

113 年 5 月公務機密宣導—

防駭客自保之道

最近傳出數家網路銀行的客戶遭駭客盜領，事實上，此事件責任釐清後網路銀行並沒有安全疏失，主要原因是個人的安全防護出現大缺口，資訊安全廠商已經掌握到肇禍的木馬程式，駭客利用鍵盤側錄功能盜取存戶的密碼，將存戶的存款提領一空。

由於木馬程式會偽裝成 IE 網路瀏覽器的名稱 iexplore.exe。它就像錄影機一樣，利用鍵盤側錄，把使用者過去所有打字的記錄全部截取下來，再透過電子郵件的方式傳回駭客的電腦裡。駭客可以輕易地找出使用者過去在網路上輸入的所有密碼，只要登入網路銀行，就可以透過「非約定轉帳」方式將存款提領一空。

駭客是如何植入後門及木馬程式？即駭客利用病毒、系統漏洞、電子郵件，或透過色情、軟體破解或其他惡意網站，偽裝成可吸引使用者執行或下載的應用程式，或利用社交工程如 MSN、Yahoo、Messenger、ICQ 等途徑，植入或散布木馬程式。

全球各地陸續傳出有銀行客戶的電子郵件遭到駭客入侵，並被植入木馬程式竊取網路銀行帳號以及密碼。對此則建議，要盡量避免使用公共電腦上網交易或使用容易猜到的密碼，例如生日；同時，個人電腦也要加強防毒與防入侵功能。

電腦只有掃毒軟體是不夠的，消費者應進一步提升電腦防護等級，如個人防火牆，入侵偵測機制等「整合防護」軟體。設定密碼時，至少高於七位數，盡量混用英文、數字，而且至少包含二個大小寫英文字母或符號，密碼的效期也儘量縮短，最好六個月換一次。