Chola
Enter a better life

GENERAL PRECAUTIONS FOR FINANCIAL TRANSACTIONS

GENERAL PRECAUTIONS

- Beware of suspicious-looking pop-ups that appear during your internet browsing sessions.
- Always check for a secure payment gateway (https:// - URL with a padlock symbol) before making online payments or transactions.
- Keep your PIN (Personal Identification Number), password, credit/debit card number, CVV, etc., private. Do not share confidential financial information with banks, financial institutions, friends, or even family members.
- Avoid saving card details on websites, devices, or public laptops/desktops.
- Turn on two-factor authentication wherever available.
- Never open or respond to emails from unknown sources as they may contain suspicious attachments or phishing links.
- Do not share copies of cheque books or KYC documents with strangers.

FOR E-MAIL ACCOUNT SECURITY

- Do not click on links in emails from unknown senders.
- Avoid opening emails on public/free networks.
- Do not store credentials like bank passwords in emails.

FOR DEVICE / COMPUTER SECURITY

- Change passwords at regular intervals.
- Install antivirus software on your devices and update them regularly.
- Always scan unknown USB drives/devices before use.
- Do not leave your device unlocked.
- Configure auto-lock on the device after a specified time.
- Do not install unknown applications or software on your phone/laptop.
- Do not store passwords or confidential information on devices.

FACTORS INDICATING THAT A PHONE IS BEING SPIED

- Unfamiliar applications are being downloaded.
- Faster than usual battery drain.
- Phone turning hot may indicate spyware is running in the background.
- A sudden increase in data usage could be due to spyware running in the background.
- Spyware may interfere with the phone's shutdown process, delaying it.
- Text messages can be used by spyware to send and receive data.

FOR SAFE INTERNET BANKING

- Always use a virtual keyboard on public devices, as keystrokes can be captured through keyloggers.
- Log out of the internet banking session immediately after use.
- Update passwords periodically.
- Do not use the same password for both email and internet banking.
- Avoid using public terminals (eg: cyber cafes) for financial transactions.

FOR SAFE INTERNET BROWSING

- Change passwords at regular intervals.
- Install antivirus software and keep devices updated.
- Always scan unknown USB drives/devices before use.
- Do not leave your device unlocked.
- Configure auto-lock after a specified period.
- Do not install unknown apps or software on your devices.
- Do not store passwords or confidential info on devices.
- Do not share private information with anyone, especially unknown persons on social media.
- Always verify the security of any webpage (https:// - with a padlock symbol), especially when an email or SMS link redirects to such pages.

FOR PASSWORD SECURITY

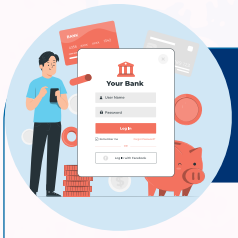
- Use a combination of letters, numbers, and special characters.
- Enable two-factor authentication wherever possible.
- Change passwords periodically.
- Avoid using personal info like date of birth, spouse's name, or vehicle numbers as passwords.

PRECAUTIONS RELATED TO DEBIT / CREDIT CARDS

- Deactivate various features of credit/debit cards like online, domestic, and international transactions if they are not needed.
- Disable Near Field Communication (NFC) features if not in use.
- Before entering your PIN at a POS or ATM, verify the transaction amount and the NFC reader.
- Do not let the merchant take the card out of your sight.
- Cover the keypad while entering the PIN.

ACTIONS TO BE TAKEN AFTER OCCURRENCE OF A FRAUD

- Block not just the debit/credit card but also freeze the bank account linked to the card by contacting your branch or customer care through official channels.
- Check and secure other banking channels like Net Banking and Mobile Banking to prevent further misuse.
- Report to the National Cybercrime Reporting Portal (www.cybercrime.gov.in) or call 155260/1930.
- Reset your mobile using the "Setting > Reset > Factory Data" option if a data leak is suspected.



HOW DO YOU KNOW WHETHER THE NBFC ACCEPTING DEPOSIT IS GENUINE OR NOT?

- Verify whether the NBFC is listed among deposit-taking NBFCs at https://rbi.org.in and ensure that it does appear on the prohibited list.
- NBFCs must display their Certificate of Registration (CoR) issued by RBI, which authorizes them to accept deposits.
- NBFCs cannot accept deposits for less than 12 months or more than 60 months. The maximum interest rate should not exceed 12.5%.
- RBI publishes updates on interest rates on its website under Sitemap/NBFC List/FAQs.

PRECAUTIONS TO BE TAKEN BY DEPOSITORS

- Insist on a proper receipt for each deposit made with the NBFC/company.
- The receipt must be signed by an authorized officer and include the date, depositor's name, amount (in words and figures), interest rate, maturity date, and amount.
- Verify if brokers/agents are authorized by the concerned NBFC before handing over public deposits.
- Note that Deposit Insurance is not available for NBFC deposits.