The Bank of East Asia, Limited, Macau Branch
("BEA Macau Branch")
Security Tips for BEA Macau Mobile

Q1: How can I tell if an SMS is sent legitimately by the bank?

In order to assist the public to verify the identities of SMS senders, The Bank of East Asia, Limited ("BEA") has participated and become a Registered Sender under the SMS Sender Registration Scheme established by the Office of the Communications Authority ("OFCA") of Hong Kong.

Starting from 28th January 2024, all SMS sent from BEA in Hong Kong will have a prefix "#" indicating that the SMS is sent by a Registered Sender. BEA's "Registered SMS Sender IDs" for SMS to Macau Branch customers with Hong Kong phone numbers will include:

- #BEAMO
- #BEA_MO
- #BEA-MO

Please note the Scheme is not applicable to:
(1) SMS messages of which receiving parties are expected to reply to the senders via phone numbers; or
(2) Hong Kong subscribers of Single-Card-Multiple-Numbers/One-Card-Two-Numbers mobile service provided by non-Hong Kong operators.

For more details about the Scheme, please visit OFCA's website (www.ofca.gov.hk/ssrs).

BEA would like to remind you under all circumstances, should stay highly vigilant when receiving SMS from unknown senders, and must not disclose to unidentified senders any personal information, bank account numbers or credit card details, transfer money or access any hyperlink in the SMS, to avoid suffering any loss.

Q2: Why my mobile device has a potential security risk?

When using BEA Macau Mobile, if we detect that your mobile device has an app listed in blacklist or downloaded from an unofficial source and that has been granted excessive permissions, a security warning will be displayed on the screen. We will restrict the access to BEA Macau Mobile from your mobile device.

BEA東亞銀行

Q3: How can I restore access from that mobile device to BEA Macau Mobile?

If you want to restore access from that mobile device to BEA Macau Mobile, you can choose one of the following methods.

Method 1 (Recommended)

Delete app(s) listed as potentially risky according to the security warning that appears in BEA Macau Mobile; or

Method 2

Go to Device Settings > Accessibility to turn off the accessibility setting for those apps to prevent others from accessing and leaking your personal information

Q4: How can I turn off the accessibility setting for application downloaded from an unofficial source with excessive permissions?

The method of changing accessibility/accessibility settings may vary between different mobile device manufacturers and operating systems.
Generally, customers can go to device "Settings"> Tap or Search "Accessibility"> select app(s) with potential risks in "Downloaded Applications" > turn off the accessibility permission of the app(s).

Q5: How can I resume BEA Macau Mobile on my mobile device?

You may:

- Use the operating system recommended by BEA and download BEA Macau Mobile through official app stores (e.g. Google Play and App Store)
- Check the security of mobile devices, and
- Check the app(s) on your mobile device, and
- Remove suspicious app(s), and/or
- Disable app(s) downloaded from unknown sources with excessive permission and maintain appropriate settings, and/or
- Stop unusual or unnecessary requests from websites, app(s) and other software/ programs on your mobile device, and/or
- Ensure the operating system and app(s) on your device installed with latest security updates or consider using the latest security software/programs to scan your device from time to time to enhance security.

Q6: How can I ensure the security of my mobile device?

- To ensure secure transactions, please download mobile app(s) from an official app store (e.g. Google Play and App Store).
- Keep the device's operating system and app(s) up-to-date with the latest security patches. Do not use BEA Macau Mobile on "rooted" devices. Install updated anti-virus and anti-spyware software, and scan your mobile device regularly.

BEA東亞銀行

Q7: Are there any security tips for using BEA Macau Mobile?

Protect your Account and Password

1. Do not use your identity card number, telephone number, date of birth, driving license number, or any popular number sequence (such as 987654 or 123456) when choosing your PIN or password. Do not use the same digit more than twice.

2. Memorise your PIN and password. Do not write them down.

3. Change your PIN and password regularly via BEA Macau Mobile. Avoid reusing of passwords from personal accounts and/or social media accounts.

4. Keep your user ID and password secret at all times. Ensure that you (and, where relevant, any authorised person) do not disclose or share this information with anyone – including any joint account holder or any financial management software or programs – under any circumstances, and do not transmit this information through email or any instant messaging software/programs. Never assign the same password for any other services (such as your internet connection, or login details for another website).

   In addition, choose login credentials, user ID, and/or passwords which are significantly distinct from your other personal accounts, especially from social media accounts.

5. Under no circumstances will BEA Macau Branch use an email, SMS, instant message, phone call, or any other method to ask for your personal information, such as your password. One-time password ("OTP"), ID number, date of birth, account/ credit card number, credit card expiry date, telephone number, BEA Macau Online account number/username, or Mobile Banking user ID. Do not disclose this information to anyone, including any person who claims to be an employee or representative of BEA Macau Branch, under any circumstances.

6. Delete any SMS/push messages that you receive after using Mobile Banking.

7. Notify BEA Macau Branch immediately of any actual or possible unauthorized use of your PIN or password, and send confirmation in writing to BEA Macau Branch without delay.

8. Check your surroundings before performing any banking transactions, and make sure that no one sees your PIN or password. Cover the keypad when you enter your PIN on any device, such as a personal computer, mobile device, or other self-service terminal.

9. Never leave your device unattended while using the BEA Macau Mobile or let any other person use your Mobile Banking.

10. Do not use a public computer or public Wi-Fi network to access Mobile Banking. Choose encrypted networks and remove any unnecessary Wi-Fi connection settings when using Wi-Fi to log in to Mobile Banking. Please disable any wireless network functions (e.g. Wi-Fi, Bluetooth, near-field communication (NFC)), or payment apps whenever such functions are unnecessary.

11. Change your PIN or password immediately if you suspect that you have been deceived by a fraudulent website or email, or through a public Wi-Fi connection, public computer, third party's device, or any other means (for example, if you fail to log in to a service website after entering your correct PIN, whether or not any alert messages appear).

12. Do not activate the SMS forwarding function which is provided by your mobile network operator. If your computer has been infected with a malicious program, the fraudster can capture your personal information, e.g. password, account no. and phone no., when you access our services with your computer. Under such circumstances, the fraudster can also activate the SMS forwarding service and divert the one time password ("OTP") SMS to the fraudsters mobile device. As a result, the fraudster can draw funds from your account with your login credentials and OTP received from BEA Macau Branch.

Beware of Online Threats

1. Do not click on URLs or hyperlinks embedded in any email, SMS, instant message, QR code, search engine, or any untrusted source to access Mobile Banking. Do not use/install any third party software or program to access BEA Macau Mobile.

   You should access BEA Macau Branch's website by typing www.hkbea.com.mo into the mobile browser directly, by bookmarking the genuine website for subsequent access, or through the BEA Macau Mobile.

2. Please note that BEA Macau Branch or our agents/business partners will not send emails to you with embedded hyperlinks or QR code presenting hyperlinks to the transactional websites or Mobile Banking applications.

3. Take precautions against hackers, viruses, spyware, and any other malicious software when sending and receiving emails, opening email attachments, visiting and disclosing personal/financial information to unknown websites, and downloading files or programmes from websites. Do not browse suspicious websites or click on the hyperlinks and attachments in suspicious emails, including but not limited to encrypted files, compressed files (zip), or messages received through WhatsApp, Line, WeChat and other e-communities.

4. Do not use apps, programs, or software from untrustworthy sources.

BEA東亞銀行

Secure Your Device

1. Use the version of operating system, BEA Macau Mobile, and browser recommended by BEA Macau Branch to access Mobile Banking. Do not jailbreak or root your mobile device.

2. Do not install or run apps from third-party sources on your device. You are recommended to set your device to block installation of apps from unknown sources and keep it properly configured.

3. Carefully read installation and/or permission requests from websites, apps, and other software and programs. Be wary of any unusual or unnecessary request.

4. Keep the operating system and apps installed on your device up to date with the latest security patches.

5. Consider using the latest versions of mobile security software/programs to scan your device from time to time to strengthen its security.

6. Check the storage, battery, and mobile data usage of apps in your mobile device from time to time to see if there are any suspicious apps. Uninstall any suspicious app when necessary.

7. Do not share your device with other people or use other people's devices to log in to BEA Macau Mobile or BEA Macau Online. Set a passcode for your device that is difficult to guess and activate the auto-lock function.

8. If your device is capable of biometric authentication (e.g. fingerprint or facial recognition), do not let any other person register his/her biometrics on it.

9. You should not use facial recognition for authentication if you have identical siblings or siblings that look like you, or if you are an adolescent with rapidly developing facial features.

10. Do not disable any features that can strengthen the security of biometric authentication, such as "attention awareness" for facial recognition (e.g. ensure that the "Require Attention for Face ID" setting is enabled).

The Bank of East Asia, Limited, Macau Branch 東亞銀行有限公司澳門分行刊發
(11/2026)