

Safe Digital Banking Practices



1. DO NOT SHARE YOUR PERSONAL INFORMATION

Never share your account details such as account number, ATM PIN, CVV number, Expiry date, Mobile Banking Password, MPIN, TPIN UPI-PIN, and OTP.



2. DO NOT RESPOND TO ANY FAKE CALL OR ANY OFFER

Any phone call threatening the blocking of your account on the pretext of non- updating 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.



03.DON'T DO ANY SUSPIOUS TRANSACTIONS

If you receive an OTP for debiting your account for a transaction not initiated by you, inform your bank immediately. If you receive a debit SMS for a transaction not done, inform your bank immediately and block all modes of debit, including UPI.

04. SECURE YOUR TRANSACTIONS –

Secure your cards and set daily limit for transactions. You may also set ATM withdrawal transaction limit through Mobile Application.

05. SET STRONG PASSWORDS

Always set strong passwords for your Mobile devices.

06. Only download apps from official app stores like Play Store.

07. Never scan a QR code to receive money.

08...Avoid using public Wi-Fi networks for online banking transactions.

Disclaimer -The content of this document are meant merely for information purpose.The information contained herein is subject to updating, revision, verification and amendment.