

## SAFE DIGITAL BANKING PRACTICES

- Never share your account details such as account number, login ID, password, PIN, UPI-PIN, OTP, ATM / Debit 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 provider or contact the branch.
- Do not download any unknown app on your phone / device. The app may access your confidential data secretly.
- Always access the official website of bank provider for contact details. Contact numbers on internet search engines may be fraudulent.
- Check URLs and domain names received in emails / SMSs for spelling errors. Use only verified, secured, and trusted websites / apps for online banking, that is, websites starting with "https".
- If you receive an OTP for debiting your account for a transaction not initiated by you, inform bank immediately.
- Do not share the password of your email linked to your bank account. Do not have common passwords for e-commerce / social media sites and your bank account / email linked to your bank account. Avoid banking through public, open or free networks.
- Do not set your email password as the word "password" while registering in any website / application with your email as user-id. The password used for accessing your email, especially if linked with your account, should be unique and used only for email access and not for accessing any other website / application.
- Do not be misled by advices intimating deposit of money on your behalf with RBI for foreign remittances, receipt of commission, or wins of lottery.
- Regularly check your email and phone messages for alerts from your financial service provider. Report any un-authorized transaction observed to your bank immediately for blocking the card / account ,so as to prevent any further losses.