

## 電子銀行安全提示

為了保障您的帳戶安全，我們提供各項保安措施並安排系統定期升級，也建議您採取以下各項保障網上活動的措施：

### 確保移動裝置的安全及版本更新（適用於手機銀行）

- 小心保管您的手提電話和 UKey。如 UKey 遺失，請立即聯繫我們更換 UKey。
- 只下載民生香港提供的官方應用程式和更新。請於 Apple App Store / Google Play Store 下載安裝或於官方網站 [www.cmbc.com.hk](http://www.cmbc.com.hk) 直接下載。請不要在其他途徑下載中國民生香港分行企業手機銀行應用程式，尤其是經可疑 QR Code 下載。
- 使用可靠的無線網路或工具，及確保其安全性。
- 為減低風險，建議使用時移動銀行時關閉移動裝置上的無線支付功能，如支付應用程式及 NFC 功能等。

### 確保使用安全的電腦及瀏覽器（適用於網上銀行）

- 客戶如需使用網上銀行服務，應確保使用正確網址登入。您可在瀏覽器上網地位址一欄直接輸入銀行正確網址 [www.cmbc.com.hk](http://www.cmbc.com.hk) 進入網上銀行服務，切勿經含有連結的郵件、網上搜尋工具或可疑彈出窗口登入。注意本行不會透過郵件向客戶發出含有嵌入式連結至網上銀行服務的內容。
- 請您安裝防火牆程式及定期更新病毒檢測軟體，以預防新病毒的入侵。
- 您應取消瀏覽器的“自動完成”功能，以避免當您鍵入密碼時，電腦會自動完成您的輸入。要啟動或取消“自動完成”功能，請打開瀏覽器，選擇“工具”-“Internet 選項”-“內容”-“自動完成設置”，取消“表單上的使用者名稱和密碼”功能。

### 使用安全的用戶別名和密碼

- 為提高安全，我們強烈建議您的登錄密碼和 UKey 密碼均採用 6 位或以上的組合，應選用一個別人不會容易猜到的密碼，並包含數位、字母及混合大小楷，例如：Ci27Ld98。
- 請緊記您的用戶別名和密碼切勿用筆寫下。切記時刻妥為保密這些資料，切勿向任何人(包括本行職員及警方)透露。

- 定期更改您的密碼，建議每 60 天更改一次。
- 當您在登入時，請確定沒有人在背後或附近察看，與及確定其他人不能透過手機螢幕看見您所輸入的用戶別名及密碼。
- 請不要在非民生銀行官方網站或其他非法網站上輸入公司的銀行帳號及密碼等資訊。

### 正確地登入/ 登出

- 建議以 UKey 登入。如以用戶別名進行登錄的用戶，建議用戶別名使用不會輕易被人猜中的組合， 避免和密碼重複使用。
- 如果您輸入不正確的 UKey 密碼且超過 6 次，您的 UKey 將被停用，需向我們重新申請新 UKey。
- 如果您在同一天內輸入不正確的登錄密碼且超過 5 次，當天不可再登入。登入次數為網銀和手機銀行共用。
- 在您每次登入時，我們會提供您的別名、上次登入渠道、時間和當日登入次數等資訊。如果您懷疑有任何不尋常的活動或對最近一次登錄時間及本日累計登錄次數等有疑問，請立刻更改登錄密碼並致電客戶服務熱線。
- 建議您選擇在每次登錄時收取短信通知，瞭解登錄資訊。
- 若在指定時間內沒有任何活動，網上銀行/手機銀行服務將自動登出，再次使用需重新登錄。
- 謹記網上銀行使用完畢後，請選擇安全退出，並及時拔下 UKey。

### 安全操作交易及定期檢閱賬戶

- 切勿透過安裝在公眾地方的電腦（例如網吧等）進行任何交易。
- 進行授權交易時，您必須仔細核對收款人的身份和賬戶資料，與 UKey 螢幕上的資訊是否吻合，才輸入 UKey 密碼。
- 留意有關確認交易的手機短訊，並核對交易資料。
- 為及時收取短訊，如流動電話號碼有所更改，客戶須儘快于網上銀行更新或通知本行以作出更新。
- 定期查閱您的戶口結餘及結單，以檢查有沒有異常的賬項。
- 發現賬戶有未經授權交易，或賬戶有任何不尋常活動，請即時聯絡我們。