BEA東亞銀行

Beware of fraudulent SMS messages and emails. Don't give away your information!

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 feel any situation is suspicious, 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 ID, account number, personal identification number ("PIN"), one-time passwords ("OTPs"), credit card numbers, etc., through any channels (including over the phone call, through emails, or by SMS).
- Never disclose your online banking login name 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.
- 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 case, please verify the sender's identity through alternative/official channels or delete the message immediately.
- Only log in to your BEA account by typing www.hkbea.com.mo into your web browser, through a bookmarked link, or through BEA Macau App, 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 online banking account and the device you use to access it

- Never disclose your online banking login name or password to third parties (including third-party-developed software/financial management tools).
- Make your passwords difficult to guess and different from those for other internet services, and change your passwords regularly.
- Regularly check and update your account information (including your contact phone number, email address, and mailing address).
- 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 our Customer Services Hotline on (853) 2833 5308.

BEA東亞銀行

提防虛假短訊及電郵，切勿輕易提供任何資料！

近期，有騙徒利用虛假短訊和電郵誘騙客戶，託詞客戶因賬戶出現異常或未能成功驗證等問題，要求客戶點擊超連結開啟偽冒網站並輸入資料。受騙的客戶往往在偽冒網站內輸入網上銀行賬戶或個人資料，例如網上銀行登入名稱、密碼或短訊一次性密碼，騙徒隨即利用盜取的客戶資料進行網上銀行交易，騙取客戶金錢。

客戶須時刻提高警覺，切勿在可疑短訊或電郵點擊超連結及開啟任何內容，當你發現任何可疑情況，應立即停止操作，慎防招致金錢損失。

防止釣魚詐騙保安貼士

- 本行職員不會經任何渠道（例如電話、電郵或短訊）要求你披露敏感資料如身份證號碼、賬戶號碼、密碼、短訊交易密碼或信用卡號碼等資料。
- 切勿向其他人透露你的電子銀行服務使用者姓名或密碼。
- 切勿經任何電子郵件、短訊、即時通訊訊息、社交媒體平台、二維碼、搜索引擎或不可靠來源內的超連結進入網頁並輸入敏感資料。
- 慎防一些潛在網絡釣魚攻擊的訊號，例如可疑的發件人地址、標題以“警告”或“FYI”為題、內容要求你輸入個人資料或按下可疑鏈接、使用通用稱呼、用威脅或緊迫性的文字、要求提供敏感資料或指示你打開附件而內容包含不清晰的拼寫／語法等，請通過另一／官方渠道驗證發件人的身份或立即將其刪除。
- 在登入電子網絡銀行服務時，應直接於瀏覽器輸入 www.hkbea.com.mo 網址、把網址設為書籤或使用東亞澳門分行手機程式，並注意登入版面有否出現任何異常情況，瀏覽器會顯示掛鎖（或鎖定）的圖案表示已建立安全通信渠道。如有懷疑，請即停止操作，切勿輸入任何資料，並請關閉視窗。

保護你的網上銀行賬戶及裝置

- 切勿向第三者（包括第三方開發軟件或理財工具）透露你的電子網絡銀行服務使用者姓名或密碼。
- 定期更改密碼，使用難以被猜破的數字和字母組合，並避免與其他網上服務使用相同的密碼。
- 定期更新在本行登記的賬戶資料，包括聯絡電話號碼，電郵地址及通訊地址。
- 確保你裝置上的作業系統，防毒軟件及應用程式更新至最新版本。
- 切勿透過公眾電腦或公共無線網絡登入電子銀行服務。
- 避免將銀行賬戶資料儲存到流動裝置。如必須儲存，避免把流動裝置外借他人。

如發現任何可疑交易或接收可疑的交易通知，請立即致電客戶服務熱線 (853) 2833 5308 與本行聯絡。