

Students' ECONOMIC FORUM

A monthly publication from South Indian Bank

*To kindle interest in economic affairs...
To empower the student community...*

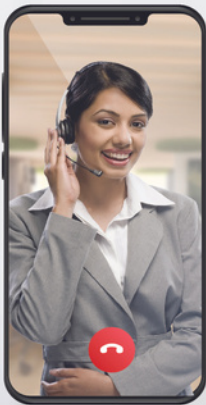
 www.southindianbank.com
Students' Corner

 ho2099@sib.co.in

PEER TO PEER (P2P) PAYMENTS



OPEN AN ACCOUNT ANYTIME, ANYWHERE IN JUST A FEW MINUTES!



Scan to Apply



With Video KYC
Account Opening



Banking simplified!



Aadhaar Card + PAN Card + Video Call
to open your Savings Account.



T&C apply

Peer to Peer (P2P) Payments

December 2023 | Theme 384

“Technologies that change society are technologies that change interactions between people”

– César A. Hidalgo

The 'SIB Students' Economic Forum' is designed to kindle interest in the minds of the younger generation. We highlight one theme in every monthly publication. Topics of discussion for this month is 'Peer to Peer (P2P) Payments'.

Definition:

Peer-to-Peer (P2P) payments refer to the direct transfer of funds between individuals. This means that people can send money to each other electronically, often using a mobile app or online platform, with the need for a Bank or other financial institution to facilitate the transaction. P2P payments leverage technology to enable users to transfer money seamlessly from one account to another.

How do they differ from traditional methods:

The key differences include:

Speed: P2P payments are often faster than traditional methods. While traditional bank transfers may take a few hours to process, P2P transactions can happen almost instantly, providing a quick and efficient way to send and receive money.

Convenience: P2P payments are highly convenient, as they can be initiated and completed through mobile apps or online platforms. Users can send money with just a few taps on their smartphones, making it easy to split bills, pay for services, or send funds to friends and family.

Lower Costs: P2P payments are often more cost-effective than traditional banking methods. Traditional financial institutions may charge fees for wire transfers or other services, and these costs can add up. P2P platforms, on the other hand, may have lower fees or even offer free transactions in certain cases.

Registration and Setup:

Setting up a P2P payment account involves a straightforward process that typically includes the following steps:

Download the App or Visit the Website:

Users need to download the P2P payment app from the relevant app store on their mobile devices or visit the platform's website.

Registration:

New users are required to register for an account. Mainly 2 types are available:

Bank's mobile/internet banking application for which each bank will have its own registration process.

UPI application - UPI is an interoperable system which allows customer to register/link the account in any UPI enabled application. Instead of using account number, UPI facilitated payment using UPI ID/ VPA.

Verification:

To ensure security and compliance, users may need to verify their identity. This can involve confirming details through email, phone, or additional identity verification steps.

Linking Bank Accounts or Cards:

To facilitate fund transfers, users typically link their P2P payment account to their bank account or credit/debit card. This step is crucial for both funding the P2P account and withdrawing funds.

Security Setup:

Users are often prompted to set up security features, such as PINs, Passwords, or Biometric authentication, to protect their accounts from unauthorized access.

Profile Setup:

Users may have the option to customize their profiles, add a profile picture, or include additional information.

Accepting Terms and Conditions:

Users are required to agree to the platform's terms and conditions, including any fees associated with transactions.

Once the registration and setup process is complete, users have a functioning P2P payment account ready to send and receive funds.

Fund Transfer:

After the setup, users can initiate fund transfers through the P2P payment platform:

Select Recipient:

Users choose the recipient from their contacts or enter the recipient's information, such as their VPA ID or phone number.

Enter Amount:

Users specify the amount they want to transfer. Some platforms allow users to include notes or descriptions for the transaction.

Choose Funding Source:

Users select the funding source for the transaction, which can be their linked bank account, credit card, or existing balance within the P2P payment account.

Initiate Transfer:

Users confirm the transaction details and initiate the fund transfer. The recipient is typically notified of the incoming payment.

Notification and Confirmation:

Both the sender and recipient receive notifications of the transaction. The recipient may need to accept the funds if it's their first time receiving a payment.

Funds Transfer:

The funds are transferred securely between the sender's and recipient's accounts. The transaction details are recorded in the transaction history. This streamlined process allows users to quickly and efficiently transfer funds to others, making P2P payments a convenient option for various financial transactions.



Security Measures:

Encryption:

Encryption is the process of converting sensitive data into a coded format to prevent unauthorized access. In the context of P2P payments, encryption protocols are implemented to safeguard users' financial information during transmission and storage.

Here's how encryption works:

Data Transmission Encryption:

When users initiate a fund transfer or perform any activity within the P2P payment app or platform, the data exchanged between their device and the platform's servers is encrypted. This is typically done using secure protocols such as SSL/TLS (Secure Socket Layer/Transport Layer Security).

End-to-End Encryption:

Some P2P payment platforms employ end-to-end encryption, ensuring that the information exchanged between the sender and the recipient is only accessible to them. Even the platform itself cannot decipher the content of the transaction.

Data Storage Encryption:

User data, including financial details and personal information, stored on servers is also encrypted. This adds an extra layer of protection in case of a security breach or unauthorized access to the platform's databases.

Tokenization:

In addition to encryption, tokenization is often used to enhance security. Tokenization replaces sensitive data (such as credit card numbers) with unique tokens, ensuring that even if the data is intercepted, it is meaningless without the corresponding tokenization system.

Regular Security Audits:

P2P payment platforms typically conduct regular security audits and assessments to identify and address potential vulnerabilities. This ongoing monitoring helps ensure that encryption protocols remain robust and effective.

Authentication:

Authentication involves verifying the identity of users to prevent unauthorized access. P2P payment platforms implement various authentication methods to ensure that only authorized users can initiate and receive payments:

Username and Password:

Users are required to create a unique username and password during the account setup. This basic form of authentication helps protect against unauthorized access.

Two-Factor Authentication (2FA):

Many P2P payment platforms offer 2FA as an additional layer of security. This often involves sending a one-time code to the user's registered mobile number or email address, which must be entered along with the password for account access.

Biometric Authentication:

Some platforms support biometric authentication methods such as fingerprint or facial recognition. This adds a higher level of security by tying access to unique physical characteristics.

Device Authentication:

Platforms may also track and authenticate devices used for accessing accounts. If a user attempts to log in from an unfamiliar device, additional verification steps may be required.

Risk-Based Authentication:

Advanced systems employ risk-based authentication, where the platform assesses the risk associated with a particular transaction or login attempt and adjusts the authentication requirements accordingly.

By implementing robust encryption and authentication measures, P2P payment platforms aim to create a secure environment for users, protecting their financial data and ensuring that only authorized individuals can access and transact within the platform.



Role of Mobile Apps in Facilitating Transactions On-the-Go:

Mobile apps play a crucial role in facilitating P2P transactions on-the-go. Users can initiate payments or request funds with just a few taps on their smartphones, providing a quick and efficient way to handle financial matters wherever they are.

The on-the-go nature of these apps is particularly beneficial for splitting bills, sharing expenses, or making spontaneous transactions without the need for physical cash or traditional banking methods.

User-Friendly Interfaces:

P2P payment apps prioritize user-friendly interfaces tailored for mobile devices. The design typically emphasizes simplicity, clear navigation, and accessibility, ensuring that users can easily understand and execute transactions without any technical barriers.

Real-Time Notifications:

Mobile apps enable real-time notifications, alerting users to incoming payments, completed transactions, and other relevant activities. This immediate feedback keeps users informed about their financial interactions and adds to the overall user experience.

Security Measures:

P2P payment apps implement security features specific to mobile devices, such as biometric authentication (fingerprint or facial recognition) and device-specific security measures. These measures enhance the security of transactions conducted on mobile platforms.

QR codes:

Quick Response codes provide a quick and efficient method for initiating payments. Each user is assigned a unique QR code linked to their P2P payment account.

To send money, users can simply scan the recipient's QR code using the camera on their mobile device. This eliminates the need to manually enter account details and streamlines the payment process.



User Tips and Best Practices for P2P Payments:

Secure Passwords:

Encourage users to create strong and unique passwords for their P2P payment accounts. Here are some tips:

Length and Complexity: Recommend passwords that are at least eight characters long and include a mix of uppercase and lowercase letters, numbers, and special symbols.

Avoid Common Words or Phrases:

Discourage the use of easily guessable passwords, such as birthdays, names, or common words.

Unique for Each Account: Emphasize the importance of using different passwords for different accounts to prevent a security breach on one platform from affecting others.

Two-Factor Authentication (2FA):

Advocate for the use of two-factor authentication to add an extra layer of security to P2P payment accounts.

Here's why 2FA is crucial:

Additional Verification: 2FA requires users to provide a second form of verification, typically a temporary code sent to their mobile device or email. This adds an extra step for account access, even if the password is compromised.

Enhanced Security: With 2FA, even if someone gains access to the user's password, they would still need the second factor (usually a device in the user's possession) to access the account.

Enable Biometric Authentication: If the P2P payment platform supports it, encourage users to enable biometric authentication (fingerprint or facial recognition) as one of the factors for added convenience and security.

Regular Password Updates:

Advise users to update their passwords regularly. Regularly changing passwords reduces the risk associated with potential breaches and unauthorized access.



Avoid Public Wi-Fi for Sensitive Transactions:

Caution users against conducting sensitive P2P transactions, such as transferring large sums of money, while connected to public Wi-Fi networks. Public Wi-Fi may not be as secure, and using it for financial transactions can expose users to potential risks.

Review Transaction History:

Encourage users to regularly review their transaction history within the P2P payment app. This helps them quickly identify any unauthorized or suspicious transactions and report them promptly.

Keep Apps Updated:

Remind users to keep their P2P payment apps updated to the latest version. App updates often include security patches and enhancements that protect against known vulnerabilities.

Enable Account Notifications:

Suggest users enable account notifications within the app. Real-time notifications for login attempts, transactions, and other account activities help users stay informed and detect any unusual or unauthorized access.

Use Official Apps:

Caution against downloading P2P payment apps from unofficial sources. Users should only download apps from official app stores to ensure they are using legitimate and secure versions of the application.

By following these user tips and best practices, individuals can enhance the security of their P2P payment accounts and reduce the risk of unauthorized access or fraudulent activities. It's crucial for users to take an active role in securing their accounts and adopting good cybersecurity habits.

Reference Links:

<https://www.nerdwallet.com/article/banking/p2p-payment-systems>
<https://www.nerdwallet.com/article/banking/peer-to-peer-p2p-money-transfers>
<https://www.investopedia.com/terms/p/peertopeer-p2p-service.asp>
<https://www.imf.org/en/Publications/fintech-notes/Issues/2023/06/16/The-Rise-of-Payment-and-Contracting-Platforms-534794>



SIB Mirror+



THE BANK ON YOUR PHONE, SIB MIRROR+



Available in 9 different languages



Instant payment to 100+ billers



Secure your account with e-Lock feature

Scan & download the SIB Mirror+ App Now!



T&C apply

UP TO **100% FINANCE**
ON YOUR CAR'S ON-ROAD PRICE



Scan to Apply



T&C apply

DRIVE YOUR DREAM CAR WITH SIB CAR LOAN



Tenure
up to 7 years



Loan for new and
used cars



Easy
documentation