Dos and Don'ts for safe Banking

Simple precautions can help you to protect your accounts and losing your hard earned money. A small list of safeguards is provided below:

1. **General**
   - ✓ Inform your Branch
     - Of change in your Name/ Address/ Mobile number/Contact numbers/Email address/Nomination details etc
     - Of any discrepancy in your account statement/passbook. Check your statement/passbook regularly.
     - Of stolen or misplaced Demand Draft/Fixed Deposit Receipt/ Cheque Book/ATM Card/Internet Banking credentials/Locker key
     - Of suspected compromise of your internet banking credentials.
   - ✓ Operate your account frequently so that it is not misused. Further, it will also ensure that your account does not turn inactive / dormant.
   - ✓ Never respond to spam emails and be especially cautious of e-mails that:
     - ask for details of your Account /Internet banking/ ATM Card/ PINs or Passwords
     - Come from unrecognized senders
     - Try to upset you into acting quickly by threatening you with frightening information

     If you receive any such e-mail, kindly report to your Branch or mail at sibcorporate@sib.co.in or customercare@sib.co.in
   - ✓ Always keep your ATM card / cheque book / Passbook / Locker key etc in a safe place, under lock and key.
   - ✓ Register for SMS alerts to keep track of all your banking transactions.
   - ✓ Protect your computer and mobile device by installing effective anti-virus / anti-spyware and update the software regularly.
   - ✓ Always use Random and Alphanumeric passwords for Internet Banking/Verified by Visa and change them frequently.
   - ✓ Do not store your Passwords / PIN on your mobile device/Laptop/Wallet/paper etc
   - ✓ Grievance can be reported online only on the official website of South Indian Bank www.southindianbank.com

2. **ATM (Dos and Don'ts)**

   Dos

   On Receipt of Card and PIN Mailer
   - ✓ Sign on the strip on the back of your Card as soon as you receive it.
   - ✓ Destroy the PIN (Personal Identification Number) mailer communication after memorizing the PIN.
   - ✓ Memorize the three digit CVV Code on the back of the card and then scratch-off the CVV number carefully without damaging the magnetic strip or put an opaque sticker on it.
   - ✓ It is advisable to change PIN at the first instance itself. Preferably PIN should be changed frequently.

- ✓ Store the ATM-cum-debit card carefully in a secure place so that the magnetic stripe does not get damaged.

While Transacting

- ✓ Beware of shoulder surfing. Shield your PIN from onlookers. Once you complete your transaction, ensure that you have your card and your receipt and then leave.
- ✓ Look for extra devices attached to the ATMs. These may be put to capture your confidential data. Inform security / bank immediately if any such device found
- ✓ Do not use on ATM, which shows some misbehavior or certain keys of keypad are not working properly
- ✓ Bank will not fix camera in such an angle that PIN number could be captured, in case if you find, then don't use the ATM and kindly report it to the branch
- ✓ If you want to cancel the transaction at any point of time, use the Cancel button in the ATM Terminal and before leaving the ATM centre ensure that 'Welcome Screen' is displayed in the Screen.
- ✓ Ensure that the card is used in your presence at POS (Point of Sale) and mandatory PIN is being entered in POS machine by yourself.

General

- ✓ Immediately inform the Bank if the ATM -cum- Debit card is lost or stolen. Please call on the help line no. 91-484-3939345, 91-484-2771343 or 91-9446475458
- ✓ Register your mobile number with the bank for getting SMS alerts for your ATM transactions.
- ✓ Any unauthorized card transactions in the account, if observed, should be reported immediately to the Bank. This will help you if fraudulent withdrawal is being done by using your Debit Card
- ✓ Periodically verify the passbook entries to ensure its correctness. Any unauthorized card transaction, if observed, should be reported immediately to the Bank

Don'ts

- ✓ Never lend your card or reveal your PIN to anyone
- ✓ Do not write your PIN on the card.
- ✓ Do not record the PIN in any other media
- ✓ Do not allow the card to be taken out of your sight in a merchant location for POS (Point Of Sale) transaction.
- ✓ Do not use your mobile while using the ATM to avoid distraction
- ✓ Never use a PIN that could be easily guessed, e.g. your birthday or telephone number.
- ✓ Don't accept assistance from anyone or from the security guard when using an ATM
- ✓ Always prefer using cards only in websites which are certified by 'verified by Visa' / 'Master card secure code' while performing Online transactions
- ✓ Never perform online transactions using your ATM/Debit card from Cyber cafés and other public computers as there is a greater chance of your credentials being compromised. Hence, always access from your personal computer(s), In case if you have to transact from a public computer, then ensure that 3D-Secure password & ATM PIN are changed immediately from a secure computer system.
- ✓ Do not get distracted in any way while using the ATM.
- ✓ Bank will never ask for any details like debit card number, ATM PIN, CVV number printed on the reverse of the card etc. Therefore, never respond / reply to emails asking for such confidential information, even if it seems as having originated from the Bank.

3. Internet Banking (Dos and Don'ts)

Dos

Ensure Secure Access

- ✓ Use best practices for creating strong passwords (alphanumeric password that uses a combination of numbers, alphabets and Special characters) and change your passwords frequently.
- ✓ Please ensure safe banking through Internet. SIB Internet Banking is best accessed using Internet Explorer version 5.5 & above, Mozilla Firefox version 3.0 & above, Google chrome & Safari with a screen resolution 1024 by 768 pixels.
- ✓ Always type the address of the bank's website in the address bar of your browser. Make sure that the page accessed only through the website www.southindianbank.com
- ✓ Please note that the login page of Sibernet has a padlock image at the bottom. The URL (address) would be secured beginning with '*https://*' The details of the SSL server certificate can be viewed by clicking on the padlock image. The address bar of the browser should be turned green color and organization name 'South Indian Bank Ltd' with SSL pad lock is prominently displayed on the address bar.
- ✓ Use the virtual keyboard (VKB) wherever available to prevent key-logger compromises as such malware can track keystrokes in a physical keyboard.
- ✓ Check the date and time of your last login when logged in to Sibernet, to ensure there has been no compromises.
- ✓ Always clear your browser cache after each session
- ✓ Protect your computer by installing effective anti-virus / anti-spyware software on your computer / mobile devices and update it regularly.

General

- ✓ Register Application for "Two Factor Authentication" and protect your Internet Banking by using One Time Password (OTP) for all kind of SiberNet Transactions
- ✓ Never share / communicate / respond your Internet Banking credentials to anyone.
- ✓ Register for Mobile Banking and get updates for all kind of transaction / Suspicious operation happened in your account

Don'ts

- ✓ Do not store passwords in a file on any device (including mobile or similar devices) without encryption. Do not let your computer remember your password. Never accept auto complete option provided by your computer/ browser.
- ✓ Never fill in any forms that you have accessed via a link through, e-mail or from any source other than from the bank with sensitive data such as User-ID, Password, PINs, and other account related information.
- ✓ Never open/download any attachments if the mail is not from a trusted source
- ✓ Do not leave your internet banking session unattended. Always logout completely. Make sure that you have: a) Logged out the application by clicking on logout button. b) Closed all the browser windows
- ✓ Never access internet banking from Cyber cafés and other public computer .Always access SIBerNet using your personal computers, as it will reduce the chances of ID theft, Phishing etc. In case if you have to then ensure that passwords are changed immediately from personnel computer

- ✓ Bank never asks for confidential information like user ID, password, debit card number, CVV, etc, via mail, SMS or bank initiated phone calls.
- ✓ Do not provide any information on a pop-up window however officially looking or appealing it may be.
- ✓ Never note down user ID and password on a piece of paper, document or mobile devices for easy retrieval.
- ✓ Never download software or files from unknown sources to avoid becoming a victim of Phishing attacks.
- ✓ South Indian Bank Ltd or any other organization in that matter will never send e-mails, SMS or make calls asking for personal information like your bank account details, passwords, etc. Please do not respond in any manner to such communication, however official they may look.