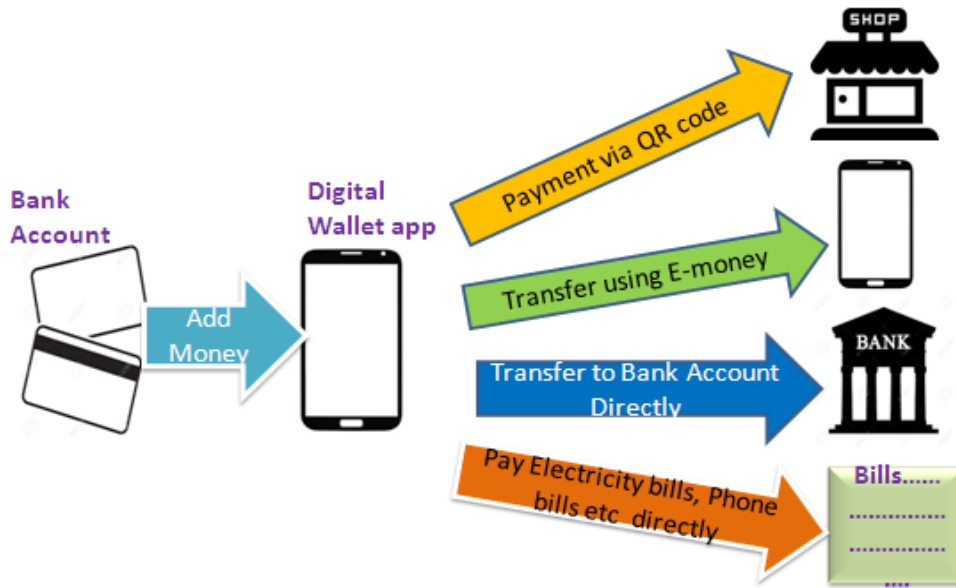




Protect Your Digital Wallets



Best Practices for Users to remain safe:

- **Keep Login Credential Secure:** Avoid writing down information used to access the digital wallets in plain view or storing them in an unprotected file to avoid their misuse.
- **Create a Unique Password for Digital Wallet:** Use hard-to-guess password unique to the digital wallet to prevent against the risk of unauthorized access.
- **Enable Passwords On Devices:** Strong passwords should be enabled on the user's phones, tablets, and other devices before e-wallets can be used.
- **Use Secure Network Connections:** It's important to be connected only to the trusted networks. Avoid the use of public Wi-Fi networks.
- **Install Apps From Trusted Sources:** The user must check for the e-wallet provider to be showing strong legacy of securely, reliably and conveniently handling sensitive financial data and providing customer support (in the event of card loss or account fraud).
- **Check Your Online Accounts Regularly:** Get monthly statements for your financial accounts and check each and every entry carefully to ensure no fraudulent transactions have been made without your knowledge.
- **Register your mobile number for Alerts through SMS and emails:** Register your mobile number for SMS and Email alerts from bank to get alert for every transaction.

Beware of the Fraudsters

Do not share confidential information like Internet banking login ID /Password /OTP /PIN /ATM-Debit /Credit Card Number / CVV/ Expiry Date to anyone. If you receive a mail or phone call asking for the same, be alert, as it is likely to be from a fraudster. **Bank or its employees will never ask for such confidential information through e-mail or over phone.**

GOOD PEOPLE TO GROW WITH

With warm regards,
Chief Information Security Officer
Indian Overseas Bank, Central Office, Chennai