辦公室機密業務作業保密

不良的辦公習慣；輕忽保密的觀念，是造成辦公室機密外洩的主因。其常見缺失及預防方法，如后：

一、影印分發重要機密文件時，應分別編號；依編號不同，分別在各件適當位置處註記，以明確持有人保密責任。影印中，若影印機夾紙故障，應即時取出，以避免遭人截取洩密。

二、傳真重要文件前，傳送方式應先以電話通知收件人，否則，在接收方傳真機未設定輸出密碼情況下，傳送完成的文件，恐發生遭人截收之慮。傳送資料完成後，雙方應以電話核對傳送張數是否相符；遇有不清晰處，應要求再傳送一次，不宜逕以電話宣讀填註，以免洩密。

三、廢棄機密文件不應逕棄於垃圾桶內；或雖做銷毀處理，但是，碎紙機銷毀能力不足，僅能碎成三釐米左右紙條；此時，若遭有心人士蒐集並予處理重組，機密文件旋即曝光，就保密性而言，焚燬優於銷毀；銷燬優於棄置。

四、主管機構密發給個人的權責代碼及密碼，係用於操作電腦以存取重要機密資料；依個人權限不同，作業範圍受嚴格限制。密碼應妥慎保管，嚴防外洩。

五、上機作業時，遇有離座需要，應即關機或離線跳出作業系統，使電腦螢幕空白，防止他人窺視機密；必要時，應加裝錄影監視系統，俾增加作業安全及追究使用責任。

六、重要秘密資料（如標單、底價單）作業時，遇有離座需要，應即妥收密件入櫃，俾防遭人抄錄或翻閱，造成洩密。

1. 機密文件在傳遞郵寄過程，常見缺失情形及預防作為：使用雙封套郵寄密件時，外封套上不宜書明函內，封存密件內容，避免引人覬覦；內、外封套寫受文地址、受文單位及受文對象，應注意是否相符，防止傳遞過程遺失。
2. 內封套上應明確書寫收文對象或密件名稱（或代號、文號），俾收文人員正確轉交有權拆閱人員，避免困擾；封口應加蓋密戳並予封實，以防止遭人拆封或竊讀機密。

資料來源：交通部公路總局新竹區監理所

網路病毒激增 社群網站是溫床

社群網站興起，成為網路駭客散播病毒的溫床。香港最新 1 份互聯網(網際網路)安全報告顯示，2010 年的網路病毒總數是過去 10 年總和；臉書(Facebook)等網站上的病毒已大大威脅網路安全。

香港中通社報導，這份由網路安全公司 Symantec 在香港發布的年度報告顯示，Facebook 等社群網站平台的流行程度吸引了大量惡意軟體，其中 1 個主要施放伎倆是向網友推薦新聞鏈接、張貼一些縮寫網址，這些縮寫網址可以經過分享在電郵或網頁上，進而連結到其他複雜網址。

按「讚(like)」是 Facebook 的一大特色，不少人希望也有個「踩(dislike)」可按，以表達「另類情緒」。Symantec 公司表示，Facebook 上一度出現「dislike」應用程序，用戶千萬不能隨便安裝，因為這將連接到包含病毒的虛假網址，導致個人資料外洩或損毀；Facebook 方面也已多次澄清這並非官方功能。

該公司表示，社群網站的不明縮寫網址，千萬不能貪玩亂點。惡意程式能夠在極短時間內連結傳播至數百或數千位受害者。99 年因駭客以各種方式入侵系統而導致的個資外洩平均使 26 萬個私人身份

曝光。舉例說，伊朗核子設施遭病毒攻擊一事震驚全球，駭客針對特定大型企業、政府機構的「空窗期漏洞」入侵電腦系統，作出「針對性攻擊」並頻頻得手。該類攻擊可能對能源、基礎建設等大型機構產生巨大衝擊，將導致城市突然停電、斷水、交通癱瘓，後果不堪設想。

該報告也顯示，隨著智慧型手機、平板電腦等移動平台的普及，網際網路受病毒威脅程度較 2010 年急升 42%。用戶如果長時間開啟藍牙、無線等裝置，幾乎等於對個人資訊安全「不設防」。

資料來源：臺中市政府財政局

紙本個資防護

因應紙本個資文件防護需求，機關應從管理面出發，並搭配技術面輔助管控，像是在列印設備上早已提供諸多功能協助管控，包括身分驗證、權限控管、機密列印與紀錄備存等功能，妥善利用這些功能，便能強化列印設備與紙本文件的個資防護，減少紙本文件帶來的個資風險。

★ 紙本文件輸出缺乏有效管控

舉例來說，列印時，一旦有個資內容的文件印出後被他人誤取，或無人領取，就是紙本個資在列印時造成的風險缺口。傳真也是紙本個資防護不能忽略的管道，像是傳真文件印出被人拿取，下班時間後輸出的傳真文件沒人控管，也會造成同樣的問題。

從個資文件的產生、傳遞、利用，直到最後的銷毀與保存，都應制定好各人員的授權與責任，同時建置機密文件的分類、分級制度，並檢視現有作業流程。而員工的個資防護教育訓練也是持續不斷要做的

事，讓員工不論是在業務流程中，或是工作習慣上，都應該有良好的個資防護觀念。

★列印工作若委外，交付企業仍有個資責任

除了自己內部列印的管控，有些機關也會將文件列印工作委外處理。但委外並不代表機關不用負責，依據個資法第 4 條規定，「受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關。」因此，機關在交付個資文件委外作業時，需要謹慎評估，並針對有關個人資料處理的業務，建立評估的標準，以便篩選出適合的配合廠商。

★紙本資料輸出後，形成管理大漏洞

過去許多列印、傳真、掃描的使用習慣，其實都是紙本個資文件管控的大漏洞，管理者應立即檢視這些問題所帶來的個資風險。

●漏洞 1 列印文件擱置在設備上，遭誤取或窺視

●漏洞 2 個資文件傳真進來後，在傳真設備上無人領取

●漏洞 3 傳真個資文件時，不小心傳送到錯誤對象

●漏洞 4 掃描歸檔結果輕易被他人存取

★ 列印前的控管做法：個資文件印出前，應先做好列印行為權限管

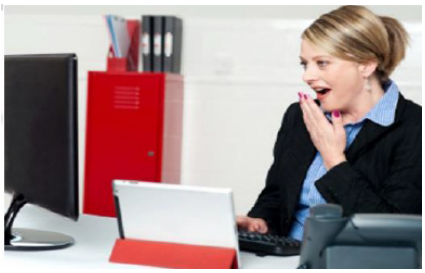
控不論是從列印設備開始管控，或是針對檔案限制使用者的列印權限，均可減少紙本機密、個資文件的管控

資料來源：Pchome 新聞

【法務部廉政署】
檢舉電話：0800-286-586
檢舉傳真電話：02-25621156
電子信箱：gechief-p@mail.moj.gov.tw

他人電腦資料，怎可亂刪？

【案例介紹】



在一家生產自行車零件公司擔任會計工作的宋姓女子，在服務期間除負責掌管公司帳務外，還兼理員工工作資料、報關業務的電腦處理工作。九十五年七月間因故離職，由於公司沒付給她當月份的薪水，因而心生不滿，臨走前將電腦主機中儲存的公司生產與營運資料，包括產品設計圖片、報關資料、帳目與客戶資料等一百八十多筆的電磁紀錄部分或全部都予刪除，留下一片「備份」光碟片就走人，後來公司方面發現電腦資料被刪，留下「備份」光碟片竟是空白片，便對宋女提出毀損電磁紀錄的告訴。

檢察官在案件偵查中，認為公司提告的屬於「告訴乃論」案件，告訴人可以撤回告訴，因此勸導雙方和解，宋女堅不認錯，指電腦內資料消失，可能是電腦當機緣故，不關她的事，而且她已經將有關資料製作備份光碟交給公司，至於光碟片何以是空白的，她也不知道！在這種情形下，告訴人公司當然不會撤回告訴，宋女便因「破壞電磁紀錄罪」被檢察官提起公訴。

這案件在法院審理期間，一審法官也曾嘗試替宋女與前服務的公司和解，宋女仍然拒絕，法院就依起訴的罪名判處拘役五十五日，因為犯罪時間是在九十五年七月間，合於民國九十六年間為紀念解除戒嚴二十週年而制定的《九十六年罪犯減刑條例》所定：犯罪在九十六年四月二十四日以前可以減刑的條件，依這條例予以減刑二分之一，減為拘役二十七日。

宋女不服判決，提起第二審上訴。被害的公司方面則認為量刑過輕，也聲請檢察官提起上訴。二審法官審理結果，認為宋女確有這種企圖

影響公司營運的事實，而且犯罪後態度不佳，將第一審法院的判決撤銷，改判有期徒刑四月，也依減刑條例減處有期徒刑二月，可以易科罰金。宋女更是不服，提起第三審上訴，報載宋女的上訴案日前已被最高法院駁回，也就是維持第二審法院的判決，這件擅自刪除他人電腦內資料釀成的刑案，至此方告判決確定。

資料來源：法務部

資訊室員工 維修檢察長電腦被起訴

【聯合報／都會地方中心記者／連線報導】【2014/01/23 聯合報】

雲林地檢署日前依妨害電腦使用罪，起訴地檢署資訊室兩名員工；據了解，二名員工疑為檢察官及檢察長林○○更新電腦時，被檢察長懷疑侵入個人帳號遭查辦。雲檢此事在司法界傳開，立即成為話題；原因是地檢署資訊室負責維護每個檢察官的電腦運作，常要更新防毒軟體，每天都得透過遠端監控施作，「這也被起訴，各地資訊室人員每天都在觸法」。有檢察官表示，法務部資訊處每天中午都透過遠端，更新全台每個地檢署檢察官的電腦，包括前一天的戶政資料，這些都沒逐一徵詢檢察官同意，若要據此論罪，「應先從法務部資訊處人員先起訴吧」。

否認入侵 仍被起訴

雲林地檢署不願證實此案是否也涉及檢察長林○○；林○○昨晚表示，妨害電腦使用罪為公訴罪，檢方發現有問題後，多次詢問兩名資訊員，兩人都否認，由於不合緩起訴要件，才會起訴「警告」，交法官協助釐清。「沒有吧！應該不會，但電腦到底有無入侵，並不清楚。」雲林地檢署多名檢察官對地檢署資訊員被起訴，表示不知道帳號有被入侵的事，全案他們不便評論，「應該去問有被入侵的人才清楚」。

長官霹靂 基層自危

被起訴的楊姓、陳姓資訊員昨天仍照常上班，但都沒有和同事談及被起訴之事。地檢署人員透露，每位長官的作風不同，他們在基層工作，

一切都只能按規章行事，很多事就不便多說。據了解，楊姓、陳姓資訊員在雲檢工作已有段時間，且歷經幾任檢察長，工作都沒出過問題。兩人是在去年八月雲林地檢署更新電腦，進行例行維修，檢察長林○○認為有檢察官帳號被入侵，事涉地檢署內部資料及個資外洩，請示法務部展開調查。

「刑法」

第 358 條：無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。

第 359 條：無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。

第 360 條：無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。

第 361 條：對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一。

資料來源：臺灣宜蘭地方法院

狀況掌握與危機處理

◎洪子晴

電影中的意外狀況總有劇本設計好的英雄前來解救，然而真實生活一旦發生意外，是無法一廂情願地期待英雄的救援。所以災禍發生時該如何自處，便成為各機關、部隊，乃至個人學習的重要課題。

「意外」並非總是「意料之外」，往往是人員未確實遵守安全規定或作業程序所致；如去年延燒全臺的塑化劑事件，就是不肖商人擅自更改配方牟取暴利所引發的風暴。災難可區分為「天災」及「人禍」，其中人禍可以靠制度加以控制並降低其發生率；天災雖無從阻止，但仍可藉經驗法則預判其災損，事先訂立處理機制並實施預防演練，以求降低損害。因此，上級的職責除建立制度外，還包括預想一切可能的狀況並訂定處理流程，即「危機處理」。

九一一事件及卡翠娜風災後，美國國土安全部研擬出 15 種「想定」，內容包括核爆、化學攻擊、自然災害、食物汙染及網路攻擊等，做為事先預判災損、事後應變處置的準則。同樣面對天災，我國軍也依「超前部署、預置兵力、隨時防救」的原則行動，並在全軍推行「風險管理」觀念，亦即事前評估可能發生的危安因素，預先提出對策、建立應變機制及教育部屬等，都與美國國土安全部的「想定」原則不謀而合。可見先進國家面臨詭譎的世界局勢及極端的氣候變遷時，已經越來越能以積極正面的態度回應，而非消極地逃避，顯示此一觀念受重視的程度。

近來人們常說：「魔鬼藏於細節中」，事情的發生必有徵兆，只是人們常不以為意；所謂「千里之堤，潰於蟻穴」，若能提高警覺、防微杜漸，便是最經濟的危機處理。我政府雖已建立許多應變機制，然而若國人缺乏危機處理的觀念，也難以發揮作用。唯有從上到下建立正確觀念、建構嚴密的網絡，方可消弭危安因素，確保國家安全、社會安定、民眾安寧。

資料來源：臺中市政府水利局

員工旅遊安全不可不知

隨著國人出國旅遊型態轉變，旅遊資訊成為我們在計畫旅行的重要參考，為了不讓我們的旅行蒙上陰影，有些旅遊常識你不可不知。

＊國內旅遊時應注意事項：

1. 行前預先規畫旅遊路線：

充分規劃旅遊路線，如需進入山區應注意是否應辦理入山證明。

2. 旅遊裝備先準備妥當：

瞭解自己身體狀況，隨身攜帶必備藥物，如暈車藥。

3. 行車遵守交通規則：

隨時注意警廣及手機報導有關交通狀況，掌握路況。

4. 注意自身旅遊安全：

- 前往山區注意落石、虎頭蜂、毒蛇
- 無救生人員管理之海邊、溪流水域，請勿游泳、戲水
- 搭乘遊艇應著救生衣，並拒絕搭乘超載、無照船艇
- 未經核准纜車或機械遊樂設施，安全堪慮，請勿搭乘

5. 勿擅自前往危險地區：

遵守警告、禁止標示規定。

6. 旅遊住宿地點應注意：

入住飯店先瞭解逃生路徑及逃生門位置。

如有貴重物品請隨身攜帶或另行存放，隨意留置房中十分危險

住房期間如產生私人費用，如洗衣、餐飲等務必離宿前至櫃台結算清楚

7. 購物請小心：

選購物品務必瞭解其品質，尤其藥品須瞭解有無副作用。

＊出外旅遊萬一不幸遇到旅遊糾紛該怎麼辦呢？

下述幾種申述管道可供使用：

交通部觀光局旅遊權益申訴管道: http://admin.taiwan.net.tw/

中華民國旅行業品質保障協會:http://www.cpc.ey.gov.tw/

中華民國消費者文教基金會:http://www.consumers.org.tw/

資料來源：新竹區公所

機關安全維護案例剖析

檢視當前各機關（構）安全防護工作上所發生之危安案例，雖案情態樣、災害程度各有所不同，但追本溯源分析、比較，總是發現有共通之性，謹歸納並分述如后：

＊一、安全防護規劃不當，致產生防護漏洞：

科技設備的裝置，雖能彌補人力之不足，若事前未能周延策畫，考量其必要性、效益性，徒有良好的設備，亦無法發揮其功能，反而喪失預防救災的先機，如：

（一）某銀行金庫發生竊案，保全系統於案發當時雖正常發出警報，惟金庫裝設之「密碼定時鎖」必須在設定時間輸入密碼，始得進入金庫捉竊賊，為此延誤保全人員處理時效，而使竊賊縱容逃逸。

（二）某國營公司機房，誤將火災受信總機設置於無人值勤之隔間內，某晚機房空調室發生電氣火災，雖經由偵煙式火警感應器迅速偵

得，並發出警報，且火災受信機亦明顯標示火災發生的地點，惟因距離值勤人員處所甚遠，以致延誤救火時機。

＊二、安全防護檢查疏漏，致延誤救援時機：

定期安全督導檢查，為先期發掘潛存影響安全因素，防患於未然的重要手段，以下二則案例，一為緊急求援連絡專線警鈴；一為緊急災害逃生緩降機，由於平日疏於檢查與保養，在緊急狀況時，非但無法發揮預期救援功能，反而成為救災的絆腳石：

（一）某國營機構架設通往管區警察局之專線警鈴，因未定期實施測試，某日，該機構適值發生竊案，警衛人員在按下專線警鈴時，卻發覺未有反應，經改以電話連絡，又發現電線已被切斷，而延誤救援時效。

（二）某消防機構人員，某日受邀做「火災逃生防護演練」，在實施以「逃生緩降機」自高樓逃離火場演練時，不幸發生緩降機纜繩斷裂情事，肇致該名消防隊員墜落重傷之意外。

＊三、安全防護觀念薄弱，致釀成意外災害：

諸多安全事件的發生，均因當事者未能確實遵守安全規定，或因一時疏於防範，而造成難以彌補的後果，諸如：

（一）某安養機構殘癱病患深夜在床上吸菸，不慎引燃棉被，釀成火災，雖該機構值勤人員緊急疏散殘癱病患並將火勢撲滅，但已造成一死一傷的慘劇。

（二）某醫院宿舍僱用保全之守衛，未能確實遵守安全規定，擅在木造崗亭以電壺燒開水，致引發電線走火而釀成火警，雖即時撲滅，已造成損害。

＊四、安全防護警覺不夠，致引發安全事件：

漫不經心，對安全規定認知產生錯覺或忽略等行為，而釀成安全傷害事件及財物的失竊，不僅個人遭受傷害，亦使單位蒙受損失，故惟有提高員工的安全警覺，貫徹執行相關工作之安全規定，始能防止意外災害的發生，或使損害降至最低，譬如：

某辦公大樓職員遺失該樓門禁刷卡卡片、按鍵密碼鎖密碼及辦公室鑰

匙一串，事後並不在意，亦未向大樓管理單位報失，亦未迅速變更密碼及更換辦公室門鎖，致於某日上班時發覺，辦公室門被打開，保險櫃內所存放之現款遭竊，後悔為時已晚。

★安全維護應有的作為：

一、做好安全狀況判斷；

二、持續辦理教育宣導；

三、加強預防應變演練；

四、強化安全值勤功能；

五、確實執行安全檢查。

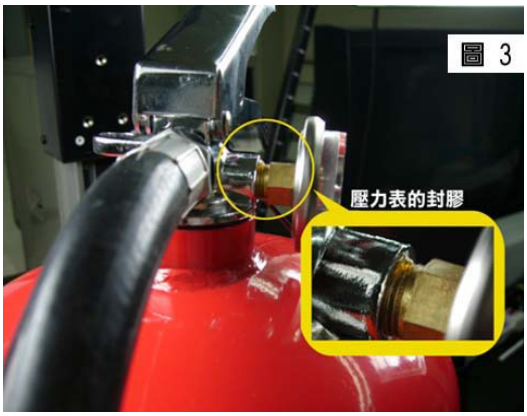
資料來源：嘉義區監理所

如何判斷滅火器送驗時，廠商有無檢查？

過去有許多不肖廠商，當民眾依規定將乾粉滅火器送驗時，並未依規定檢查乾粉滅火器是否壓力不足、內管破損、粉末結塊…，廠商僅將滅火器擦拭，重新貼上一個標籤就交差了事。但是怎麼判斷廠商是否作弊，其實很多人不知道，總以為送驗之後就應該是正常堪用，殊不知自己已經白白花了許多冤枉錢，還讓自己陷入未知的危機中。

要查證廠商有無作弊，其實非常容易，只要在滅火器送驗前做一個非常簡單的動作就可以了。拿一支油性簽字筆畫一條線，這條線要從乾粉的噴頭底部劃到瓶身。（圖 1）

因為乾粉滅火器如果有打開檢查過（圖 2），重新將噴頭鎖回去時，這條線理論上不會剛好連在一起（圖 4），就算有連在一起，那種機率也是很低，不會每一支滅火器的線都連在一起。（如果您願意用封條的方式也可以）



當然很多人會想我隨便打開一下，再鎖回去就會出現標線岔開之現象，何難之有？事實上乾粉滅火器只要打開過，蓄積在滅火器內的壓力會漏掉，一定要重新充填壓力，否則壓力表的指針會歸零。打開滅火器及充填壓力，這兩個動作已是檢驗中最麻煩的步驟，其他諸如檢查乾粉是否結塊、內管有無老化都是輕而易舉的事，負責檢驗的廠商，既然打開了，就會加以檢查，實在沒有必要大費周章將滅火器打開，重新灌氣後，只為了要讓這條線看起來沒有連在一起。

此外滅火器上有一個壓力表，應該也要拆下檢驗，因為壓力表必須校對，才能顯示正確刻度，而為了檢驗廠商有無實際實行，一樣在壓力表與噴頭接合處畫一條線，因為壓力表組裝時會用封膠加以固定，而封膠可以在接合處看得出來（圖 3），如果所畫直線及封膠之位置均未變動，這個廠商檢驗費用又比別人低，就算廠商大言不慚的標示檢驗合格，也不要相信，因為滅火器檢查都有一定的成本，奉勸大家千萬不要貪小便宜，更要為了自身安全，趕快將筆準備好，開始在滅火器上畫線吧。

資料轉載自新竹區監理所

多一分檢查 少一分危險

1週匯出五百萬 假撿警梗騙不停

詐騙集團的假檢警手法短短1週騙走陳姓男子5百萬元！日前歹徒冒充醫院人員，表示陳男名字遭到冒用申請醫療給付，接著又由自稱臺中市警局「廖隊長」來電說明陳男健保卡遭冒用一案，表示會有一位臺北地檢吳檢察官要求陳男到案說明，然廖隊長卻跟陳男說去了會被「羈押」，建議可以申請「分案檢查」，透過匯款給「監管單位」，才不會被傳喚、房子也不會被查封，陳姓男子為保護財產安全，立刻匯出了第1筆120萬元給詐騙集團，接下來連續一周廖隊長天天來電和陳男討論案情，並要求他匯款至不同「監管」帳戶，前後總共匯了578萬元。

家住中部的陳姓被害人（29年次，男）今年3月初在家中接到詐騙集團佯裝奇美醫院，指陳男身分遭冒用申請健保給付，為釐清案情，醫院轉接臺中市警局的「廖隊長」辦案，廖隊長向陳男表示，因為健保卡遭冒用一案，需帶現金150萬元至臺北地檢吳檢察官澄清，但「廖隊長」恐嚇陳男若去臺北地檢會遭到「羈押」，可以申請「分案調查」並匯錢給監管單位，財產才不會被查封也不會被傳喚，陳男非常擔心，於是在3月5日匯出第1筆120萬元。接著廖隊長每天致電陳男討論案情進度，最後都要求陳男不斷匯款，就這樣被騙走了5百多萬元。直到一個多月後，新北市政府警察局三重分局查獲詐騙集團，於帳戶記錄中發現陳男帳號，轉知臺中市政府警察局通知被害人並製作筆錄，陳男才始知遭詐。

刑事警察局呼籲，檢警不會監管任何的人帳戶，更不會要求收取現金或存簿，提醒民眾聽到「身分遭冒用申請健保給付」、「現在電話幫

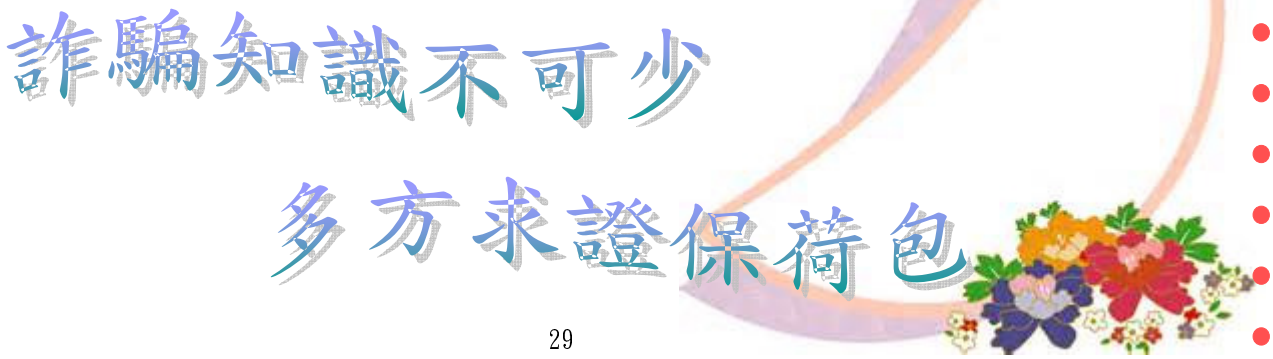
你做筆錄」、「等下傳真公文給你」、「法院幫你保管金錢」、「監管帳戶」等關鍵字時，絕對是詐騙！因為積欠健保、電信費用均是用紙本通知繳費，現行法令檢警更不可能用電話做筆錄及傳真公文(公文必定要紙本)，更遑論監管帳戶或保管金錢，希望各位年輕朋友回家多向家中年長者宣導，必要時可在電話旁邊放置假檢警詐騙的文宣或專刊，如果真的無法判斷是不是詐騙，歡迎利用電話撥打 165 反詐騙諮詢專線查證。

英語程度檢定考試多益(TOEIC)考生遭冒名電話詐騙

英語程度檢定考試多益(TOEIC)，台灣區總代理忠欣公司被冒名行使詐騙，告知考生重複報名或報名失敗，要求考生到 ATM 重新操作辦理退款或匯款，自 5 月 25 日起已有多名考生受騙。

忠欣公司在多益(TOEIC)官網指出，考生完成報名、繳費程序之後，多益測驗 / 托福測驗不會以電話要求考生操作 ATM、變更付款條件及程序。測驗報名進度可透過官方網頁查詢，若有任何問題請撥打客服專線 02-2701-7333。若有接獲類似電話，請勿理會並提高警覺，撥打 165 反詐騙諮詢專線報案，以確保安全。

警方亦再次呼籲，ATM 只能「提款」跟「匯款」，不具有退款、身分驗證或解除設定等功能，詐騙集團經常竄改來電顯示號碼，民眾接到陌生電話，切勿僅憑來電顯示號碼就輕信對方的身分與說詞，若來電顯示號碼開頭有「+」號，代表該通電話來自境外，更要提高警覺，應牢記「一聽、二掛、三查證」的口訣，先聽清楚電話內容，然後確實掛斷電話，再親自撥打 165 反詐騙專線查證，避免遭到詐騙。



《內政部警政署防詐十招》

一、「天下沒有白吃的午餐 」：戒除貪念，遠離中獎詐騙。

二、不接「不顯示來電」電話，幫助您拒絕詐騙。

三、「法院電話語音通知出庭」是詐騙：勿聽信電話內歹徒指示，辦理任何金融開戶或轉帳。

四、多管閒事當雞婆：住宅電話信箱勤觀察，提防詐騙歹徒盜轉接電話。

五、小心申辦信用卡或行動電話：親自前往指定門市申辦最保險，勿至不明商家，以免個人資料外洩。

六、小心網路聊天室陷阱：切勿留下家中地址、電話或個人影像，以免成為勒索肥羊。

七、小心網路援交陷阱：ATM 無法辨識憲警身分，切勿聽信歹徒指示操作，以免遭恐嚇詐財。

八、網路購物要小心：線上刷卡先確認網站真假 ；「一手交錢 ， 一手驗貨」交易有保障。

九、防詐騙 3 要領 ：「冷靜」、「查證」、「報警」。

十、請牢記警政署防詐騙專線「 165 」：「 165 」全年不打烊，受理諮詢、檢舉或報案。

165 反詐騙諮詢專線

警政署為加強預防詐欺犯罪，設立「反詐騙諮詢專線 165」電話，提供民眾諮詢。

凡遇不明可疑電話，不論手機或市話，只要撥打「165」即可由專人為您說明並研判是否為詐騙事件。。

優惠手機報你知~請小心電話行銷詐騙

近期有民眾接獲電信業者來電，聲稱老客戶購買手機有優惠。

165 提醒民眾，透過電話行銷購買手機、3C 產品等應小心，在優惠的行銷包裝之下，可能隱藏著品質不佳的產品及高額的電信費率，而有消費糾紛，亦有可能因此使民眾的個資外洩，成為受詐騙的高風險族群。

如果民眾有購機或門號需求，宜前往門市洽詢，更能獲得詳細的 3C 產品資訊及費率。

詐騙招數揭秘

透過電話行銷購買手機、平板電腦時應小心優惠的行銷包裝之下，可能隱藏著**品質不佳的產品**及**高額的電信費率**，而有**交易糾紛**，亦有可能因此使民眾的**個資外洩**，成為**受詐騙**的高風險族群。如果民眾有購機或門號需求，**宜前往門市洽詢**，更能獲得詳細的3C產品資訊及費率。

內政部警政署 165反詐騙諮詢專線

資料轉載自 yahoo 網頁