

手機銀行安全資訊

關於留意流動裝置惡意軟件（Malware）騙案資訊，請見“最新/重要保安資訊”。

下載個人手機銀行應用程式注意事項

- 如發現任何可疑下載的程式，切勿嘗試登入及停止操作。
- 謹防下載假冒流動應用程式，被植入釣魚 / 木馬程式盜取登入資料。
- 不要複製和安裝不確定來源的手機銀行用戶端軟件。
- 如發現任何不正常運作，例如出現異常版面或登入緩慢，請即停止操作。

手機銀行的保安措施嚴密？

- 本行的網站採用了嚴密的 TLS 加密技術，透過個人化的登入名稱及密碼保障客戶登入手機銀行安全。
- 我們同時採用防止重複登入措施，即同一客戶不能於不同手機或電腦同時登入。
- 如客戶使用服務時靜止了一段指定時間，登入將被自動終止連線，防止任何未經授權的交易。
- 本行的手機銀行獲 Sectigo 頒予安全認證。

使用手機銀行時應特別注意的事項？

- 切勿在瀏覽器選擇儲存或保留密碼，並關閉瀏覽器的「自動完成」設定，防止第三者從瀏覽器盜取您的登入資料。
- 避免使用公眾地方或欠缺密碼保護的無線網絡（即 Wi-Fi）登入手機銀行，建議使用已加密及可靠的網絡連接互聯網以登入手機銀行。
- 為流動裝置設定自動鎖定功能及避免於環境擠迫的地方登入手機銀行，並留意在個別流動裝置輸入密碼時，有關密碼可能以明碼的方式放大，間接讓第三者窺視登入資料。
- 關閉無需使用的無線網絡功能（如 Wi-Fi、藍牙、NFC）或支付應用程式。如需使用 Wi-Fi，應選用加密的網絡，並關閉 Wi-Fi 自動連線設定。
- 避免使用他人的流動裝置登入手機銀行及讓他人使用您的流動裝置。

- 建議在流動裝置安裝防火牆及防病毒軟件/手機保安應用程式，並定期更新。請參考香港電腦保安事故協調中心網頁：<https://www.hkcert.org/mobile-security-tools>，選擇合適的應用程式。
- 為確保網上交易安全穩妥，使用本行流動應用程式時，本行會檢查流動裝置是否使用已被破解及符合基本保安要求的操作系統，客戶或將不能透過相關的流動裝置使用手機銀行，請注意相關提示訊息。
- 每次使用手機銀行，請先核對上一次登入及登出的紀錄；您亦應定期檢查賬戶結餘及核對交易紀錄。
- 本行為客戶提供手機銀行（個人及企業）的登錄記錄；客戶可登入手機銀行後查閱近期登入記錄，包括登入時間、位置資訊、和設備資訊，以便及時發現潛在異常活動。
- 如發現可疑情況，請即與本行聯絡。

客戶須妥善保管個人密碼及個人資料並對此負責

- 請牢記密碼，切勿將密碼寫在任何已安裝手機銀行的裝置，或經常與此等裝置放在一起的物件上，亦切勿把密碼儲存在手機內或以任何形式記錄密碼而不加掩飾。
- 切勿選用您的個人姓名、出生日期、身份證 / 護照號碼、電話號碼、幸運數字、及其他容易被猜中的個人資料、號碼或文字作為密碼或登入資料，並避免使用於其他網站登記的密碼作為登入密碼。
- 切勿向任何人（包括銀行職員及警方）透露您的手機銀行用戶名稱及密碼，亦不應隨便向任何人透露您的個人資料，如身份證 / 護照號碼、出生日期等。
- 切勿讓第三者使用您的手機銀行或密碼。
- 請定期更改密碼。
- 如遺失或外洩密碼或遺失保安設備，或懷疑密碼 / 保安設備遭盜用，或發現賬戶有未經授權的交易，請即與本行聯絡或直接聯絡香港警方。
- 請定期透過官方軟件應用商店（如 Google Play，App Store 及香港華為應用市場等）或本行網站下載並安裝本行流動應用程式、其他應用程式、手機操作系統及瀏覽器的最新版本。切勿嘗試安裝來源不明的軟件/應用程式。如發現任何可疑的程式，切勿嘗試下載、登入及應即時停止操作。

使用手機銀行進行交易注意事項

- 切勿隨意透過任何社交平台獲取不知明的二維碼以進行付款交易，請確保來源可靠。
- 當掃描二維碼時，請提高警覺並確保二維碼的來源可靠。

- 在掃描二維碼或經識別代號付款前，應仔細核對收款人屏蔽名稱的提示。
- 在掃描二維碼付款前，應仔細核對商店或商戶之名稱。
- 請仔細核對由二維碼產生之交易資料是否正確。
- 完成交易後，請核對銀行所發出之交易紀錄。
- 除非您進行轉賬或支付服務等交易，切勿隨意向他人展示由本銀行應用程式所生成的二維碼。
- 您須採取一切合理的審慎措施，穩妥保管您的流動裝置。假如您發覺您的流動裝置遺失或被盜用，或曾發生任何未經授權交易，請即與本銀行聯絡或直接聯絡香港警方。

使用生物認證服務時應特別注意的事項？

- 當您成功登記「生物認證」服務後，任何儲存於您的流動裝置之指紋或 Face ID 均能使用「生物認證」服務。您必須確保只有您的指紋或 Face ID 儲存於您的流動裝置，並確保流動裝置上用作儲存指紋或 Face ID 及登錄「生物認證」服務的保安密碼或編碼保密。
- 基於保安理由，切勿使用已被破解的流動裝置。
- 如要取消「生物認證」服務，您可以透過登入手機銀行關閉設定。請注意於取消「生物認證」服務後，您的指紋或 Face ID 仍儲存於您的流動裝置上，您可考慮因應情況自行決定刪除有關資料。
- 如您的流動裝置的指紋或 Face ID 記錄曾經變更，您的「生物認證」服務會被暫停，您需要重新登記或啟用「生物認證」服務。
- 如您有理由相信您的生物認證資料可能與其他人相同或非常相似，切勿使用生物認證資料作生物認證。例如您有雙胞或三胞胎兄弟姊妹的話，切勿使用面孔辨識功能作認證。
- 如您的生物認證資料正在或將會經歷迅速發展或改變，切勿使用有關生物認證資料作生物認證。例如您正值青少年時期，面部特徵正迅速發育，切勿使用面孔辨識功能作認證。

若我在交易中途，有電話來電或忽然失去了網絡訊號，如何確認已成功遞交交易指示？

- 如指示已成功遞送及執行，手機銀行的版面會顯示有關交易的參考編號。您亦可查看最近十筆交易紀錄，以確認指示是否已成功遞送及執行。