NCB 南洋商業銀行

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、手機銀行、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

- 為保障您的網上銀行賬戶安全，於網上銀行或手機銀行登入版面增加驗證碼。客戶在登入網上銀行或手機銀行服務時，除需要輸入網上銀行號碼/用戶名稱、密碼外，需同時輸入「驗證碼」。
- 為保障您的銀行賬戶安全，客戶在登入南商 e+查看賬戶信息或更新開戶申請資料時，除需要輸入「短訊一次性密碼」外，還需輸入「南商 e+登錄密碼」。
- 為了進一步加強互聯網交易安全，客戶於網上銀行及手機銀行辦理指定交易時，必須使用「雙重認證」及以指定方式接收交易通知，才可繼續辦理有關交易。有關網上及手機使用雙重認證辦理指定交易的詳情，請瀏覽本行網頁：「電子銀行服務 > 雙重認證」。
- 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、發出一次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；
  - 切勿讓任何其他人士使用其認證因素；
  - 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後，應儘快通知本行；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，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)。
- 客戶在登入電子銀行服務時，本行絕不需要客戶在保安編碼器上輸入任何資料以產生登入編碼。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，請立即與本公司聯絡。
- 客戶應警惕涉及網上交易和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信而產生的後果。

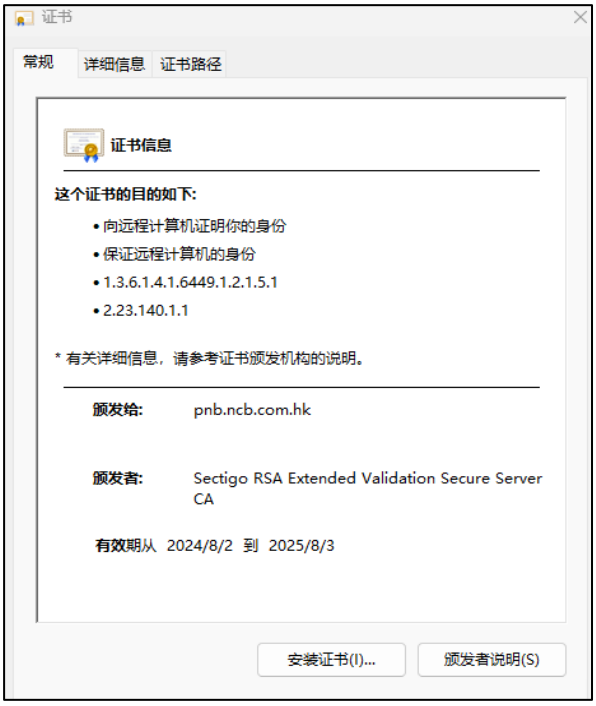
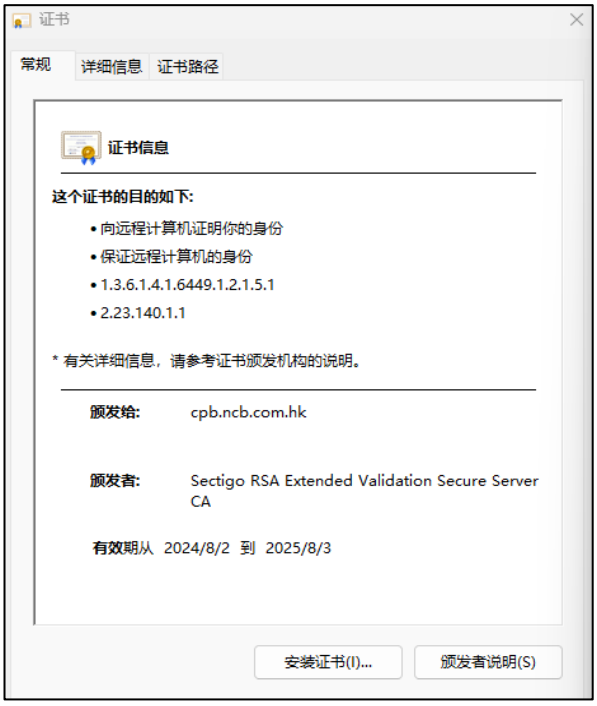
網上保安提示及資訊

我們為您提供的保障

- 本行採用國際認可的 Transport Layer Security (「TLS」)加密技術，保障資料傳送的安全，防止第三者盜取客戶的資料。
- 網頁伺服器設有防火牆，防止未經授權人士進入本行的系統。
- 本行系統會記錄客戶的登入次數。如客戶連續多次輸入錯誤的登入密碼，有關網上銀行服務會被即時暫停。
- 如客戶正使用的網上服務靜止（即沒有任何操作指示）了一段指定時間，服務將被自動終止連線，以防止任何未經授權的交易。
- 本行為客戶於網上銀行/手機銀行服務提供「流動保安編碼」及「保安編碼器」作為雙重認證工具；部份指定交易服務會為客戶提供以手機短訊形式發出的一次性短訊密碼進行驗證。
- 為確保您可以收到本行的通知信息以保障您的網上交易安全，若您的通訊資料有所變更，請登入網上銀行(設置 > 更新客戶資料)並使用雙重認證以更新個人資料。您亦可前往任何一間分行辦理。
- 若您通訊資料有所變更，而您所變更的通訊資料與您已登記您的識別代號相同（包括手機號碼或電郵地址），請登入網上銀行修改有關識別代號資料。

安全憑證

本行採用擴展驗證 SSL 證書，讓客戶可透過檢視瀏覽器的地址欄，核定所進入的網頁是否本行的真確網頁。Microsoft Internet Explorer 版本 9 或以上瀏覽器的地址欄為綠色，是擴展驗證 SSL 的其中一個保安特徵。如客戶選用 Microsoft Internet Explorer，亦可在網上銀行的登入版面上按「安全鎖」標誌，以查閱證書內容，包括其有效日期及以下資料。請注意，各項資料的顯示方式會因不同瀏覽器版本而有所差異。有關擴展驗證 SSL 證書詳情，請瀏覽證書發行者 Sectigo 的網頁。

 個人網上銀行 發給：pnb.ncb.com.hk 發行者：Sectigo RSA Extended Validation Server CA	 企業網上銀行 發給：cpb.ncb.com.hk 發行者：Sectigo RSA Extended Validation Server CA

符合基本保安要求的瀏覽器

為確保客戶資料安全，請安裝建議的瀏覽器版本登入網上銀行服務：

個人網上銀行	企業網上銀行
● Microsoft Edge (版本 14 或以上) ● Mozilla Firefox (版本 72 或以上) ● Apple Safari (版本 10 或以上) ● Google Chrome (版本 80 或以上)	● Google Chrome（版本 80 或以上） ● Mozilla Firefox（版本 72 或以上） ● Microsoft Edge（版本 14 或以上） ● Apple Safari（版本 10 或以上）

網上保安提示

1. 防範偽造網站

   請保持警覺並注意任何試圖冒充本行網址的偽造網站。客戶必須完全確定登入本行網站，否則不應提供任何相關的網上服務資料。

2. 欺詐電郵

   請注意，電腦病毒、特洛伊軟件及黑客程式可透過電子郵件傳播，蠕蟲病毒更可將病毒複製及發送至電郵地址簿上各收件人。因此，客戶不應開啟並應即時刪除來歷不明的電子郵件，亦不要透過電子郵件或

短訊提供的超連結或二維碼登入網上服務。如需開啟電子郵件內的附件，亦應先進行病毒掃描。此外，客戶應提高警覺，以防騙徒藉電郵進行不法活動。

如涉及匯款交易，請勿單靠電郵往來辦理。客戶應使用其他渠道(例如：電話、傳真等)確認交易內容及收款人資料後才完成匯款。

欺詐電郵例子一：商業層面電郵詐騙
騙徒對一名海外買家及其服務供應商在過去數月的電郵往來進行監視。當該名黑客瞭解了有關交易詳情後，便利用與服務供應商名字相近的假電郵地址，指示買家將款項匯往一欺詐賬戶。

欺詐電郵例子二：冒領遺產詐騙
騙徒發出電郵並聲稱為銀行職員，指其一名已去世的客戶留下巨額定期存款，無人認領。騙徒邀請收件人訛稱為去世客戶的親屬以領取存款。如收件人同意合作，騙徒便要求收件人先繳付款項，以支付文件費用。最終收件人被騙去有關款項。

欺詐電郵例子三：未經授權的設備綁定及資金轉賬
騙徒冒認銀行發出嵌入超鏈接的欺詐電郵，客戶輸入其電子銀行帳戶資料和短信一次性密碼。詐騙者利用銀行的移動應用程序，使用有關資料和一次性密碼將其移動設備連接到受害者的銀行賬戶。儘管設備綁定有延遲執行期，但客戶仍被欺騙，通過提供幫助（例如輸入另一個短信一次性密碼）來幫助欺詐者在延遲期後激活其設備。詐騙者可以成功登入客戶的銀行賬戶，並利用其在未經授權的情況下將資金轉移到外國銀行賬戶。

3. 欺詐即時通訊訊息
客戶務請提高警惕，留意任何冒充本行或冒充銀行職員發出的詐騙性即時通訊訊息。這些消息通常會誘使接收者提供個人或帳戶詳細信息，以進行身份識別或參與投資計劃。客戶不應回复這些消息、點擊任何可疑鏈接、下載任何可疑文件或提供任何信息。

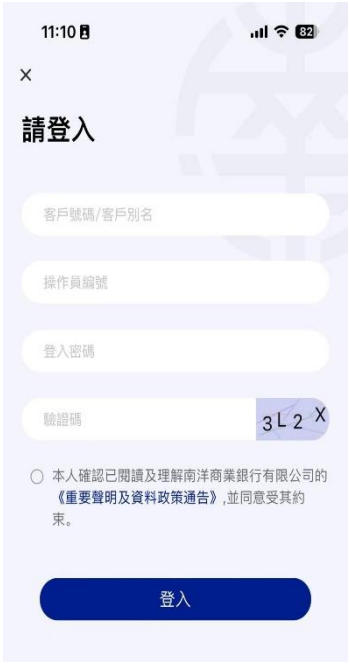
4. 瀏覽器中間人攻擊
近日發現有個別企業客戶的電腦懷疑受特洛伊木馬程式攻擊，在登入企業網上銀行時，電腦顯示一個虛假網頁，除要求客戶輸入登入名稱、密碼外，並同時要求客戶輸入由「保安編碼器」發出的一次性「交易確認編碼」 。

為保障客戶使用網上銀行服務的安全性，請客戶經常保持警覺，在登入網上銀行時，應注意登入版面有否出現任何異常情況 (例如有不尋常的視窗彈出，及/或電腦操作出現異常緩慢的情況等)，如有懷疑，切勿按照可疑網頁上的指示操作輸入任何資料，並請即關閉視窗。本行在客戶進行「指定交易」時，才會要求客戶輸入由「保安編碼器」發出的一次性「交易確認編碼」；在登入網上銀行時，本行不會要求客戶輸入該一次性「交易確認編碼」。(請參閱以下網上銀行登入版面)

本行藉此機會提示客戶應在其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，同時應避免進入可疑網站或從該等網站下載軟件，亦不要隨便開啟來歷不明的電郵內的附件。切勿點擊或打開可疑或疑似銀行發出之電子郵件中的附件或超連結。您可透過本行的網站 http://www.ncb.com.hk 或使用本行手機銀行應用程式登入網上銀行，切勿透過任何電子郵件、短訊或互聯網搜索器提供的超連結登入網上服務。如有疑問，請聯絡本行，以核實銀行是否確實發送了有關電子郵件。

個人網上銀行登入版面	手機銀行登入版面
	
客戶輸入網上銀行號碼/用戶名稱、網上銀行密碼及驗證碼，然後按「登入」	客戶輸入網上銀行號碼/用戶名稱、網上銀行密碼及驗證碼，然後按「登入」

NCB 南洋商業銀行

企業網上銀行	企業網上銀行
客戶輸入客戶號碼/客戶別名、操作員編號及企業網上銀行密碼、驗證碼登入企業網上銀行	如客戶已設置「雙重認證登入」，需在「保安編碼器」輸入企業網上銀行生成的「挑戰碼」以獲取由「保安編碼器」發出的一次性「交易確認編碼」以登入企業網上銀行
	
企業手機銀行	企業手機銀行
	

5. 偽冒電郵、短訊及即時通訊訊息的常見特徵

- 請慎防「網絡釣魚」的騙徒訛稱本 行 之名發出虛假電郵、短訊及即時通訊訊息，企圖誘騙您提供賬戶資料、密碼、個人資料或信用卡號碼。下列為一些偽冒電郵、短訊及即時通訊訊息常見特徵，有助保持警惕。
- 內容出現語法不通、錯別字或拼寫錯誤。
- 內容通常涉及本行的重要訊息或要求提供個人資料以核實賬戶，例如：大額轉賬的交易通知或須啟用新的安全功能的通知，並要求點擊超連結或開啟附件。
- 電郵一般包含超連結或附件。屏幕顯示的超連結看似本行網址，但當用滑鼠指向電郵顯示的連結時是其他網址。

6. 妥善保管個人密碼及個人資料

- 當收妥密碼函件後，應盡快透過網上服務更改密碼，然後將密碼函件銷毀。
- 請牢記密碼，切勿將密碼寫在或儲存在任何網上服務的裝置，或經常與此等裝置放在一起的物件上，亦切勿以任何形式記錄密碼而不加掩飾。
- 請定期更改密碼，切勿選用個人姓名、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，並避免使用已於其他網站登記的密碼作為登入密碼。
- 切勿向任何人(包括本行職員及警方)透露網上銀行服務用戶名稱及密碼，亦不應隨便向任何人透露任何個人資料，如身份證/護照號碼、出生日期等。
- 切勿讓第三者使用您的網上銀行服務。
- 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。
- 請仔細核對月結單、通知書及確認書上的交易內容，如發現有錯漏或不正常交易，應即時通知本行。
- 您可透過網上銀行查詢您的賬戶交易紀錄，快捷方便。

7. 保護您的個人電腦

- 請定期下載並安裝操作系統及瀏覽器的更新程式。
- 請為個人電腦安裝防火牆。
- 請為個人電腦安裝病毒偵測軟件，並定期更新病毒定義檔及進行病毒掃描。
- 請設定難以猜破的鎖機密碼及使用自動上鎖功能。
- 切勿下載或安裝來歷不明的程式，亦不應開啟可疑的檔案或電子郵件，以防止黑客程式或電腦病毒盜取您的個人資料。
- 如透過無線網絡使用網上服務，客戶必須加強安全設定。

8. 使用網上銀行服務時須注意的安全措施

- 切勿在公共地方(如網上咖啡室或網吧)的公用電腦使用網上銀行服務。
- 只設定及使用可靠的無線網絡上網。
- 切勿透過任何電子郵件、短訊或互聯網搜索器提供的超連結或二維條碼登入網上服務。
- 登入網上服務前，請關閉其他瀏覽器視窗。此外，在使用網上銀行時，切勿同時開啟其他瀏覽器及瀏覽其他網站。
- 在登入網上服務時，請確定沒有其他人在旁窺視，以免洩露您的用戶名稱及密碼。
- 每次使用網上服務時，請先核對上一次登入及登出的紀錄；客戶亦應定期檢查賬戶結餘及核對交易紀錄。如發現可疑情況，請即與本行聯絡。

- 當完成網上交易後，必須按「登出」離開系統，同時亦須關閉瀏覽器及刪除瀏覽器的暫存及歷史資料。
- 切勿在未登出網上銀行服務前離開電腦。
- 有關其他使用互聯網時應注意的保安措施，請參考常見問題。

9. 檢視及調整各項服務限額
- 請定期檢視您的各項服務的交易限額並作出適當調整以符合您的交易需要。

手機銀行安全資訊

如何下載個人手機銀行應用程式？
- 客戶可於手機的瀏覽器鍵入"www.ncb.com.hk/app"下載流動應用程式；
- 官方軟件應用商店 (Google Play 及 App Store) 搜尋"NCB"免費下載流動應用程式。
- 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體。
- 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 128 位元加密技術，透過個人化的登入名稱及密碼保障客戶登入手機銀行的安全。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。

如何登入手機銀行？
- 請透過官方軟件應用商店下載"NCB (商業)"流動應用程式，開啟應用程式並按“登入”後，以相關網上銀行號碼/用戶名稱及密碼登入手機銀行。

手機銀行有否獲得任何安全認證？
- 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。

- 為確保您的網上交易安全穩妥，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。
- 每次使用手機銀行時，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。
- 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，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(Google Play 及 App Store)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。
- 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。
- 當掃瞄二維碼時，請提高警覺並確保二維碼的來源可靠。
- 在掃瞄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。
- 在掃瞄二維碼付款前，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，進入「流動保安編碼」關閉生物認證設定選項。請注意於取消「流動保安編碼」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。

登出手機銀行後，是否需要關閉瀏覽器？

- 本行建議您登出系統後同時關閉瀏覽器。此外，您亦須定時刪除瀏覽器的暫存及歷史資料。

南商 e+流動應用程式安全資訊

如何下載南商 e+流動應用程式(「南商 e+」)？

- 客戶請透過官方軟件應用商店 (Google Play 及 App Store) 搜尋"南商 e+"免費下載流動應用程式。
- 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應用程式用戶端軟體。
- 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。

南商 e+的保安措施？

- 南商 e+採用了嚴密的 128 位元加密技術，透過本人的手機號碼及短信一次性密碼保障用戶登入南商 e+的安全。如用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行爲。

如何登入南商 e+？

- 請透過官方軟件應用商店下載南商 e+，開啟應用程式，需輸入用戶本人的手機號碼和短訊一次性密碼登入南商 e+。
- 用戶在登入南商 e+ 查看賬戶信息或更新開戶申請資料時，除需要輸入本人手機號碼、短訊一次性密碼外，還需同時輸入「南商 e+登錄密碼」。

使用南商 e+時應特別注意的事項？

- 避免使用公眾地方或欠缺密碼保護的不安全無線網絡(即「Wi-Fi」)使用本流動應用程式。使用流動應用程式建議使用已設定及可靠的網絡連接互聯網。
- 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南商 e+，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)。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。
- 避免使用他人的流動裝置登入南商 e+及讓他人使用您的流動裝置。
- 用戶應避免連接流動裝置至任何懷疑被電腦病毒感染的個人電腦，以防流動裝置亦被感染，同時，建議在流動裝置安裝防火牆軟件及防手機病毒軟件。不應使用已被破解的 iPhone 或 Android 手機流動裝置嘗試使用流動應用程式，以防潛在保安漏洞，並可在軟件應用商店下載合適的流動保安應用程式，您可參考香港電腦保安事故協調中心網頁：https://www.hkcert.org/mobile-security-tools，選擇合適應用程式。

- 為確保您的個人資料安全穩妥，使用本流動應用程式時，本行會檢查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裝置使用本流動應用程式，請注意相關提示訊息。
- 用戶需為流動裝置設定自動鎖定功能，及切勿選用容易被猜中的個人資料、號碼或文字作為密碼，並避免使用於其他網站登記的密碼作為登入密碼。 請定期透過指定官方軟件應用商店(詳情請參閱本行網站) 或本行網站下載並安裝本流動應用程式及其他應用程式、手機操作系統及瀏覽器的更新程式。
- 下載或使用南商 e+時，本行會記錄您的移動設備資訊（包括 IP 位址、設備 ID 和作業系統）、登錄和登出時間，以用於操作優化、統計分析和反欺詐。相關資訊的保留時間不會超過實現目的所需的時間。
- 用戶須妥善保管南商 e+登錄密碼及個人資料並對此負責：
  - 請牢記南商 e+登錄密碼，切勿將密碼寫在任何南商 e+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、號碼或文字作為南商 e+登錄密碼，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)透露您的登錄密碼，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南商 e+流動應用程式或登錄密碼。
  - 請定期更改登錄密碼。
  - 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。
- 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，請即與本行聯絡或直接聯絡香港警方。

若我在南商 e+上提交開戶申請時中途退出，是否還能繼續原有的申請流程？

- 如您還未提交申請，南商 e+和微信官號手機開戶申請頁面均不保留申請過程中填寫的信息或上傳的文件。

若我忘記安全問題答案及南商 e+登錄密碼，要如何重設密碼？

- 如您還沒有提交銀行開戶申請，可以通過短訊一次性密碼驗證身份來重設登錄密碼和安全問題；
- 如您已遞交開戶申請但尚未開立銀行賬戶，只能通過短信一次性密碼驗證身份後，通過取消開戶申請來重設密碼和安全問題；
- 如您已提交申請且銀行賬戶已開立，將無法重設密碼，只能通過在線聊天室聯繫客服或親臨分行查看銀行賬戶信息。

微信官號安全資訊

搜尋本行微信官方賬號時，請參照本行註冊的 WeChat ID - NCB_HK，以確保微信官號的服務及資訊由本行提供，切勿於未經認證的微信賬號透露任何個人及賬戶資料，如有疑問，請與本行職員聯絡。

使用微信官號時應注意的事項：

- 進行綁定時，用戶需使用個人網上銀行賬戶、密碼及於本行登記的手機號碼收取的「短訊一次性密碼」進行驗證。
- 切勿透過任何電子郵件或短訊提供的超連結或二維碼登入微信官號。
- 切勿在微信對話框輸入個人敏感資料，本行不會以微信對話框要求用戶提供其賬戶號碼、私人密碼或任何個人資料。

- 如欲瞭解更多綁定時需注意的事項，可於微信對話框輸入「綁定服務指南」關鍵字查詢。
- 如有查詢、報告保安問題或要求取消綁定，請致電：+852 2616 6628
- 為確保客戶資料安全，建議操作系統及瀏覽器如下：
  - iOS 9.0 或以上(預設瀏覽器)，WeChat 8.0.45 或以上
  - Android 4.4 或以上(預設瀏覽器)，WeChat 8.0.45 或以上
- 請定期下載並安裝流動應用程式、操作系統及瀏覽器的更新程式。

自動櫃員機及提款卡的安全資訊

保護個人密碼及提款卡

- 若您選擇銀行預設密碼，請在收妥提款卡及密碼後，謹記您的個人密碼並將密碼通知書銷毀。
- 請在收妥提款卡及密碼通知書後，再通過網上銀行、手機銀行、24 小時提款卡服務熱線(852)26166266，或至我行任一分行辦理提款卡激活手續。
- 請在激活提款卡後，儘快通過自動櫃員機或分行辦理更改密碼。
- 請您采取合理步驟妥善存放卡，並將認證因素保密以防止欺詐行爲。
- 請小心保管您的提款卡，應毀滅印有個人密碼的通知書並牢記您的個人密碼及定期更改密碼。
- 請勿直接將密碼抄下或記錄，而不加掩藏。無論在任何情況下，請避免在提款卡上或任何其他經常與提款卡放在一起的物件上，寫上個人密碼。
- 基於安全理由，您應避免使用身份證號碼、出生日期、電話號碼、常見數字組合(如 123456)或其他容易被人猜中的數字組合作為密碼。同時避免以相同密碼來操作其他服務，包括登入網上銀行或其他網址。
- 不應讓任何其他人士使用您的提款卡或認證因素。
- 請您在發現卡有異常或可疑交易后，應儘快通知本行。
- 警方及銀行職員不會要求您透露個人密碼；在任何情況下，切勿向他人透露個人密碼。
- 用自動櫃員機前請留意鍵盤保護罩有否異樣(如被移除或加裝鏡頭)及插卡口和鍵盤有否可疑裝置。如發現可疑裝置，應立即通知有關銀行。
- 當您在自動櫃員機或消費終端機輸入個人密碼時請以手遮蓋鍵盤，請確保您的個人密碼及賬戶資料不會被第三者看見。
- 本行或因應情況向您發放保安提示手機短訊或通訊，如收到後請即時查閱。
- 如您發現或懷疑您的提款卡及/或認證因素遺失、被盜用、外洩或遭未經授權使用，應即致電 24 小時提款卡服務熱線 (852) 2616 6266。
- 在您通知本行您的提款卡/認證因素遺失、被盜取或認證因素或提款卡的資料已經泄露前，您有可能承擔因您的提款卡被用作未經授權交易而產生的有關損失。如您未作出任何欺詐或嚴重疏忽行爲，並在發現您的提款卡/認證因素遺失或被盜取，或認證因素或提款卡資料已遭泄露後，在可能情況下儘快通知本行，您就此類提款卡損失要承擔的責任以本行指明的限額為限，但不應超過 500 港元。此限額僅適用於有關卡賬戶關聯的損失。

小心處理提款

- 當您提款時請避免分心而忘記提取鈔票及提款卡，並應即時點算鈔票數目及保留任何單據。
- 請勿取去他人遺留於自動櫃員機出錢槽的鈔票或插卡口的提款卡，應待鈔票或提款卡自動退回機內。

防範提款卡騙案

- 提款卡騙案包括盜取提款卡或相關資料：姓名、卡號、有效日期及驗證碼/ CVV 碼。騙徒通常會透過惡意軟件、偽冒電郵、釣魚網站，甚至從垃圾箱中的提款卡相关信件獲取提款卡的詳細資料。您在棄置提款卡相关信件前，应先将其撕碎損毀。假如您發覺您的提款卡被盜或曾發生任何未經授權交易，請即與本行聯絡或直接聯絡香港警方。

安全使用境外自動櫃員機

- 您可憑提款卡於境外《銀聯》網絡自動櫃員機提款，每筆提款交易手續費為港幣/人民幣 50 元。如需了解目的地的自動櫃員機位置及能否支援境外提款，可瀏覽《銀聯》網頁：www.unionpayintl.com/hk/
- 為加強保安，所有提款卡於境外自動櫃員機之提款限額預設為港幣 0 元。如需要在境外提款，請預先在離港前透過網上銀行、手機銀行、銀通網絡自動櫃員或 24 小時提款卡服務熱線 (852) 2616 6266 設置有關提款限額及有效限期。 詳情請瀏覽"加强香港境外自動櫃員機服務保安措施的通知": www.ncb.com.hk/nanyang_bank/popup1/ncb_esm_chi.html

安全使用境外刷卡消費服務

- 除可憑卡透過「易辦事」消費，您亦可在香港、中國內地及海外，於接受「銀聯」的商戶刷卡付款。若有需要，您可通過分行、24小時提款卡服務熱線(852)26166266申請關閉境外消費服務

自動櫃員機的正常入卡位

存支票機的正常入卡位

存鈔機的正常入卡位

被裝置讀卡器的入卡位

雙重認證工具

為提升網上保安，本行網上及手機銀行為客戶提供「保安編碼器」及「流動保安編碼」作為雙重認證工具。為了方便視障人士使用網上銀行/手機銀行，本行還提供具有語音功能的"安全密碼器"。客戶必須使用「保安編碼器」或「流動保安編碼」及同意以指定方式接收交易通知，方可於網上及手機進行「指定交易」。有關網上及手機使用雙重認證辦理指定交易詳情，請瀏覽本行網頁：「電子銀行服務 > 雙重認證」。

此外，企業客戶可於任何一家分行申請「保安編碼器」作為雙重認證工具。

流動保安編碼

「流動保安編碼」為您帶來安心及便捷的理財體驗，南商流動應用程式內置「流動保安編碼」功能，啟用後便無須攜帶實物「保安編碼器」。

當您於指定型號流動裝置完成啟用程序後，便可即時透過自訂密碼或「生物認證」開啟「流動保安編碼」，以確認手機銀行指定交易。此外，您亦可使用「流動保安編碼」產生的一次性「保安編碼」/「交易確認編碼」，確認個人網上銀行指定交易。

「流動保安編碼」的注意事項：

- 基於保安理由，客戶只可於一部流動裝置上啟用「流動保安編碼」。並請勿在他人的手機上登入手機銀行及啟用「流動保安編碼」。
- 個人客戶於成功啟用「流動保安編碼」後，所持有的「保安編碼器」(如有)將會自動被停用。如客戶重新使用「保安編碼器」，需要先於流動裝置上停用「流動保安編碼」，並前往本行各分行重啟「保安編碼器」，企業客戶可透過企業網上銀行重啓。
- 請妥善保管已啟用「流動保安編碼」的流動裝置，如發現或懷疑已啟用「流動保安編碼」的流動裝置遺失或被竊，可以透過另一流動裝置停用流動保安編碼。
-

「生物認證」

如您啟用「流動保安編碼」，您可同時於指定型號的流動裝置上登記使用於流動裝置上的「生物認證」（例如：指紋、Face ID）以：

- 登入手機銀行
- 開啟「流動保安編碼」以確認手機銀行指定交易
- 開啟「流動保安編碼」以獲取一次性「保安編碼」/「交易確認編碼」以確認個人網上銀行指定交易

如需了解如何啟用「流動保安編碼」、操作系統要求及兼容流動裝置，請瀏覽：www.ncb.com.hk/1/etoken

請您妥善保管您的生物認證資料，包括且不限於指紋、面貌特徵或其他由本行不時認可的生物特徵等, 並確保指定流動裝置上用作儲存生物認證資料及登記生物認證的保安密碼或編碼保密。如您懷疑或發覺您的生物認證資料被盜用，請即與本行聯絡或直接聯絡香港警方。

保安編碼器

客戶可透過本行網上銀行、任何一間分行申請「保安編碼器」。收到客戶申請後，我們會將「保安編碼器」郵寄至客戶登記的通訊地址。

當您使用「保安編碼器」時，請注意以下事項：

- 客戶必須於本行登記手機號碼及啟動雙重認證功能後，方可申請「保安編碼器」。客戶可親臨本行任何一家分行辦理。
- 當客戶收到「保安編碼器」後，請即登入網上銀行，並按指示啟用「保安編碼器」。
- 客戶不用安裝額外軟件 / 驅動程式，亦不需依賴第三方單位傳輸授權碼，安全可靠。
- 客戶登入網上銀行時，可選擇輸入「保安編碼器」顯示的一次性「保安編碼」，令網上服務倍添安全。
- 客戶於進行「指定交易」時，需於「保安編碼器」上輸入是次交易的資料(如登記賬戶號碼)，從而產生一次性「交易確認編碼」。

- 請妥善保管「保安編碼器」，切勿將「保安編碼器」交予第三者使用或隨意擺放。如有遺失或損毀，請即與本行職員聯絡。

「保安編碼器」是怎樣運作的？

- 每個「保安編碼器」具有獨立的機身編號，並內置資料及時鐘。在您啟用「保安編碼器」後，內置的時鐘將與本行系統同步。當您按下「保安編碼器」的按鈕後，「保安編碼器」即會根據資料及內置時鐘，產生一次性的「保安編碼」。此編碼只於短時間內有效，並只供系統核實客戶身份之用。如您未能於時限內輸入「保安編碼」，則需要重新按鈕以獲取新的「保安編碼」。

如何使用「保安編碼器」？

- 因應不同的交易類別，客戶可使用「保安編碼器」獲取不同的「保安編碼」，並根據網上指示進行驗證
  - 客戶在登入網上銀行或進行「一般交易」時，只需按「保安編碼器」右下方的按鈕，液晶顯示屏即會顯示一組六位數字所組成的「保安編碼」。「保安編碼」只可使用一次，並於短時間內有效。
  - 客戶進行「指定交易」時，請按「保安編碼器」左下方的按鈕，然後使用數字鍵輸入網上以紅色標示的數字資料。輸入所需資料後，請按「保安編碼器」左下角的按鈕，液晶顯示屏即會顯示一組由六位數字所組成的「交易確認編碼」。「交易確認編碼」只可使用一次，並於短時間內有效。

於網上銀行輸入「保安編碼」或「交易確認編碼」後，為什麼仍不能核實我的交易指示？

- 網上銀行未能核實您的交易指示，可能是以下原因所致：
  - 客戶輸入了錯誤編碼
  - 客戶輸入編碼時已超過了編碼的有效時間
  - 「保安編碼器」受到撞擊或曾受過熱、過冷、潮濕或磁場等環境影響
- 請根據網上指示重新輸入一個有效的「保安編碼」或「交易確認編碼」。如仍未能核實交易指示，請與本行職員聯絡，以重設編碼器狀態。
- 若在重設編碼器狀態後，仍未能完成核實程序，客戶可免費更換一個新的「保安編碼器」。

如果「保安編碼器」的液晶體螢幕顯示「BATT」訊息，我應該怎麼辦？

- 「BATT」意指「保安編碼器」的電池將耗完。該電池一般可使用 3 至 5 年，惟視乎使用情況而定。如客戶須更換「保安編碼器」，請親臨本行任何一家分行辦理。請注意，「保安編碼器」的電池不能更換，任意改動「保安編碼器」的內部零件將導致設備失靈。

啟用「保安編碼器」的「一次性密碼」及「完成指定交易通知」手機短訊

- 啟用「保安編碼器」的「一次性密碼」及「完成指定交易通知」手機短訊(如有)只會傳送至您於本行登記的手機電話號碼。即使您已啟動以下的本地手機服務供應商提供的「短訊轉駁服務」，上述短訊亦不會被轉送至其他手機電話號碼：
  - 數碼通電訊有限公司
  - 香港移動通訊有限公司
  - 和記電話有限公司
  - 中國移動香港有限公司

- 請仔細核對本行透過手機短訊及電郵發出的交易資料是否與您在網上/手機銀行上辦理的交易相符，如有任何疑問，請即時與本行聯絡。

常見問題

甚麼是 Secure Socket Layer (SSL) 128 位元加密技術？

- 網上銀行所採用的 128 位元加密技術，為現時在商界廣泛應用的網上保安標準。所有透過網上服務傳送的資料均會以此技術進行加密處理，以保障客戶資料的安全。

當我設定密碼時需注意甚麼？

- 不應使用出生日期、身份證/護照號碼、電話號碼或英文姓名作密碼。
- 不應使用連續三個或以上的相同英文字母或數字，例如「333」、「bbb」等。
- 不應使用順序的英文字母或數字，例如「123」、「abc」等。
- 不應使用與用戶名稱相同的密碼。

我需要在甚麼時候更改密碼？

- 您應定期更改密碼。如客戶於一段時間內未有更改密碼，本行系統將自動提示客戶更改。

我應如何保護個人資料？

- 當您使用網上服務時，可能需輸入個人資料（如身份證/護照號碼、出生日期等）作為額外身份核證，但您應保持警惕，不要隨便向任何人透露上述個人資料，並應妥善處理載有個人資料的文件（如個人信件及月結單等）。

為何需要更新操作系統及瀏覽器？

- 定期檢查及下載軟件供應商提供的「增補程式」，有助修正操作系統或瀏覽器的保安問題，避免您的電腦受到病毒或黑客入侵及盜取資料。

我應如何設定無線網絡的保安措施？

- 無線網路存取點 (Access Point 或「AP」) 應避免太接近門窗，以減低被第三者截收並破解無線網路內容的風險。
- 開啟保護無線網路的設定，切勿向任何人透露您的無線網路保安設定。

使用互聯網需注意甚麼保安措施？

- 如使用電子工具儲存個人資料，請將資料加密，以防止第三者盜取及使用。
- 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資料。
- 關閉視窗系統的「檔案及列印分享」功能，並限制電腦使用者的存取權限，以免第三者透過網絡盜取您的個人資料。
- 切勿下載或安裝非法或來歷不明的軟件，以免感染電腦病毒或木馬程式。在開啟任何外來檔案前，先以防毒軟件進行掃描。

我可以從哪裏獲得更多關於使用網上銀行及自動櫃員機服務的保安資訊？

- 香港金融管理局 –智醒消費者 網上銀行
  https://www.hkma.gov.hk/chi/smart-consumers/internet-banking/#using-internet-banking-services
- 香港金融管理局 – 智醒消費者自動櫃員機
  https://www.hkma.gov.hk/chi/smart-consumers/atms/
- 香港銀行公會 - 參考資訊「智醒消費者 安全小貼士」
  https://www.hkab.org.hk/tc/useful-information/smart-consumer#security-tips
- 香港警務處有關網絡安全及科技罪案
  https://www.police.gov.hk/ppp_tc/04_crime_matters/tcd/
- 政府資訊科技總監辦公室 –「資訊安全網」
  https://www.infosec.gov.hk/tc/

本行熱線及網址

- 客戶服務熱線 (852) 2616 6628
- 24 小時提款卡服務熱線 (852) 2616 6266
- 24 小時電子銀行保安熱線 (852) 2616 6628
- 網址 www.ncb.com.hk
- 個人網上銀行 https://pnb.ncb.com.hk/#/login
- 企業網上銀行 https://cpb.ncb.com.hk/#/login