

保安資訊

本頁列載南洋商業銀行有限公司（「本行」）有關的電子銀行服務的保安資訊。電子銀行服務指透過互聯網、無線網絡、自動櫃員機、電話網絡或其他電子網絡、終端機或設備提供的銀行服務，包括但不限於本行網上銀行（個人及企業）、手機銀行（個人及企業）、南商 e+ 流動應用程式（「南商 e+」）、電話銀行、自助服務及微信官號等。

最新 / 重要保安資訊

提防流動裝置惡意軟件（Malware）騙案

識別惡意軟件

- 惡意軟件會在未經用戶同意下，入侵、破壞其流動或電腦裝置系統，或從中獲取資料。惡意軟件包含間諜軟件、電腦病毒和特洛伊木馬程式。
- 間諜軟件是一種在未經用戶允許下安裝的軟件，它會隱藏不誠實的目的去監察和記錄用戶資料 / 網上行為，及收集和傳送擷取得來的資料（如身分識別資料，包括用戶名稱、密碼及信用卡號碼等）給未經授權的第三方而從中獲取利益。
- 病毒可能藏有具破壞性的編碼，能潛進某系統之多種程式、資料檔或設備，以及擴散到同一網絡下的不同系統，最終引致受影響的裝置故障和資料損失。
- 另一種惡意軟件為特洛伊木馬程式，它會偽裝成看似無害的程式，但能夠在用戶不知情下控制其裝置和進行不法活動。

如何妥善應對

- 客戶應透過認可的官方應用商店（如 Google Play，App Store 及華為香港應用市場等）搜尋「NCB」免費下載南商個人手機銀行（「NCB 南洋商業銀行」）、企業手機銀行（「NCB 企業版手機銀行」）及南商 e+ 流動應用程式（「南商 e+」）。
- 保持裝置的配置正確（例如不允許安裝來自未知來源的應用程式等）。
- 安裝應用程式前，仔細評估應用程式的請求權限，請勿隨意授權第三方取得手機完整控制權或共享螢幕畫面，如果發現可疑權限需求，切勿安裝相關手機應用程式。

- 應在個人電腦安裝防火牆軟件及防電腦病毒軟件，並且不時更新。
- 切勿用 Jailbreak（越獄）或 Root 機等手法改裝流動裝置或使用已被這些手法改裝的流動裝置以確保接駁電子銀行服務裝置安全和保密。
- 在任何情況都不應使用來歷不明的應用程式。切勿點擊不明短訊、電郵、網頁或社交媒體內容中的連結或從這些連結下載任何檔案。如發現任何可疑下載的程式，切勿嘗試登入及停止操作。
- 客戶應確保使用電子銀行服務的設備不受到電腦病毒感染或不被未經授權的惡意、破壞性或損壞性程式碼進入以取得、使用或更改客戶的密碼、「生物認證」（例如：指紋、Face ID）或個人資料。
- 為保障客戶賬戶安全及應對網絡詐騙風險，本行已暫停手機銀行（個人及企業）在流動裝置的屏幕截圖及錄屏功能。同時，如本行識別到您的 Android 裝置有潛在風險，例如：您的裝置上安裝了可疑應用程式，或已啟用「協助工具」/「無障礙功能」等相關輔助功能的應用程式；遇上此等情況，您的南商流動應用程式將有機會無法繼續使用。本行建議即刻刪除可疑應用程式，或關閉有關應用程式的相關輔助功能，以保障您的賬戶安全。

警惕詐騙來電、手機短訊、電郵

識別詐騙來電、手機短訊、電郵

- 來電者可能自稱來自銀行或其他金融機構，可能會邀請您申請個人貸款等金融服務，並以欺詐手段誘騙您提交個人資料或存入款項至指定賬戶以申請銀行服務；或聲稱您的銀行賬戶或銀行卡出現異常，要求提供您的個人資料以核實身份或查核交易。
- 騙徒可能通過預先錄製的語音訊息來電，通知您銀行戶口出現異常，要求您透露敏感個人資料包括賬戶號碼、用戶名稱及登入密碼等，以讓他們作出「調查」。他們亦可能假冒電訊公司、網上購物或支付平臺客服，或是速遞公司職員、本地和內地官員等身份，以不同理由要脅你提供個人資料，或將款項轉到指定銀行賬戶以騙取金錢。
- 在冒充過程中，騙徒可能相應提供了銀行職員的資料（因為騙徒可以通過不法手段獲得這些資料）或提供像真度極高的其冒充機構之員工證或名片，亦可能裝作不畏懼身份核實，提供虛假的職員編號等資料，以圖增加可信度。同時，偽冒來電通常通話音質較差，仿佛是長途電話來電。

如何妥善應對

- 詐騙電話安全提示

- 客戶應提高警覺，慎防偽冒銀行的欺詐電話及語音訊息來電。
- 客戶應注意不要向來電者提供任何敏感性的個人資料（包括登入密碼和其他認證資料，如一次性密碼，「保安編碼器」或「流動保安編碼器」所產生的一次性「保安編碼」等）。如有疑問或曾向可疑第三者提供過個人資料，請致電本行 24 小時保安熱線（852）2616 6628，並立即向警方報案（或致電香港警務處反詐騙協調中心的 24 小時諮詢熱線 18222，尋求警方協助）。
- 請注意，本行絕不會透過電話、短訊或電郵收集您的敏感個人資料（包括登入密碼和其他認證資料，如一次性密碼，「保安編碼器」或「流動保安編碼器」所產生的一次性「保安編碼」等），亦不會透過預錄語音訊息通知您銀行戶口出現異常。若收到自稱是銀行職員的電話或語音訊息請提高警惕。慎防偽冒銀行的欺詐電話及語音訊息來電。
- 為保障客戶利益，本行已經加入由通訊事務管理局辦公室推出的「短訊發送人登記制」，為幫助您更好識別本行已登記的發送人名稱，請前往本行網頁（本行網頁>「關於南商」>「客戶通知」>）閱覽“有關南洋商業銀行實行「短訊發送人登記制」通知”詳情。
- 當接到自稱是電訊公司、網上購物或支付平台的客服，或是速遞公司職員、本地和內地官員等的來電或訊息時，您可先在官方途徑核實來電號碼和對方身份，切勿急於向不明人士轉賬或透露個人資料。
- 接到可疑來電時您可以採取的措施
 - 客戶應注意，本行職員致電客戶時，會向客戶提供包括且不限於以下資料：致電職員姓名、員工編號、聯絡電話、核實來電者身份的方法，並提示客戶可通過致電本行 24 小時保安熱線（852）2616 6628 以核實來電者身份。
 - 當接到自稱是本行職員的來電時，您可按對方提供的資料作初步判斷。您可以進一步詢問來電者所屬部門/分行名稱和辦公室號碼，並確認他們是如何獲得您的電話號碼和賬戶資訊的。如果來電者不願意提供資訊，請立即掛線。
 - 若您曾向或懷疑曾向偽冒來電者提供個人資料，請致電本行：（852）2616 6628，並向警方報案（或致電香港警務處反詐騙協調中心的 24 小時諮詢熱線 18222，尋求警方協助）。
 - 如果您向來電者提供了密碼，請立即更改。
 - 如果您需要暫停網上銀行賬戶服務，請致電本行：（852）2616 6628（如欲恢復網上銀行賬戶服務，您可前往本行的任何一間分行重啟相關服務）。
- 您可以循以下途徑核實來電者的身份：

- 撥打本行 24 小時保安熱線 (852) 2616 6628 (選擇語言後按“9”)；或：
- 在本行網站 “聯絡我們 > 網上查詢與保安問題 ” 上填寫並提交表格，本行將於 1-2 個工作日內跟進；或：
- 親臨分行。

慎防網絡釣魚

識別「網絡釣魚」

- 「網絡釣魚」是一種常見的詐騙手法。騙徒會偽裝成銀行、網上付款服務供應商及網上購物平臺，透過電子郵件、短訊或假冒網上購物平臺內即時通訊方式，誘使對方提供敏感個人資料及認證因素（如登入密碼、一次性密碼等）。網絡釣魚電子郵件內亦可能包含惡意超連結、二維碼或附件，引導對方至非法網站。一旦連接到仿冒網站，受害人通常會被要求輸入個人資料或認證因素（如登入名稱、賬戶號碼、登入密碼、一次性密碼）。「網絡釣魚」網站會收集受害人輸入的一切資料，騙徒利用該等資料盜取您賬戶金錢利益而令你招致損失。

如何妥善應對

- 本行不會透過第三者網站、第三者手機應用程式或以電郵、手機短訊、即時通訊或致電要求客戶提供其個人資料及認證因素（如登入名稱、賬戶號碼、登入密碼和其他認證資料，如一次性密碼，「保安編碼器」或「流動保安編碼器」所產生的一次性「保安編碼」等）。亦不會透過短訊或電郵超連結、二維碼或附件，引導客戶到本公司網站或流動應用程式進行交易。客戶必須小心保管其個人資料及認證因素，如客戶收到此請求，請即與本行聯絡。
- 為確保交易安全，客戶應在瀏覽器網址欄內直接鍵入本行的網址以登入網上銀行。切勿透過任電郵、短訊、二維碼、互聯網搜索器或社交網絡平臺提供的超連結，或非本公司認可的第三者網站或流動應用程式登入本公司的網上銀行。如有懷疑、請立即停止操作，切勿輸入任何資料，關閉視窗。
- 客戶在登入電子銀行服務時，請注意登入版面有否出現任何異常情況（例如：不正常的彈出版面、視窗運作緩慢、重覆要求客戶輸入密碼等）。切勿透過不明 Wi-Fi 或公用電腦登入網上銀行。
- 在進行網上交易時，於輸入認證因素進行交易驗證前，請小心核對交易詳情，例如：交易類別、交易金額及貨幣等，以確認是實際上進行之交易，不要盲目輸入一次性密碼。輸入任何資料或進行交易前，須檢視該網頁地址是否真實與可信。如有查詢，請立即與本行聯絡。
- 使用流動電話號碼、電郵地址、FPS 識別碼（FPS ID）或以二維碼進行付款前，請小心核對付款詳情，

包括收款人名稱。如有任何懷疑，請先向收款人確認。

其他重要保安資訊

- 客戶不應透過第三者網站、第三者手機應用程式、電郵、短訊或即時通訊訊息中的超連結、二維碼或附件登入網上/手機銀行或提供任何敏感性的個人資料。為確保交易安全，客戶應在瀏覽器網址欄內直接鍵入本行的網址以登入網上銀行，或從官方認可的應用商店下載和安裝應用程式以登入手機銀行服務。
- 客戶應注意就電子銀行服務的保安問題應負的責任，包括及時閱覽及遵守本行《服務條款》及為保障客戶而不時列明的有關保安措施。
- 客戶有責任採取合理步驟，確保接駁電子銀行服務所用的任何裝置（如個人電腦、發出一性密碼的保安裝置和儲存數碼證書的智能卡）或認證因素（如個人密碼及認證令牌）安全和保密，包括但不限於：
 - 銷毀印有其密碼的文件；
 - 請留意採用生物特徵、軟令牌或裝置綁定作為進行相關交易的認證因素之一所涉及的風險（認證因素遺失、被竊、資料外洩或遭未經授權使用），以及確保裝置和認證因素安全的相關保護措施。如發現可疑裝置，以及在發現其卡或賬戶有異常或可疑交易後，應盡快通知本行；
 - 切勿讓任何其他人士知道及使用其認證因素；
 - 絕對不可將其密碼寫在任何使用電子銀行服務所需的裝置之上，或其他經常與此等裝置放在一起或放在附近的物件上；
 - 不應直接寫下或記錄密碼，而不加掩藏；
 - 在發現其賬戶有異常或可疑交易/活動後，請即致電本行 24 小時保安熱線（852）2616 6628 申報相關異常情況並要求即時暫停網上銀行帳戶服務；及
 - 需要確保其在本行登記用於接收本行重要通知的聯絡方式（例如用於網上付款的短訊及電郵通知）是最新且真實有效的，以便有關通知能夠及時向客戶發送。
- 如客戶發覺或相信其接駁電子銀行服務所用的認證因素或裝置遭泄露、遺失或被盜用，又或者其賬戶曾錄得未經授權交易/活動，客戶必須在合理可行的情況下儘快通知本行。
- 除非客戶作出欺詐或嚴重疏忽行為，如未能妥善保管接駁電子銀行服務的裝置或認證因素，否則客戶無須對因經其賬戶進行的任何未經授權交易而蒙受的直接損失負責。此點規定不適用於下文“自動櫃員機及提款卡的安全資訊”所載有關透過卡進行未授權交易的規定。

- 若損失是因客戶的欺詐行為而引致，客戶將要承擔所有損失。若損失是因客戶嚴重疏忽（可能包括在知情情況下容許他人使用其裝置或認證因素），或者因客戶在發覺或相信其接駁電子銀行服務所用的認證因素或裝置遭洩露、遺失或被盜用，又或其賬戶曾錄得未經授權交易後，未能在合理切實可行的情況下盡快通知本行而引致，客戶亦可能要承擔所有損失。客戶如未能遵守本文所載的保障措施而導致損失，此點的規定亦可能適用。
- 客戶在登入電子銀行服務時，請注意登入版面有否出現任何異常情況（例如：不正常的彈出版面、視窗運作緩慢、重覆要求客戶輸入密碼等）。客戶如有任何懷疑，切勿按照可疑網頁上的指示操作或輸入任何資料，並請即終止電子銀行服務的操作。如有查詢，請與本行聯絡。
- 客戶必須小心保管其個人資料（包括個人生物認證資料）。本行不會以電郵、手機短訊、即時通訊或致電要求客戶提供其個人資料，如用戶名稱、密碼、一次性密碼或其他賬戶資料。
- 在進行交易時，於輸入一次性密碼進行交易驗證前，請小心核對交易詳情，例如：交易類別、交易金額及貨幣等，以確認是實際上進行之交易。如有查詢，請立即與本行聯絡。
- 客戶應警惕涉及將卡綁定到移動支付服務的銀行卡詐騙，以保護其支付卡、卡信息和身份驗證相關的資料。
- 客戶可能需要承擔未能妥善保護其實體卡、卡信息和身份驗證信息的後果，特別是因忽視銀行卡前和卡後交易相關通知而產生的後果。