BEA東亞銀行

有關電子網絡銀行服務及東亞銀行流動理財保安問題之重要事項

此等重要事項適用於個人及企業電子網絡銀行服務及東亞銀行流動理財（統稱「電子網絡銀行服務」）。請在使用電子網絡銀行服務或東亞銀行流動理財前細閱及同意下列保安要點：

（1） 在任何時候，必須將你用於電子網絡銀行服務、自動櫃員機、東亞銀行流動理財、東亞銀行手機程式渠道及i-Token服務的所有電子網絡銀行賬戶號碼、櫃員機卡號碼、使用者身份識別/姓名及私人密碼（「密碼」）保密。在任何情況下，請確保你（及有關連的任何被授權人士（如適用））不向任何其他人士（包括任何聯名賬戶持有人或財務管理軟件或程式）披露或分享，及將此等資料以電子郵件或任何即時通訊軟件或程式傳送。你亦不應將相同的密碼用於其他服務（如接駁互聯網或登入其他網站）。

此外，你應選擇與你的其他個人賬戶（特別是社交媒體賬戶）明顯不一樣的登入憑據、使用者身份識別/姓名及/或密碼。

（2） 當發覺或懷疑你的電子網絡銀行賬戶號碼、使用者身份識別/姓名及/或密碼未經授權而被他人使用時，必須立即通知東亞銀行有限公司（「東亞銀行」），並即時以書面確認。若你發現已啟用i-Token服務/生物認證功能的裝置有任何遺失或被竊，你應立即致電網上理財客戶服務熱線（852）2211 1321。

（3） 東亞銀行及與其有關連的任何人士均無須知悉你的密碼。在任何情況下，不可將此等資料披露或分享給任何人，包括東亞銀行職員或警方。

（4） 當你對聲稱來自東亞銀行的網站或應用程式有懷疑時，應立即聯絡東亞銀行確認。

（5） 不要在你的電腦、手機或平版電腦（統稱為你的「裝置」）下載或使用來歷不明的應用程式、程序或軟件以登入或使用電子網絡銀行服務、東亞銀行流動理財或東亞銀行手機程式。在你安裝此等程式前應先了解該等程式的所需權限。

（6） 使用東亞銀行建議的操作系統及瀏覽器版本登入或使用電子網絡銀行服務、東亞銀行流動理財或東亞銀行手機程式。確保你裝置上的作業系統及應用程式已安裝最新的安全更新。

（7） 請透過手機官方應用商店（App Store或Play Store）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」或已破解「超級用戶權限」的裝置使用該程式。

（8） 只經www.hkbea.com登入電子網絡銀行服務。切勿開啟任何電子郵件的附件或經任何電子郵件、短訊、即時通訊訊息、二維碼、搜索引擎或任何不可靠來源內的網址或超鏈結以登入或使用電子網絡銀行服務。

你應直接於瀏覽器輸入www.hkbea.com網址或把該網址設為書籤以瀏覽東亞銀行網頁。

（9） 當你在個人裝置使用電子網絡銀行服務、東亞銀行流動理財或東亞銀行手機程式時，應不時監察是否有其他應用程式在裝置的系統內共同運作，並停止不必要的應用程式。

（10） 取消瀏覽器提供的「自動完成」功能。此功能於某些瀏覽器會記錄你所輸入的資料。如有需要，可參考瀏覽器的「説明」功能。

（11） 登入電子網絡銀行服務或東亞銀行流動理財或東亞銀行手機程式前，應先關閉所有其他瀏覽器視窗。

（12） 每次登入電子網絡銀行服務或東亞銀行流動理財時，請先於首頁檢查上次登入此服務的日期及時間。

（13） 避免與他人共用你的裝置，及切勿容許任何第三者在你的裝置上登記其生物識別憑據。不要使用他人的裝置登入電子網絡銀行服務、東亞銀行流動理財或東亞銀行手機程式。

（14） 如有可疑的視窗彈出或有異常的網頁要求你提供額外的個人資料，或你的裝置網絡/通訊量不正常地緩慢，應立即登出你的電子網絡銀行服務或東亞銀行流動理財及使用你最新版本的防毒軟件掃瞄你的裝置。

（15） 在完成操作後，確保登出電子網絡銀行服務或東亞銀行流動理財，並清除瀏覽器內的緩衝存儲。

（16） 定期檢查賬戶交易及電子結單。如發現任何問題（例如遺失櫃員機卡）或任何可疑及/或未經授權之交易，請立即通知東亞銀行。

（17） 切勿在使用電子網絡銀行服務或東亞銀行流動理財時離開你的裝置，亦不要讓他人使用你的電子網絡銀行服務或東亞銀行流動理財。為防止他人未經授權使用，為你的裝置設立自動上鎖和啟用密碼鎖功能，並在你的裝置被竊或遺失時啟動遠端清除功能。

（18） 切勿透過公眾電腦或公共無線網絡登入電子網絡銀行服務或東亞銀行流動理財。當使用Wi-Fi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。

（19） 當收發電子郵件、開啟電子郵件附件、瀏覽及告知個人/財政資料予不知名網站及下載網站內的檔案或程式時，請慎防駭客、病毒、間諜軟件及任何其他惡意程式入侵。切勿瀏覽可疑網站或開啟可疑電郵或開啟透過可疑電子郵件、WhatsApp、Line、微信及其他電子媒體所接收訊息內的超連結及附件（包括但不限於加密文件及壓縮文件（zip））或掃描載於其中的二維碼。

（20） 請不時使用適當及安裝最新版本的防火牆、防毒及防間諜軟件來定期掃瞄你的裝置。

（21） 不時更新你的瀏覽器及應用程式以支援Transport Layer Security（TLS）或更高標準的加編密碼程式，並確保沒有選用在瀏覽器內儲存或保留使用者身份識別/姓名及密碼的設定。

（22） 刪除你的電腦內共享的檔案及印表機，尤其當可經寬頻接駁、無線網絡或類似裝置使用互聯網時。

（23） 當首次使用服務時，必須立即更改你的密碼，並銷毀載有密碼之任何文件。請牢記你的密碼，切勿用筆記下。

（24） 建議選用數字（0至9）和英文字母（A至Z）的組合為電子網絡銀行服務的密碼。切勿以身份證號碼、電話號碼、出生日期、駕駛執照號碼或任何常用之數位組合（如987654或123456）作為你的密碼或櫃員機卡密碼。

（25） 請將櫃員機卡、結單、支票簿、其他重要文件及接駁電子網絡銀行服務或東亞銀行流動理財所用的任何保安裝置放在安全的地方。切勿將你的電子網絡銀行賬戶號碼及使用者身份識別/姓名與密碼存放在一起，亦切勿將你的櫃員機卡及櫃員機卡密碼放在一起。如需棄置載有個人資料的文件，請先行銷毀該文件。

（26） 請經常更改你的密碼及櫃員機卡密碼。

（27） 進行交易時需先留意四周環境，切勿讓他人得知你的使用者身份識別/姓名或密碼。當在任何裝置輸入密碼時，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。如有懷疑請即通知東亞銀行。

（28） 檢查東亞銀行URL上的名稱，以確認東亞銀行網址之真實性。當進行證實及加編密碼程式時，螢幕上將顯示一個狀似鎖或匙的保安圖標。

（29） 如懷疑已被偽造網站、偽造電子郵件，或透過公共無線網絡、公用電腦或第三者裝置或其他途徑欺騙（例如：輸入正確密碼後不能登入有關服務網站，無論有沒有顯現任何警告訊息），請立即更改密碼。

（30） 當你透過短訊收到一次性密碼或保安編碼，在輸入一次性密碼或保安編碼前須確認短訊中的登入或交易資料是否正確。在收到東亞銀行的短訊、信箱訊息或推送通知後，及時查核交易資料是否正確。如發現可疑情況，應立即通知東亞銀行。即使你已登記使用流動電話服務供應商的短訊轉傳服務，載有一次性密碼的短訊亦不會轉至其他手機號碼。

（31） 如你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。

（32） 在提供個人資料予網站前，先查閱網站的私隱政策聲明及安全防護措施聲明。

（33） 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）或附近有可疑活動，應立即取消操作並通知東亞銀行。

（34） 在自動櫃員機提款後，請即時點算鈔票並妥善保存所有交易收據，以便日後核對你的賬戶記錄。切勿取去他人遺留於出錢槽的鈔票或插卡口的櫃員機卡，應待鈔票或櫃員機卡自動退回機內。

（35） 交易完成後，依指示取回鈔票（如提取現金）、交易收據（如適用）及櫃員機卡，切勿將你的櫃員機卡推回機內。

（36） 於外遊前審慎設定你的海外自動櫃員機提款功能之生效及終止日期，並在外遊回來後終止有關功能。

（37） 不時檢查你裝置中各應用程式對儲存空間的用量、耗電量及數據用量，以偵察任何可疑的應用程式。必要時移除任何可疑應用程式。

（38） 如你於本行登記的流動電話號碼、電郵地址及/或通訊地址記錄已更改或已失效，請立即到本行任何一間分行更新個人資料。在你使用i-Token服務前，請先登記你的流動電話號碼和電郵地址。

（39） 為提防受騙，回覆電郵前應先經其他渠道核實電郵發送人的身份。

（40） 定期留意和遵照東亞銀行提供的保安提示。

中文版本只供參考。中英文版本如有歧異，以英文版本為準。

Issued by The Bank of East Asia, Limited 東亞銀行有限公司刊發