

CYBER SECURITY



CYBER DOs

- Choose strong user IDs and passwords by choosing a combination of upper and lower-case letters, numbers and symbols that are difficult for hackers to guess.
- Change your password regularly.
- Use your own personal device (Mobile/computer/laptop/tab) to do financial transactions and email communication.
- Keep the software/antivirus of your device up to date. It protects you against threats.
- Keep your home/office Wi-Fi password secured. It protects your information/data.
- Keep your personal and financial information secret.
- Verify your statement of account for transactions. Call your branch in case you find any transaction suspicious.
- Take advantage of dual or multifactor authentication. Many Web sites now offer securities beyond just a username and password, such as a token, smartcard, PIN, or even user-selected security images that you will recognize upon login.

CYBER DON'Ts

- Never use your name, address, date of birth, social security, or common words as your password.
- Never write your password anywhere, memorize instead.
- Do not use the same password or PIN for several accounts.
- Never use a public device (computer/laptop/tab) available in cafes, public library, etc. to log in to your bank account.
- Never use free/open public Wi-Fi to do financial transactions. Hackers may access your personal/financial information.
- Never download unauthorized software/app. There may a malware/virus attached to it.
- Never open email attachments or click on links in unsolicited or suspicious looking emails. This can install a malware or lead you to a fictitious website designed to defraud you.
- Never disclose your credit card number, PIN or online banking password to anyone.



State Bank of India
(California)

