



Safe Digital Banking Practises

- **Never share your account details such as account number, login ID, password, PIN, UPI-PIN, OTP, ATM /Debit card / credit card details with anyone**, not even with bank officials, however genuine they might sound.
 - Any phone call / email threatening the blocking of your account on the pretext of non-updation of KYC and suggestion to click link for updating the same is a common modus operandi of fraudsters. **Do not respond to offers for getting KYC updated / expedited. Always access the official website of your bank / NBFC / e-wallet provider or contact the branch.**
 - Always access the official website of bank / NBFC / e-wallet provider for contact details. **Contact numbers on internet search engines may be fraudulent.**
 - If you receive an OTP for debiting your account for a transaction not initiated by you, inform your bank / e-wallet provider immediately. If you receive a debit SMS for a transaction not done, inform your bank / e-wallet provider immediately and block all modes of debit, including UPI. If you suspect any fraudulent activity in your account, **check for any addition to the beneficiary list enabled for internet / mobile banking.**
 - Regularly check your email and phone messages for alerts from your financial service provider. **Report any unauthorized transaction observed to your bank / NBFC / Service provider** immediately for blocking the card / account / wallet, so as to prevent any further losses.
 - Secure your cards and set daily limit for transactions. You may also set limits and activate / deactivate for domestic / international use. **This can limit loss due to fraud.**
- 