

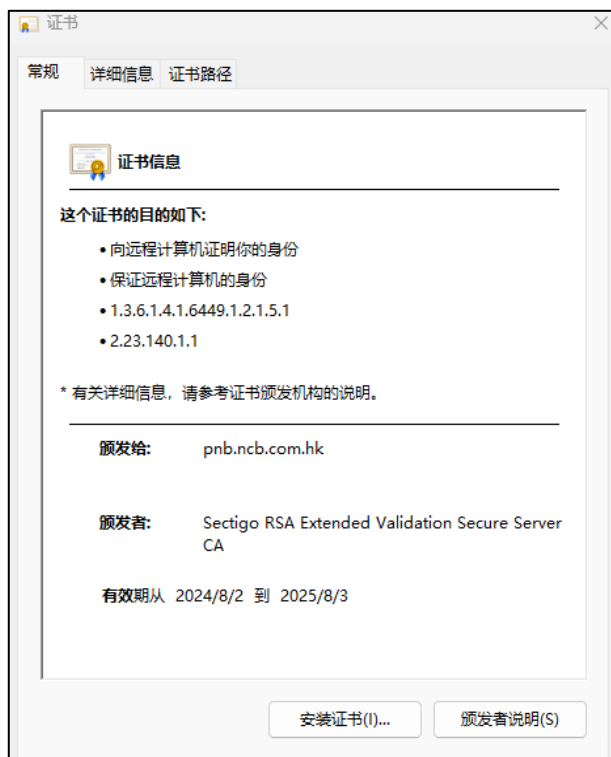
網上保安提示及資訊

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。
- 本行網上銀行及手機銀行設有多種網路安全保護方案，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。
- 本行於網上銀行(個人及企業) 為客戶提供操作日誌查詢功能，支持客戶查閱登入記錄，包括登入時間、位置資訊、和瀏覽器資訊，以便及時發現潛在異常活動。
- 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。
- 如客戶在已經登入網上銀行的情況下登入同一賬戶的手機銀行，則網上銀行服務將被自動終止連線。
- 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。詳情請參閱「雙重認證工具」。
- 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(如電郵地址或通訊地址) 有所變更，請登入網上銀行(設定 > 更新客戶資料)，並使用雙重認證以更新個人資料。若您需更新手機號碼等通訊資料，請前往任何一間分行辦理。

安全憑證

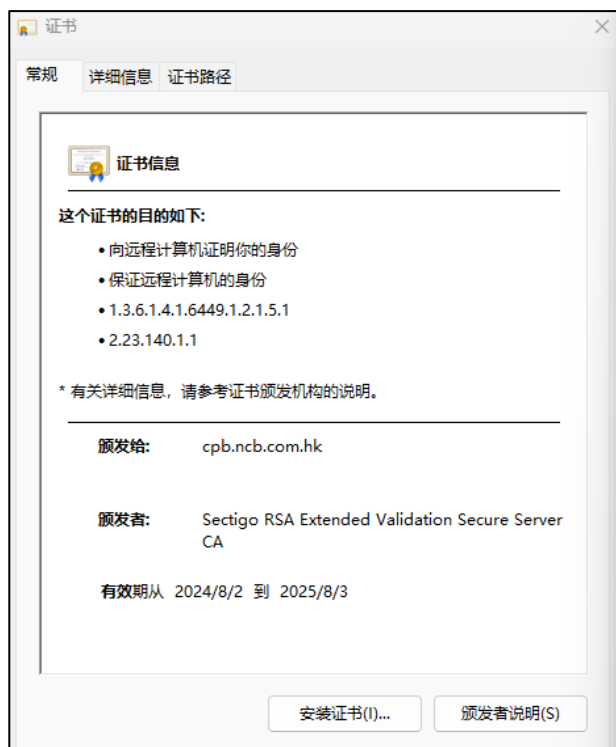
- 本行採用擴展驗證 SSL 證書，讓客戶可透過檢視瀏覽器的地址欄，核定所進入的網頁是否本行的真確網頁。
- Microsoft Internet Explorer 版本 9 或以上瀏覽器的地址欄為綠色，是擴展驗證 SSL 的其中一個保安特徵。如客戶選用 Microsoft Internet Explorer，亦可在網上銀行的登入版面上按「安全鎖」標誌，以查閱證書內容，包括其有效日期及以下資料。請注意，各項資料的顯示方式會因不同瀏覽器版本而有所差異。有關擴展驗證 SSL 證書詳情，請瀏覽證書發行者 Sectigo 的網頁。



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**

- 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)

- **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)

網上保安提示

防範偽造網站

- 請保持警覺並注意任何試圖冒充本行網址或網上銀行服務的偽造網站。客戶必須完全確定瀏覽或登入本行官方網站或網上銀行服務，否則不應提供任何相關的網上服務資料。

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賬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。

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賬戶詳細信息，以進行身份識別或參與投資計劃。客戶不應回復這些消息、點擊任何可疑鏈接、下載任何可疑文件或提供任何信息。

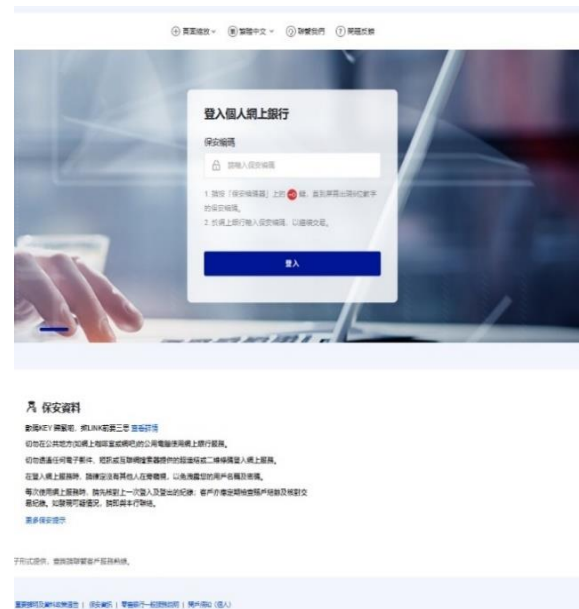
瀏覽器中間人攻擊

- 曾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。

請參閱以下網上銀行/手機銀行登入版面

- **個人網上銀行登錄**

持有「保安編碼器」或「流動保安編碼器」客戶必須以「雙重認證」方式登入，輸入網上銀行號碼/用戶名稱、網上銀行密碼及驗證碼後，點擊「登入」，客戶需進一步輸入由「保安編碼器」或流動裝置上的「流動保安編碼器」所產生的一次性「保安編碼」以登入個人網上銀行。



● 個人手機銀行登錄

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」。



< 請登入

網上銀行號碼/用戶名稱

登入密碼

☐ 記住用戶名稱

忘記網上銀行號碼/用戶名稱或登入密碼?

登入

立即開戶

數碼KEY請緊密，撤LINK前鑒三思

已透過分行申請網上銀行及手機銀行，[立即激活](#)
經此渠道提供的服務之相關條款及細則將以電子
形式提供，查詢請聯絡線上客服。

客戶須知 幫助中心

或者以「生物認證」進入個人手機銀行。



09:27 5G

< 切換用戶



4040****



點擊Face ID識別登入

密碼登入

數碼KEY請緊密，撤LINK前鑒三思

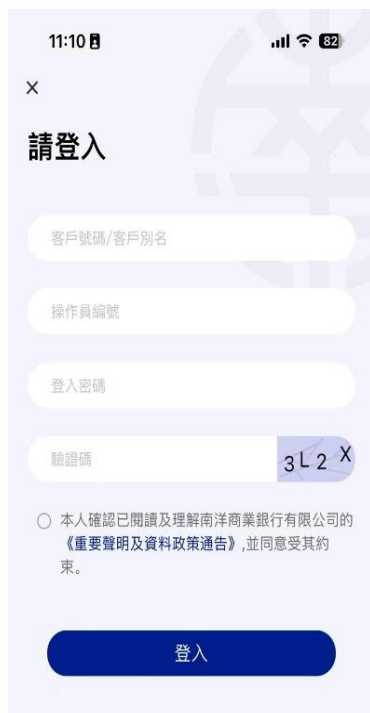
● 企業網上銀行登錄

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「双重认证登入」，需在「保安編碼器」輸入企業網上銀行生成的「挑戰碼」以获取由「保安編碼器」发出的一次性「交易确认编码」以登入企業網上銀行。

● 企業手機銀行登錄

客戶輸入網上銀行號碼/用戶名稱、操作員編號及網上銀行密碼及驗證碼，然後按「登入」。



11:10

×

請登入

客戶號碼/客戶別名

操作員編號

登入密碼

驗證碼 3L2X

☐ 本人確認已閱讀及理解南洋商業銀行有限公司的《重要聲明及資料政策通告》，並同意受其約束。

登入

或者以「生物認證」進入企業手機銀行。



11:09

×

請登入

點擊Face ID識別登入

使用密碼登入

數碼KEY鍵幫助，撤LINK前變三思

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，企圖以各種方式誘騙您提供賬戶資料、密碼、個人資料或信用卡號碼。
- 「網絡釣魚」的騙徒發出虛假電郵、短訊及即時通訊訊息內容出現語法不通、錯別字或拼寫錯誤。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。

妥善保管個人密碼及個人資料

- 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或登入資料，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和賬戶活動記錄，快捷方便。

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。

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（或共用移動設備）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。
- 請定期檢視您的各項服務的交易限額並作出適當調整（如降低轉賬限額）以符合您自身的安全保障需要。