Advanced International Journal for Research (AIJFR)
E-ISSN: 3048-7641 ● Website: www.aijfr.com ● Email: editor@aijfr.com

Cyber Hygiene and Digital Payment Safety among College Students: An Economic Perspective on Online Financial Behaviour

Ms. Sonia Roy Varghese

ASM College of Commerce, Science & Information Technology

Abstract

The acceleration of digital financial ecosystems has fundamentally reconfigured transactional behaviour, particularly through the proliferation of mobile payment platforms and internet-based financial services. While such innovations have enhanced efficiency and financial inclusion, they have concurrently intensified exposure to cyber risks, including phishing, identity compromise, and transactional fraud. Within this context, cyber hygiene—defined as the systematic adoption of preventive digital security practices—emerges as a critical determinant of secure financial engagement.

This study critically examines the level of cyber hygiene awareness and digital payment safety practices among college students, a demographically significant and technologically active user group. Employing a structured survey methodology, the research evaluates behavioural patterns, awareness levels, and adherence to cybersecurity protocols in digital financial transactions. The empirical findings reveal a pronounced asymmetry between the widespread adoption of digital payment systems and the limited application of essential security practices, particularly in areas such as multi-factor authentication and verification mechanisms.

The study argues for the institutionalization of cybersecurity education within academic ecosystems to strengthen digital financial resilience. Enhancing cyber hygiene practices among young users is imperative not only for mitigating individual financial risk but also for reinforcing systemic stability within the digital economy.

Keywords: Cyber hygiene, digital payments, cybersecurity awareness, digital economy, financial behaviour

1. Introduction

The integration of digital technologies into financial systems has engendered a structural transformation in contemporary economic activity. The increasing reliance on mobile applications, digital wallets, and internet banking platforms has facilitated real-time, low-cost, and highly accessible financial transactions. This shift is particularly pronounced in emerging economies, where digital payment infrastructures have expanded rapidly.

In the Indian context, platforms such as Google Pay, PhonePe, and Paytm have achieved significant penetration, especially among younger, technology-oriented populations. College students constitute a critical segment within this ecosystem, characterized by high transaction frequency and extensive digital engagement.

However, the expansion of digital financial services has been accompanied by a parallel escalation in cyber vulnerabilities. Threat vectors such as phishing attacks, malicious applications, deceptive payment interfaces, and social engineering techniques increasingly exploit behavioural and informational gaps among users. This underscores the relevance of cyber hygiene as a foundational element of secure digital participation.

Cyber hygiene encompasses a set of routine, preventive practices aimed at safeguarding digital identities and financial data. These include the use of robust authentication mechanisms, periodic system updates, cautious interaction with digital interfaces, and adherence to secure transaction protocols. Despite its importance, the extent to which such practices are understood and implemented remains uneven across user groups.

This study seeks to evaluate the level of cyber hygiene awareness among college students and to analyse their financial behaviour within digital payment environments. By doing so, it contributes to the broader discourse on digital financial security and behavioural economics.

2. Objectives of the Study

- To critically assess the level of cyber hygiene awareness among college students
- To examine usage patterns of digital payment platforms within the student population
- To evaluate the extent of adoption of financial safety practices in digital transactions
- To identify potential vulnerabilities arising from inadequate cyber hygiene

3. Literature Review

The increasing digitization of financial services has led to a growing body of interdisciplinary research examining cybersecurity awareness, user behaviour, and digital financial risk. Cyber hygiene, as a behavioural construct, has gained prominence in understanding how individual practices influence vulnerability to cyber threats.

Von Solms and Van Niekerk (2013) conceptualize cybersecurity as an evolution from traditional information security, emphasizing that technological safeguards alone are insufficient without active user participation. Their work highlights that individual awareness and routine security practices are essential components of a comprehensive cybersecurity framework.

Kshetri (2016) analyses the economic dimensions of cybercrime, arguing that the expansion of digital financial systems has simultaneously increased the scale and sophistication of cyber threats. The study underscores the economic costs associated with cybercrime and stresses the importance of strengthening user-level security awareness to mitigate financial risks.

From a behavioural perspective, Hadlington (2017) identifies human factors as a critical determinant of cybersecurity effectiveness. The study finds that users often engage in risky online behaviour due to

overconfidence, lack of technical knowledge, or habitual negligence. This behavioural vulnerability is particularly relevant among younger users who exhibit high digital engagement but inconsistent security practices.

Bada and Nurse (2019) further extend this argument by emphasizing the role of structured cybersecurity education in influencing user behaviour. Their research demonstrates that awareness programs significantly improve users' ability to recognize and respond to cyber threats, thereby reducing susceptibility to attacks.

In the context of financial technology, Gomber et al. (2018) examine the transformative impact of fintech innovations on financial service delivery. While digital payment systems enhance efficiency and financial inclusion, the authors caution that their sustainability depends on robust security frameworks and informed user participation.

Additional studies have explored the relationship between digital literacy and financial security. Anderson (2020) highlights that security engineering must account for both technological design and user behaviour, as even well-designed systems can be compromised by weak user practices. Similarly, Whitman and Mattord (2021) emphasize that cybersecurity is a shared responsibility between system providers and end users.

Recent empirical studies have also focused on cybersecurity awareness among students. Gupta (2021) finds that although students are frequent users of digital platforms, their understanding of cyber threats remains superficial. The study suggests that awareness does not always translate into safe practices, indicating a gap between knowledge and behaviour.

Mishra (2022), in the Indian context, examines the rapid growth of digital payments following policy initiatives and technological advancements. The study highlights that while adoption rates have increased significantly, security awareness has not kept pace, thereby exposing users to financial fraud.

Reports by international organizations such as the World Bank (2022) emphasize that cybersecurity is a foundational requirement for the stability of the digital economy. The report notes that inadequate cyber hygiene at the user level can undermine trust in digital financial systems and hinder long-term economic growth.

Furthermore, behavioural economics provides additional insight into user decision-making in digital environments. Users often prioritize convenience and speed over security, leading to suboptimal protective behaviour. This tendency is particularly evident in the adoption of digital payment systems, where ease of use may overshadow risk considerations.

Collectively, the literature indicates that while digital financial technologies offer substantial benefits, their effectiveness is closely linked to user awareness and behaviour. Cyber hygiene emerges as a critical factor in bridging the gap between technological advancement and secure usage, especially among digitally active populations such as college students.

4. Research Methodology

The present study adopts a **descriptive research design** to systematically examine the level of cyber hygiene awareness and digital payment safety practices among college students. A descriptive approach is considered appropriate as the study seeks to analyse existing behavioural patterns, awareness levels, and usage trends without manipulating any variables.

Research Approach

The study follows a **quantitative research approach**, focusing on the collection and analysis of numerical data to identify patterns and relationships in students' digital financial behaviour. This approach enables objective measurement of awareness levels and the extent of adoption of cybersecurity practices.

Data Collection

The research is based on **primary data**, collected through a structured questionnaire designed specifically for this study. The questionnaire consisted of close-ended questions to ensure uniformity in responses and ease of statistical analysis. The questions were divided into three key sections:

- Usage of digital payment platforms
- Awareness of cyber hygiene practices
- Adoption of cybersecurity measures

The questionnaire was distributed among students through both online and offline modes to ensure a broader response base.

Sample Size and Population

The study was conducted among **120 undergraduate college students**, representing a segment of young digital users who frequently engage in online financial transactions. This group was selected due to their high exposure to digital payment systems and relevance to the research objective.

Sampling Technique

A **convenience sampling method** was employed for data collection. This non-probability sampling technique was chosen due to ease of access and time constraints. While it allows for efficient data collection, it may limit the generalizability of the findings.

Data Analysis Techniques

The collected data was systematically analysed using **percentage analysis**, which facilitated the interpretation of response distribution across different variables. The results were presented through:

- Tabular representation for clarity
- Graphical representation (charts/figures) for visual interpretation

These tools helped in identifying trends in digital payment usage and levels of cybersecurity awareness among students.

Reliability and Validity

To ensure the **reliability** of the data, the questionnaire was designed using clear and unambiguous language, minimizing the possibility of misinterpretation. The **validity** of the study was maintained by

aligning the questionnaire with the research objectives and focusing on relevant variables related to cyber hygiene and digital financial behaviour.

Limitations of the Study

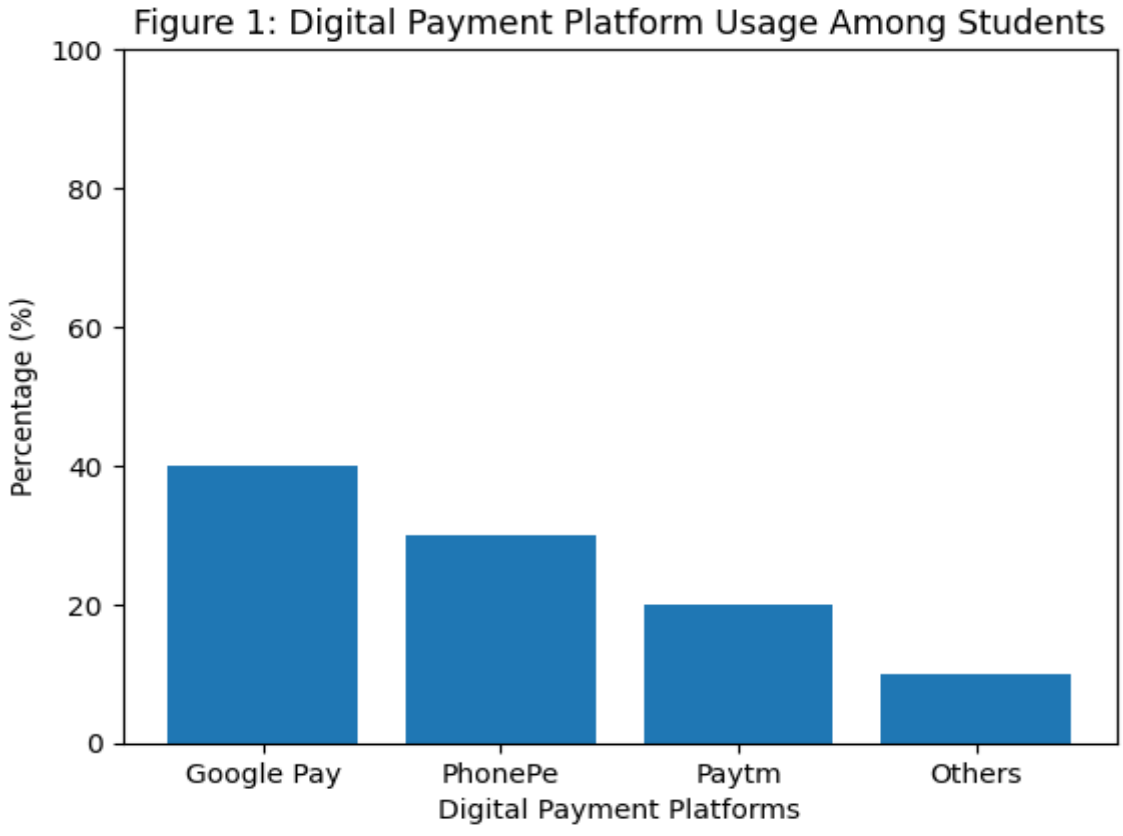
Despite its contributions, the study has certain limitations:

- The use of convenience sampling may not fully represent the broader student population
- The sample size is limited to 120 respondents
- The study relies on self-reported data, which may be subject to response bias

5.Data Analysis and Interpretation

Table 1 Digital Payment Platforms Used by Students

Platform	Number of Students	Percentage
Google Pay	48	40%
PhonePe	36	30%
Paytm	24	20%
Others	12	10%



Interpretation

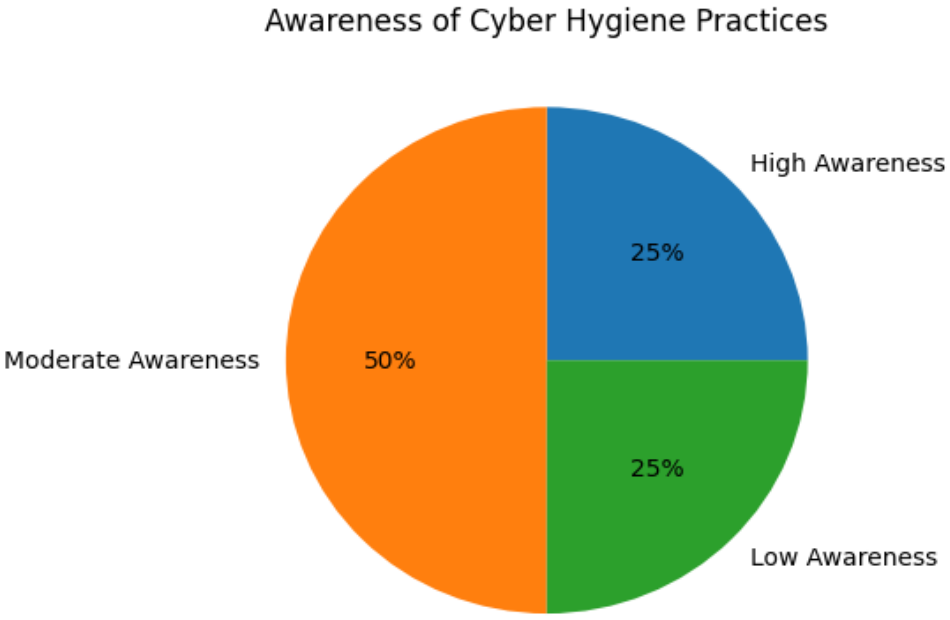
The distribution of responses indicates a **high concentration of usage among a few dominant digital payment platforms**, with Google Pay emerging as the most preferred option among respondents. This trend reflects the presence of **network effects**, where widespread adoption reinforces platform preference due to familiarity, ease of use, and peer influence.

The relatively lower usage of alternative platforms suggests limited diversification in payment behaviour, which may increase dependency on specific applications. From a cybersecurity perspective, such concentration could amplify systemic risk if users rely heavily on a single platform without adequate security awareness.

Furthermore, the findings highlight that students prioritize **convenience, accessibility, and transaction efficiency**, often overlooking platform-specific security features. This indicates that while adoption is high, security considerations are not the primary determinants of platform choice.

Table 2 Awareness of Cyber Hygiene Practices

Awareness Level	Students	Percentage
High Awareness	30	25%
Moderate Awareness	60	50%
Low Awareness	30	25%



Interpretation

The data reveals that **half of the respondents fall within the moderate awareness category**, indicating a basic understanding of cyber hygiene practices but insufficient depth for effective risk mitigation. The equal proportion of students in high and low awareness categories (25% each) suggests a **polarization in cybersecurity knowledge levels**.

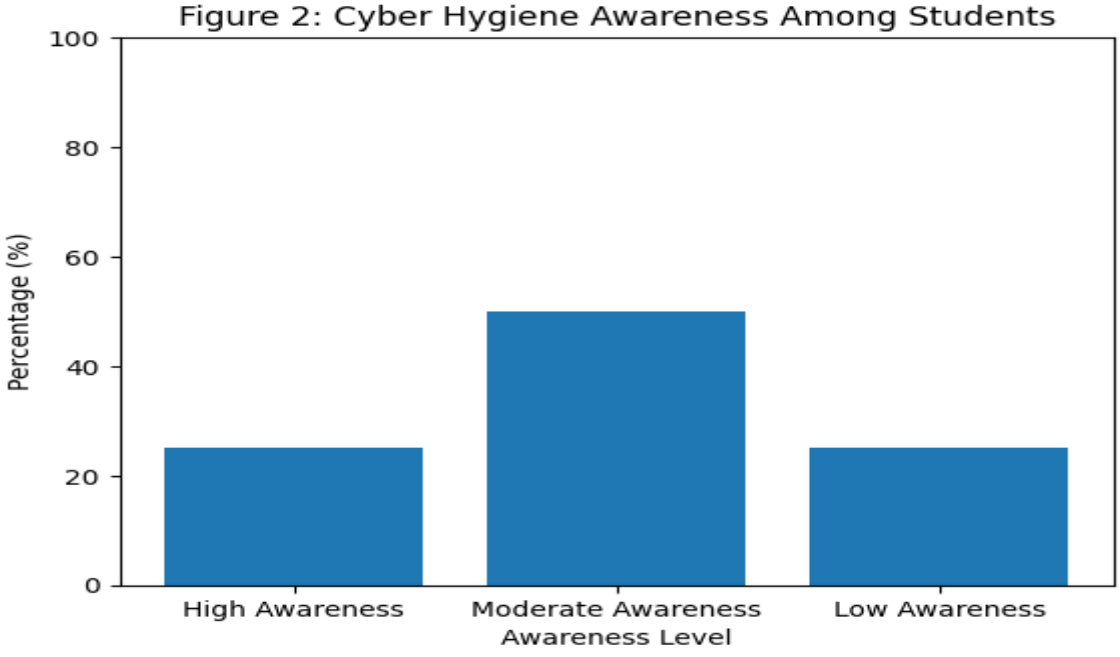
This distribution reflects a critical gap between **exposure to digital technologies and comprehension of associated risks**. While students are frequent users of digital payment systems, their awareness does not proportionately align with their usage intensity.

From an analytical perspective, moderate awareness may lead to **inconsistent security behaviour**, where users follow certain practices selectively rather than systematically. This partial awareness increases vulnerability, as cyber threats often exploit minor lapses in user behaviour.

Table 3 Cyber Safety Practices Followed by Students

Safety Practice	Students Following	Percentage
Strong Passwords	70	58%
Two-Factor Authentication	45	38%
Checking Payment Links	65	54%
Regular App Updates	50	42%

Figure 2: Cyber Hygiene Awareness Among Students



Interpretation

The findings indicate that while a majority of students adopt **basic cybersecurity measures**, the implementation of more advanced and effective practices remains limited. The relatively higher use of strong passwords and link verification suggests a **surface-level engagement with cybersecurity**, primarily driven by awareness of common threats.

However, the comparatively low adoption of two-factor authentication—one of the most effective security mechanisms—highlights a **significant behavioural gap between awareness and action**. This may be attributed to perceived inconvenience, lack of technical understanding, or underestimation of risk.

Similarly, the moderate level of regular application updates suggests that students may not fully recognize the importance of system maintenance in preventing vulnerabilities. This reflects a broader tendency among users to prioritize immediate usability over long-term security.

Overall, the data demonstrates that cybersecurity practices among students are **fragmented rather than comprehensive**, exposing them to potential financial and data-related risks.These graphs show that **digital payment usage is high among students, but cyber hygiene awareness is still developing**

6. Conclusion

The findings of the study clearly indicate that digital payment platforms have become an integral part of financial behaviour among college students, driven by convenience, accessibility, and technological familiarity. However, this widespread adoption is not adequately supported by a corresponding level of cyber hygiene awareness. A significant proportion of students demonstrate only moderate understanding of cybersecurity practices, and the inconsistent application of essential safety measures such as two-factor authentication and secure verification processes exposes them to potential cyber threats.

The study highlights a critical imbalance between technological usage and security preparedness, suggesting that increased digital participation does not automatically translate into safer online behaviour. This gap is largely influenced by behavioural factors, including limited risk perception and preference for convenience over security. In this context, cyber hygiene must be viewed not merely as a technical requirement but as a behavioural and educational necessity.

Therefore, it is essential for educational institutions and policymakers to integrate structured cybersecurity awareness programs and digital literacy initiatives into the academic environment. Strengthening cyber hygiene practices among students will not only reduce individual financial vulnerabilities but also contribute to the development of a more secure and resilient digital economy.

References

1. S. Von Solms and J. Van Niekerk, “From information security to cyber security,” Computers & Security, 2013.
2. N. Kshetri, “Cybercrime and cybersecurity in the global economy,” Telecommunications Policy, 2016.
3. L. Hadlington, “Human factors in cybersecurity,” Computers & Security, 2017.

4. M. Bada and J. Nurse, “Developing cybersecurity education,” IEEE Security & Privacy, 2019.
5. P. Gomber et al., “On the fintech revolution,” Journal of Management Information Systems, 2018.
6. R. Anderson, Security Engineering, Wiley, 2020.
7. M. Whitman and H. Mattord, Principles of Information Security, Cengage, 2021.
8. A. Mishra, “Digital payments in India,” International Journal of Finance, 2022.
9. S. Gupta, “Cyber security awareness among students,” Journal of Information Security, 2021.
10. World Bank, “Cybersecurity and the digital economy,” 2022.
11. V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, “User acceptance of information technology: Toward a unified view,” MIS Quarterly, 2003.
12. D. Kahneman, Thinking, Fast and Slow, Farrar, Straus and Giroux, 2011.
13. A. Acquisti, L. Brandimarte, and G. Loewenstein, “Privacy and human behavior in the age of information,” Science, vol. 347, no. 6221, pp. 509–514, 2015.
14. Reserve Bank of India, “Report on Trends and Progress of Banking in India,” RBI, 2023.
15. National Payments Corporation of India, “UPI Product Statistics,” NPCI Reports, 2023.
16. S. Sheng et al., “Anti-phishing Phil: The design and evaluation of a game that teaches people not to fall for phish,” Proceedings of SOUPS, 2007.
17. ENISA, “Cybersecurity Culture Guidelines,” ENISA Report, 2018.
18. IBM Security, “Cost of a Data Breach Report,” IBM, 2023.
19. KPMG, “India Fraud Survey Report,” KPMG India, 2022.
20. Deloitte, “Digital Banking Consumer Survey,” Deloitte Insights, 2023.
21. S. Furnell and K.-L. Thomson, “From culture to disobedience: Recognising the varying user acceptance of IT security,” Computer Fraud & Security, 2009.
22. J. R. Anderson and S. Agarwal, “Practicing safe computing: A multimedia empirical examination of home computer user security behavioral intentions,” MIS Quarterly, 2010.