機密維護常識彙編（96 年 9 月份）

＊現代國民應有的保防認知

保防工作為世界各國維護國家安全必有之工作，

各國保防機構或有名稱不同，但精神與內涵殊途同歸。

自兩岸開放民間交流以來，人民交流熱絡，互動頻繁，在經濟方面儼然已出現互依互存的態勢。然而在兩岸往來頻繁之際，共諜可能透過諸如探病、奔喪或婚姻關係以及依親等合法方式進入臺灣，亦有利用臺灣海岸線綿長特性，以偷渡等非法方式滲入臺灣社會，竊取包括政治、經濟、科技與軍事等各種機密，危害國家安全影響之巨，絕非國人所能想像。由我國政府陸續破獲的多起共諜涉及竊密案件看來，顯示出兩岸之間「政治對立、軍事對峙」之勢並未因民間交流而有所改變，更證明中共謀我之心態日趨積極、密切，軍事恫嚇、外交打壓、滲透統戰、拉攏分化手段，無所不在，在敵暗我明的情況下，落實全民保防維護國家安全確為當務之急。

令人遺憾的是，隨著時代變遷，多數國人已逐漸忽略「機密維護」的重要性，甚至有部分人士，出現對保防工作的質疑或抱持錯誤認知，認為保防工作是少數保防人員的工作，誤以為「保防」是思想控制、監視他人、打小報告或限制他人的工作，因而對於保防工作產生厭惡、鄙視等偏差的觀念。事實上，保防工作為世界各國為維護國家安全必有的作為，各國亦多設有保防機構，或有名稱不同，但其保防工作之精神與內涵全世界應是殊途同歸的，對於政府機關或是私人企業，均是必要的設置。

中華民國是一個開放的社會與民主、自由的國家，更是 2 千 3 百萬國人生命之所繫的樂土，維護國土之安全就是所有國人共同的責任，因此，建立機密

維護及防制敵諜共識並且積極落實，就是維護國家安全首要之務。吾人除了嚴密保護措施外，更應深植堅定的保密警覺與理念。

保防工作應從自身做起，平時即應養成嚴謹的生活態度，離開辦公室時抽屜應上鎖，公文應依機密等級妥適處理，保持辦公桌的整潔，不應該將文件放置於桌上或是壓在桌墊底下，同時注意影印、電腦查詢文件的保密，影印後的廢紙應做好銷毀的動作，不要在公開場合談論有關業務機密等，時時提高警覺，以建構綿密保防網絡，讓我們從日常生活中來體認保防工作。

保密工作是整體性、全面性的，其目的乃在防止洩密事件的發生，故保護國家機密實為現代國家每一個國民應有之責任，更是身為國家公務員必要的基本義務與道德修養，且機密維護亦為經常性、持續性之工作，不容稍有疏忽或鬆懈，惟有確實貫徹執行各項保密措施，恪遵個人保密規定，做到「人人保密」、「時時保密」，以提高保密警覺，養成良好保密習性，加強保密防護措施，落實保密安全檢查，使我們的保密工作做到百無一疏，萬無一失，才能維護國家機密，也惟有人人提高警覺、落實全民保防要求，國家的利益和安全才得以確保，國人才能永享自由民主生活。（本資料摘自於清流月刊/林 緯）

＊分享軟體洩密 9 單位 58 份筆錄 刑局緊急攔截

警用電腦因員警自行安裝「Ｐ２Ｐ」分享軟體，導致許多筆錄、偵查報告外洩，刑事局目前已清出九個警察單位，五十八份資料遭上傳或下載，並立即展開攔截動作，並呼籲民眾趕緊將資料移除，若再有上傳筆錄資料，將依違反妨害電腦使用罪展開偵辦。

刑事局強調，今年二月份就通報各警察機關，明令警用電腦不得使用「Ｐ２Ｐ」分享軟體下載遊戲、音樂及電影，經科技發展中心透過程式清查，已

查出台北市警局、高雄市警局、台北縣警局、高雄縣警局、台南縣警局所屬的派出所、偵查隊有九個單位有警用電腦洩密的問題，其中以台南縣警局新營分局民治派出所超過十份以上的偵查報告、失蹤人口、指證筆錄外洩最多。

刑事局副局長高政昇表示，警用電腦洩密一案，警方已連夜移除外洩資料，由於**員警個人使用不當，違背電腦安全使用規定，將追究行政責任，另刑法一百三十二條洩露國防以外之機密也處罰過失犯，若經調查確屬違法將送辦。**

高政昇指出，因「Ｐ２Ｐ」分享軟體的程式設計，只要透過上網連結，電腦上的資料就會被下載，刑事局目前除全面清查，積極移除相關資料外，也呼籲民眾自行移除，切勿繼續流傳，否則將觸犯妨害電腦使用罪及民事侵權行為。【中國時報／蔡旻岳／台北報導】

＊如何維護電腦設備安全

一、厲行管制措施：

電腦設備於各使用單位裝機測試完成後，使用單位宜建立相關之管制卡，並由使用人或保管人簽章，妥善使用與保管，以明責任。機關中之電腦設備應一律由資訊部門負責安裝、維修及管制，各使用單位不得擅自拆卸電腦或其週邊設備。使用人不得操作與自己業務不相關之軟體系統；未經資訊部門同意，不得擅自加裝介面卡或變更硬碟規格。機密或較敏感資料應儲存於軟碟磁片或燒錄於光碟中，嚴禁儲存於電腦硬碟中，並由專人保管，停止操作時應將磁碟片（或光碟片）抽出，並將螢幕上之資料消除。儲存機密資料磁碟片，除經權責主管核准，不得擅自攜出辦公處所。各單位對應用系統軟體使用人之身分碼，應定期造冊交資訊部門保存，以便稽核。

二、建構防範災害設施：

電腦設施應置於通風良好，無水氣、乾燥之冷氣房中，勿受日光直接曝曬，辦公室應有乾粉式防火滅火設備，不得存有易燃易爆物品。電腦應加裝防止雷擊自動跳電裝置，及不斷電設備，並注意地震及颱風等天災的防範措施。

（一）建立備份回復系統：

重要的電腦系統，應設計使用自動切換備援電路，如┐多路由┴設計及自動電話線撥接備援，以免資料不當毀損。各項檔案應依性質，分別訂定備份數，並定期備份。重要檔案宜備份三份以上，其中一份儲放於防火櫃內，一份儲放於異地建築物之防火櫃內。各項程式檔案之更新與註銷均應依照一定的程序進行，並訂定電腦系統回復標準程序及注意事項貫徹執行。

（二）落實程式安管：

單位內對於電腦程式及其設計、測試、製作、使用、維護等均應管制。管制事項包括程式指令、工作控制語言、程式變更申請、程式製作標準等及操作說明、測試報告、變更報告等相關文件。使用終端機與其他機關主機連線作業者，應由權責單位核准後列管，並於系統內限制其可運作範圍。程式設計完成時，由非原程式設計人審核，以杜流弊；程式一經核定，不得擅自更改，如有變更必要時，應報請權責長官核准。單位對於重要的程式應用系統，應詳加評估是否已具備適當及足夠的安全保護措施後，始得使用。

（三）防範電腦病毒侵害：

不使用來路不明之磁片，不使用非經許可之軟體程式；在電腦設備中加裝防毒軟體，及妥善網路防毒措施。要求電腦廠商於例行維護

作業時，加強掃毒檢查，並適時更新防毒軟體。電腦使用中，如懷疑有病毒侵入，例如無法正常開機、資料無法讀取或出現異常畫面等，應立即反映資訊部門妥處。

（四）加強人員及門禁管制：

對非管理或未經許可之人員應管制其進入資訊部門，並加強警衛巡查或保全監視系統，以確保門禁安全。電腦需維修廠商維修時，應派員在場監督，如需攜出進廠檢修時，單位應完成設備攜出手續，方可放行。進用資訊人員時，應先辦理資格審查，及完成保密切結。並保證離職後，仍負有工作期間職務上應守密之義務，如有違背，依法檢討刑事、民事責任。

結語

使用電腦已是人類邁向二十一世紀不可或缺的技能與工具，它猶如一柄無堅不摧的利刃，吾人運用得宜，則可揮灑暢快、事半功倍；若持用不當或輕率疏忽，則可能反噬自己。身為國家公務人員，在運用電腦資訊，方便行事，為民服務的同時，亦應考慮到資訊安全與公務機密維護更是公務員應有的責任與素養，吾人應時時惕勵檢討，要有正確使用電腦的觀念及管理辦法，使電腦皆能按照正常規範來使用，才能達到維護電腦資訊機密及安全的目的。

＊查證才能防止被騙

不明電話先查證，機密資訊不外洩。

一、故事內容

案例一

94 年 2 月起，一名不務正業，沈溺於打電玩及簽六合彩的陳姓男子，為了支應龐大的開銷，竟然假冒超商老闆，藉以欺騙店員，而他利用這種方法，短短的五個月就在南臺灣騙了一百多家店，獲利超過千萬元。

陳姓男子的方法很簡單，他先是利用電話簿分類廣告刊的超商電話，然後打電話到超商佯裝成老闆，並詢問店內的電玩營業情形，接著指示店員「等一下會有一個便衣警察到店裡面收規費，你只要把錢裝進信封裡，有人去拿時就交給他，如果沒有照辦，出了事你要負全責！」結果店員不疑有他，也沒有仔細查證，再加上店裡面擺放電玩機台，竟然乖乖地就把收銀機裡的錢交給陳姓男子，等到隔日真的老闆來查帳，店員才知受騙。

陳姓男子也用同一種手法去詐騙網咖店員，先打電話假冒老闆，然後以更換新軟體的名義，要求店員將店內的電腦搬到店門口，接著再以電腦工程師的名義將電腦搬走，並以每台五、六千元的低價轉手賣出，同樣的詐騙手法，陳姓男子只不過運用了電話及被害人的大意就輕易地騙到上千萬元。

案例二

94 年 10 月間，汐止一處正在施工的工地發生了一起詐騙案，七、八名男子趁著謝姓負責人出國期間，向該工地主任詐騙價值三百萬元的打樁用挖管機。

整起事件發生經過是，一名自稱「阿草」的男子，趁著謝姓負責人出國期間夥同七、八名友人，向工地主任出示一份轉讓證明書，並表示負責人已將工地機具賣給他，工地主任檢查證明書後，確定有公司的用印和負責人的簽名，因此不疑有他地讓這些人搬走打樁用挖管機，結果謝姓負責人返臺後，才發現這原來是一起詐騙案件，而嫌犯只利用了一張紙就輕易地騙走了價值三百萬元的打樁機。

二、經驗教訓

(一)從以上的二個案例，我們可以了解到「查證」的重要性，而這二個案例也清楚地告訴我們，不管在任何的情況下，都應該要詳加查察辨證，尤其是在緊急的狀況下。事實上，「查證」的功夫不僅對一般的企業機構是重要的，對國家政府更是重要；從以上二個案例中可以看的出來，新進人員因為對老闆不熟悉，再加上缺乏警覺性，結果只透由電話和一張證明書，就輕易地騙到現金和打樁機，幸好這只是在一般的民間機構，如果他是一名間諜的話，那將可能對國家或政府機關造成嚴重的傷害。

(二)其次，只藉由電話或是一張紙便能得到對方的信任，不但能夠詐騙到金錢，更能騙到價值昂貴的打樁機。由此可見，詐騙是無孔不入的，它不需要浪費太多的人力，也不需要大筆的金錢，只要事先編排設局及擁有一張能言善道的嘴巴，就可能造成對國家政府或是企業機構的危害，這也難怪各式詐騙案層出不窮。

(三)上述的案例，我們應該引以為借鏡，在接獲陌生人及有違常情的電話時，應該要隨時查證清楚，否則不僅是個人金錢或財物遭受詐騙，一旦公務機密外洩，影響的範圍更可能造成公司或政府機關的莫大傷害。因此大家應該熟記「不明電話先查證，機密資訊不外洩」，大家都應該謹慎小心才是！

（本文作者為臺北縣淡江高中教官/陳宏煇）

＊從現代科技談保防

務人員應自我要求跟上潮流，才能及早建立新的保防危機意識。

記得大學時代上軍訓時，曾聽過教官講過一段真人實事：國外有一位官拜少將的情報人員，每天穿著光鮮筆挺的軍服上班。在他擔任機密要務之際，保防工作實行得滴水不漏，幾近苛求，也因此每次上級長官所交付的任務均能順利遂行。然而自從他換了新的裁縫師之後，每次一經手機密文件，

過沒多久便被各大媒體登上版面，所洩漏的軍機差點讓他丟了官，直到他卸任之後，將那套軍服高掛塵封，有時拿出來睹物思情一番，才發現那套軍服胸前的第二顆鈕扣與其他鈕扣形式有點不同，於是拿去請專家鑑定，後來才發現那顆鈕扣是一台袖珍針孔攝影機，當將軍坐在辦公桌前處理文件或打字時，眼前的機密一覽無遺，真相才因此大白，而那位裁縫師於事跡敗露後被逮補，才發覺他原來是敵對國派來臥底的情報員，藉由平凡的身分與高精密的儀器滲透於對方情報陣營，藉此竊取機要以掌握敵情。

這則案例雖然帶有幾分不可思議，猶如電影情節般充滿懸疑，然而卻給了我們一個值得省思的方向：當時代在進步，物質生活不斷提昇的同時，許多潛藏的危機及隱憂會隨著高科技而加重。就以目前的個人資料來說，如果我們的電腦軟體沒有安裝防火牆，或者保管個資的機關疏於防備，便極有可能遭到駭客入侵而使權益受損，反觀軍中機密亦是如此。在電腦週邊設備、電子通信器材、監測控管儀器發展迅速的現代，身為保防環節中的一分子，如果無法隨著科技進步而自我加強資訊新知，很容易便會因落伍而失去先機，甚至無法預估可能發生的危安因素。所以政府機關的精英幹部，應該自我要求跟上潮流，才能及早建立新的保防危機意識。

再說，二十一世紀的戰爭型態已進入太空科技的領域，幾乎所有的先進武器都是透過微電腦控制執行，而反制與反反制作戰也倚賴高精密的偵測儀器相互較勁。如果我們能透過虛擬世界的高可塑性、輕巧便利及無遠弗屆的傳輸改良我們的武器系統，在日積月累之下，必能有可觀的研究成果，然而，此種能力若是被敵人用來滲透、入侵乃至癱瘓我國防資訊網路，所面臨之危機損失絕非一朝一夕所能挽救。如果我們能著重培養資訊人才，及早奠基於資訊保防教育，今後之精良部隊必能落實資訊保防觀念，同時藉由自我平日進修而提升相關常識，如此才能將國防安全帶入科技的潮流中。

「水可載舟，亦可覆舟。」當我們手中拿著多功能的照相手機，胸前掛著新穎的 MP3 隨身碟時，不妨想想這些資訊器材如果用來偵蒐機密，竊取情報，其後果必然不堪設想，想要每個人都能建立資訊科技保防的安全觀念，深知資訊洩密的嚴重後果，那麼安危的死角便可減少許多，資訊的流通將更有保障。

科技文明的一日千里，對人類而言往往各有利弊，端看我們如何善用發揮其長處，使生活更便利，而國家安全也是如此。唯有借重資訊工業的發達，推動行政效率及國防戰備，才是萬民之福。

（本資料摘自於清流月刊）