International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

A Study on Digital Payments and Cybersecurity

Dr. R. Blessie Pathmu[1], Ms. Raji Edwin.R[2]

[1]Assistant Professor, School of Management Studies, Sathyabama Institute of Science and Technology.
[2] MBA, School of Management Studies, Sathyabama Institute of Science and Technology.

ABSTRACT

This study explores how cybersecurity awareness and trust impact user engagement with digital payments. Based on responses from 110 active users of UPI, mobile wallets, and online banking, the research employs SPSS tools to analyze correlations between awareness, trust, and usage. Results show that higher cybersecurity knowledge and perceived platform security significantly boost user confidence and transaction frequency. The findings highlight the importance of user education, transparent communication, and robust security features in promoting safer and more widespread adoption of digital payment systems.

INTRODUCTION

Digital payments have revolutionized financial transactions, offering speed and convenience through tools like UPI, mobile wallets, and QR codes. However, this shift has heightened cybersecurity concerns, from phishing to fraud. While security features like OTPs and biometrics exist, their impact depends on user awareness and trust. This study explores how these factors influence digital payment usage. Through survey-based analysis, it examines whether cybersecurity knowledge and trust affect user behavior. Understanding these dynamics can help stakeholders design more secure, user-friendly payment systems in today's fast-evolving digital landscape.

REVIEW OF LITERATURE

Digital payments offer ease but come with cyber risks. Sharma and Sinha (2021) emphasize fraud response systems to build trust, while Gupta et al. (2020) highlight the role of encryption and multi-factor authentication. Regulatory efforts like RBI mandates and user education are crucial for secure digital payment usage.

OBJECTIVES

Primary Objectives:

- Assess user awareness of cybersecurity practices in digital payment systems.
- Analyze how cybersecurity concerns affect the frequency of digital payment usage.

Secondary Objectives:

- Identify commonly used security features and evaluate their perceived effectiveness.
- Examine the link between user trust and perceived platform security.
- Provide recommendations to enhance user education and strengthen digital payment security features.

RESEARCH METHODOLOGY

This study used a descriptive approach with primary data collected through an online questionnaire targeting 110 Indian users of digital payment platforms. Convenience sampling was used, and SPSS tools like regression, correlation, and descriptive statistics were applied to analyze user perceptions of cybersecurity in digital transactions.

HYPOTHESES

Hypothesis - 1:

- Null Hypothesis (H0): There is no statistically significant correlation between users' awareness of cybersecurity practices and their frequency of digital payment usage.
- Alternative Hypothesis (H1): There exists a statistically significant correlation between users' awareness of cybersecurity practices and the frequency with which they engage in digital payment transactions.

Hypothesis - 2:

- Null Hypothesis(H0): There is no significant relationship between users' trust in digital payment platforms and their perception of the platforms' cybersecurity features.
- Alternative Hypothesis(H1): There is a significant relationship between users' trust in a digital payment platform and their perception of its cybersecurity robustness.

DISCUSSION:

- **Hypothesis 1:** The study confirmed that higher cybersecurity awareness leads to more frequent digital payment usage, with regression analysis showing a statistically significant relationship ($\beta = 0.577$, $p < 0.01$). This supports the hypothesis that awareness influences user behavior, rejecting the null hypothesis that awareness does not affect usage.
- **Hypothesis 2:** A significant positive correlation ($r = 0.568$, $p = 0.000$) between trust in digital platforms and perceived cybersecurity was found. This supports the hypothesis that trust is influenced by visible security features, rejecting the null hypothesis that no relationship exists between trust and perceived cybersecurity.

CONCLUSION:

Cybersecurity awareness and trust play pivotal roles in encouraging digital payment usage. Users who are well-informed about security are more confident in their transactions. To enhance adoption, financial institutions must focus on user education, clear security features, and transparent communication, ensuring a secure and inclusive digital economy.

REFERENCES

1. **Gupta, S., Bansal, A., & Goel, R. (2020).** Cybersecurity challenges in digital payments: A user-centric perspective. Journal of Information Security Research.
2. **Kaur, G., & Malik, A. (2020).** Consumer awareness and adoption of digital payment systems in India. Global Journal of Management and Business Research.
3. **Ministry of Electronics and Information Technology (MeitY). (2023).** Digital India: Cybersecurity and Digital Payments.
4. **Mishra, R., & Dubey, S. (2021).** Impact of cybersecurity awareness on the usage of digital wallets.

Journal of Financial Services Technology.
5. **Reserve Bank of India. (2022).** RBI Annual Report 2021-22: Progress in Digital Payments.
6. **Sharma, M., & Sinha, A. (2021).** Building trust in digital financial services through effective fraud response systems. International Journal of Cybersecurity Intelligence and Cybercrime.
7. **Singh, A., & Choudhary, P. (2022).** Perceived trust and security in digital payments: A structural equation modeling approach. International Journal of Digital Economy.