PREVENTIVE MEASURES FOR BANKING FRAUD

ujjivan SMALL FINANCE BANK
A SCHEDULED COMMERCIAL BANK

ujjivan SMALL FINANCE BANK
A SCHEDULED COMMERCIAL BANK

PREVENTIVE MEASURES FOR BANKING FRAUD

ATM/POS

DO's

- Memorise your PIN. Do not keep your card and PIN together.
- Stand close to the ATM while entering your PIN in order to prevent onlookers or hidden cameras from capturing sensitive information.
- Periodically change your card PIN to reduce the risk of unauthorized access. Avoid using easily guessable PINs, such as birthdays or simple number sequences
- Keep your card in a secure wallet or cardholder and avoid leaving it unattended.
- Before entering PIN at any Point of Sale (POS) site or while using the card at an NFC reader, you must carefully check the amount displayed on the POS machine screen and NFC reader.
- Cover the keypad with your other hand while entering the PIN at a POS site/ATM.
- Avoid handover of your debit/ATM card to stranger and never share your debit card/ATM PIN to anyone.

DON'Ts

- Do not share your PIN or card with anyone.
- Do not take the help of strangers for using the card or handling cash.
- Never let the merchant take the card away from your sight for swiping while making a transaction.
- Never entertain and share the credentials of debit card, Aadhaar, PAN, customer ID if any unknown person visits your residence in the guise of employee of bank.

UPI

DO's

- REMEMBER that UPI PIN is not needed to receive UPI Payments.
- Always verify the identity of the person you are sending money to.
- Always verify the beneficiary details while making payment through QR Code.
- Change your UPI PIN regularly. Avoid using easily guessable PINs, such as birthdays or simple number sequences.
- Always remember to disable/delink your account from UPI application once you change your mobile number in your account.

DON'Ts

- Do not allow anyone to make UPI payments using your mobile.
- Do not accept random unknown collect request.
- Do not click/open on any random links.
- Avoid carrying out transactions while speaking with a third party on call.
- Do not share private information with anyone, particularly unknown persons on social media.
- Do not use same passwords for your email and internet banking.

ujjivan SMALL FINANCE BANK
A SCHEDULED COMMERCIAL BANK

IB/MB (IMPS/NEFT/RTGS)

DO's

- Beware of suspicious looking pop ups that appear during your browsing sessions on internet.
- Always verify security of any webpage (https:// - URL with a pad lock symbol), more so when an email or SMS link is redirected to such pages.
- Log out of the internet banking session immediately after usage.
- Update passwords on a periodic basis.
- Avoid visiting unsecured/unsafe/unknown websites.
- Avoid using/saving passwords on public devices.
- Avoid entering secure credentials on unknown websites/public devices/unknown Links.
- Please ensure to dial genuine toll-free number of the bank for any queries. Kindly verify the number when receive any call from toll-free number.
- Avoid using public terminals (viz. cyber cafe, etc.) for financial transactions.
- Always use secure downloaded app to access MB, do not download app from unsecure website/unknown source

DON'Ts

- Do not share private information with anyone, particularly unknown persons on social media.
- Do not use same passwords for your email and internet banking.
- Do not download unknown application on request of third party.
- Remote access/screen sharing apps can be used by fraudsters to gain access or view your screen so avoid using such Apps while making financial transactions.

ECOM

DO's

- Avoid sending card and account details through e-mail to prevent from malicious use by others.
- Please ensure to dial the genuine toll-free number of the bank for any queries. Cross check the number when you receive calls in the name of toll-free number.

DON'Ts

- Never share card details over phone or with anyone in person as it is an easier way for others to get access to your confidential card information and make the online transactions.
- Never forward any SMS on being asked by an unknown person posing as your bank or government official.

AEPS

DO's

- Always check transaction notifications immediately.
- Ensure the agent or merchant using the biometric device is authorized.
- Cover the fingerprint scanner during use to prevent unauthorized capture of fingerprints.
- Regularly monitor your bank account for unauthorized transactions.
- Report lost Aadhaar card or unauthorized transactions to your bank and the UIDAI helpline.

DON'Ts

- Don't share Aadhaar number, OTPs or bank details with anyone, including agents.
- Don't use AEPS services in unverified or suspicious locations.
- Never allow someone else to scan your fingerprint without your consent.