State Bank of India
(California)

Tips for Safer Mobile Banking

- Use your fingerprint, biometrics or a passcode on your phone to help safeguard your information in the event your device is lost or stolen.

- Make sure you do not share any passwords with anyone and for optimum mobile security, do not allow friends or family to enroll their fingerprint or other biometric authentication on your phone.

- Creating a strong password and changing them every 90 days is a good way to protect your device, the apps and tools that are housed in your device. Avoid using names or real words and if possible, create something memorable, but avoid using social security numbers, phone numbers or birthdates. Do not use your bank passwords for any other sites as fraudsters know people reuse their passwords. A strong password consists of 10 - 12 characters or more and should contain at least one uppercase letter, number and symbol.

- Turning on notifications and alerts is a good way in knowing of any suspicious activity or if there are any attempts in changing your personal information, such as phone numbers, address or ID.

- Make sure your device is set up for automatic updates in order to update your software timely. This is a crucial part of your mobile security. Updates include repairs to existing bugs and security issues in order for your devise to run smoothly and safely.

- Make sure the apps you download are from a trusted app store. The safest practice is to download apps from the official app store for your device. Make sure you are reviewing the apps permissions to find out what access you are granting the app.

- Avoid open or unknown Wi-Fi networks; you should never access your bank accounts through an open or unsecure Wi-Fi network.

- Be aware of shoulder surfers, this is the most basic form of identity theft.

- Wipe your device before you donate, sell or trade using specialized software or using the manufacturers recommended techniques.

- Be cautious when opening links and attachments in emails & texts, especially from senders you don’t know.

- Keep your financial institution informed, if you lose your device, change your phone number or if you suspect of any fraudulent activity in your account.
- WiFi, VPN, or Bluetooth should be turned off when not in use because this exposes your device to unwelcomed connections.