SBI (Canada) Internet Banking Security

SBI (Canada) allows you to transact, through Internet, over a completely secure medium, protected by the most stringent security systems. All your transactions travel via an SSL encrypted medium (128-bit SSL tunnel).

SSL Certificates provide you the evidence of the server's authenticity which safeguards users from trusting unauthorized sites and allows the session to be encrypted.

- This is provided by a World's leading Internet Certification Authority, which in this case is, VeriSign
- Look for the padlock symbol either in the address bar or the status bar (mostly in the address bar) but not within the web page display area. Verify the security certificate by clicking on the padlock.
- Clicking on the lock will allow you to see the VeriSign Certificate authenticating the site.
- While we are taking measures to make sure your online transactions are secure, you could also do a few things to ensure the security of your transactions.

Each customer is provided with a User ID and Password. Your password is generated in such a way that it is only known to you. In addition, we guard against unauthorized entry/viewing in the following ways:

- To prevent somebody from guessing your password and getting unauthorized access to your account, your User ID is locked immediately in case of three consecutive wrong password entries.
- To prevent an unauthorized person from viewing your Net Banking account in case you leave your computer idle, we close your Internet session in case of inactivity for an extended period of time.

IMPORTANT SECURITY TIPS FOR SAFE ONLINE BANKING

- ✓ Access your bank website only by typing the URL in the address bar of your browser.
- ✓ Please ensure that URL address begins with https, the letter ‘s’ at the end of ‘https’ means ‘secured’.
- ✓ Look for the padlock symbol either in the address bar or the status bar (mostly in the address bar) but not within the web page display area Verify the security certificate by clicking on the padlock

- ✓ Do not enter login or other sensitive information in any pop up window
- ✓ Do not click on any links in any e-mail message to access the site.

Beware of Phishing attacks

- ✓ Phishing is a fraudulent attempt, usually made through email, phone calls, SMS etc seeking your personal and confidential information

- ✓ SBI (Canada) or any of its representative never sends you email/SMS or calls you over phone to get your personal information, password. Any such email/SMS or phone call is an attempt to fraudulently withdraw money from your account through Internet Banking. Never respond to such email/SMS or phone call. Please report immediately on report.phishing@sbi.co.in if you receive any such e-mail/SMS or Phone call. Immediately change your passwords if you have accidentally revealed your credentials.

- ✓ Do not be lured if you receive an e-mail/SMS/phone call promising reward for providing your personal information or for updating your account details in the bank site.

- ✓ Having the following will improve your internet security:
  - o Newer version of Operating System with latest security patches.
  - o Latest version of Browsers (IE 7.0 and above)
  - o Firewall is enabled.
  - o Antivirus signatures applied

- ✓ Scan your computer regularly with Antivirus to ensure that the system is Virus/Trojan free.

- ✓ Change your Internet Banking password at periodical intervals.

- ✓ Always check the last log-in date and time in the post login page.

- ✓ Avoid accessing Internet banking accounts from cyber cafes or shared PCs.