



# 交通部公路總局臺中區監理所政風室 公務機密維護宣導

## 機關電子郵件密碼「鍵盤排序」易遭駭客破解

行政院最新一期資安月報指出，某機關4月被發現電子郵件帳號密碼外洩事件，經機關調查發現外洩帳號密碼多採用鍵盤位置排序，例如1qaz@WSX，雖符合長度及複雜度要求，仍易遭駭客破解，建議相關機關應加強宣導避免採用鍵盤排序設定密碼或常見字符轉換的字母，降低密碼遭破解風險。

最新一期資安月報指出，4月蒐整政府機關資安聯防情資共6萬9964件，經分析資安聯防情資，可明確辨識的威脅種類，第1名為掃描刺探類佔62%，主要是外對內連線大量阻擋事件及外部主機執行掃描探測攻擊；其次為入侵攻擊類佔16%，主要是網頁攻擊行為及國外IP攻擊行為；第3名是政策規則類佔15%，主要是帳號持續登入失敗。

資安月報指出，近期Java應用程式框架Spring Framework遭揭露存在遠端程式碼執行漏洞，發現近期若干外部IP嘗試探測政府機關Spring框架相關漏洞，傳送夾帶惡意字串的參數請求，以及使該框架處理資料綁定(Data Binding)時執行遠端程式碼，如新增網頁後門等，技服中心已透過聯防監控月報，提供相關防護建議予各機關參考。

另外，資安月報提到，4月某機關電子郵件帳號密碼外洩，經調查後發現，外洩帳號的密碼多採用鍵盤位置排序，如1qaz@WSX，雖然符合長度及複雜度要求，仍易遭駭客暴力破解。

月報表示，政府機關規定使用者密碼設定須符合複雜度原則，駭客常採用密碼暴力破解，後續已請使用者修改外洩帳號的密碼，並加強內部宣導，避免採用鍵盤排序設定密碼，或者是常見字符轉換的字母，例如P@ssw0rd。

根據資安月報統計，去年政府機關多次發生因使用身分證字號、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，已要求各機關資通系統應禁止使用弱密碼，降低駭客入侵產生的資安風險。

資料來源：【中時新聞網 (2022-06-04 發表)】

<https://www.chinatimes.com/realtimeneews/20220604001469-260407?chdtv73173>