BEA東亞銀行

保安提示

東亞銀行有限公司（「東亞銀行」或「本行」）採用先進保安措施防止未經授權者盜用客戶的銀行賬戶，提供全面保障的網上服務。為確保您的交易及個人資料安全，建議您先閱讀以下保安提示。

1. 保安提示要點

- 本行職員不會經任何渠道（例如電話、電郵或短訊）要求您披露敏感資料如香港身份證號碼、賬戶號碼、密碼、i-Token 提供的一次性密碼或信用卡號碼等資料。在任何情況下，不可將個人資料透露給任何人，包括本行職員或警方。
- 切勿向其他人透露您的東亞網上銀行/企業電子網絡銀行/東亞企業網上銀行服務之登入號碼/使用者名稱或密碼。
- 切勿打開電子郵件之附件，或點擊附於任何電子郵件、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並進入網頁及輸入敏感資料 – 特別是您的登入資料。如需使用網上服務，應直接於瀏覽器輸入www.hkbea.com網址、把網址設為書籤或使用東亞銀行的官方流動應用程式。
- 如您遇到可疑來電、網購賣家、交友邀請、招聘廣告、投資網站等，建議您在進行交易前可在「防騙視伏器」查詢相關平台帳戶名稱、收款賬戶、電話號碼、電郵地址、網址等，以評估詐騙及網絡安全風險。(「防騙視伏器」網址: https://cyberdefender.hk/)
- 採取措施以提防網絡釣魚詐騙（例如假冒來自政府或金融機構為主題的網絡釣魚詐騙等）、駭客、病毒、間諜軟件及其他惡意程式入侵。
- 及時留意本行發出的短訊/電郵交易提示，並定期透過電子渠道（包括東亞網上銀行/企業電子網絡銀行服務/東亞企業網上銀行及東亞銀行的官方流動應用程式等）查閱賬戶交易及結單。若發現可疑情況，應立即通知本行。
- 請設定一個難以猜破而不含空格的密碼，密碼要求為至少八個字元，包含大小寫兼用的字母、特殊符號及數字。避免使用容易讓人取得的個人資料，如電話號碼或出生日期作為密碼。該密碼應與其他網上服務之密碼不同，並定期更改密碼。
- 使用官方軟件並確保您裝置上的作業系統及應用程式已裝有最新的安全更新，不時更新防毒軟件和防間諜軟件並定期掃瞄您的裝置。
- 切勿在不同網上或社交媒體的賬戶使用相同的密碼。如您懷疑有人得知您的密碼，建議您立即更改密碼，如需要可聯繫本行尋求幫助。

2. 使用電子渠道（包括東亞網上銀行/企業電子網絡銀行服務/東亞企業網上銀行及東亞銀行的官方流動應用程式）

- 登入時需先留意四周環境，切勿讓他人得知輸入的資料和使用後正確地登出。
- 為確保交易安全，請透過官方應用商店(如:Google Play，App Store 或華為應用程式市場(國際版)) 或透過本行官方網站下載東亞銀行的官方流動應用程式，並切勿在任何已被「越獄破解」或「超級用戶權限破解」的裝置使用。
- 首次使網上服務時應立即更改您的密碼，然後銷毀載有密碼之文件。
- 每次登入本行電子渠道時，請留意上次登入的日期及時間或「確認訊息」。

- 如您於本行登記的流動電話號碼及/或電郵地址已更改或已失效，請即到本行任何一間分行或登入東亞網上銀行/企業電子網絡銀行服務/東亞企業網上銀行更新個人資料。
- 使用流動電話號碼、電郵地址、FPS 識別碼、二維碼或賬戶號碼進行「轉數快」小額轉賬、或對未登記/已登記賬戶進行轉賬時，務必核實交易資料，包括收款人名稱及金額。如您對交易有疑問，請於執行交易前先向收款人確認。
- 為防止他人未經授權使用，本行建議您為您的裝置設立自動上鎖、啟用密碼鎖及啟動遠端清除等功能。當您的裝置有遺失/被盜的情況，建議您登入東亞網上銀行/企業電子網絡銀行服務/東亞企業網上銀行更改您的東亞網上銀行/企業電子網絡銀行服務/東亞企業網上銀行密碼，並停用您的 i-Token (如適用)。
- 當發現或懷疑您的賬戶被他人未經授權使用時，請立即通知本行。
- 請妥善保管用以登入電子渠道的電腦及手機。如您的裝置能使用生物認證（如指紋或面容辨識），切勿停用任何有助提升生物認證安全性的功能，並不要讓任何人在您的裝置上登記其生物信息。
- 如您有多胞胎或面容相像的兄弟姊妹，或正處於面部特徵可能快速發展的青春期，請不要使用面部辨識作認證。
- 切勿透過公眾電腦或公共/不知名無線網絡登入網上服務。當使用 Wi-Fi 登入網上服務時，應選用加密的網絡，並移除不必要的 Wi-Fi 連線設定。如無須使用請關閉 Wi-Fi、藍芽、NFC 等無線網絡功能。
- 避免透過免費或不可靠的虛擬專用網絡使用網上服務，如果需要使用遠程控制技術來使用網上服務，請利用沒有漏洞的可靠軟件。
- 細閱網站、應用程式和其他軟件及程式的安裝及/或許可請求。切勿於您的裝置上安裝或運行來自第三方/來歷不明的應用程式，必要時移除任何可疑應用程式。
- 定期檢查並更新您的系統瀏覽器及東亞銀行的官方流動應用程式。
- 當使用公共 USB 充電站充電手機或設備時，需留意情況以避免感染惡意軟件。
- 請勿在可疑網站或應用程式提交文件（例如身份證掃描檔案，銀行賬單和信件）。

3. 使用自動櫃員機服務

- 請緊記您的密碼及切勿將自動櫃員機卡與密碼一起存放。
- 首次使用自動櫃員機卡時應立即更改您的密碼，然後銷毀載有密碼之文件。
- 進行交易時需先留意四周環境，切勿讓他人得知輸入的密碼；輸入密碼時，請遮掩按鍵。
- 在香港使用自動櫃員機時，請先檢查鍵盤保護罩是否完好無損，如有懷疑請即通知銀行。
- 如在自動櫃員機發現任何可疑裝置(例如微型讀卡器、針孔相機或假鍵盤等)或附近有可疑活動，應立即取消操作並通知銀行。
- 交易完成後，依指示取回鈔票(如提取現金)、交易收據(如適用) 及自動櫃員機卡，切勿將您的自動櫃員機卡推回機內。

- 完成提款交易後應即時點算鈔票，並妥善保存所有交易收據，以便日後核對您的賬戶記錄。
- 切勿取去他人遺留於出錢槽的鈔票或插卡口的自動櫃員機卡，應待鈔票或自動櫃員機卡自動退回機內。
- 於出遊前審慎設定您的海外自動櫃員機提款之生效及終止日期。在您外遊回來後請關閉此功能。
- 如發現您的自動櫃員機卡/密碼遺失或失竊，請立即通知本行任何一間分行、登入東亞網上銀行或致電以下熱線報失：

  (852) 2211 1818 (辦公時間)
  (852) 2211 1862 (非辦公時間)

4. 使用視像櫃員服務

- 進行交易時，需先留意四周環境，切勿要求/接受陌生人的協助。
- 當你使用自動櫃員機卡後，請妥善存放及保管。
- 使用視像櫃員服務時，如您發現任何可疑裝置(例如微型讀卡器、針孔相機或假鍵盤等)或附近有可疑活動，應立即取消操作並通知銀行。

5. 使用電話理財服務

- 為防止欺詐行為，請將電話理財密碼保密。
- 切勿將電話理財密碼告知他人(包括本行職員或警方)。
- 切勿讓他人使用您的電話理財密碼進行查詢/交易。
- 定期更改您的電話理財密碼以確保安全。

6. 雙重認證

- 為提升網上交易安全，本行已為相關電子渠道提供雙重認證服務。進行指定交易*時，您需要輸入 i-Token 提供的一次性密碼/ i-Token 密碼[%]或本行發出的短訊交易密碼[#]。
- 請妥善保管您的雙重認證工具。切勿讓您的安全設備（包括已啟動 i-Token 或接收「短訊交易密碼」的手機）處於無人看管狀態，或讓其他人使用或控制該設備。
- 切勿向任何人透露發送至您手機或由 i-Token 提供的一次性密碼。
- 切勿在任何已被「越獄」或「超級用戶權限」的裝置安裝使用 i-Token。
- 在輸入一次性密碼/ i-Token 密碼之前，請詳細檢查交易內容。

[%]客戶必須於本行登記流動電話號碼及電郵地址後，才可登記及使用 i-Token。

*指定交易包括轉賬至未預先登記的香港東亞銀行及其他本地銀行賬戶、轉賬至未預先登記的內地及英國東亞銀行賬戶、提升交易限額、繳交商戶賬單(「政府或法定機

構」、「公用事業機構」、「教育：小學或中學」及「教育：專上或專業學府」類別除外)、建立上述交易類別的預設指示或範本、進入網上投資服務(包括股票、基金、掛鈎存款相關服務、電子認購新股服務和外匯/貴金屬孖展交易服務)、更改個人資料及任何本行不時新增的交易類別。

即使您已啟動香港流動電話服務商提供的「短訊轉駁」服務，本行所發出載有「短訊交易密碼」的流動短訊亦不會被轉送至其他電話號碼。

7. 防止詐騙資訊

- 若您對任何推廣東亞銀行產品或服務之中介公司/代表的身份有懷疑，應立即透過官方渠道致電本行與職員核實來源。
- 若您早前在開立戶口時提供給本行的身份證明文件已遺失及/或隨後已更換，或您懷疑您的個人資料、結單或賬戶資料可能已被洩露或盜取，應立即通知本行。
- 慎防偽冒短訊及語音訊息來電，如您對來電者有懷疑，應立即透過官方渠道致電本行與職員核實。
- 慎防有騙徒偽冒為東亞銀行集團的職員行騙，慎防未經授權股票交易，如發現您的賬戶有任何可疑或未經授權的交易，應立即透過官方渠道致電本行與職員查詢。
- 回應電郵要求前請先經其他渠道核實電郵發放者身份，提防受騙。
- 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”為題和內容要求您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您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。
- 在輸入信用卡資料和/或「短訊交易密碼」之前，請確定網站是可信任的。
- 密切留意綁定流動付款服務到信用卡時，相關綁定短訊會發送到您的手機。
- 採取預防措施以保護您用以進入東亞銀行的官方流動應用程式或已激活流動付款服務的所有手機，並防止其他人使用該手機。
- 為避免您墮入任何網絡詐騙的陷阱，建議您留意香港金融管理局、香港警務處或其他授權機構發出的防騙資料及最新消息。

8. 更多保安資訊

如欲了解更多保安資訊，請前往：

https://www.hkbea.com/html/tc/bea-security-tips.html