

麥寮鄉公所政風室 115 年 9 月機關安全維護宣

1. 遠距辦公資安小錦囊-遠距會議篇

司法機關根據檢舉，發現包括健保局中部分局，以及台北市、縣警員、移民署官員，涉嫌將政商名流、大牌藝人等包羅萬象的個人資料，賣給業者牟利，觸犯貪污及違反電腦處理個人資料保護法等罪。據指出，本案是因某些政商名流私密資料遭媒體曝光，且無端接到詐騙集團電話指名道姓，甚至把個人住處、家庭狀況、健保卡等個資詳實說出後，才警覺到個人資料已遭外洩，向檢察及調查單位提出檢舉後，案情才爆發出來。

據瞭解，檢察及調查單位搜索查扣到的證物，至少有千筆以上的個人資料，包括上市公司負責人、也有政府高層官員，甚至連大牌藝人也涵蓋在內。由於被害人的身分大都特殊，檢察及調查單位均堅持封口，不肯透露。至於被洩漏的資料，包括入出境、戶籍住所、身分證字號、電話、車籍及婚姻狀況等。

探究本案，不論最終偵辦結果如何，僅就相關公務人員說詞觀之，不論係因人情請託或自身不察遭假冒上級或其他單位長官人員矇騙而代為查詢民眾個人資料，其行政違失已甚為明顯，更遑論如係將民眾個人資料提供予業者並收取酬金，則恐將導致刑責之究罰，殊值同仁作為借鏡，以免誤蹈法網。

公務員應依規定使用查詢資訊系統，並注意民眾個人資料之保護，切勿擅自或接受人情請託代為查詢個人資料，如係上級長官要求代為查詢，應先行確認身分並依規定辦理，避免發生資料外洩或遭不法利用情事；同時應依法行政，嚴守工作立場，潔身自愛，切不可因貪圖不法利益而觸法。

2. 遠距辦公資安小錦囊-遠距會議篇

越來越多企業單位讓員工遠距辦公，來因應企業可能遭遇之各種緊急事件。因此遠端視訊會議相關系統的使用量遽增，引發相關資安議題。身為遠端視訊會議的使用者，我們該如何做好資安防護呢？

以下八點資安防護提醒：

1、選用無資通安全疑慮的視訊會議軟體

2、選擇可信賴的下載軟體管道

在可信賴的官方網站或 app store 下載軟體，以避免安裝到含有惡意程式的偽冒軟體或 APP。

3、謹慎確認會議邀請與連結

來路不明的會議邀請或連結，極有可能是惡意連結，請勿點選避免受駭。

4、限制會議參與者

所有的會議建議設定密碼限制，並由會議發起人於會議開始前確認參與成員的身分。

5、避免在公開社群分享會議連結

請直接提供給與會者連結，如此可以最大限度地避免不相關的人員得知會議並混入會議中竊取商業機密。

6、謹慎使用螢幕共享的功能

會議中若需使用螢幕共享的功能，需限制特殊指定人士才可使用並共享。

7、更新至最新的軟體版本

8、確保使用設備的安全性

使用者參與線上視訊會議的資訊設備以及網路連線方式，皆需符合企業訂定之資安標準(ex: 限定使用資訊設備、不使用免費網路連線等)。

遠距辦公政策實施同時，企業與員工應積極做好資安準備，以避免發生資安事件，守護企業重要商業資產的安全性。