

# 臺中市東勢區公所115年1月份公務機密維護宣導專欄

## 【對電腦網路犯罪之認識】

目前國際間最嚴重的犯罪就是「電腦網路犯罪」，除了透過電腦暗中轉移金錢外，有專偷重要情報的，如報稅記錄、技術機密、公司帳戶、郵寄名單、銷售計畫、人事資料，和其他單位內部機密的許多資料。而台灣近來透過網路犯罪的方式，如電子郵件、聊天室、手機上網等都可能成為犯罪工具，而破案率卻低於十分之一。以警方查獲之經驗來說，網路犯罪以網路色情為大宗，犯罪集團透過888、學術網路張貼援交、包養訊息等，將被害人約出來後下藥迷姦，然後偷取手機銷贓。網路上也販賣搖頭丸，並以拍賣網站進行詐欺。

網路駭客入侵民間或政府機構之電腦，竊取機密資料情形非常嚴重，這不是安全技術不夠，而是一時疏失或沒有警覺性，尤其許多單位沒有專職網路電腦資訊安全人員，防範難以周全。駭客之攻擊以散布電腦病毒，或植入木馬程式竊取資料較為常見，據犯罪偵查統計，發現不管是被害人或嫌疑犯的電腦，約有五分之一都曾被植入木馬程式，當事人還不自知，此由於木馬程式體積小，有很好的隱藏功夫，它會自動安裝在系統的開機登錄檔，在你下次開機後直接執行，當它們在執行任務時，有些工作管理員在處理程序時，看不到任何蛛絲馬跡，因電腦沒有任何表面反應，所以使用者如正在使用網路銀行或股票下單，你的資料會在不自覺中流失，因為電腦已在偷偷執行駭客命令。如具有分享功能之電腦，一人「中毒」，整個系統可能都有危險。

刑事警察局曾破獲典型網路駭客案，1名軍醫涉嫌以電腦駭客之手法入侵國內各（網際網路服務提供者）電腦網路，刪除系統資料，並竊取相關資料。另數年前警大招生，身兼電腦程式撰寫、資料處理、主辦電腦閱卷三大任務之某電算中心主任，竄改考生成績記錄，其行為並構成偽造文書罪。

所以要提醒各位同仁，使用公務電腦應遵守資訊安全使用規定，不瀏覽不當網站，不隨意開啟不明郵件、使用隨身碟等存取設備應謹慎，避免成為病毒傳播得媒介，培養良好的電腦使用習慣，才能降低感染病毒的風險。

## 【公務人員違規備份資料洩密案例】

政府機關於處理行政事務時，基於行政處理的必要，常會收集大量的個人資料儲存在電腦。例如：稅務機關擁有各納稅義務人的納稅資料、醫院擁有病人病歷資料、地政機關擁有各不動產所有權及相關權利的歸屬資料等等。上述資料攸關個人權益，屬於民眾隱私權的一部分，如因保管或處理不當，極易肇生觸法之虞。

由於個人資料走向電腦化的結果，「隱私權」極易遭受侵害，其情形猶如工業發展極易破壞生態環境一般，故公務員對於因公務上持有之資訊資料應善盡保密的責任，否則，一旦疏怠洩漏，不僅將造成民眾精神、財產或名譽上的損失，自己更要承擔法律責任，不可不戒慎！

張員係某機關公務人員，經常利用值日之便，在該機關內使用單位個人電腦，整理職務上所持有之秘密文書，其間為求便利，曾違反「電腦作業人員洩密違規懲處標準」規定，擅自將未經核准之國防以外應秘密之文書，分別儲存於私人攜帶式硬碟機資料庫中。日後因該電腦硬碟磁軌損壞當機，致前揭機密資料存放於硬碟中，渠未依電腦維護規定清除記憶內容，交付廠商維修，廠商因維修需要又將資料存於其硬碟機中保存，經修復後，再將先前保存於其個人電腦中資料輸回使用，事後卻忘記將其保存於個人電腦內之文書檔案刪除，嗣因案需要檢調專案小組持搜索票搜索陳宅時，在其電腦中查獲機密資料，本案廠商因不知情被判無罪，張員之行為已分別構成妨害軍機治罪條例第二條第四項「過失洩

漏職務上持有之軍機」罪及刑法第一百三十二條第二項「公務員因過失洩漏國防以外之秘密」罪，案經法院審理後，認為張員係一時疏失觸犯刑章，且洩漏之資料均無具體事證足以證明有外洩他人情形，且審酌張員犯罪後深表悔悟等情況，量處張員有期徒刑一年二月，並依法緩刑二年。本案顯示張員平日對資訊安全缺乏警覺性，使用電腦仍停留在單純事務工具之心態，復因方便行事誤觸刑章，殊值所有公務員警惕，切記不可洩的機密，並要防範因電腦運用疏忽而洩漏職務上所保管的機密文件。目前政府為強化國力並提高行政效率，積極推動電子化政策，電腦已是公務機關處理公務的主體設備，因工作或電腦週邊設備更新，需要外送專業公司維修，應注意流程管制監督系統，並嚴密安全防護措施，方能防制洩密事件發生

法務部廉政署檢舉電話 0800 286586

臺中市東勢區公所政風室檢舉電話 04-25872106轉63

郵件地址：42265 臺中市東勢區豐勢路518號

電子郵件信箱 lee7910@taichung.gov.tw



恪遵保密規定

臺中市東勢區公所政風室提醒您