BEA東亞銀行

Security Tips

The Bank of East Asia, Limited ("BEA" or "the Bank") has adopted the latest security technology to prevent unauthorised access to customers' bank accounts and provide a well-protected online services. You are encouraged to read the following advice to ensure the safety of your transactions and information.

1. Major Security Tips

- The Bank's staff will never ask for sensitive information such as your HKID, account number, Personal Identification Number ("PIN"), one-time passwords ("OTPs") generated with i-Token, credit card number, etc., through any channels (such as phone calls, email, or SMS). Do not disclose or share such information with anyone, even BEA staff or police officers, under any circumstances.
- Never disclose your BEA Online/ Corporate Cyberbanking/ BEA Corporate Onlinelogin number/ username or password to anyone.
- Avoid opening any email attachments or clicking hyperlinks embedded in any email, SMS, instant message, social media platform, QR code, search engine, or any untrusted source to access webpages and enter your sensitive information – especially your login details. Only use our online service by typing www.hkbea.com into your web browser, through a bookmarked link, or through BEA's official mobile applications.
- If you encounters suspicious calls, online sellers, friend requests, job ads, investment websites, etc., you are recommended to check the account name, payment account, phone number, email address, URL,etc. through the Scameter to assess the risk of fraud and cyber security before making any transaction. (Scameter website: https://cyberdefender.hk/en-us/)
- Take precautions against phishing scams (such as scams purportedly from government body or financial institution) hackers, viruses, spyware, and other malicious software.
- Always check your SMS/email transaction notifications from the Bank in a timely manner, and regularly check your transaction history and statements in e-Channels (including BEA Online/ Corporate Cyberbanking/ BEA Corporate Online and BEA's official mobile applications). Inform the Bank immediately in case of any suspicious situations.
- Make your passwords difficult to guess by creating a minimum of eight characters with no space and contains uppercase letter, lowercase letter, special character(s) and number(s). Avoid using easily accessible personal information such as telephone number or date of birth as your passwords. Make them different from passwords for other internet services, and change your passwords regularly.

- Use official software and keep the operating system and apps installed on your device up to date with the latest security patches. Install anti-virus and anti-spyware software, keep them updated, and scan your device regularly.
- Never use the same password for different online or social media accounts. If you suspect that someone has learnt your password, it is suggested that you change it immediately and contact with the Bank for assistance, if necessary.

2. Use of e-Channels (including BEA Online/Corporate Cyberbanking/ BEA Corporate Online and BEA's official mobile applications)

- Be alert to your surroundings before logging in. Make sure no one sees what you enter and log off properly after use.
- To ensure secure transactions, please download BEA's official mobile applications from an official app store (e.g. Google Play, App Store or Huawei AppGallery (global version)) or at our official website and do not use the app on any "jailbroken" or "rooted" devices.
- Change your PIN immediately when using your online service for the first time and destroy any documents containing your PIN.
- Please take note of your last login date and time or "Identity Message" every time you log in to one of our e-Channels.
- Visit any of our branches or login to BEA Online/ Corporate Cyberbanking/BEA Corporate Online to update personal information if your mobile phone number and/or email address recorded in the Bank has been changed or become invalid.
- Verify the transaction details including the payee name and amount when making "FPS" small-value transfers or transfers to registered/non-registered accounts using a mobile phone number, email address, FPS ID, QR code, or account number. If you have any enquiries, confirm with the payee before making the transaction.
- To prevent unauthorised access by others, you are suggested to set up auto-lock, passcode lock and enable remote wiping. If your device being loss/theft, it is recommended to change your BEA Online/Corporate Cyberbanking/BEA Corporate Online PIN by logging into the BEA Online/Corporate Cyberbanking/BEA Corporate Online and deactivate your i-Token, if applicable.
- Notify the Bank immediately of any actual or suspected unauthorised access of your account.
- Protect your computer and mobile phone which are used for logging into the e-Channels. If your device is capable of biometric authentication (such as fingerprint or facial recognition), do not disable any features that strengthen the security of biometric authentication and do not let any other person register his/her biometrics on it.

- 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.
- Do not use a public computer or public/unknown Wi-Fi network to access online services. Make sure to use an encrypted network when logging in to online services through Wi-Fi, and remove the settings of any unnecessary Wi-Fi connections. Disable wireless network functions such as Wi-Fi, Bluetooth, NFC, etc. when not in use.
- Avoid using online services through free or untrusted Virtual Private Networks (VPNs). If you need to use remote access technology to access online services, please use trusted software without publicly known vulnerabilities.
- Carefully read the installation and/or permission requests from websites, apps, and other software and programs. Do not install or run apps from third-party/untrustworthy sources on your device, and uninstall any suspicious apps.
- Regularly check and update your system's web browsers and any of BEA's official mobile applications on your devices.
- Be alert if using public USB charging stations for your mobile phone or device to avoid malware infection.
- Do not submit documents (such as scanned identity documents, bank statements, or letters) to any untrusted website or app.

3. Use of ATM Services

- Remember your PIN and do not keep it with your ATM card.
- Change your PIN immediately when using your ATM card for the first time and destroy any documents containing your PIN.
- Be alert to your surroundings before conducting any transactions. Make sure no one sees your PIN, and cover the keypad when you enter your PIN.
- Check that the protective keypad cover is intact before using any ATM in Hong Kong. Contact the Bank immediately if in doubt.
- Should you notice any suspicious devices in an ATM (such as a micro-skimmer, pin-hole camera, fake key pad, etc.) or any suspicious activities around you when performing an ATM transaction, cancel your transaction and inform the Bank immediately.
- Retrieve your banknotes (if withdrawing cash), transaction receipt (if applicable), and ATM card as instructed after your ATM transaction is completed. Never try pushing your ATM card back into the ATM.
- Count your banknotes immediately after withdrawing cash. Keep all transaction receipts and check them against your account records.

- Do not take away any banknotes left behind by someone else at the cash dispenser or ATM card left in the card insertion slot. Let the ATM retract the banknotes and/or ATM card automatically.
- Set the effective date and expiry date of overseas ATM cash withdrawal function before travelling. Disable the function when you have returned from travelling.
- If your ATM Card/PIN is lost or stolen, please inform the Bank to report lost the ATM card immediately by visiting any of our branches, logging in to BEA Online, or calling our hotline:
  (852) 2211 1818 (during office hours)
  (852) 2211 1862 (during non-office hours)

4. Use of i-Teller Services

- Be aware of your surroundings and do not ask for/accept assistance from strangers when performing transactions.
- After you have used the ATM card, please keep and safeguard it properly.
- Should you notice any suspicious device in the i-Teller (such as a micro-skimmer, pin-hole camera, fake key pad, etc.) or any suspicious activities around you when performing a transaction, cancel your transaction and inform the Bank immediately.

5. Use of Phone Banking

- In order to prevent fraud, please keep your Phone Banking PIN secret.
- Never disclose your Phone Banking PIN to anyone (including BEA staff or police officers).
- Do not allow anyone to use your Phone Banking PIN to perform enquiries/transactions.
- Update your Phone Banking PIN regularly to ensure safety.

6. Two-Factor Authentication

- To enhance security for online transactions, the Bank provides a two-factor authentication service for its e-Channels. You are required to enter an i-Token OTP/ i-Token PIN[%] or SMS OTP[#] sent by the Bank to confirm designated transactions*.
- Safeguard your devices for two-factor authentication. Do not leave your security device (including your mobile phone which has i-Token activated or receives SMS OTPs) unattended or allow anyone to possess or control your security device.
- Do not share any OTP sent to your mobile phone or provided by i-Token with other people.
- Do not install i-Token on any “jailbroken” or “rooted” devices.
- Carefully check the transaction details before entering your OTP/ i-Token PIN.

[%] You are required to register your mobile phone number and email address with the Bank before you can register and use i-Token.

[*] These transactions include fund transfers to non-registered accounts with BEA Hong Kong and other local banks, fund transfers to non-registered BEA accounts in China and the United Kingdom, transaction limit increases, bill payments to merchants (except the "Government or Statutory Organisation", "Utilities", "Education: Primary or Secondary School", and "Education: Post-secondary or Specialised Institution" categories), setting up scheduled instructions or templates for the above-mentioned transactions, access to online investment services (including Stocks, Unit Trusts, Linked Deposit-related services, eIPOs, and Foreign Exchange/Precious Metal Margin Trading services), change personal information and any new transaction types as prescribed by the Bank from time to time.

[#] SMS OTPs cannot be forwarded to any other phone number, even if you have enabled the "SMS forwarding" service with your mobile phone service provider in Hong Kong.

7. Fraud Prevention Information

- If you have suspicions about the identity of any apparent intermediary/representative who promotes BEA products or services, you should immediately make a call to the Bank through official channels to verify.
- Notify the Bank immediately if you lose and/or subsequently replace any identity documents which you registered with BEA when opening your account, or if you have any suspicion that your personal information, statements or account details may have been compromised or stolen.
- Beware of bogus SMS messages and voice message calls. If you are suspicious about the identity of any callers, call the bank immediately through official channels to verify.
- Beware of fraudsters who impersonate staff of the BEA Group. Beware of unauthorised share-trading transactions. If you notice any suspicious or unauthorised activity related to your account, you should make a call through an official channel and verify with the Bank immediately.
- To avoid being deceived by a message, verify the sender's identity through alternative channels before taking any action.
- Beware of potential phishing attacks with common signs, such as a malicious sender address, subject heading with a “warning” or “FYI” label, a request that you enter personal information or click on a suspicious link, generic salutation, threat or false sense of urgency to trick you, demand for sensitive information or instruction to open an attachment, poor spelling/grammar, etc. In any such case, please verify the sender’s identity through alternative/official channels or delete the message immediately.

- Before entering your credit card information and/or an SMS OTP, please ensure the website is trustworthy.
- Keep alert when linking your credit card to any mobile payment service. An SMS will be sent to your mobile phone once your card has been linked successfully to a mobile payment service.
- Take precautionary measures to protect all mobile devices you own which can be used to access any BEA's official mobile application or activated mobile payment service, and prevent others from accessing it.
- To prevent you from falling into the trap of any cyber scams, you are recommended to pay attention to the anti-deception materials and the latest news issued by Hong Kong Monetary Authority, Hong Kong Police Force or other authorized institutions.

8. More Security Information

To learn more about security issues, please go to
https://www.hkbea.com/html/en/bea-security-tips.html