

BEWARE OF SIM SWAP FRAUD.

Outsmart the scamsters by being prudent.

SIM-SWAP Fraud is a new trick in the book of scamsters, where they get a new SIM card issued against your registered mobile number and get the OTP on their phones. Outsmart the scamsters by taking precautions.

- Please be vigilant on SIM deactivation as it may be an indication of SIM-SWAP (SIM cloning) Fraud. In case of any sudden/unauthorized SIM deactivation, please contact the bank (1800 425 1809 or 1800 102 9408) immediately.
- Always secure digital transactions using "e-lock" feature in the bank's Mobile App "SIB Mirror+". e-lock is enhanced to set a limit for digital channel transactions.
- Do not respond to communication asking to block your SIM.
- Do not share your mobile number on any Social Media Platforms.
- 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.
- Customers are advised to make payments using secured avenues such as Bank website, ATM display etc. while making payments through QR code.
- Customers are advised not to make payments through QR codes circulated through various Social Media, unknown sources/persons, email or displayed in prominent places as it can be easily tampered by fraudsters.

