機關公務電腦遭駭客攻擊案例

案例 1：某機關資安監控中心在 100 年 2 月下旬發現多起可疑的資安威脅事件，駭客攻擊手法疑似利用該機關張○的電子郵件帳號，將檔案壓縮並封包寄送至特定 Gmail 信箱。據了解，張員平時是在實體隔離電腦處理機敏業務，但須緊急以大量紙本輸出機敏業務資料時，因實體隔離電腦未配置專屬印表機，遂將機敏業務資料先存入隨身碟，再使用連結外網的公務電腦列印。沒想到卻遭駭客入侵該連網電腦，作為攻擊跳板，導致張○的電子郵件帳號被盜用，並在不同的電腦上，將取得機敏資料寄送至同一免費電子郵件信箱（Gmail），而張○表示對於上情從未知悉。嗣該機關資訊單位立即備存張○郵件資料，並停用張○的電子郵件帳號。

案例 2：某機關組長李○負責機敏業務，該機關資訊室於 99 年 3 月間偵測發現其所使用的公務電腦屢遭外部 IP 侵入測試，意圖取得其公務電子郵件資料，資訊單位立即予以阻擋並反向查證 IP 位址，經查共有 10 組 IP 位址，分別來自國內、亞洲及歐洲各國。按李○擔任該機關簡任主管要職，並負責有關 ECFA 等重要業務，其公務電腦的資料多為重要決策及專案相關文件，若遭有心人士刻意盜取利用，影響甚鉅。

該機關除已加強資訊安全宣導及進行公務電腦個人密碼更新作業外，另為避免發生類似情事，爰將相關可疑 IP 資料函請調查機關協助偵處。

案例 3：某中央部會首長辦公室專門委員陳○所使用的電腦，經資訊單位於 99 年 8 月派員進行例行性檢查，發現有異常登錄情況，且該電腦硬碟部分機敏資料遺失，疑遭駭客入侵。案經循線查溯至該部業管單位承辦人的公務電腦是駭客入侵源頭，推測入侵原因係承辦人接收駭客所寄發夾帶後門程式的木馬郵件。該機關隨即關閉相關電腦管理者的登入權限，以防堵繼續擴散。按該部業管單位正在辦理兩岸經貿合作協商業務，與對岸接觸頻繁，議程聯繫多使用電子郵件，致不易區分是否為社交工程信件，若信件經不肖駭客仔細安排，則不易發覺。本案顯示承辦機敏業務同仁資安意識不足，除應加強宣導確實使用實體隔離電腦辦理機敏業務外，並適時告知相關案例及資安作業規範，以為警惕。