

# Good Practices For A Safe Digital Banking Experience

## DOs and DON'Ts

### ONLINE AND MOBILE BANKING

#### DOs



- Use only verified and trusted browsers and HTTPS secured websites for payments
- Ensure you change passwords frequently
- Always keep your payment applications updated with the latest version

#### DON'Ts



- Never store login credentials on phone, also don't enter credentials on untrusted kiosks
- Avoid transacting through public devices and on unsecure/open networks
- Refrain from sharing your mobile banking PIN or Internet Banking password with anyone, especially over phone

### UNIFIED PAYMENTS INTERFACE (UPI)/ BHIM

#### DOs



- Make sure you transfer money only to the intended beneficiaries
- Check the payment collect request details for correct beneficiary and amount before making the payment

#### DON'Ts



- Never share or write down your UPI PIN
- Refrain from transferring money without verifying the recipient first

### CREDIT AND DEBIT CARD

#### DOs



- Always keep an eye on your card during usage and promptly take it back
- Always check if there is any discrepancy between the transaction SMS details and actual transaction
- Ensure that you securely dispose of receipts and statements

#### DON'Ts



- Avoid sharing card details and PIN with anyone
- Do not leave your credit or debit card with anyone
- Do not share password/ OTP/ PIN with anyone

