

# 資訊時代應具備之資訊安全基本技巧- 身分鑑別

蒲樹盛(Peter Pu)

peter.pu@bsigroup.com

BSI 英國標準協會 副總經理(Vice President)

IRCA 國際註冊主導稽核/主任講師

過去在BSI的電子報中，個人多針對國際標準(International Standards)或管理制度(management Systems)之理論及發展趨勢撰文介紹。近來有些不同想法，許多客戶或讀者不一定具備應用機會，所以，希望透過淺顯易懂之方式，將一些重要但簡單之觀念提出，相信可以為更多讀者提供一個資訊安全新知及應用技巧的管道。

## 資訊時代風險大增

資訊化加速全球化現象，幾乎所有作業均離不開電腦與網路，創造出許多機會，但也產生許多威脅，其中「資訊安全」便是最重要的議題之一。全球有許多案例顯示，愈來愈多的風險是經由人為蓄意或疏忽，而導致資訊安全事件所產生的傷害，包括：歹徒利用個人資料進行金融詐騙、竊取商業機密、竄改個人或商業資料獲取利益、蓄意破壞、各種天災等，其他類型之資訊惡意行為，如網路釣魚(Phishing)、駭客入侵及木馬程式等均愈來愈普遍，影響也越來越大，技術日益複雜，甚至造成組織服務中斷等重大傷害。就個人或組織而言，若不能確保敏感資訊受到良好保護，一旦遭受危害，則可能會造成無可彌補之遺憾！

## 個人資訊安全基本防護技巧-身分鑑別

許多不法活動均是透過「未經授權存取」導致。在資訊安全的領域中，常會聽到兩個名詞：識別(Identification)與鑑別(Authentication)。其中「識別(Identification)」是用以瞭解使用者為誰，如：登入網路銀行時，會要求使用者輸入帳號或ID；但如何確認該「登入者」確實是帳戶擁有者本尊？便須透過「鑑別(Authentication)」機制進行確認，而最常見且簡單之鑑別方式便是要求輸入通行碼>Password)(一般口語常稱為密碼)。但因使用者對於通行碼之使用過程及方式過於輕忽，使用簡單之傻瓜密碼或懶人密碼(如：4個0、4個1、1234、生日、電話號碼或身分證前後幾碼)，或英文字典單字，或將通行碼直接抄在紙上置於螢幕或鍵盤下，均極易導致有心人員冒用「您的身分」而通過「鑑別(Authentication)」機制成功登入。

保護好身分鑑別機制是十分重要的，今天介紹幾種身分鑑別機制，希望大家可以選擇最安全的方式保護自己：

1. 使用安全強度足夠的密碼：

建議將帳戶分為不同的安全等級。某些網站的帳戶一定要使用安全強度較高的密碼，包括字元長度(建議 8 碼以上)、內容複雜度(包括文字數字或符號)、定期更換(可有效防止遭冒用)，例如：銀行、購物網站或組織重要系統(如學籍系統)。而有些網站則比較不重要，例如：同學部落格或論壇等不會包含個人隱私資訊之網站，便可使用一組容易記憶的密碼。一般以下分享幾種簡易之安全強度足夠的密碼記憶方法：

- 字串對應法: 一般太長的字串記不住，才會想把它記下來，但這是非常不安全的。所以我們可以記憶一組短字串(如：我愛你)，再利用鍵盤輸入對應方式(如：注音輸入法ㄨㄟㄩˇㄛㄟㄩˇ)，將密碼轉為ji394su3.
- 數學公式法: 將數學計算轉成密碼，例如： $80*12=960$ ，即為 9 碼包括數字及符號之密碼。
- 雜湊字元法：在一組安全密碼中再多加幾個字。例如：原本的密碼是ji394su3，若用於校務電子郵件時，可以加上mail字串，雜湊至原密碼中(我以加底線幫助識別)，成為 maji394su3，用以區隔不同帳戶之用。

切記：不可用明文方式記載密碼，不可用電子郵件或經由他人轉交密碼，不要在公用電腦上(如：機場、車站)輸入密碼！

2. 雙因素鑑別 (two-factor authentication)：結合密碼和第二項鑑別載具，如：IC 晶片卡或自然人憑證、或隨機產生的一次性使用密碼(OTP, One Time Password)。目前已應用在銀行網路 ATM 等金融高風險活動。甚至有三條件的認證系統：再加上一項生物鑑別辨識，例如指紋、虹膜、臉型辨識等。短期內生物鑑別辨識可能還無法成為主流，原因為費用較昂貴、可靠度及使用者接受度不足等因素。
3. 憑證符記(token)：設計特定之電子憑證載具設備，發給特定使用者供鑑別之用。目前已應用於網路遊戲使用者，避免帳號密碼或寶物被盜狀況。
4. 位址鑑別(IP)：原理是核對使用者上網的所在位址(IP)，未經授權者便無法於取得密碼後於其他地點登入。不過，使用者也因此只能在固定地點上網登入。保障多一分，但限制也多一點！

試想，當他人假借您的身分登入系統，竊取或竄改重要資料後，後果您如何承擔？若因此涉及法律，情何以堪！所以選用安全的密碼是保護資訊安全的第一步！