# 密碼強度 Strong Password

## 前言：

現今日常生活中，你的提款卡需要密碼才能領錢，網路銀行需要帳號密碼才能登入，網路購物同樣需要帳密，學校 mail 也一組密碼，其他 mail 又是一組，一個人從頭到腳、從家裡到戶外，記再多組帳號密碼都不夠，你覺得你真的記得住嗎？況且依據當代人的生活模式，帳號在很簡單的情形下就可以被查詢的到(例如帳單、收據及共用電腦)，但唯有密碼是絕對需要花時間破解的。

在走進了電腦的世界裡，你所遭遇到的第一道防線也是所有資安環境最重要的一環，那就是「密碼管理」，對駭客而言，密碼太過複雜他會選擇先跳過（不代表不偷）先找比較好下手的處理，就跟小偷偷車一樣，大鎖太普通，一下就偷走，太難會選擇放棄，本篇將帶領各位瞭解密碼管理的重要性。如何用中文的好處與鍵盤的排序建立一組強壯、複雜、優質的密碼。

## 密碼管理重點：

在開始介紹密碼管理前，我們先來認識何謂「字典檔」，它是一個文字檔（.txt），簡單的說，只要在英文字典內可查到的英文單字大多都會被放在這個文字檔內。裡面放置的就是一般所謂的懶人密碼，也就是單純常用的英文單字*、數字組合*、英數組合*，每個單字與數字組合都是工具要嘗試破解的「Key」，簡單的說只要你的帳號密碼出現在字典檔中,被破解的風險會相對的提高。

英文單字：以系統具有權限的帳號為例，administrator、admin、root、guest、你的英文名字、帳號名字、主機名稱亦或是鍵盤上的橫列直排的排列等。

數字組合：1234、生日組合、身份證字號、市內電話、手機、分機、各種 ID 或員工編號等。

英數組合：舉個例子來說，英文名字 John 再加上生日 65 年 03 月 12 日，就可以得到如下組合，john650312 或 650312john 等。

**優質（強壯、複雜）密碼設定原則：**

**例：password -> P@ssw0rd**(僅供參考，此字串組合已列在多數字典檔攻擊內)

1. 設定**至少** 8 個字元的密碼。
2. **避免**重複或連號的字母、數字。（aaaccbb、112233）
3. 使用**數字、英文字母大小寫、符號**穿插的字串。(a、A、[~!@#$%^&*]、)

**管理重點：**

1. **至少**三個月更換一次密碼。
2. **避免**重複設定已用過的密碼。
3. **避免**使用字典查詢得到的字串，意即常見之單字。
4. 避免使用太過複雜，自己也記不住的密碼。

5. 不可用明文方式記載密碼。
6. 不要告訴別人，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、網咖等）輸入密碼並儲存於公用電腦上。

接下來跟各位介紹如何用簡單的中文句轉換成強壯、複雜、優質密碼

例1：「嘉義大學」簡單的四個中文字如何變成密碼？

嘉義大學 -> ru8u4284vm,6 看得出來嗎？來個分解步驟對應鍵盤注音輸入嘉「ru8」義「u4」大「284」學「vm,6」這樣就符合上面說得八個字元以上，沒有連續重複，英數符號混雜，這裡再做些許修改，把某些英文字母的小寫改成大寫，要破解就又變得很困難。

無蝦米輸入「嘉義大學」對應出來是什麼呢？「yorovbkidnsnz」，嘉「yorov」義「bki」大「dn」學「snz」，那再把出現「o」的改成「0」，其他英文字母找一些改成大寫就可以變成一組「中等優質密碼」，相信英文字典不會有這個字的。

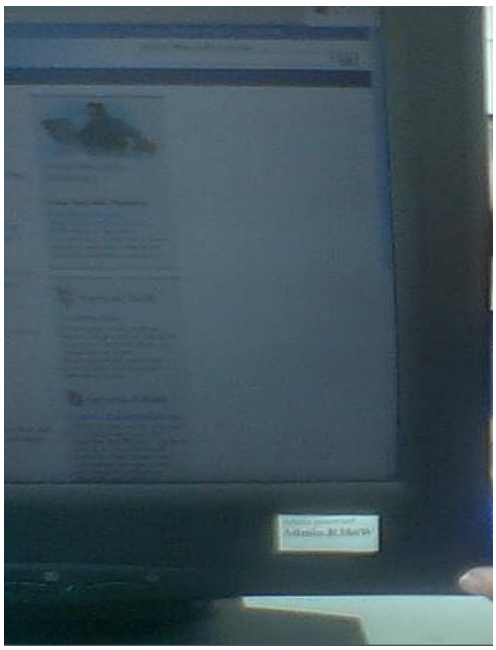
那如果倉頡輸入會變成怎樣？嘉義大學「grtrtghqikhbnd」嘉「grtr」義「tghqi」大「k」學「hbnd」。

舉這樣的例子字典檔破解或是暴力破解都是需要一段很長的時間才解的出來，等解出來你已經又換一組新密碼了。

註：中文輸入習慣會按空白鍵選字，密碼輸入時就不要再按空白鍵了，直接字母對應即可，雖然以密碼來說空白鍵是一個字元，但是建議不要按空白，以防所要登入系統被鎖住，造成失效。

例2：就請各位想想自己的口頭禪，或是自己好記得中文字詞或一句歌詞，對應鍵盤會有什麼組合？

當然如果單純只是數字、英文大小寫、符號雜湊的密碼是記不住的，當然有人會想出好記得方法（懶人作法），請看以下的錯誤示範。


密碼很好記吧！而且大家都幫你記住了。千萬不要這樣拿memo紙把帳號密碼貼在螢幕邊邊、鍵盤底下、電話底下、電話聽筒。千辛萬苦想出來5年才會被破解的密碼，結果有心人士看到，3秒鐘就把你5年的心血都捲走了。當然，在此提醒，沒有破不了的密碼，只是破解的時間長短。

優質密碼檢測網站，這是可以測試你設定的密碼優不優、強不強、好不好

中央研究院計算中心密碼強度檢測：
http://security.ascc.sinica.edu.tw/infosec-test/testpass.php
微軟：
http://www.microsoft.com/taiwan/athome/security/privacy/password_checker.mspx
The Password Meter：http://www.passwordmeter.com/

## 多一點確認，少一分損失

資料提供：數聯資安（圖片來源）
國立嘉義大學電算中心