密碼安全設定

2012 年 3 月

手冊內容

§ 前言

1. 密碼強度不足，使你危機四伏
2. 剖析不良的密碼設定方式
3. 密碼安全設定原則

§ 前言

密碼遭破解，個人資料遭盜用及隱私相片曝光

隨著資訊科技與網際網路的普及，越來越多的生活習慣產生了改變，人們開始習慣將生活的點滴、相片等資訊，透過網路與親朋好友分享，雖然享受著資訊科技所帶來的方便，但此同時，許多潛藏的危機亦開始不斷影響著我們。

新聞時常報導某個網路相簿遭人破解，存放的私密照片與影片外流，被大量下載及轉錄，追根究柢即因為網路相簿沒有設定密碼，或密碼太過於簡單，才會遭人輕易破解與散布。

根據國外研究指出，在實際資安測試中，發現企業商用系統中有近 5% 的密碼設定為 Password1，非常容易就遭受外部入侵成功。這種安全強度不足的弱密碼問題，讓入侵者輕鬆冒用身分，取得合法存取資料的權限，更讓資訊安全防禦設備形同虛設，所造成的危害不可輕忽。

根據資安報告指出，資訊外洩事件中，29%是利用薄弱、易於猜測的密碼入侵，是 2011 年排行第一的資訊外洩根源。此外，更有高達三分之二的受害單位，在收到第三方通知時才驚覺自己的資料已遭外洩。由此可知，密碼安全設定的問題，已經是資訊安全防護的重要議題！

本手冊將說明密碼設置的安全原則，以及如何強化密碼強度的小撇步，提醒大家一定要好好管理自己的密碼，不要讓自己因為一時疏忽成了無辜的受害者。

2. 密碼強度不足，使你危機四伏

在電腦與網路世界裡，我們透過不同的帳號，以代表或區別各自的身分，而密碼就是用來驗證身分的正確性，簡單來說，帳號就像我們住的房子，而密碼就是大門的門鎖，如果帳號沒有設定密碼，就像未上鎖的大門，陌生人都可以輕易的進出，對安全造成極大隱憂！

密碼就是一道鎖，越是重要的資料，越要有嚴密安全的防護！

「暴力破解」輕鬆解開弱密碼

所謂的「暴力破解」，就是利用電腦程式，反覆不斷地嘗試輸入密碼，直到密碼被破解為止。

因為密碼是由字元所組成，若密碼長度太短，或是未混合使用數字、英文大小寫或特殊字元，這種強度不足的「弱密碼」很容易在短時間內就被破解囉！

下表是密碼被暴力破解的實驗統計結果，如配上不斷成長的電腦運算能力，若要破解強度不足的弱密碼，還真是易如反掌！

密碼長度	英文字母 (26 字元)	英文字母+數字 (26+10 字元)	英文字母大小寫 (52 字元)	含特殊符號字元 (96 字元)
4	0	0	1 分鐘	13 分鐘
5	0	10 分鐘	1 小時	22 小時
6	50 分鐘	6 小時	2.2 天	3 個月
7	22 小時	9 天	4 個月	23 年
8	24 天	10.5 個月	17 年	2287 年
9	21 個月	32.6 年	881 年	21 萬 9000 年
10	45 年	1159 年	45838 年	2100 萬年

1. 剖析不良的密碼設定方式

大部分電子信箱、網路相簿、網路遊戲或聊天室等線上服務皆採用會員制度，為了使用這些服務，總是得申請一堆的帳號，連帶著就有無數組密碼要記住，有時因貪圖方便，或是怕記不住密碼，在設定密碼的時候，往往會不自覺地犯了許多錯誤。

情況 1. 千萬要避免的密碼設定方式

下列為嚴重錯誤的密碼設定方式，這種設定方式極為不安全，請千萬要避免：

- 不設定密碼（空白密碼）
- 使用簡單字元組合（如 1234、abcd、111111 等）
- 密碼與帳號相同
- 使用生日、身分證字號、英文名字等個人資料
- 使用公司、部門、單位名稱
- 使用與系統管理相關專有名詞（如 admin、password 等）

情況 2. 應盡量避免的密碼設定方式

以下是一般人常使用的密碼設定方式，雖然便於記憶與使用，但密碼強度仍稍嫌不足，設定密碼時應盡量避免：

- 英文單字或片語（如 superman、iloveyou 等)
- 隨意數字組合
- 連續字元組合（如 mnopqr、87654 等）
- 鍵盤順序組合（如 asdfgh、1qaz 等）

一些強度不足的密碼設定方式，仍然可以交叉運用，輕鬆地讓你的密碼能夠方便好記，又可符合安全強度要求喔！

3. 密碼安全設定原則

(1) 不使用懶人密碼

懶人密碼就是使用者貪圖一時方便，使用極為簡單的密碼設定（如 123456），甚者是使用空白密碼，或將密碼與帳號設定相同，而這種毫無強度的密碼設定，是十分危險的！

(2) 長度與複雜度

密碼長度應至少 8 碼以上，並且混合大小寫英文字母、數字及特殊符號，一個複雜度符合安全要求的密碼應至少包含：

- 一個大寫英文字母
- 一個小寫英文字母
- 一個數字
- 一個特殊字元，如：！@ # $ % & 等

(3) 密碼無明顯含義

密碼設定應避免單純使用單字或片語，因為容易遭到字典檔攻擊而被破解，或是有特殊意義之名詞組合（如：家人的姓名、生日或興趣），皆使得意圖入侵者有跡可循。

(4) 避免重覆

不要為了方便，把自己的所有網路服務都設定成同樣的帳號與密碼！這樣一來，反而提供了有心人士一個最方便的機會盜用與假冒你所有的網路身分。

(5) 定期更新

除了密碼設定要符合安全性要求，定期更新也是密碼安全防護的重要一環，建議應至少每 60~90 天重新設定新密碼。

密碼設定小撇步，善用技巧簡單好記

為確保密碼不會輕易遭受破解，設定密碼時請務必遵循前述的安全原則，此外也可以參考以下幾種方式，讓複雜的密碼變得輕鬆好記囉！

- **穿插法**

  以兩個英文字或數字穿插，不過若使用兩段數字的穿插就沒有意義囉！

  範例：Love 與 2012 穿插後變成 **L2o0v1e2**

- **字母位移法**

  將英文字母位移數個字，如 A 向後位移一位變成 B，D 向後位移兩位變成 F。

  範例：LOVE 往後位移一個字母變成 **MPWF**

- **順序位移法**

  將有意義的字面重新排列順序，可降低字面的明顯意義，如將奇數與偶數字元對調，或以任一固定序列進行位移。

  範例：將 LOVE 字元以 2143 重新排序變成 **OLEV**

- **鍵盤位移法**

  利用電腦鍵盤之位置進行位移，如 A 向右移兩位為 D，B 向左移一位為 V。

  範例：將 LOVE 在鍵盤向左位移兩個字母變成 **JUXQ**

- **替換法**

  利用字形或發音相近的英文字母與數字交互替換，例如可以將英文字母 O 換成數字 0，字母 S 換成數字 5。

  範例：LOVE 替換後可變成 **L0V1**

- **輸入法變化**

  其實中文輸入法即是種最簡單又有效的變換方式，只要把特定的幾個中文字，採用不同的輸入法鍵入，即是一串旁人難以理解的密碼囉！

  範例：將「我愛你」採注音輸入法成為 **JI3 94 SU3**，倉頡輸入法則為 **HQI BBPE ONF**，無蝦米輸入法則為 **IX ENHP PNS**。

- **掐頭去尾法**

  利用一段話（或一段歌詞），取每個英文單字字首當成密碼。

  範例：An Apple A Day Keeps The Doctor Away 取第一個字就是 AAADKTDA。

只要你能靈活運用以上幾種變換方式，設定簡單又好記的安全密碼一點都不難喔！

王大明 生日為 2/9

1.使用無蝦米輸入法替換

王大明 → KEDNDUE

2.加入生日日期 2/9

→ KEDNDUE2/9

3.以 1357924680 順序位移

→ KDDE/ENU29

4.再將雙數的英文字母變小寫

→ KdDe/eNu29

如此一來要破解密碼就很困難了，而且只要記住原始的明文和自己的編碼規則就行了！