公務家辦洩密肇因分析與預防作為

資料來源：轉載自臺中市政府政風處

●為何公務家辦容易造成資料外洩？

因為機關內部的電腦有層層嚴密的防護措施，有專業資訊技術人員的監控防護，而家中的私人電腦防護能力通常較為薄弱，很容易遭到駭客入侵或感染病毒、木馬等惡意程式，造成資料的外洩。現今大家對網路的應用與需求已不可同日而語，但也讓有心人士覬覦網路所帶來龐大的政治、經濟與軍事效能，因此，機密維護工作的落實與否，其結果已超越人們所能預判的範疇，其後的發展演變，亦非個人行為所能掌握與操持，影響所及更非個人生死榮辱所能彌補於萬一；洩密之嚴重後果由此可想而知。

●案例

范小峯身為國軍高階軍官幹部，理應為士官兵之表率，明知單位再三宣導「嚴禁將公務攜返家中處理」之規定，且其曾於 97 年 4 月間因違反前述規定而遭該管記過 2 次處分，猶不知警惕， 竟因個人誤認在家中處理公務時，只要不連接網際網路且作業完成後將電子檔刪除，即不致外洩資料；殊不知該電腦因未以防毒軟體掃瞄病毒或設定 Windows 作業系統之防火牆等防護網路安全措施，仍有機會遭惡意程式感染並擷取資料外傳，肇致洩密情事發生。探究其洩密肇因，不外乎以下幾點：

一、漠視保密作業規範。
二、個人法紀觀念淡薄。
三、資訊安全常識不足。
四、資安管控機制失調。
五、個人品行習性不佳。
六、保密安全警覺鈍化。
七、心存僥倖貪圖便利。
八、掃毒軟體未保常新。
九、資訊保密紀律鬆散。
十、監督機制日久玩忽。

●結論與建議

在最近的數十年內，人類的生活已有重大的改變，我們不但要熟悉已在使用的科技，還要學習運用新科技；在這種快速變動的環境中，我們除應不斷學習新知，也要懂得防護自身的安全。將來使用電子設備是無可避免的潮流，「e 化」更是未來生活必定的趨勢。目前在電腦網路的運用上，要完全避免病毒或駭客的襲擊是不容易的，所以我們必須要有正確的觀念與應對措施，才能在安全的前提下，享用電腦和網路帶來的便捷。以下的作為應是電腦使用者的基本安全素養：

一、使用正版軟體

盜版軟體除了侵害智慧財產權、運用上不如正版軟體來得穩定外，也常挾帶惡意程式，導致電腦中毒或被入侵，資料被竊取或遭篡改，甚至成為惡意郵件的散播者。

二、重要資料加密

為避免重要資料外流，最基本的功夫就是將重要檔案加密，並且設定為隱藏檔案，置於特定的目錄夾內，以降低被人搜尋發現的機會。

三、不公務家辦

若將公事帶出辦公室不僅會增加洩密之風險，且因家中電腦在安全機制上往往不如辦公室，又可能多人使用該電腦，甚至早已被植入木馬，所以公務家辦經常成為資料外流的主因。

四、避免開啟不明網站或不明郵件

許多不明網站之網頁或不明郵件經常暗藏或被寫入惡意程式，同時藉由驚聳誘人的標題或連結，吸引他人點閱，藉以散播惡意程式或竊取帳號密碼等，造成當事人的財產損失、資料被竊。

五、定時更新病毒碼與掃毒

惡意程式翻新與變化的速度非常快，所以我們最基本的防護必須定時更新掃毒引擎與病毒碼，時常進行掃毒以降低電腦被駭的風險。現代人時時應有「預防勝於治療」的觀念，若能事先採取預防措施，則能降低電腦被駭、資料外洩或受損的威脅。因此，落實電腦的安全防護，除了要有正確的觀念外，更應從日常生活中養成資通安全的正確習慣，才能自然而然避開網路世界暗藏的危機，將網路使用的風險降至最低。