



STANDARD OPERATING PROCEDURE FOR DIGITAL BANKING

Awareness helps you
prevent security threats.

- Always use strong passwords and regularly change the passwords of your devices/online accounts. The same password should never be used at multiple sites.
- It is strongly recommended to enable multifactor authentication (like app based OTP, Digital certificate etc.) wherever possible in online accounts.
- Never open attachments in unsolicited emails, even if the email seems to be from your contacts. Never click on the URLs in those emails and be vigilant of suspicious attachments.
- It is recommended to install anti-virus in all devices and update it frequently, which will help reduce the gravity of online attacks.
- Operating systems and all applications should be regularly updated with the latest version.
- Secure your digital transactions using "e-Lock" feature in Bank's Mobile Banking App "SIB Mirror+".
- Users are advised to contact the Bank only through the toll free numbers available in Bank's official website (<https://www.southindianbank.com/>).
- Avoid applying updates / patches available from any unofficial channels.
- It is recommended that users download applications from legitimate stores that have security in place to minimize the chances of downloading malicious applications.
- Never Share any account credentials/Password/PIN/OTP/CVV etc. Bank will never ask for such details.
- In case of any suspected/unauthorized transaction in your account, please contact the Bank (1800 425 1809 or 1800 102 9408) immediately. For more details visit - <https://www.southindianbank.com/> or contact your nearest South Indian Bank Branch.

#SafeBankingWithSIB