公務機密宣導

如何提升密碼強度

新聞案例

根據行政院最新一期資安月報，110年12月事中資安事件通報數量較前年同期增加25.49%，主因是駭客竊取郵件帳號密碼有升溫跡象。月報指出，近期駭客以帳號異常行為通知為由，**寄送含有釣魚網站連結的社交工程電子郵件**，企圖騙取政府機關人員電子郵件帳號密碼...。

月報同時提醒，**110年政府機關屢次發生因使用如身分證字號、生日、電話，或是123456等簡單規則的弱密碼，導致資通系統遭破解、機敏資訊外洩之情事**，各機關資通系統應禁止使用弱密碼，並依循GCB密碼原則，且評估重要資通系統採用多因子驗證機制，以及帳號多次登入錯誤應有鎖定機制...。

（摘自：中央社新聞「駭客攻擊頻傳 政院籲機關禁用簡單密碼」，111年1月15日 ）

案例分析

在資訊發達的今日，日常生活跟資訊的關係也越來越密切，每天要使用的密碼越來越多，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。

但是，即使系統要求如此嚴謹，仍然常發生密碼被破解的危安事件。一般人以為系統有設定密碼便萬無一失，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！

案例分析

Microsoft建議使用者，在建立密碼時應該注意它的強度。**「強密碼」**在設定時，要注意以下幾件事：**密碼的長度至少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**，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。

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等強度不足的「弱密碼」，很容易在短時間內遭到「暴力破解」——亦即利用電腦程式，反覆不斷地嘗試輸入密碼，直到密碼被破解為止。

另外，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**。

改善及策進作為

1. 千萬要避免的密碼設定方式：極為不安全的密碼

(1)不設定密碼(即使用空白密碼)、使用簡單字元組合(如1234、abcd、111111)、密碼與帳號相同。

(2)使用生日、身分證字號、英文名字等個資；公司、部門、單位名稱；系統管理相關專有名詞(如 admin、password 等)。

2. 應盡量避免的密碼設定方式：密碼強度稍嫌不足

(1)英文單字或片語(如superman)、連續字元組合(如mnopqr、87654)、鍵盤順序組合(如 asdfgh、1qaz)。

(2)隨意數字組合。

改善及策進作為

3. 密碼安全設定原則

(1)**具有足夠長度與複雜度**：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。

(2)**密碼應無明顯含義**：密碼設定應避免單純使用單字或片語，或是有特殊意義之名詞組合(如家人的姓名、生日或興趣)，以免意圖入侵者有跡可循。

(3)**不同帳號之密碼避免重覆，各密碼並應定期更新**。

改善及策進作為

4.透過交叉運用數種單獨存在時強度不足的密碼設定方式，讓密碼能夠方便好記，又符合安全強度要求！可參考以下方式：

(1)**穿插法**：例如以兩個英文字或數字穿插，如將Love與2012穿插後變成L2o0v1e2。

(2)**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LOVE字元以2143重新排序變成OLEV。

(3)**替換法**：利用字形或發音相近的英文字母與數字交互替換，例如可將英文字母O換成數字0，字母S換成數字5。如：LOVE替換後變成LoV1。

資料來源：

1.中央社新聞「新聞駭客攻擊頻傳 政院籲機關禁用簡單密碼」，111年1月15日
https://www.cna.com.tw/news/aipl/202201150174.aspx
2.清流月刊102年11月號「您的密碼夠不夠安全？」
https://www.mjib.gov.tw/FileUploads/eBooks/bc8a61b1157b4078b1fa88c76bbe1320/Section_file/d80cf048687c4c5e89545fbb1580e2ba.pdf
3. 教育部全民資通安全素養推廣計畫「密碼安全設定學習手冊（一般民眾版）」
https://isafe.moe.edu.tw/sites/default/files/03_%E5%AF%86%E7%A2%BC%E8%A8%AD%E5%AE%9A%28%E4%B8%80%E8%88%AC%E6%B0%91%E7%9C%BE%29.pdf

——花蓮縣政府政風處關心您！