BEA東亞銀行

Recently, fraudsters have been sending out fake SMS messages and emails, which claim abnormalities or unsuccessful verification of customers' accounts and contain hyperlinks to fraudulent websites. Having clicked on the links, customers were asked to provide their Cyberbanking or personal information, such as their Cyberbanking login name and password, or a one-time SMS password. The fraudsters then used the information provided to conduct unauthorised Cyberbanking transactions and steal customers' money.

Customers should stay vigilant at all times and never click on embedded hyperlinks in a suspicious SMS or email. If you encounter any suspicious situation, please stop the process immediately to avoid potential monetary loss.

Security Tips about Phishing Scams

Our staff will never ask you for sensitive information such as your passport number, HKID number, account number, personal identification number ("PIN"), one-time password ("OTP") sent to your mobile device, Debit Card number, etc. through any channels (including over the phone, through email, or by SMS).

Never disclose your Cyberbanking login details to anyone.

Avoid opening any email attachments and/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.

Beware of potential phishing attacks with common signs, such as a malicious sender address, a subject heading with a "warning" or "FYI" label, a request that you enter personal information or click on a suspicious link, a generic salutation, a threat or false sense of urgency to trick you, a demand for sensitive information or an instruction to open an attachment, poor spelling/grammar, etc. In any such cases, please verify the sender's identity through alternative/official channels or delete the message immediately.

Only log in to your BEAUK account by typing www. hkbea. co. uk into your web browser, through a bookmarked link, or through BEAUK's official mobile applications, and stay vigilant for anything abnormal when logging in to Cyberbanking. A padlock (or lock) icon displayed in your web browser indicates a secure communication channel. If you are in any doubt, please stop the operation, do not enter any data, and close the window immediately.

Protect your Cyberbanking account and the device you use to access it

Never disclose your Cyberbanking login details to anyone.

Make your passwords difficult to guess and different from those for other internet services, and change your passwords regularly.

Regularly check to make sure your information with us (including your email and mailing address) is up-to-date. Make changes if necessary, following these steps:
Log in to "Cyberbanking" > go to "My Details"

Keep your operating system, anti-virus software, and apps installed on your device up-to-date with the latest security patches.

Do not access your Cyberbanking services using public computers or public wireless networks.

Avoid storing your Cyberbanking account information on any mobile devices. If storing such information is compulsory, make sure that others cannot access your device.

If you notice any suspicious transaction or transaction notification, please immediately report it by calling us on 0808 180 3838.

Click here to learn more about the Bank's Cyberbanking security precautions.

The Bank of East Asia, Limited
75 Shaftesbury Avenue, London W1D 5BB, United Kingdom
Website: www.hkbea.co.uk
Telephone: +44 (0)20 7734 3434
Email: info@hkbea.co.uk