



使用網路銀行

小 秘 訣



多一點注意，
就能少一點損失



隨著網路蓬勃發展，愈來愈多的金融產品及服務都透過網路銀行提供，而以「網路釣魚」手法詐騙民眾個人資料也層出不窮，因此，消費者在享受網路銀行便利性的同時，更應重視交易的安全性，以及如何妥善保護個人資料（包括：姓名、出生年月日、身份證字號、學歷、銀行帳號等，所有足以識別該個人之資料），以降低個人資料被盜用的風險，保障自我權益。



金管會提供您常見的各式「網路釣魚」手法及使用網路銀行的安全小秘訣，時時謹記這些小秘訣，就可多一層防護網，降低交易的風險。

壹、常見的各式「網路釣魚」手法：

一、發送暗藏木馬之電子郵件：

- * 駭客發送之電子郵件中暗藏木馬程式，用以監測受害者的電腦，木馬程式可記錄受害者電腦的鍵盤敲擊記錄及螢幕畫面擷取圖，因而盜取受害者之電子郵件、聊天記錄及密碼等個人資料。木馬程式並可將受害者的網路行為傳出，以進一步分析利用。

二、註冊相似度極高之網域（網站）名稱：

- * 駭客利用極為相似的字母或數字（如：英文字母小寫l與數字



@ 使用網路銀行 小 秘 訣

1、英文字母n與h等）註冊與「正牌」銀行相似度極高的網域名稱，誘騙民眾誤上假網站，以網站陷阱的方式盜取受害者之「帳號」、「密碼」。

- * 目前申請註冊網域無須受檢核，只要在網路註冊並付款後即可使用，故駭客透過架設假網站以誘使民眾誤入網路釣魚陷阱的案例層出不窮。

三、於假網站植入木馬程式：

- * 當民眾點選駭客架設的假網站後，駭客利用暗藏網頁框架以隱藏惡意程式碼，讓民眾執行其預先上傳的數個網頁程式，再自動連回「正牌」的銀行網站，使民眾沒有感覺任何異樣，但實際上卻已執行了駭客暗藏的網頁程式碼，並已下載多個木馬程式於民眾的個人電腦，作為竊取電腦內個人隱私資料之用。

四、刊登網路關鍵字廣告服務：

- * 駭客於各大入口網站的搜尋行銷服務刊登「關鍵字廣告」，民眾上網搜尋「網路銀行」、「金融資訊」等條件時，搜尋結果的最上方即出現駭客刊登的「關鍵字廣告」。
- * 駭客刊登的「關鍵字廣告」係經過精心設計，一般民眾很難查覺該網站連結係假冒的網站。

貳、「木馬程式」的惡意行為：

一、盜取帳號、密碼及憑證等個人隱私資料：



- * 當民眾連結不明網頁時，就會被下載木馬程式（包括遠端遙控功能及鍵盤側錄程式），側錄其上網時所輸入的帳號、密碼，並搜尋電腦所有磁碟是否存有憑證檔案後，將憑證及鍵盤操作紀錄的帳號、密碼傳送至遠端的駭客主控台。
- * 駭客以取得的憑證、帳號及密碼，登入受害者的網路銀行及各式網站會員帳戶，即可盜取個人資料或任意轉帳。

二、蒐集特定對象資料進行客製化犯罪行動：

- * 犯罪集團針對特定對象進行極為詳盡的資料蒐集並建檔，再利用該等資料運用社交攻擊手法，進一步取得其使用網路銀行、行動電話或語音電話服務所需的個人身分驗證資料。
- * 藉由取得的個人身分驗證資料，假冒受害者以通過客服人員所提問的身分驗證資訊，並套出更多受害者的個人隱私資料，進行各種假冒身分的詐騙行為。

參、使用網路銀行的小秘訣：

一、確認網路銀行網址：

- * 如果您不清楚銀行的正確網址，交易前請先打電話向往來銀行查詢，千萬不要透過其他不明網頁或是電子郵件連結，以免被偽造網站詐騙。
- * 因使用網路服務，而須輸入您的個人



@ 使用網路銀行 小 秘 訣

資料前，請先確認該服務的安全性及合法性，避免進行未經授權的交易，而承擔損失風險。

- * 隨時核對銀行帳戶明細，做好帳單管理，網路銀行交易完成後，應儘速檢核是否正確，一旦發覺或懷疑網路銀行帳戶、密碼未經授權而被他人使用時，立即以電話或其他約定方式通知銀行。



二、網路密碼的設定：

- * 請勿使用「懶人密碼」（如：出生年月日、身分證字號或電話），儘量使用英文字母、數字及特殊符號的組合來設定密碼，此外，也請注意要定期更改密碼。
- * 請勿將所有帳號都設定同樣的密碼，最好每個帳號都有單獨的密碼及登入資料，以減低被盜用的風險。
- * 不要以個人相關資料（如：出生年月日、身分證字號或電話）做為密碼提示的問題或答案，避免犯罪集團蒐集個人相關資料後，即可利用密碼提示猜到密碼。

三、網路密碼的保管：

- * 不要透過未加密的電子郵件寄送網路密碼及個人資料，以免遭駭客截取；且勿將個人隱私資料過度於網路上曝光，以免成為有心人士覬覦之對象。



- * 儘量記住密碼及個人資料，不要寫在記事本、提款卡或存摺等上面，更不要將密碼與存摺、卡片等置放於同一處，避免因未收妥疏忽而被竊取或窺視。
- * 應提高警覺防範詐騙集團套取密碼及個人資料，例如：詐騙集團假冒銀行人員套問金融卡密碼，或假藉通知使用者資料過期需更新，以基於安全考量進行身分驗證為由，而套取帳號、密碼等個人資料。
- * 使用網路服務時，千萬不要因懶惰或怕忘記密碼，而將密碼及登入資料儲存在電腦中，最好每次都自行鍵入較為安全。

四、使用晶片金融卡及網路自動櫃員機(Web ATM)加強網路交易之安全：

- * 以晶片金融卡進行網路交易時，個人密碼不會在網路上傳輸，扣款銀行是依據每筆交易一次有效的交易驗證碼，判斷是否同意完成交易，即使木馬程式或駭客在網路環節中盜錄交易資料、持卡人密碼，也無法製造偽卡或產製假交易。
- * 民眾使用金融機構所提供之網路ATM服務進行交易時，金融機構會以SSL機制確保傳輸資料訊息的隱密性與完整性，可避免傳輸中的資料遭有心人士從中竊取或竄改。



@ 使用網路銀行 小 秘 訣

- * 若未持有晶片金融卡就無法完成網路ATM交易，因此晶片金融卡的安全性明顯強於傳統密碼控制，故請多加使用晶片金融卡於金融機構所提供之網路ATM進行查詢、轉帳、購物、繳費、繳稅等交易。
- * 民眾應於網路ATM交易完成後即取出卡片並妥善保管，避免因忘記取出造成遺失卡片的風險。

五、使用行動電話、個人數位助理(PDA)及無線網路應注意事項：

- * 使用行動電話及個人數位助理(PDA)進行網路交易前，請安裝防火牆及防毒軟體，並設定一個不易被猜解的密碼，同時請記得開啟加密功能，並備份資料，且於不使用或不需要藍芽功能（個人裝置間短距離通訊之無線傳輸技術）時，予以關閉，以避免他人意圖連結您的行動電話及PDA，進而竊取您的個人資料。
- * 設定您的無線網路基地台時，請記得更改預設的密碼和使用者名稱，開啟加密功能，並請小心使用無線網路名稱及廣播網路名稱(SSID)，以減少每個有相容裝置的人可能和您的無線網路建立連結，截取您傳輸資料的風險。
- * 使用公用的無線網際網路前，請關閉「檔案和印表機共享」及「電腦對電腦（點對點）傳輸網路」功能，清除「我的最愛」網路清單，加密所有檔



案，且不要傳送敏感性的資料。

六、使用電腦應注意事項：

- * 請不要經由公用電腦（例：網咖、圖書館等）使用網路銀行服務，如有必要，應隨時小心背後是否有人窺視。
- * 離開座位前或使用網路銀行完畢後，記得按「登出」離開網頁，同時將網際網路選項中的 Temporary Internet Files 及記錄(history)刪除，再將視窗一一關閉。
- * 請勿點選打開來路不明的電子郵件、賀卡及附件檔等，以避免駭客入侵您的電腦，竊取個人資料。
- * 關閉個人電腦之分享檔案夾，避免個人或公務資料外洩，及被植入木馬程式的風險。
- * 確保您的電腦有最新的安全更新程式（或稱 patch 補丁程式）。
- * 請於您的電腦加裝正版安全性防衛軟體（例：防火牆或防毒軟體），並隨時更新病毒碼，以減少木馬程式（後門程式）、病毒、蠕蟲及其他程式惡意碼入侵您的電腦，側錄個人資料。



@ 使用網路銀行 小 秘 訣



※瞭解資訊，到哪裡查？

- * 各銀行網站及客服專線
- * 銀行公會網站「消費者專區」

<http://www.ba.org.tw>

總機 (02) 8596-2229

- * 銀行局「銀行百寶箱」網站

<http://www.banking.gov.tw>

總機 (02) 8968-9999

不當催收檢舉專線 (02) 8968-9722

※心有千千結，到哪裡解？

- * 各銀行客服或申訴專線
- * 銀行公會單一申訴窗口

信用卡專線 (02) 8596-2333

其他業務專線 (02) 8596-2345

債務協商專線 (02) 8596-1627 · 8596-1629

※暴力催收及詐騙等非法行為，向誰申訴？

- * 暴力脅迫催收申訴專線：

內政部警政署110或0800-000-110

- * 反詐騙諮詢專線165

歡迎多加利用！



使用網路銀行 小 秘 訣



行政院金融監督管理委員會 編製