# Do's & Dont's

## Do's

1. Download Mobile Banking app only from trusted sources, such as link sent by bank or directly from bank's website or google paly store.
2. Password protect your mobile phone to prevent unauthorized use by others.
3. Install anti-virus software on your mobile device and update it regularly.
4. Enable automatic Mobile Operating System (Android) updates or download Mobile OS patch updates regularly to keep your Mobile OS patched against vulnerabilities.
5. Be careful and check authenticity of any app while downloading from app store of Google.
6. Always Log out of Mobile app after use.
7. Keep your login id and password information safe and secure.
8. Change your passwords regularly.
9. Use a password that is difficult to guess. Do not use sequences of numbers like 1234 etc. Don't use personal information like your date of birth, Car/Bike Nos. etc. as password. These are easy to crack or guess.
10. Clear data from your mobile browser cache and cookies frequently.
11. Register your mobile number with bank for receiving SMS Alerts on your mobile to keep track of your banking transactions.
12. Inform the bank to update your bank records whenever you change your Mobile number to ensure that OTP/SMS notifications are not sent to someone else.
13. Report a lost or stolen mobile immediately to your mobile service provider and law enforcement authorities. Block your mobile banking applications by contacting the bank.
14. If you suspect that someone knows your PIN/Password, change it immediately.
15. Regularly check your bank statements and transaction history for any irregularities.
16. Check your last login information displayed on screen upon every login to ascertain that there is no unauthorized login.
17. If you find your mobile number inactive, please contact your mobile service provider immediately to know the reason. Ensure that your number is not being used on duplicate SIM fraudulently.
18. If you have to share your mobile with someone else or send it for repair/maintenance, clear cache; temporary files and other sensitive information stored in the memory.
19. Fund Transfer can be made only to the pre added beneficiaries by the Customer. Delete those beneficiaries from your list, which are not required for further transactions.
20. Always type in your confidential account information. Do not copy paste it.

## Dont's

1. Don't download/install unauthorized or unofficial applications from app store displaying name similar to Panchsheel Bank. In case of suspicion, check app authenticity with the Bank before using them.
2. Never store your mobile banking user id and passwords(PIN), CIF in your mobile devices. Don't save confidential information such as your debit/credit card numbers, CVV numbers on your mobile phone.
3. Never share your personal information like Customer ID(CIF), passwords(PIN), OTP, details of Cards or bank accounts etc. over the phone, SMS or email with a stranger or any third party posing as representative of the bank, RBI, Income Tax department etc. Bank never asks for your confidential information via phone or email.
4. Don't add beneficiary without due validation of the beneficiary account details to avoid fund transfer to wrong beneficiary.
5. Don't send your password or PIN to anyone via text message or email.
6. Don't keep the same passwords for multiple accounts/applications.
7. Don't write down your passwords. Try to memorize it.
8. Don't say your password or PIN aloud as other people can hear you.
9. Don't follow the instructions as contained in SMS received from untrusted source.
10. Don't keep your mobile Bluetooth visibility turned on for everyone. Turn off mobile Wi-Fi and Bluetooth services when not required.