華南商業銀行

網路銀行/行動裝置應用程式安全小秘訣

只要掌握「網路銀行/行動裝置應用程式」操作安全小秘訣，您就可安心享受具備最高安全且操作便利的『華南銀行網路銀行/行動銀行』卓越的數位金融服務。

~~目錄~~

◎ 如何自我保護

1. 設定網路銀行密碼時提高警覺

ANS：

① 為了不讓有心人士輕易猜中您的密碼,提醒您不要使用身分證字號、生日、電話號碼或具規則性排列等容易被猜中的英文字串或數字作為密碼，並應妥善保管及不定期的「變更密碼」也是保管密碼的好方法。

② 切勿使用您在其他網路服務的帳戶名稱及密碼，例如電子郵件或網路簡訊，以免被有心人士猜中。

2. 切勿向任何人透漏或寫下您的網路銀行密碼

ANS：

您應該是唯一知道您的網路銀行密碼的人。請確實保密您的網路銀行密碼，避免書寫於實體卡片上，切勿向任何人透露。

3. 養成定期更改網路銀行密碼的習慣

ANS：

基於保障客戶使用本行網路銀行的安全，您的簽入密碼及轉帳密碼，最少一年內須變更，且到期前一個月，在您簽入網路銀行時，提醒您作密碼變更、避免重複使用相同密碼，並限制您的密碼不可與您身分證字號相同。

4. 設定網路銀行密碼時提高警覺

ANS：

① 您必須清楚知道每一個與您共用電腦的人，同時嚴格限制任何未經授權人士使用您的電腦，並且必須安裝個人防火牆及病毒測試軟體。

② 為了預防您離開電腦過久，以致遭他人竊用，若您欲離開本行網路銀行，敬請務必執行簽退，並關閉瀏覽器，以保障您的權益及帳戶安全。本系統會在您逾十分鐘未做任何交易時，自動執行簽退網路銀行服務。

5. 避免提供個人資料及金融資料

ANS：

一般的電子郵件與網頁並沒有受到安全加密的技術保護，當您無法確認傳輸的資料可受到網路安全機制的保護，千萬不要向任何人透露您的密碼。無論在任何情況下，本行不會詢問客戶的密碼，因此您接獲任何人士的詢問，請不必理會，若您需要與本行連絡，請直接撥打本行客服專線：

中國大陸地區：86-755-25832208 轉存匯部門【服務時間：深圳分行營業時間（週一至週五 9:00~15:30）】；

台灣地區/其他海外地區：886-2-2181-0101【服務時間：24 小時】。

6. 避免在公共電腦及網咖上進行任何網路銀行交易

ANS：

① 當您在公共場所使用電腦時，要記得確實簽退「網路銀行」並關閉瀏覽器，以避免藉由瀏覽器回上一頁的功能，而洩漏資料予第三人。

② 請您不要勾選"記住"「身分證字號/統一編號/網銀識別代碼」和「代號」的功能，以避免洩漏資料予第三人。

7. 確實核對網址

ANS：

① 當您利用網路銀行交易時，在登入網銀時應留意核對所登入的網址，以避免不慎進入假網站。本行之個人網路銀行網址為 https://netbank.hncb.com.tw、企業網路銀行網址為 https://ibank.hncb.com.tw，https 是有「s」加密保護的喔！本行網路銀行是採用 SSL 128bits 最高安全等級加密，以確保客戶的資料在網路上是以加密的機制傳輸。請多自行輸入本行網址，以避免進入駭客仿冒本行之網站，騙取帳戶資訊。

② 您可使用瀏覽器「加到我的最愛」功能，增加以後使用的方便性，並避免通過郵件或其他網站提供的連結登入。您亦可在簽入網路銀行之前，在瀏覽器頁面連續兩次點選金鑰小圖示，檢視此認證是否為發給本行之"netbank.hncb.com.tw"或"ibank.hncb.com.tw"有效認證，以確保進入本行之網站。

8. 妥善保管交易明細表

ANS：

只要您透過網路銀行進行任何的網路動作，如：轉帳、查詢和支付等交易，應保存最後執行動作的資料或予以記錄，如發現異常交易或帳務差錯，立即與本行聯繫，出示網路紀錄，避免造成損失。

9. 遠離來源不明的電子郵件

ANS：

您也許會收到像似好友或是公司的電子郵件，但是事實上有些偽造的電子郵件很有可能會讓你在不知情的情況下，下載病毒程式或是木馬程式，或是將您引導到一個偽造的銀行網站。因此切勿閱讀與開啟不明電子郵件的附件檔案。

10. 其他注意事項

ANS：

(1)請勿將您的密碼揭露予他人。

(2)請安裝防毒軟體及防火牆，並隨時將防毒軟體及防火牆更新至最新狀態，以保護您的電腦避免遭受病毒或惡意程式入侵。

(3)請關閉檔案及印表機分享設定，以避免個人或公務資料外洩，及被植入木馬程式的風險。

(4)請考慮將您的個人隱私等敏感性資料或重要資料使用加密技術（例如：檔案加密…）加以保護。

(5)請不要安裝來源不明的軟體或程式。

(6)請刪除垃圾郵件或連鎖信,也不要打開來自陌生人的電子郵件附件，以避免駭客入侵您的電腦，竊取個人資料。

(7)請勿將您的個人、財務或信用卡等資料留於不熟悉或有安全疑慮的網頁。

(8)請定期備份重要的資料。

(9)請勿使用不能信任的電腦或設備。

(10)簽入網路銀行時應核對您上次簽入的網路位址和時間，如有任何疑慮，請立即與本行聯繫。

(11)執行網路銀行交易後，應檢查您的帳上餘額，如有任何疑慮，請立即與本行聯繫。

(12)本行網路銀行採用高安全性的 EV SSL，若您看到 SSL 伺服器憑證的警告訊息時(例如：此網站的安全性憑證有問題…)，請確認連結網址的正確性，如有任何疑慮，請立即與本行聯繫。

(13)交易完畢後請按「登出」按鈕退出網路銀行，以確保您真的簽退成功。

(14)離開網路銀行後，請關閉瀏覽器，避免有人利用瀏覽器回上一頁的特性，偷窺您查詢過的歷史資料。

(15)為確保您享受到最高水平的安全性，您應使用最新版本的瀏覽器，以支持 SSL 128 bits 加密或更高的加密標準。

◎ 小心網路釣魚（Phishing）

Phishing 與英文「fishing」（釣魚）發音相同，兩者意義也差不多。若引用直接中文典故：「姜太公釣魚，願者上鉤」是最佳翻譯。

網路釣魚是一種新興網路詐騙手法，多半是利用偽造電子郵件與網站作為「誘餌」，輕則讓使用者不自覺洩漏個人資料，成為垃圾郵件業者的名單；嚴重一點，電腦可能會被植入木馬程式，破壞系統或讓重要資訊遭竊。而最危險的情況是：誘騙使用者的銀行帳號密碼、信用卡號與身分證字號等機密資料，釣魚者再伺機偷竊金錢或有價資訊。

網路釣魚所用的誘餌千奇百怪，包括偽裝成知名銀行或線上服務業者通知使用者資料過期、無效需要更新，或者是基於安全理由進行身分驗證，要求使用者重新確認銀行帳號密碼或信用卡號。只要使用者一時不察經由電子郵件指引的網址，連結偽造得一模一樣的帳號登錄頁，就成了數位版姜太公手中「願者上鉤」的肥美大魚。

如果您發現釣魚網站，或者有任何疑慮，請立即與本行聯繫。

◎ 小心詐騙郵件

詐騙集團常假冒銀行名義發出難辨真偽的電子郵件，如您收到此類信件，請主動提供此類不法信件予本行。

☆ 提醒您：

華南銀行絕對不會寄發電子郵件要求客戶揭露帳戶資訊或任何密碼，請提高警覺，千萬不要回覆此類郵件，並立即刪除。若有任何問題或收到任何可疑郵件，請隨時與本行客服中心聯絡：

中國大陸地區：86-755-25832208 轉存匯部門【服務時間：深圳分行營業時間（週一至週五 9:00~15:30）】；

台灣地區/其他海外地區：886-2-2181-0101【服務時間：24 小時】。

1. 什麼是詐騙郵件

ANS：

所有的網路使用者都應該了解什麼是詐騙郵件，雖然它們難以辨識，但一般的詐騙郵件通常都會要求您點選一個連結網址並將您引導到一個仿造的假網站，然後再要求您提供、更新或確認機密的個人資料；為了讓您上當，他們也許會明示或暗示您現在發生了一個可能威脅到您帳戶的緊急情況。

☆ **提醒您：造假詐騙郵件希望獲取的資料：**

＊ ATM 密碼或預借現金密碼。
＊ 信用卡有效號碼。
＊ ATM/信用卡、現金卡卡號。
＊ 身分證字號。
＊ 銀行帳號。
＊ 網路銀行簽入代號及密碼。

2. 辨識詐騙郵件

ANS：

① 登入某冒用偽造的網路銀行時，除 ATM 卡號及密碼外，還要求您輸入其他機密資料。
② 寄發緊急、有時間限制或是要求您提供、更新或確認機密資料(如：登入用的使用者代號或密碼、身分證字號、ATM/信用卡、現金卡卡號與密碼或信用卡到期日)的電子郵件；或要求您在 e-mail 的空格內，填入機密的個人或帳戶資料。

3. 辨識詐騙郵件

ANS：

假如您收到造假詐騙郵件，請隨時與本行聯絡，並將詐騙郵件提供給我們；將有助於我們加緊調查、杜絕這些詐騙郵件，防止更多人受騙。

☆ **提醒您：**

假如您無法認出某筆特定交易內容，或懷疑有人正在竊取您的帳戶資料，請立即與本行聯絡。

◎ 網路詐騙問答集（Q&A）

Q：何謂網路詐騙郵件？

ANS：

網路詐騙郵件就是仿造銀行的規範與設計，事實上卻是在網路上行使詐騙密碼與竊騙個人資料的不法份子所設計的圈套，這些冒用銀行名義所發出的電子郵件，似乎讓使用者也難辨真偽。提醒您千萬不要回應，並馬上刪除。

Q： 收到要求更新網路銀行密碼及資料的不明來源郵件時，應如何處理？

ANS：

當您收到難辨真偽郵件時，除請在第一時間通知本行，並請馬上刪除此種郵件，千萬不可回覆，以免上當到造成損失。

Q： 我該如何保護自己？

ANS：

很多人擔心網路銀行交易的安全性，事實上，只要好好保管您的網路銀行帳戶名稱及密碼，確保您的電腦系統及軟體設有保護裝置，並在上網時提高警覺，就可以安心在網路銀行進行交易。

Q：如何確保網路銀行安全性？

ANS：

一．設定網路銀行密碼時提高警覺：

1. 避免選用容易被猜中的號碼或字母組合，例如：出生年月日。
2. 切勿使用您在其他網路服務的帳戶名稱及密碼，例如電子郵件或網路簡訊，以免被有心人士猜中。
3. 密碼不可是連續數字，且不可使用重複的字元。

二. 切勿向任何人透露或寫下您的網路銀行密碼：應該唯有您才是唯一知道您的網路銀行密碼的人。

三. 切勿向任何人透露或寫下您的 OTP 之一次性密碼。

四. 應妥善保管金融卡、OTP 安控卡，避免遭任何人持有、使用或毀損。

五. 養成定期更改網路銀行密碼的習慣，避免重複使用相同密碼。

六. 保護您的電腦：您應清楚知道每一個與您共用電腦的人，同時嚴格限制任何未經授權人士使用您的電腦，並且必須安裝防火牆軟體及安裝病毒檢測軟體。

七. 避免在公共電腦及網咖上進行任何網路銀行交易。

八. 避免提供個人資料與金融資料。

◎ 貼心的小叮嚀：四勿三要

四勿

- 勿使用具有連貫性等容易被有心人猜到的數字設定密碼。
- 勿向任何人透露或寫下您的網路銀行代號、簽入密碼及 OTP 產生的一次性密碼。
- 勿提供個人資料及金融資料予他人。
- 勿在公共電腦及網咖上進行任何網路銀行交易。

三要

- 要定期更改網路銀行密碼。
- 收到不明來源可疑郵件，請您立即通知華南銀行。
- 要妥善保存交易明細表。

◎ 貼心的小叮嚀：行動裝置應用程式（行動銀行及隨行保鑣）

1. 下載「華銀行動網」、「隨行保鑣」APP，請至 Google Play 或 App Store 下載 APP。
2. 勿隨意開啟電子郵件、即時通訊所傳送之附件檔案。
3. 勿任意安裝第三方及共享軟體，勿點選不明網址及下載不明程式。
4. 安裝防毒軟體，並經常更新病毒碼、應用程式及作業系統。
5. 應妥善保管行動銀行簽入之 ID、代號及密碼，並定期更新，儘量不要寫在記事本等處。
6. 應妥善保管「隨行保鑣」APP 開啟密碼。
7. 勿在公共無線網路環境使用行動銀行及隨行保鑣，不使用行動銀行時應馬上登出。