您的密碼夠不夠安全？

設定複雜度較高的密碼，以及在不同系統不要使用同組密碼，是維護資通安全的基本認知。

資料來源：清流月刊中華民國一百零二年十一月號

◎魯明德

在資訊發達的今日，人們的日常生活跟資訊的關係也越來越密切，我們每天所要使用的密碼也越來越多，多到我們可能都記不住。以前可能只要用簡單的幾個數字就可以應付，但因密碼被破解的案例越來越多，很多系統已要求使用者採用複雜度高的密碼，以確保安全。

小潘看到這則新聞，直覺密碼不是都由自己設定的嗎？怎麼會被人家知道？這個疑問放在心裡多日，趁著與司馬特老師下午茶的機會提出。司馬特老師表示：一般人以為系統設定密碼就萬無一失，實際上這是太樂觀的想法；Intel 公司做過實驗，一組由數字及字母組成的 6 字元密碼，在短短的 1.18 分鐘就可以被破解。

小潘聽完立即問道：如果把密碼設長一點，是不是比較安全？司馬特老師接著回應：美國科技網站 Ars Technica 曾經做過實驗，發現就算密碼以加密的雜湊形式呈現，駭客利用暴力攻擊法，仍可在 1 小時內破解超過 1 萬筆的密碼。那麼要怎麼樣才能設出一組較為安全的密碼呢？Microsoft 建議使用者，在建立密碼時，應該注意它的強度，也就是讓它不容易被猜到或是被破解，最好是電腦的所有使用者帳戶都使用強式密碼。強式密碼在設定時，要注意以下幾件事：密碼的長度至少要有 8 個字元，且不能包含使用者名稱、真實姓名或公司名稱，也不能包含完整的單字，與先前用過的密碼也要完全不同。除了強式密碼外，Microsoft 也建議可以用強式複雜密碼，它除了跟前述強式密碼一樣的條件外，密碼的長度要在 20 到 30 個字元之間，而且最好不包含文學或音樂作品中的常見詞句，以及字典中的詞句。

小潘聽完司馬特老師的說明，隨即想到曾在網路看到單因素

認證及雙因素認證，一直弄不懂是什麼意思，便把這個問題也順便提出。

司馬特老師接著說明，大部分的入口網站採用單因素認證，當使用者需要取得資源或登入系統時，網站會提示用戶輸入帳號和密碼。系統採用加密方式，將帳號和密碼傳送到伺服器端進行比對，其中帳號用來辨識使用者的身分，密碼就是所謂的單因素認證；如電子郵件、線上遊戲等系統的登入機制都屬於這種單因素認證。雙因素認證則是結合使用者所知道的「內容」與所擁有的「物品」兩種因素，作為身分識別之用，當使用者通過此兩種因素認證時，就能登入應用程式或網站；其中使用者所知道的「內容」，包括密碼和身分證號碼等，而所擁有的「物品」則是指動態密碼卡、IC卡、磁卡等。日常生活中最常見的雙因素認證，即是銀行或郵局的自動提款機，使用者到提款機前，必須先插入提款卡，此即為使用者所擁有的物品，再輸入個人所設定的密碼，此即使用者所知道的內容，兩項認證都要同時通過，才能存取帳戶的款項。

隨著網路的發達，個資外洩所造成的盜刷事件也層出不窮，但是民眾透過網路銀行、行動銀行進行繳費、轉帳的頻率也越來越多，而且已成為習慣，為了避免個人資料因為使用網路服務而外洩，於是有銀行業者推出網路銀行簡訊動態密碼確認機制，作為線上交易時的安全機制。簡訊動態密碼的服務，是當客戶透過網路銀行或行動銀行進行特定交易時，系統就會自動發送一封內含6位數交易驗證碼的簡訊到客戶所登記的手機號碼中，客戶必須在交易過程中，輸入該組6位數交易驗證碼，才能完成交易驗證。這樣的防護機制是為了確保該筆交易是由客戶本人進行而非遭他人盜用，以確保客戶的交易安全性。

小潘聽了司馬特老師的一番說明，對於密碼的安全有了進一步的認識。最後，司馬特老師還是語重心長地做了結論：由於資訊科技的進步，各種維護資訊安全的技術不斷被研發出來，但是維護密碼的安全至少要做到兩點：不同的網路系統要有不同複雜度的密碼、不要在所有系統上使用同一組密碼。