Awareness of Cyber Security 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 12 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 OTP.

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 https://www.boi.com.sg and then choose << Internet Banking >>.
- Before inputting your password in the window of Internet Banking screen, make sure it is SSL enabled.

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.

Phishing Attacks

Key takeaways

a. What is phishing and how to protect yourself?

- Phishing attacks are used by cyber criminals to fraudulently obtain personal information and credentials. Typically, a user is tricked into believing the authenticity of an email or a SMS, and tricked into clicking on a malicious Uniform Resource Locator (“URL”) link.
- When the user clicks on the URL link, he/she will be directed to a fraudulent website requesting for personal information such as credit card numbers or user credentials (e.g., user account, PIN, One-Time-Password). With these stolen credentials, fraudsters would attempt to access the user’s online accounts to perform unauthorized transactions.
- 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.
- In recent cases of SMS phishing attacks, the fraudsters target victims with text message scam sent via an alphanumeric sender ID ("alpha tag") to masquerade as an FI. Alpha tags, which can include digits, text, and special characters, are used to give a 'sender' name to the SMS messages. By spoofing the SMS alpha tag, the SMS appears more legitimate, making detection difficult.

b. Be alert to phishing attempts. Note that your bank will not ask you for your personal details over emails.

c. Do not click on any link or open attachments in suspicious emails that appear to be from your bank.

d. Fraudsters would post fake advertisements or phishing web links on search sites so that they would appear when victims searched for a specific Banks' / Financial Institutions' (FIs') contact numbers or websites. Believing that the search results are legitimate, victims would call the number shown in the fake advertisements and speak to a fraudster impersonating as Bank / FI staff, where victims would be social engineered into performing fund transfer to the fraudster's account. Victims could also be led to a phishing website and divulge their online financial services credentials, setting the stage for fraudulent activities.

e. If you think you have become a victim of phishing, contact your Bank / Financial Institutional immediately.

How to avoid phishing attacks

Phishing (pronounced as "fishing") is a common technique used by criminals to trick you into giving away your personal information. They could do this by using emails, SMS, or phone calls.

If you fall prey to phishing and have given your personal information and online banking credentials, criminals may use the information to access your online banking accounts and transfer money out of your bank accounts.

Beware of bogus emails or SMS

You may receive a fake email or SMS that looks like it is sent from your bank to trick you into believing that the email or SMS is authentic. The email or SMS typically contain alarming messages so that you will take notice, such as informing you that your online account has been hacked or regulatory bodies suspect that your account is used for money laundering. You will typically be asked to click on a link to verify your account. The URL will then bring you to a fake website that looks exactly like your bank's login page. The criminals will be able to steal your login username, login passwords, and OTP when you key in these details into the fake website.

With your stolen credentials, the criminals will be able to access your online banking accounts and perform unauthorized transactions on them.

To protect yourself from falling prey to phishing, remember the following:

- Never give out your personal details by email.
- Your bank will NEVER send you emails or SMS asking you for your personal information.
- Do not open attachments or click on any link in suspicious emails or SMS.
- Always enter the full URL or domain name of your bank on your browser address bar.
- Install firewall, and anti-virus and anti-spyware in your computer. Update them regularly.
- Avoid online banking in public areas such as cyber-cafes.
- Log off each time you complete online banking activities.
- Select passwords that are difficult to guess. Change them often.
- If you think you have become a victim of phishing, contact your bank immediately.

Beware of bogus phone calls

Criminals may also call and trick you into believing that they are bank officers, government officials or the police. The caller ID on your mobile phone may even appear as “999”. Criminals typically use scare tactics to threaten you and make you believe that you have committed a crime.

Criminals may then ask you to give them your online banking credentials so that they can “check” your online accounts. If you do so, the criminals will be able to login to your online banking accounts and wipe out all the money in your bank accounts.

Here are some tips to protect yourself from bogus phone calls. Always keep the following in mind:

Government officials or Bank Officers will NEVER call you to ask you for your personal information, such as your online banking credentials.

- When in doubt, always hang up the phone.

- If the caller ID displays “999” or any “Emergency Telephone Number” based on the country of location, hang up and call or visit your nearest police post to verify the authenticity of the call.

Business Email Compromise (“BEC”) Scams

- In BEC scams, fraudsters typically study the profile of the target company to understand the management structure, payment process and the employees involved.

- The fraudsters would usually employ social engineering techniques and other cyberattacks such as installing malware to compromise and infiltrate the company’s system and endpoint devices. After gaining access to the Senior Management email account, the fraudster would study his/her day-to-day activities and interactions. Next, the fraudster would use the compromised email account or a “look-alike” email account to send an email to trick the company’s employee, customer or business partner to make a payment to rogue accounts or a purchase of gift card/voucher. A common tactic is to imitate the manner in which the Senior Management sends payment instructions or reply to an on-going email conversation to make the request appear credible.

The following measures to be taken as a safeguards against these scams:

a. Implement strong access controls (e.g. strong password controls, multi-factor authentication) on email accounts of users with payment authority;

b. Establish a robust process and controls to verify the authenticity of a payment request or change of payment accounts to a new party;

c. Protect internal company knowledge that could be exploited by fraudsters such as individual contact who has the authority to request payments; and

d. Conduct regular security awareness programmes to educate their staff and customers on steps to protect themselves from such fraud or scam.

Data Synchronization of Mobile Devices

- Some smart phones have features that allow data synchronization between the mobile device and online storage or cloud services in near real time. Information that could be synchronized includes SMS, email, etc.

- For smart phone users who had / have enabled the abovementioned data synchronization, sensitive information sent via SMS or emails by Financial Institutions (FIs), such as one-time passwords (OTPs), could be accessed by criminals if their login credentials to the online storage or cloud services have been compromised. Exposed OTPs together with online banking credentials or credit card information that had been harvested from the customers can potentially be used by criminals to perform fraudulent financial transactions.

- Please be advised of such cyber risks and the need to secure your mobile devices and related Online accounts.

Rising Trend in Mobile Malware

There are domestic scams that involved the use of malicious Android malware to perform fraudulent transactions through banking application/s. The malwares available on GitHub and is notable for its plug-and-play functionality, allowing it to be easily deployed by scammers with minimal IT knowledge.

For your own security, please be advised to perform the necessary actions:

- Only download and install applications from the official application stores (i.e., Google Play Store for Android & Apple Store for iOS). As an added precaution, check the developer information on the application listing, as well as the number of downloads and user reviews to ensure it is a reputable and legitimate application.

- Disable the option to “Install Unknown App” or “Unknown Sources” in the mobile settings.

- Exercise caution when clicking on advertisements embedded within applications that lead to third-party website prompting files downloads.

- Do not grant permission to persistent pop-ups that request for access to your device’s hardware or data.

- Ensure that mobile devices are installed with updated anti-virus/anti-malware applications that can detect and remove malware.

- Regularly update the mobile devices’ operating systems and applications to benefit from the latest security patches.

****