|| Volume 9 || Issue 8|| August 2025 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

A STUDY ON USER AWARENESS AND THREAT PERCEPTION IN DIGITAL PAYMENT

Mrs. K. Balambal
Head, Department of Commerce & Management, Sri Sarada Niketan College of Science for Women, Karur -5.

Abstract: The increasing adoption of digital payment systems has brought convenience and speed to financial transactions, but it has also opened new avenues for cyber threats. From phishing attacks to data breaches, cybersecurity issues in digital transactions are a growing concern for users, businesses, and regulators alike. This paper investigates the level of cybersecurity awareness among digital payment users, particularly in semi-urban regions. Using primary survey data from users, the study examines user behavior, threat perception, and security practices. Findings suggest a considerable awareness gap and highlight the need for proactive user education, better platform-level security design, and regulatory enforcement to ensure safe digital payment ecosystems.

Keywords:*Cybersecurity, Digital Payment Systems, User Awareness, Online Threats, Data Protection, Safe Practices*

I.INTRODUCTION:

The digital transformation of the financial sector has led to widespread use of digital payments in both urban and rural areas. From Unified Payments Interface (UPI) to mobile wallets and internet banking, digital platforms have replaced cash-based transactions for many consumers. However, as the adoption of digital payments grows, so does the vulnerability to cyber threats. India's Digital India initiative has significantly accelerated the shift to digital finance. Yet, despite technological advances, the cybersecurity awareness of users remains limited. Phishing, identity theft, data breaches, and malware are just a few of the risks users face daily. This paper aims to evaluate how users perceive such risks and the measures they take to protect themselves during digital transactions.

II.REVIEW OF LITERATURE

Several researchers have emphasized the need for strengthening cybersecurity in digital finance. Rao (2023) found that users often overlook basic safety measures like password updates and website verification. Pavithra (2021) revealed a correlation between user trust and security features like biometric authentication.

A report by RBI (2022) notes that though banks comply with cybersecurity standards, customers are still vulnerable due to limited awareness. Another study by Kumar (2021) emphasized that digital payment apps must adopt user-friendly security designs to encourage safe practices. Together, these studies indicate that while technical solutions are improving, human factors like behavior and education are the key challenges.

USER AWARENESS IN DIGITAL PAYMENT SYSTEMS

User awareness refers to the understanding and attentiveness of digital payment users regarding the risks, safety practices, and proper usage of online financial transaction systems. In the context of digital payments, it includes knowledge of secure practices such as using strong passwords, enabling two-factor authentication (2FA), recognizing phishing attempts, updating software regularly, and avoiding unverified platforms.

Despite the rapid adoption of digital payment systems through UPI, mobile wallets, and internet banking, a large section of users-particularly in semi-urban and rural areas-exhibit limited awareness of cybersecurity threats. Many users are unaware of how cyberattacks occur or how to identify suspicious links, fake apps, or fraudulent messages.

Lack of user awareness contributes significantly to vulnerabilities, making individuals easy targets for cybercriminals. Studies have shown that even educated users often ignore or delay important safety measures such as password updates or app security settings (Rao, 2023). This gap between awareness and action indicates that digital literacy alone is insufficient unless it includes focused cybersecurity education.

Enhancing user awareness is crucial not only for individual safety but also for the integrity of the entire digital payment ecosystem. Financial institutions, app developers, and regulatory authorities must work collaboratively to conduct awareness campaigns, integrate safety tips within apps, and ensure that users are empowered to safeguard their digital transactions.

CYBERSECURITY THREATS

- There are a lot of cyber threats that an individual needs to know about to ignore the cyber threats. Cybercriminals could any one of them to trap a victim. We carefully need to know about such threats that are commonly known as malware, phishing, and email spamming.
- Malwares are the hidden and very dangerous malicious software that can cause severe damage to our system and could help criminals gain unauthorized access to our computer.
- Phishing is a huge cyber-attack in which our sensitive information such as passwords, credit card numbers, or personal data saved into our system is taken by the cyber criminals.
- Whereas in email spamming, a large amount of Spam emails that are of no use to us are often sent which contain misleading information and are sent to trap the user and steal their data.
- Cybercriminals is always looking for poor victims who they can trap easily. They always try to find new ways to break into an individual system and if they find a problem with software or the server, or old systems with known issues, they easily break into the system and steal the information. They look for weak passwords, Un updated apps, or old operating systems which help them to hack the system easily. People are tricked too because people aren't careful while checking their system.

- The cyber-attacks can be very dangerous if they steal our identity or we lose our money through fraud calls or if leaks our private information. It can cause huge problems like it can ruin our reputation or give us economic struggle or we get into serious legal trouble.

IMPORTANCE OF CYBERSECURITY IN DIGITAL PAYMENTS

1.Protect Sensitive Information:

The average financial services employee has access to 11 million files. Unfortunately, online transactions are vulnerable to hackers. They are highly motivated by money to obtain information, especially personal banking information. Vulnerable systems are at high risk, which can have catastrophic consequences for businesses and individuals. Cyber security for digital payments is critical to protecting sensitive information.

2.Fraud Prevention:

Money laundering, identity theft and fraud are common problems when shopping online. Using machine learning and fraud detection mechanisms, cyber security programs can analyze patterns of events to detect suspicious activity. This helps prevent theft/fraud in real time.

3.To Avoid Large Fines and Legal Consequences:

When shopping online, customers trust companies to keep their information (card/bank information) safe. All merchants must comply with payment industry requirements such as PCI DSS to ensure customer protection. If your business operates in the European Union, you must comply with the PSD2 Strong Customer Authentication (SCA) standard. Multi-factor authentication helps reduce theft or fraud. Ignoring these legal requirements as a business can put you at risk of:

- damages if necessary
- legal fees
- large fines from administrative authorities

4. Reduce Charges:

Most charges occur when the cardholder disputes a charge/transaction on their account They may not recognize the fee and consider it fraudulent, so they request a refund from their bank. This is especially common in online stores.

Secure payment gateways can help reduce fraudulent charges by verifying the cardholder's identity, saving you from financial losses and chargeback fees.

5. Positioning as a Global Company:

Cross-border regulations are not uniform. Different countries have different legal frameworks and security standards or regulations; which must be considered. By implementing secure payment gateways compatible with multiple countries, businesses can have a global audience.

6. Protect your Reputation: When Uber suffered a data breach in 2016, customer perception dropped 141%. Data breaches lead to customer distrust and negative publicity. The reputation of the brand guides the entire business. Business organizations sometimes spend millions of dollars building their brand image. When a single data breach can bring down the entire effort, you begin to understand the importance of cybersecurity across the entire payment infrastructure.

III.FINDINGS AND DISCUSSION

A significant number of users are aware of cyber risks associated with digital payments, the actual implementation of safe practices remains notably low. Among the various safety measures, biometric authentication emerged as the most commonly used, followed by regular password updates and the use of two-factor authentication (2FA). However, users generally show little initiative in verifying the security features of websites or mobile applications and rarely read platform security policies. Interestingly, the analysis indicated that educational background and occupation had no significant impact on users' cybersecurity behavior, suggesting that awareness and action do not always correlate with educational levels or professional fields. Furthermore, a common attitude observed among respondents is the expectation that digital platforms themselves are responsible for ensuring transaction security. As a result, many users fail to take personal responsibility for safeguarding their digital payment activities.

SUGGESTIONS

- To improve cybersecurity awareness and behavior:
- Financial institutions should conduct mandatory customer awareness campaigns.
- Mobile apps should integrate pop-up tips and security tutorials within their platforms.
- Regulatory bodies should mandate a baseline of security literacy for digital payment providers.
- Schools and colleges should include cybersecurity basics in digital literacy curricula.
- Cybersecurity updates and alerts should be more user-friendly and engaging.

IV.CONCLUSION

Digital payments have revolutionized how financial transactions occur, bringing convenience to millions. However, as users rely more on these platforms, they also expose themselves to cyber risks. This study revealed a considerable gap between user awareness and their actual behavior in protecting digital transactions. Bridging this gap requires a joint effort from government, financial institutions, app developers, and end users. Strengthening cybersecurity awareness through education, policy, and design can help build a safer, more inclusive digital economy.

V.REFERENCES

1. Pavithra B. (2021). Digital Banking and User Awareness. Turkish Journal of Computer and Mathematics Education.

2. Rao, P.B. (2023). Cybersecurity in Online Transactions. International Journal of Modern Computing.
3. RBI (2022). Annual Report on Digital Payment Security. Reserve Bank of India.
4. Kumar, M. (2021). A Study on E-Banking Risks and Customer Behavior. International Journal of Finance Research.
5. CERT-In (2023). Guidelines on Cybersecurity for Digital Payments. Government of India.