Awareness of Cybersecurity Risks

Privacy, Security Precautions & Good Practices

Bank of India, Singapore (BOIS) is committed to maintain good practices on Customer Privacy & Security Precautions as far as possible to create and maintain a secure environment for its customers. BOIS encourages its customers to similarly observe best practices that are within their control.

Best Practices of the Bank:

- **Collection Of Customer Information** – We will not make unsolicited requests for customer information through email or the telephone, unless customers initiate contact with us. We will use information collected as minimally as possible, mainly to assist us in customizing / delivering services and products that are of interest / useful to our customers. Under no circumstances we ask customers to reveal their Personal Identification Numbers (PINs) or Passwords.
- **Handling of Customer Information**- We have established strict confidentiality standards for safeguarding information of our customers.
- **Disclosure Of Customer Information** - Unless we have the customer's agreement or are required by law, we will not disclose customer information to external parties.
- **Compliance By External Parties** - External parties, who, in the course of providing support services to us, may come into contact with customer information, are required to observe our security and privacy standards.

Best Practices of the Customers:

- **Customers Role in Safeguarding their Personal Data and Account Information** - The customer is responsible for keeping the Internet Banking Password & One-Time Password of 2FA confidential. Failure to do so will expose the customer to risks i.e. like leakage of account details. BOIS will not be responsible for losses suffered by customers as a result of:
  - ✓ Misuse of its Internet Banking services;
  - ✓ Negligent handling or sharing of Passwords;
  - ✓ Leaving a computer unattended during an online session;
  - ✓ Failure to immediately report known incidents of unauthorized account access.

- If you receive an e-mail claiming to be from Bank of India regarding updating sensitive account information, please do not share and let us know by forwarding the e-mail to boi.singapore@bankofindia.co.in or contact us at +65-62220011.

IMPORTANT: *If you have apprehension that someone else has come to know sensitive information of your account or any other personal information, please inform us immediately.*

Using Strong Passwords:

- Password should be at least 8 letters with combination of letters (a to z), numbers (0 to 9) and special characters ($, #, * etc.), (1 Alphabet Lower case or Upper case) without repeating any digit or character more than once.
- Password should not contain special characters like < > ? \ & = ‘ |
- Password should not be based on User IDs, Personal Telephone Number, Birthday or other personal information.
- Passwords must be kept confidential and not be divulged to anyone and recorded anywhere.

- Password should be changed regularly or when there is any suspicion that is has been compromised or impaired.
- The same Password should not be used for different websites, applications or services, particularly when they relate to different entities.
- Customer should not select the browser option for storing or retaining user name and password.
- Customer should not share the Used-ID, Password and Star-Token PIN.

Confirming the Website address of the Bank:

- The first Login to Internet Banking application in a new PC/Laptop is to be done only through the Homepage of our Website.
- Login to the Homepage at http://www.boi.com.sg and then choose << Internet Banking >>. It opens in a separate POP-UP frame get Star-token installed which will create an icon on your system desktop.
- At all other times Internet Banking Login to be done only through Star-Token icon created (during the first Login on any new system) by the system on the Desktop of your system.
- Before inputting your password in the window of IB screen, make sure that 128-bit encryption seal (VeriSign) on the Right-End Corner of the page.

Use Secured computer:

- Do not use a computer or a device, which cannot be trusted.
- Install anti-virus, anti-spyware and firewall software, particularly when they are linked via broadband connections, digital subscriber lines or cable modems. Update anti-virus and firewall products with security patches or newer versions on a regular basis.
- Computers should be regularly scanned to protect your systems from spyware, keystroke loggers, viruses, worms and other Trojans by using the updated anti-spyware / anti-virus software and firewalls.
- Please clear browser cache after online session and log-off the online session and turn off the computer when not in use.
- Remove file and printer sharing in your computers, especially when they have internet access via cable modems, broadband connections or similar set-ups.
- Consider using encryption to protect highly sensitive or confidential information.
- Do not install software or run programs of unknown origin.

Beware of Fraudulent / Phishing E-mails.

- Beware of Phishing attacks - There could be fraudulent mails going out to customers of various Banks luring them to update sensitive account information like User IDs, Passwords, even transaction Passwords, etc., by clicking on an e-mail link or visiting a website. Kindly do not respond to such Phished emails, as our Bank does not send such e-mails.
- Delete junk or chain emails.
- Do not open email attachments from strangers.
- Do not disclose personal, financial or credit card information to little-known or suspect websites.

****