Saraswat Bank | 100 Years Young

Saraswat Co-operative Bank Ltd.
(Scheduled Bank)

Precautionary measures while availing Digital Banking facilities

Online banking is safe and convenient as long as you take adequate and simple precautions. Please make sure you follow the advice given below:

i. Visit our secure Internet banking site directly. Avoid accessing the site through a link from another site or an e-mail and verify the domain name displayed to avoid spoof websites.
ii. Log out of Internet banking when your session is complete. Use the 'Log Out' button to log out so that the session closes. Do not just close the window to log off.
iii. Log off your PC when not in use.
iv. Avoid using Internet Banking on unsecured networks like airports, railway stations, cyber-cafes or any other public network / wi-fi, etc.
v. Update your computer / laptop with the latest version of your browser (Internet Explorer, Google Chrome, etc.)
vi. Install security programmes to protect against hackers, virus attacks or any malicious programmes. Update your security programme or antivirus on regular basis.
vii. Install a suitable firewall to protect your device / laptop / mobile, etc. and its contents from outsiders.
viii. Disable the 'File and Printing Sharing' feature on your operating system.
ix. Preferably use virtual keypad while conducting electronic financial transactions / internet banking.

Apart from your obligations when using Internet Banking, you will need to take additional care to protect your device when using a mobile application or any other form of social media to access banking services:

i. Do not leave your device unattended and logged into a Mobile Banking service
ii. Lock your device to prevent unauthorised use of your Mobile Banking service
iii. Notify us as soon as possible if your device is lost or stolen
iv. Update your Mobile Banking App as and when a new version / upgrade is released.
v. Update your mobile operating system to ensure that the latest security patches are available on your mobile.
vi. Purchase your mobile phone from an authorized dealer.
vii. Ensure to check the authenticity of all Apps downloaded on your mobile. Do not download Apps from untrusted sources.

Log out of Mobile Banking application once you are done using it. Check your account and transaction history regularly.

Do not share your internet / Mobile Banking security information or disclose your password as response to any e-mail (even if it appears to have been sent from our bank). Please inform us of the same for us to investigate. Neither the police nor we will ever contact you to ask you to reveal your online banking or payment card PINs, or your password information.

For creating PIN / Password:

a. Use the following guidelines to create a strong password:

• Do not use familiar names which are easily discoverable (self, spouse, children, parents, pets, etc.)

• Avoid using commonly known facts about yourself (hobbies, birthdays, favourite sports, etc.)

• Do not use words found in the dictionary as software programmes can search for probable words and guess the password. Instead combine misspelt words to prevent a dictionary attack

• Use at least six or more characters. More the characters in a password, the more secure it is

• Utilize a combination of letters and numbers to make it more difficult for a person / software programme to guess your password

• Use special characters (@, #, %, $, etc.) to make the password more difficult to crack

• Use a combination of upper- and lower-case letters which helps to create a more secure password b.

b. Do not use the following to create a *PIN:

• birth dates, months or years;

• sequential numbers (e.g. 3456);

• number combinations that may be easily guessed (e.g. 1111);

• parts of your telephone number;

• parts of numbers in the order in which they are printed on any of your cards;

• other easily accessible personal data (e.g. driving licence, your vehicle number or other numbers easily connected with you)

*This is only an illustrative and not exhaustive list.

Precautions for preventing unauthorised transactions in your account:

Do not:

• Allow anyone else to use your card, PIN, password or other security information.

• Write down or record your PIN, password or other security information.

• Store your password(s) in your Browsers (such as Internet Explorer, Google Chrome, Firefox, etc.) or on e-Commerce sites or in mobile handset.

• Save your Mobile Banking Login and password on your phone

• Give your account details, password / PIN / OTP or other security information to anyone, including those who claim to be authorized representatives of the bank.

• Respond to any communication asking for your Bank account credentials (Internet banking password, ATM PIN, CVV, Card expiry date, etc.)

• Respond even if any message threatens discontinuation of facility or makes an exciting offer or mentions any other reason. All such communication through letters, e-mails, mobile phones, SMSs, etc. should be ignored.

• Fall prey to fictitious offers / lottery winnings / remittance of cheap funds in foreign currency from abroad by certain foreign entities / individuals. These could include Indian residents acting as representatives of such entities / individuals. These messages often appear to be from a friend, bank or other legitimate source directing you to certain websites designed to trick you into providing personal information such as your user name and password or credit card information.

• Click a link in any suspicious e-mails / SMS, and don’t provide Code of Bank’s Commitment to Customers – January 2018 your information unless you trust the source e-mail / SMS.

• Allow anyone else to see you enter your Password in a PC / mobile handset or to see the PIN when you use your card at ATMs or at Points of Sale (POS) counters.

Always:

• Change your PIN / Password at regular intervals – at least every 3 to 6 months. Do not repeat your previous passwords.

• Memorize your PIN, password and other security information and destroy the written communication, if any, received by you.

• Take reasonable steps to keep your card safe in your personal custody and your PIN, password and other security information secret at all times.

• Use different PINs or Passwords for different cards or devices

• Use a power-on / access password for your computer / laptop / mobile and a screensaver password on your computer / laptop / mobile so that no one else can use it without your consent. Immediately inform (through authorized officials of bank or authorized channel) your bank on change of your e-mail ID or mobile number.

Please safeguard your card by taking the following measures:

• Sign your card as soon as you receive it

• Do not leave your card unattended (in a wallet / purse) or in a location (e.g. your vehicle) from where it could be removed without being noticed

• Do not give your card to anyone or let anyone else use your card including at merchant establishments (e.g. restaurants, petrol pump, etc.)

• Always remember to take your card back after using it

• Inform us if you change your address with documentary proof so that, whenever required, a replacement card is sent to your correct address.

• Complaints relating to disputed / failed ATM transactions are to be lodged with card issuing bank (through authorized officials or channel).