機密維護常識彙編（101 年 12 月份）

＊公務員應慎防洩密情事發生

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，並依法判刑二年。

法□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，切記不可洩漏職務上所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。

＊「利用職務查詢電腦洩漏機密遭判徒刑」

壹、違法（紀）事實：

甲為某分局派出所警員，乙係甲之兄，甲、乙兄弟有一共同友人丙，以販賣人頭支票為業。八十五年七月間，丙自報紙得知，檢調單位正在查緝販賣人頭支票集團，並發現可疑車輛跟蹤，遂請甲利用派出所內之電腦，查詢該車號是否為檢調單位之公務車，以防止被查獲。甲受丙之囑託後，乃利用警用電腦查詢，得知該等車牌號碼，

均為調查站所使用，並將查詢結果告知乙，轉通知丙運用，以規避調查單位犯罪查緝行動。

案經相關單位發掘後，移送地檢署偵查，認為甲所為，係觸犯刑法第一百三十二條第一項之洩漏國防以外秘密罪嫌，而乙係共同正犯，故皆依法提起公訴，並經高分院判決，甲、乙洩漏國防以外應秘密之文書，各處有期徒刑三月

貳、檢討與分析

一、保密係公務員應盡義務之一，「公務員服務法」第四條即規定：「公務員有絕對保守政府機關機密之義務，對於機密事件無論是否主管事務均不得洩漏，退職後亦同。」調查機關之查緝犯罪行動屬於公務機密事項，故應予以保密。

二、甲因個人情誼，將調查機關之查緝犯罪行動洩漏予犯罪集團，已明顯違反「公務員服務法」之規定，更觸犯刑法洩密罪責，其係知法犯法，咎由自取。而乙雖非公務員，但與具公務員身分之甲共同犯罪，依刑法第三十一條第一項規定仍以共犯論，故依同法條論罪處斷。

參、建議與改進

一、由於電腦科技發展日新月異，對於資料之管理、存取與維護固然提供了快速便捷的功能，但是如果作業管制稍有不慎，則極易遭他人盜用；因此，各公務機關依法建檔存儲之機密文書資料，均應妥善採取保密措施，以防外洩。

二、公務員如有職務上之需要，可依循行政體系規定之程序，取得公務電腦中之資料，但有些資料係涉及機密，不可任意展示、傳閱他人或私自保存，以避免洩密。因此，吾等同仁平日於執行公務時，對於應保密之事務，應特別小心謹慎，以免因不慎或誤解，而觸犯法網。

三、洩密是貪瀆行為中最常見之案例，如洩露底價、提供私人身分資料等，檢討其原因，不外為利慾薰心或一時疏忽所致。近來消防機關承辦民眾申請案件日益增多，其中若有涉及隱私或安全顧慮者，應多方瞭解可能滋生之問題，謹慎行事，避免洩密，更嚴禁利用職務之便洩漏機密，而生違法犯紀之情事。（本資料摘自於內政部消防署）

＊電腦伺服器遭駭客利用

本會附屬機構 XXXX 電腦伺服器遭駭客利用，做為攻擊美國 3M 公司網站之跳板。

（一） 案情說明：

１．本處九十一年二月二日接獲美國 3M 公司資訊安全人員電子郵件，稱本會 XX XX 伺服器，對該公司進行入侵式偵測。

2 . 本處告知該單位 , 該單位研判「網管系統」未更新造成 , 旋即自行更新版本。

３．二月八日美國 3M 公司再告知，該單位伺服器仍持續對該公司入侵。

（二） 處理情形：

１．本處立即派員前往處理，經查：「該單位雖更新版本，惟先被植入木馬程式病毒無法清除」，最後正本清源：「格式化刪除全部硬碟所有資料後，重新安裝所有系統解決」。

２．經研判該單位駭客入侵方式為循「網管理系統漏洞」主動入侵，或「上網下載不明軟體」造成，已告知該單位資訊人員切實遵照本會（九十）五月二八日輔統字第八二九號函規定：

（１） 隨時上網更斯網管（原承購之微軟公司）系統，以強化防禦功能。

（２） 禁止上網下載非法或不明軟體。

＊電 話 滲 透

壹、真實案例

曾在美國國家安全局擔任安全顧問的伊拉在其所出版的「大盜入侵」一書中，詳實地紀錄他如何入侵企業，並且以電話滲透某知名金融機構，成功獲取到敏感資料的經驗，伊拉真實的案例是這樣的：

伊拉的工作，主要就在於各大企業進行安全滲透測試。首先他選定了一家大型金融機構，藉由網路查詢到該金融機構的相關資訊，並透過電話簿查到該金融機構在當地的辦事處，而伊拉就在當地的辦事處順手取得該金融機構的年報及總公司內部部門的電話。

伊拉接著從年報中，找到該金融機構中許多主管與員工的姓名，然後再由網路搜尋功能查到這些人員的歷史新聞資料。從中選定一位主管，並且冒充該金融機構公關部門的人，打電話給這名主管的秘書，以欲在公司的刊物上報導這名主管的優異表現為由，和秘書小姐閒聊了起來。慢慢地秘書小姐也失去了戒心，在沒有防備的情況下，她告訴了伊拉這名主管的一些私人資料，包括家中成員及興趣嗜好等等。

緊接著伊拉又偽裝成該名主管，打電話給各部門秘書，要求他們寄一份員工電話簿給下游承包商（也就是伊拉），沒有多久，伊拉就收到一本本嶄新的電話簿，而裡面包含了所有員工的姓名，以及聯絡電話。

伊拉到此可說已經滲透成功了，但他還不死心，他想進一步了解該金融機構還有沒有哪些漏洞，於是他決定進入該單位的電腦系統裡，但先決條件是要獲得網路帳號的使用者識別碼與密碼。

伊拉選定新進人員做為下手的目標，他認為新進人員最沒有戒心，而且剛進公司對公司環境和其他人員也不大熟悉。伊拉打電話到新進人員管理部門，偽稱是某高階主管的助理，因為主管要親自歡迎新進人員，需要新進人員名單，恰巧該部門負責人不在，而接電話的又是新進的辦事員，新辦事員二話不說就答應了，半小時後就把新進人員名單 mail 到伊拉的電子信箱裡。

接下來，伊拉一個一個打電話給這些新進員工，告訴他要實施有關電腦安全方面的訓練，但需要員工的電腦型式、系統名稱，以及使用者的識別碼與密碼，而在套取密碼的過程中，伊拉會先問些基本問題，然後再告訴他們一些簡單的安全規則，就這樣伊拉輕而易舉地突破了該金融機構的安全防護系統，順利地侵入該單位。

貳、經驗教訓

（一）這個案例告訴我們，不管在任何的情況下，都應該嚴守秘密。事實上，「保守業務機密」不只對國家政府是重要的，對一般的企業機構更是重要；從案例中可以看的出來，新進人員因為對單位不熟悉，再加上缺乏警覺性，結果

伊拉只經由電話就套取出個人的識別碼與密碼，而讓伊拉輕易地滲入公司電腦系統裡，還好伊拉只為測試工作需要，如果他是一名間諜，該金融機構將可能造成嚴重的傷害。

（二）其次，伊拉只藉由電話便一層層地入侵金融機構內部，不但獲得員工的電話簿，還得知高階主管的一些私人資料，以及新進人員的識別碼與密碼。由此可見，電話滲透是無孔不入的，它不需要浪費太多的人力，也不需要大筆的金錢，只要有一張嘴巴，就可能造成對國家政府或是企業機構的危害，這也難怪簡訊、電話詐騙案層出不窮，即使政府、警政機關一再宣傳，還是無法有效遏阻，詐騙案仍是一而再、再而三地發生。

（三）上述的案例，我們應引以為借鏡，除在個人工作崗位上戮力以赴外，在接獲陌生電話，或是與他人閒聊時，都應隨時養成保密的習性，並謹守個人本分，否則一旦業務上應保守的機密或是個人資料外洩，影響的不只是個人本身而已，更可能造成公司莫大的傷害。須知「謹言慎行莫大意，快意多嘴禍害多」，大家都應該謹慎小心才是！