MBSB
BANK

Security Alert

Dear Customers of MBSB Bank, we are dedicated in providing you with a secured online banking service. We would advise you to be very vigilant in protecting your computers and mobile devices from malwares and viruses when you perform internet banking activities. You should be directly logged into MBSB Bank's website and only begin your transaction after you see your chosen security icon and phrase.

If you are in doubt, do not hesitate to contact us through our customer service hotline immediately at 03-20963000.

4 Most Common Types of e-Banking Scams

E-mail Scams

An e-mail scam, widely known as 'phishing' is an e-mail scam involving a fraudster randomly sending forged e-mails. Purportedly from financial institutions or publicly known organisations to lure victims into revealing their internet banking login credentials, these e-mails are then used to perform transactions by asking e-mail credentials, credit card numbers, bank account numbers and/or passwords.

These e-mails are designed to appear legitimate to gain the trust of the recipient. The content of the e-mail typically attempts to inflict a sense of urgency and panic in order to trick customers into revealing confidential information on a fake website/popup.

Phone Scams ("Macau" Scams)

In such cases, the fraudster usually attempts to obtain sensitive information over a voice call. The fraudster normally tries to gain the victim's trust by impersonating a credible individual such as a banking authority or a police investigation officer. Victims may not verify the received calls made by such purported persons thinking that the calls are from regulators so called, to avoid embarrassment or as a result of "warnings" given by the "officer".

SMS Scams

An SMS scam usually involves SMS-es initiated by a fraudster to trick victims into believing that they have won a contest/reward and which attempt to lead them into compromising their banking information and/or create an internet banking facility without the victim even realising it.

This type of scam may also involve 'identity theft' since an unauthorised person usually pretends to be a valid account holder and access the customer's account (usually through the internet), unknown by the account holder.

Malware and Ransomware Scams

Malware and ransomware scams, involve a scammer trying to infect a victim's device either with malware or ransomware. The scammer will use plenty of means to deceive the victim into clicking on an infected link or opening/downloading a malicious attachment/product, from setting up fake websites to sending fake emails to the victim.

Essentially, infect a victim's device and steal personal, company, or financial info off of it, like login credentials, credit card info, employee data, and various passwords, for example. The scammer can then use the info to steal money from the victim, or just expose them to identity theft.

ATM, CDM and CRM Security Tips

Check for anything unusual at or around ATMs, CDMs and CRMs and card reader slot before inserting your card

- Always be aware of your surroundings when using ATMs, CDMs and CRMs
- Always cover the keypad when entering your PIN
- Create PINs that cannot be easily guessed by anyone. Avoid including the following items in your PIN:
    - Simple number sequences like 1234 or 0000 (including repetition: 1122 or 2233)
    - Significant dates, such as your birth year or spouse's birthday
    - Any part of your Identity Card number , Passport number or Driving License number
    - Any part of your address or phone number
- Check your accounts regularly for any unusual transactions

10 Banking Security Tips to Protect Yourself

- Always ensure the MBSB Bank Internet Banking URL is 'https://www.mbsbjourney.com/rib/' for individual or 'https://www.mbsbjourney.com/corporate/' corporate. Never access MBSB Bank Internet Banking from attachments or websites links or in any e-mails.
- Your security image must always be displayed when logging onto MBSB Bank Internet Banking
- Never share your user ID and password with anyone including your immediate family member i.e. spouse, children etc.

- Change your password immediately if you suspect it is known to a 3rd party.
- Always access your online banking account from a secured location.
- Do not perform any internet banking transactions using public computer / WiFi.
- Ensure that you have installed internet security. For example, anti-virus / anti-malware software on your computing devices for added protection.
- Do not use "jailbroken" or "rooted" devices for online banking. “Jailbreaking” or “rooting” a device exposes the device to additional malware.
- Always clear your browser cache when you log out of MBSB Bank Internet Banking as they may contain your account numbers and other sensitive information.
- Always check your account after making any transaction online. Verify whether the right amount has been deducted from your account. If you see any discrepancies in the amount, inform the bank immediately.
- Always ensure the TAC SMS you receive matches your request while performing MBSB Bank Internet Banking online transaction for individual.

Steps to clear browser cache

Mobile browsers

Android

The steps to clear your cache, cookies, and history may differ depending on the model of your Android device and your preferred browser. However, you should be able to clear your cache and data from your application management settings menu:

1. Go to Settings and choose Apps or Application Manager.
2. Swipe to the All tab.
3. In the list of installed apps, find and tap your web browser. Tap Clear Data and then Clear Cache.
4. Exit/quit all browser windows and re-open the browser.

Chrome for Android

1. Tap Chrome menu > Settings.
2. Tap (Advanced) Privacy.
3. From the "Time Range" drop-down menu, select All Time.
4. Check Cookies and Site data and Cached Images and Files.
5. Tap Clear data.
6. Exit/quit all browser windows and re-open the browser.

Safari for iOS

1. Open your Settings app.
2. Tap Safari.
3. Tap Clear History and Website Data and confirm.
4. Exit/quit all browser windows and re-open the browser.

Chrome for iOS

1. Tap Chrome menu > Settings.
2. Tap Privacy.
3. Tap Clear Browsing Data.
4. Choose the data type you want to clear.
5. Tap Clear Browsing Data.
6. Exit/quit all browser windows and re-open the browser.

Desktop browsers

Chrome

1. In the browser bar, enter:

   ```
   chrome://settings/clearBrowserData
   ```

2. At the top of the "Clear browsing data" window, click Advanced.
3. Select the following:
   - Browsing history
   - Download history
   - Cookies and other site data
   - Cached images and files

   From the "Time range" drop-down menu, you can choose the period of time for which you want to clear cached information. To clear your entire cache, select All time.

4. Click CLEAR DATA.
5. Exit/quit all browser windows and re-open the browser.

Firefox

1. From the History menu, select Clear Recent History.

   If the menu bar is hidden, press Alt to make it visible.

2. From the Time range to clear: drop-down menu, select the desired range; to clear your entire cache, select Everything.

3. Next to "Details", click the down arrow to choose which elements of the history to clear; to clear your entire cache, select all items.

4. Click Clear Now.

5. Exit/quit all browser windows and re-open the browser.

Microsoft Edge

1. In the top right, click the Hub icon (looks like star with three horizontal lines).

2. Click the History icon (looks like a clock), and then select Clear all history.

3. Select Browsing history, then Cookies and saved website data, and then Cached data and files. Click Clear.

4. After the "All Clear!" message appears, exit/quit all browser windows and re-open the browser.

Internet Explorer 11

1. Select Tools > Safety > Delete browsing history....

   If the menu bar is hidden, press Alt to make it visible.

2. Deselect Preserve Favorites website data, and select:

   - Temporary Internet files or Temporary Internet files and website files
   - Cookies or Cookies and website data
   - History

3. Click Delete. You will see a confirmation at the bottom of the window when the process is complete.

4. Exit/quit all browser windows and re-open the browser.

Safari 8 and later

1. From the Safari menu, select Clear History... or Clear History and Website Data....

2. Select the desired time range, and then click Clear History.

3. Go to Safari > Quit Safari or press Command-Q to exit the browser completely.