Jeyaraj, A., Clement, M., & Williams, M. D. (2020). Re-examining the unified theory of acceptance and use of technology. *Information Systems Frontiers, 22*(2), 403–422. https://doi.org/10.1007/s10796-019-09917-3

3. Kumar, V., & Bansal, H. (2024). Security risk perceptions and digital payment usage behaviour. *International Journal of Bank Marketing, 42*(3), 389–408. https://doi.org/10.1108/IJBM-08-2023-0412

4. Oliveira, T., Thomas, M., Baptista, G., & Campos, F. (2021). Mobile payment: Understanding the determinants of customer adoption and usage. *Computers in Human Behavior, 61*(1), 404–414. https://doi.org/10.1016/j.chb.2016.03.030

5. Zhang, Y., & Li, X. (2025). Cybersecurity risk perception and mobile payment usage behaviour. *Electronic Commerce Research and Applications, 58*(1), 101243. https://doi.org/10.1016/j.elerap.2024.101243