客戶重要通知

詞彙定義

1. "本行" – 指澳門商業銀行股份有限公司
2. "本網站" – 指澳門商業銀行互聯網網站 (www.bcm.com.mo)
3. "電子銀行" – 指【BCM Net 網上銀行服務】、【BCM eCorp 商業銀行服務】、【網上證券買賣服務】及【流動證券買賣服務】
4. "電子網絡" – 指互聯網及/或流動數據網絡

閱覽須知

1. 本網站及電子銀行服務部份資料只提供中文或英文內容。
2. 如欲達致最佳瀏覽效果，請以 1024 x 768 解像度及 Internet Explorer 8.0 或以上瀏覽本網站及有關之電子銀行服務。
3. 本網站及電子銀行服務的網頁或版面效果可能會因使用不同瀏覽器而有所差異。
4. 用戶需在電腦內安裝 Adobe Acrobat Reader 5.0 或以上閱覽某些需下載的文件或表格。

資料及材料之使用

本網站及電子銀行服務內所包含之資料及材料，不論是由本行或任何其它資料提供者提供，均並非蓄意向用戶提供任何專業忠告。本行不會對任何投資產品及服務承擔任何責任或作出擔保，而此等產品及服務均存在相應的投資風險。

免保證

本網站及電子銀行服務內所包含之資料及材料，不論是由本行或任何其他資料提供者提供，均只供參考之用，並且會不時作出修改而毋須預先通知用戶。雖然本行會盡力務求資料之準確，但本行對上述資料及材料之準確性或完整性不予保證。

互聯網通訊

客戶明白到電子網絡可能會因為未能預計的擠塞、開放和公開性質及其他原因之情況下，導致電子網絡未必是可靠的通訊媒介，而這些不可靠性是在銀行可控制範圍之外。這些因素可導致交易傳送延誤、資料錯誤傳送、執行指示延誤、執行指示和發出指示時的價位偏差、銀行和客戶在通訊上的誤會和錯誤、傳送缺失、阻礙等等。

責任之承擔限制

於任何情況下，本行或其僱員均不會對任何人因登入、使用或不能使用本網站及/或電子銀行服務而引致之任何損失或損毀承擔任何責任或賠償，不論該等損失或損毀為直接的、間接的、特別的、意外的或後果性的損失。

超連結政策

為方便用戶，本行可能會在本網站及/或電子銀行服務提供超連結至互聯網上的其他網站，但該等第三者網站並非與本行有任何關係或聯繫。本行僅此聲明，所有列入該等超連結的第三者網站，僅為協助用戶瀏覽和作參考之用。

除非本行明確聲明，提供超連結至本網站及/或電子銀行服務以外或第三者的網站並不表示本行推薦，同意，認可，保證或介紹任何第三者或其產品或服務，亦不可視為本行與該等第三者及任何網站有任何形式的合作。此外，除非本行明確表明或同意，本行不是用戶與第三者網站的供應者或任何第三者所訂立的合約安排中的其中一方。

本行高度強調及忠告用戶必須自行承擔任何因使用超連結引致的風險。本行概不會對任何因使用超連結而引起的直接或間接的任何損失、損害或其他可能引起的後果承擔責任。本行亦不會對該等第三者網站所提供的內容之準確性、真確性及其他情況負上任何責任。

本網站提供超連結至含有可供下載軟件之第三者網站僅為方便用戶而設。對於用戶在下載或安裝該等軟件時所遇到的任何問題或一切困難，本行概不負責。請緊記，使用任何從電子網絡下載的軟件可能受許可證協議的約束和限制。雖然本行並無責任，但本行仍提醒用戶必須遵守該等軟件的許可證協議條款。如閣下違反許可證協議，可能侵犯了有關軟件供應商的知識產權，而本行亦不會承擔任何責任。

當閣下使用超連結服務時，無論是本網站、電子銀行服務或連結其他第三者網站，請務必細閱有關網站的使用條款及章則。

版權
根據版權條例，本網站及電子銀行服務內包含之所有資料及材料均屬本行及其資料提供者所有。任何人士在未經本行同意下，不得拷貝、複製或分發本網站及電子銀行服務內包含之所有資料及材料。

網絡保安

使用電子銀行服務進行網上交易是否安全？

本行的電子銀行服務提供多項網上交易的保安措施，以確保客戶之銀行及賬戶資料得到適當保障：

- **Transport Layer Security (TLS) 128-元位加密**
  為確保資料保密，本行的系統採用 TLS 加密技術。客戶和本行之間所有透過電子網絡傳送的資料，會以此技術加密，以保障客戶的賬戶資料安全。當客戶連線時，請留意瀏覽器右下角狀態列所顯示的「安全鎖」標誌。這些標誌及信息是用作提示客戶的網上交易資料已作加密處理。

- **用戶名稱及密碼**
  為加強網上保安，客戶必需設立「用戶名稱」及定時更改「登入密碼」。

- **雙重認證技術**
  本行的系統引入雙重認證技術，採用兩種不同性質的認證方法，包括“您已知的資料”(例如登入賬號及密碼)及“認證工具” (例如：保安編碼器) 以核實用戶身份。客戶只需申請保安編碼器，即可安心辦理指定銀行交易及服務。

- **自動結束控制 (靜止時限)**
  電子銀行服務提供自動結束時間控制，如在十五分鐘內沒有使用任何功能或進行交易，連接電子銀行服務之接駁將會自動終止。

- **電子證書**
  本網站的伺服器已安裝賽門鐵克(Symantec)電子證書，以確認本行之身份 。

澳門商業銀行採取哪些保安措施防止電腦駭客？

電子銀行服務的保安對於銀行及客戶都是其中一個非常關注的問題；雖然電子銀行服務帶來方便及快捷的銀行服務，但如果沒有適當的安全及保護措施，駭客入侵或網上的漏洞便會潛在危機。因此，本行採取多項融合科技與管理的措施以確保本行網絡的高度安全。

- **打擊電腦駭客的措施**
  為防止駭客入侵，本行專責網絡保安的同事會監察任何駭客試圖入侵本行監察系統，以確保網絡安全。如果客戶懷疑自己的戶口有非授權的交易指示或涉及保安問題的事件，請立即與本行聯絡。

- **防火牆**
  本行的網上系統及伺服器均安裝了雙重知名防火牆，不斷地探測及防止未授權之人仕進入系統。

- **加密技術**
  本行系統採用了互聯網認可標準的 128 元位「TLS」加密技術以確保客戶的瀏覽器與本行伺服器之間的傳送得到保密。換句話說，客戶和本行之間所有透過電子網絡進入電子銀行服務而傳送的重要資料，均會以此技術加密，以保障客戶的個人資料安全。

- **Cookies**
  電子銀行服務使用 Cookies 存取每次連結的識別碼 (Session identifier) ，以識別在該連結時用戶的身份。當連結完結時，該 Cookies 便會過期。

- **安全電郵**

一般電郵的安全措施未必能確保安全，但「BCM Net 網上銀行服務」的系統特別設有【聯絡本行】的電郵功能，並引用相關的加密技術，而所有經本行以此功能傳送給客戶的個人或交易資料已採用該系統的保密技術加密。

- **私人密碼**
  為加強客戶的私人密碼的保密程度，本行透過適當的條例以防止客戶採用容易被推測的密碼，以防止被人盜用；如不能使用相同的號碼及字母或連續數。本行建議客戶避免使用生日日期、電話號碼或姓名等容易被人盜用的數據作為私人密碼。

- **登入記錄**
  為提高客戶的警覺性，當每次登入電子銀行服務時，本行會提供有關客戶於上一次登入網上理財的資料。如客戶發現有任何不符的地方，請立即與本行聯絡。

客戶應採取怎樣的保安措施保護自己的密碼安全？

除了本行的保安措施之外，客戶亦須採取以下適當步驟以確保自己的密碼安全：

- **有效及妥當運用閣下的密碼**
  電子銀行服務密碼乃為保障客戶使用網上理財服務及進行交易的安全而設，請勿隨便公開。閣下並應留意以下保管用戶密碼及保安編碼器需注意之事項：
  - 請勿在任何情況或向任何人透露閣下的私人密碼，包括閣下的親友及本行的職員。當客戶收到私人密碼之通知信後，請牢記上載之私人密碼，然後撕掉通知信，並於首次成功登入後立即作出更改。
  - 請勿使用容易被猜中的號碼作為密碼，如閣下的生日日期、身份證號碼、電話號碼或類似的數字或閣下的姓名的可辨認部份。
  - 請勿寫下或紀錄密碼而不加掩藏。
  - 請勿使用於其他網站登記使用之用戶號碼或密碼作為私人密碼或以您的私人密碼接駁其他服務（如接連互聯網或其他網址）。
  - 請勿讓他人士使用閣下的私人密碼。
  - 請設定難以猜破及與其他服務不同的密碼，並定期更新。
  - 設定密碼時同時使用小寫和大寫字母，並使用字母、數字和特殊字符的組合。
  - 絕對不可將密碼寫在任何使用電子銀行服務平台等所需的裝置上(例如：保安編碼器)及其他流動裝置上，或其他經常與此等裝置放在一起或放在附近的物件上，或隨身物品上，如手袋或銀包。
  - 閣下應經常更改電子銀行服務私人密碼，例如每隔 30 天便將密碼更改一次。
  - 當發現遺失、被盜取或懷疑其他人擅用閣下的私人密碼，請立即通知本行。同時，您亦應該立刻更改私人密碼，以防止未經授權人士使用您的網上賬戶。
  - 切勿將保安編碼器交由其他人士使用、保管或控制。
  - 請必小心保管閣下的保安編碼器，切勿亂放。
  - 避免使用瀏覽器的「記住網站密碼」之功能。當瀏覽器提示「是否記住此網站密碼」時，切勿選擇「是」。

- **切勿隨便透露閣下的密碼及個人資料**
  - 本行不會向客戶索取網上理財、電話理財或自動櫃員機服務等的登入資料或個人資料，這包括客戶的用戶名稱、密碼、賬戶號碼、身份證或護照號碼、地址及電話等。
  - 除了要在電郵中給予客戶更親切的感覺而顯示客戶名字外，本行不會在電郵中透露上述資料，或要求客戶回覆電郵確認任何私人資料。
  - 客戶必須提防要求索取閣下的密碼和/或其他個人資料的可疑電話，電郵，手機短訊或釣魚網站。

- **保護閣下的電腦**
  - 於電腦上安裝「個人防火牆」，能探測及防止未獲授權的人仕透過不同的途徑進入閣下的電腦盜取資料或下載有害的程式。若閣下為寬頻用戶，本行更建議客戶儘快向客戶的電腦或軟件供應商選取最適合的「個人防火牆」。
  - 而安裝「病毒防護軟件」能檢測常見的電腦病毒 (如:「特洛伊木馬」) 以防止電腦駭客竊取閣下的賬戶資訊或摧毀閣下的電腦檔案。一般的「病毒防護軟件」都需要定期更新版本，這樣，閣下才可以獲得最先進的保護，以確保自己的資料獲得週全保障。
  - 請勿開啟不明及可疑來源的電郵附件，它們可能含有病毒。
  - 避免進入可疑網站或從可疑網站下載軟件、檔案或應用程式。
  - 如果有任何不尋常的彈出式視窗和 / 或電腦速度異常緩慢，請立即登出本網站或電子銀行服務，並以最新版本的病毒防護軟件掃描電腦或瀏覽器。

- **保護閣下的網上交易**
  - 應留意登入本網站及/或電子銀行服務及過程有否異樣（如出現可疑的彈出視窗、被要求提供額外的個人資料等）及是否有人窺看密碼。
  - 請勿使用共用或公眾電腦登入電子銀行服務，因為閣下不能確保那些電腦內沒有被安裝駭客程式。
  - 避免透過公共無線網絡登入本網站或電子銀行服務。
  - 請勿中途離開閣下的電腦工作間及於每次使用電子銀行服務後，先按「登出」(Logout)功能，以免遭他人盜用賬戶。請謹記只關閉瀏覽器是不能登出電子銀行服務的。
  - 除非閣下仍在使用互聯網，否則應避免在不使用電腦時保持連線狀態，尤其是使用寬頻上網時更應加注意。
  - 電子銀行服務的首頁顯示客戶上一次登入服務的日期及時間。閣下應經常檢查該資料。如有任何懷疑，請立即與本行聯絡。
  - 請小心核對閣下的交易指示，於確定後，指示便不能更改或推翻。
  - 定期登入電子銀行服務以查閱戶口結餘、進支紀錄及交易紀錄，當發現有懷疑的交易項目，應立即通知本行。
  - 及時查閱由銀行發出的手機短訊及通訊，並查核有關交易紀錄。若發現可疑情況，應立即通知銀行。
  - 請勿將流動電話的來電及短訊轉駁至其他不明來歷的流動電話號碼或設備。如需到海外旅遊，建議閣下使用相同 SIM 卡及電話接收來電及短訊，避免使用轉駁功能。

- **注意電郵騙案**

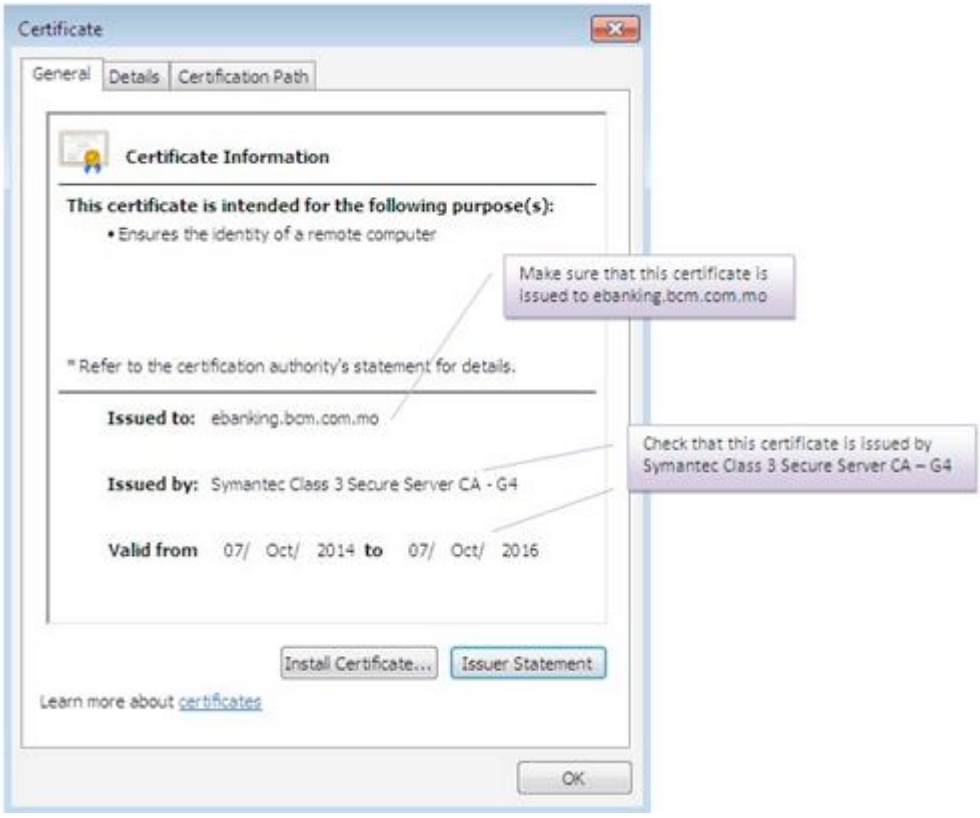
  電郵於現今社會是一種普遍的溝通方式，一般會用以聯絡親友以及商業上的伙伴。有些不法分子會利用駭客技術入侵電郵戶口，以各種方法騙取受害人匯款。而有些受害人亦因此受騙，蒙受鉅額金錢損失。閣下需對可疑電郵保持警覺，提高對此類騙案的防範意識，包括匯款前主動以電話、傳真或其他方式確認對方真正身份或該項要求的真確性，以防止此類案件的發生。請閱讀「**客戶應採取怎樣的保安措施保護自己的密碼安全？**」並採取防範措施以預防黑客入侵電腦。

- **確保閣下所瀏覽的網頁是本行轄下的加密保安網頁**

  如遇騙徒向大規模金融機構的客戶發出帶有欺詐成份的電子郵件。這些電郵會引導客戶按超連結至偽造網站，藉此要求客戶按入用戶名稱、私人密碼、個人資料及銀行機密資料。為保護閣下的個人及私人資料，切勿於電郵中按會直接聯繫到電子銀行服務的超連結。閣下可從您的瀏覽器直接登入；如果閣下已將 www.bcm.com.mo 加入到「我的最愛」，更可從中選擇該連結登入。這能避免被引導至偽造網站。**緊記：**由本行所發出的電郵不會有超連結直接指向登入電子銀行服務的網頁。

當輸入用戶名稱及密碼或重要的個人資料前，請檢查螢幕右上角是否有的「安全鎖」的出現。「安全鎖」代表安全連結。只須按下鎖扣，即可查察安全憑證詳請。

以下是 Internet Explorer 安全憑證的螢幕顯示範本以供參考：



注意：如客戶按下「安全鎖」後發現任何信息與以上所顯示的不符，請聯絡本行提供資料或協助。

為防止連結到假的網上銀行服務，請避免使用電郵內或其他網站上的連結去直接登入網上銀行服務。

如果您發現可疑的銀行網站，請不要輸入任何資料(包括用戶名稱、私人密碼)，並應立即通知銀行。

指定服務之保安措施

使用流動理財服務及/或流動交易平台服務(下稱流動銀行服務)應注意的事項

- 閣下必須採取上述一切合理步驟以妥善保管有關服務之私人密碼以登入流動銀行服務，並確保其安全和保密以防止欺詐行為。
- 當完成使用流動銀行服務後，請即時登出有關之應用程式。
- 不時監察流動通訊裝置的運作環境，停止不必要的應用程式在系統內共同運作。
- 經常登入查詢閣下的戶口結餘，股票持倉，交易指示和交易紀錄。
- 在閣下的流動通訊裝置使用由認可供應商提供的獲授權或正式的應用程式。
- 請勿使用 Jailbreak(越獄)或 Root 機等手法破解閣下的流動通訊裝置，並使用合法及未經私自修改的作業系統。
- 經常更新閣下的流動通訊裝置的作業系統和應用程式，並應從官方應用程式商店或可信的來源下載及升級應用程式。
- 不要將閣下的流動通訊裝置放置在無人看管的地方。
- 啟動流動通訊裝置的自動上鎖功能及解鎖密碼，並應設定難以猜破的密碼。
- 在公眾地方使用閣下的流動通訊裝置時，請以安全的網絡連接互聯網及避免透過公共無線網絡登入流動理財服務。
- 關閉無需使用的無線網絡功能（如 Wi-Fi、藍芽、NFC）。如需使用 Wi-Fi，應選用加密的網絡，並移除不必要的 Wi-Fi 連線設定。

澳門商業銀行（"銀行"）

保障客戶的私隱為本銀行之政策，亦被視為我們其中一項首要的工作。本銀行將嚴謹地遵守法律及監管當局所訂立之個人資料保護法例，並會培訓及督導員工一貫地執行有關個人資料保護政策。

當任何人士瀏覽我們的網址時，除了更新到訪者人數外，我們將不會收集其個人資料。在整個網址上，我們只會因應客戶提出的有關申請/查詢而收集其個人資料，並且在收集的同時，將收集資料的目的及用途，向客戶闡明。為了確保個人資料的保安及保密，我們採用了加密法傳輸於 BCM Net 網上銀行服務內所收集的資料。本銀行不會在沒有告知客戶的情況下收集其個人資料。

當個人資料被收集後，只有被授權之員工才能夠查閱，而在未得客戶同意前或除法律要求外，所有資料均不會透露予任何外間機構。為有效地服務各客戶，我們會不時將服務/產品的推廣資料及優惠寄予客戶。

聯絡我們：
本銀行將會不斷地作內部檢視，以確保客戶的私隱得到尊重和保障。閣下可參閱有關客戶資料的客戶通知以了解其他詳情。若有任何查詢，請與我們聯絡：

澳門商業銀行
資料保障主任
澳門南灣大馬路 572 號
電話: 8791 0669
傳真: 2859 5817

＊如中、英版本在文義上有任何差異，概以中文版本為準。

資料更新於二零一七年四月