BEA東亞銀行

有關電子網絡銀行服務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（統稱「電子網絡銀行服務」）。請在使用電子網絡銀行服務前細閱及同意下列保安要點：

（a） 在任何時候，必須將你用於電子網絡銀行服務及自動櫃員機渠道的所有電子網絡銀行賬戶號碼、櫃員機卡號碼、私人匙、電子證書密碼及個人密碼（「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）不向任何其他人士（包括任何聯名賬戶持有人）披露及將此等資料以電子郵件傳送。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）。

（b） 當發覺或懷疑你的電子網絡銀行賬戶號碼、密碼或電子證書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。

（c） 東亞銀行及與其有關連的任何人士均無須知悉你的密碼、私人匙/電子證書密碼。在任何情況下，不可將此等資料告知任何人，包括但不限於自稱為東亞銀行代表或僱員的人士。

（d） 在完成操作後，確保登出電子網絡銀行服務及東亞銀行手機程式，並清除瀏覽器內的緩衝存儲。

（e） 切勿在使用電子網絡銀行服務時離開你的電腦或流動裝置。為你的電腦及/或流動裝置設定難以猜破的鎖機密碼及啟動自動上鎖功能。

（f） 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。當使用Wi-Fi登入電子網絡銀行網上理財服務或流動電話理財服務時，應選用加密的網絡，並移除不必要的Wi-Fi連線設定。如無須使用無線網絡功能（如Wi-Fi、藍芽、NFC），請謹記關閉此功能。

（g） 當收發電子郵件、開啟電子郵件附件、進入及告知個人/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。切勿瀏覽可疑網站及開啟可疑電郵或透過WhatsApp、Line、微信及其他電子媒體所接收訊息內的超連結及附件。

（h） 請不時使用適當防火牆、防病毒軟件及防間諜軟件，掃瞄你的個人電腦及流動裝置。

（i） 不時更新你的瀏覽器及應用軟體以支援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用戶名稱、密碼/電子證書密碼的設定。

（j） 刪除你的電腦內分享的檔案及印表機，尤其當可經有線數據器、寬頻接駁、無線網絡或類似裝置使用互聯網時。

（k） 當首次使用服務時，必須立即更改你的密碼，並毀滅載有舊密碼之所有函件。

（l） 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、櫃員機卡或電子證書密碼，及不應使用同一數位多於兩次。

（m） 請牢記私人密碼及電子證書密碼，切勿用筆記下。

（n） 切勿將你的電子網絡銀行賬戶號碼、使用者身份識別及電子證書與你的密碼及電子證書密碼存放在一起。

（o） 當進行銀行交易時，須先留意四周環境，切勿讓第三者得知你的密碼或電子證書密碼。

（p） 請經常更改你的密碼及櫃員機卡/電子證書密碼。

（q） 檢查東亞銀行URL及電子證書上的名稱，以確實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。

（r） 立即將你於核證機構所載資料的變更通知東亞銀行。如你因未能履行通知東亞銀行之責任而引致損失或索償，東亞銀行無須負責。

（s） 在電子證書已被取消、撤銷或變成無效後，請勿使用該證書。

（t） 請立即設定密碼以保障你的電子證書。

（u） 當你透過手機短訊收到一次性密碼，在輸入一次性密碼前須確認短訊中的交易資料是否正確。在收到東亞銀行的手機短訊及/或通知後，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。

（v） 確保你的電子證書及其私人匙為不可複製並存放於安全的媒體。當使用完後從電腦移除該裝置。

其他事項

（1） 如懷疑已被偽造網站、偽造電子郵件，或透過公共無線網絡、公用電腦或第三者電腦欺騙（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。

（2） 切勿使用來歷不明的軟件或程式。

（3） 切勿經任何電子郵件內、搜索器或任何不可靠來源內的超連結登入東亞銀行網站。

（4） 避免讓太多人使用你的電腦，並應設定電腦的個人密碼。

（5） 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「說明」功能。

（6） 請於使用電子網絡銀行服務前關閉瀏覽器的其他視窗。

（7） 應直接於瀏覽器的網址列內輸入電子網絡銀行或東亞銀行網址，登入電子網絡銀行服務。

（8） 只經www.hkbea.com登入電子網絡銀行服務。

（9） 每次登入電子網絡銀行服務時，請先檢查上一次登入此服務的日期及時間，該資料顯示於登入首頁「歡迎」訊息的下方。每次登入電子網絡銀行流動電話理財服務後，請於首頁檢查你的「東亞銀行確認訊息」。

（10） 切勿使用/安裝任何軟件或程式使用電子網絡銀行服務。

（11） 使用東亞銀行建議的操作系統、東亞銀行手機程式及瀏覽器版本登入電子網絡銀行服務。切勿用Jailbreak（越獄）或Root機等手法改裝手機及平板電腦。

（12） 定期檢查賬戶結餘和交易報告。如發現任何問題（例如遺失櫃員機卡）、任何可疑或未經授權之交易，請立即通知有關東亞銀行職員。

（13） 定期留意和遵照東亞銀行提供的保安提示。

（14） 如對任何聲稱為東亞銀行所屬的網站或手機程式有懷疑，應立即聯絡東亞銀行確認。

（15） 請將電子證書、櫃員機卡、銀行結單、支票簿、其他重要文件及接駁電子網絡銀行服務所用的任何保安裝置和設備放在安全的地方。如須棄置載有個人資料的文件，請先行毀滅該文件。

（16） 在任何情況下，東亞銀行絕對不會使用電子郵件、手機短訊、電話或任何其他方式要求你提供個人資料，如密碼、香港身份證號碼、護照號碼、出生日期、信用卡號碼或信用卡到期日等資料。東亞銀行亦不會要求客戶經電子郵件或手機短訊的超連結登入東亞銀行網站。

（17） 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。

（18） 當在任何裝置（如私人電腦、櫃員機）或自助/公眾終端機輸入密碼時，請遮掩按鍵。

（19） 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，或你的電腦網絡/通訊量不正常地緩慢，應立即登出你的網上服務/賬戶及使用你最新版本的防毒軟件掃瞄你的電腦。

（20） 為確保你可收到本行通知，東亞銀行必須存有你最新的流動電話號碼、電郵地址和通訊地址記錄。如有更改，請立即到任何分行更新資料。

（21） 防止電郵騙案－回應電郵前請先核實電郵發放者身份，以防受騙。

（22） 小心保管櫃員機卡，切勿把密碼與櫃員機卡放在一起。

（23） 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，請立即通知東亞銀行。

（24） 在使用自動櫃員機時，如發現任何可疑裝置（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。

（25） 在自動櫃員機提款後，請即時點算鈔票並確保交易無誤。切勿取去別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。

（26） 如須於境外提款，請預先透過指定途徑啟動有關功能、設定審慎的提款限額和有效日期，亦可預先向東亞銀行查詢你的櫃員機卡可否於預期的目的地使用。

中文版本只供參考。中英文版本如有歧異，以英文版本為準。

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