廉政宣導~1

已當監考員仍申請加班，詐領加班費

壹、 案情摘要

某機關約聘人員小孫，明知其已獲聘為公務人員升等考試監場人員，將於民國 100 年 11 月 13 日執行監考作業，同日不可能另至機關加班，惟其竟基於詐取加班費之犯意，於同年 11 月 11 日於該機關加班請示單上填寫加班時間「2011 年 11 月 13 日上午 9 時至同日下午 17 時共計 8 小時」、加班事由「協助總務科製作 100 年座談會開會相關資料」等不實內容，使不知情之各級長官逐級核准。嗣於同年月 14 日，因遭人匿名檢舉上開虛報情事，經該機關政風室查獲上情而未及領取加班費。

貳、 偵處情形

一、小孫對於被檢舉事項坦承不諱，該機關政風室爰策動小孫至地檢署辦理 自首。

二、 案經檢察官偵查終結，認小孫涉犯刑法第 339 條第 1 項、第 3 項之詐欺取財未遂罪，惟以緩起訴為適當，乃定 2 年之緩起訴期間，而為緩起訴處分，並命 其向國庫支付新臺幣 5 萬元。

三、 小孫經該機關考績會決議核予申誡 1 次處分。

參、 弊端癥結

一、 審核作業未臻嚴謹小孫以協助總務課製作會議資料為由申請加班，主管人員因未能掌控部屬當日之工作狀況，致未能將其申請予以核退。

二、 未落實加班查核作業小孫當日擔任公務人員升等考試監場人員，事實上不可能另至該機關加班，如該機關如能落實加班查核作業，當日即可發現異常，機先處理。

肆、 具體改進措施或建議

一、 落實實質審核機制單位主管對於屬員之申請加班，須依其每日工作量及實質內容加以審核，而非流於形式；機關應制定加班查核作業相關規定，由人事機構不定期（包含假日）辦理抽查。另針對同仁申請於假日至機關加班，或申請於機關外加班之情形，單位主管應不定時進行督訪，除瞭解同仁加班狀況，適時予以協助外，並可收嚇阻之效。

二、 落實平時考核，機先風險控管主管人員應注意同仁生活交往狀況，善盡監督考核之責，如發現屬員有作業違常或生活違常之情事，應即時予以適當輔導，機先防範違紀情事發生。

三、 加強廉政法治教育利用各種公開集會場合，向機關同仁加強宣導相關加班費請領之相關規定，使同仁瞭解詐取加班費所應負之法律責任，避免因一時不察或心存僥倖而觸犯法令。

•資料來源: 臺中市政府水利局·政風室

廉政宣導~2

包庇下屬

(1) 案情摘要：

A為甲機關技術員，負責廢棄品收繳、分類、儲存及配合廠商就廢棄品標售提領作業等工作。

某年乙公司得標甲機關「○○○廢品標售」採購案，A擔任廢品庫廢品管理人之職務，對該等廢品之提領作業有指揮監督廠商職權，竟基於藉勢、藉端勒索財物之犯意，向乙公司之負責人B要求支付80萬元，B不甘被勒索，遂於交付現金時錄音錄影， B再將錄音帶及錄影光碟透過甲機關不知情承辦人C轉交給A之主管D。

嗣後D於檢視錄影帶發現上情，旋約談A說明，約談間A坦承確實有收取廠商現金，惟D恐舉發上述貪污犯行，將導致採購案節外生枝而無法順利結案，爰基於對A貪污犯行不予舉發之犯意，裁示A速將該筆現金返還廠商，並就其所收受上開錄音帶及錄影光碟，既不予以登記留存稽查，亦不向上簽報。

本採購案提領貨物程序完成後，D又以A「工作努力成效良好」為由，考核A嘉獎1次，未再就A所遭檢舉貪污之事宜為進一步之調查，企圖掩蓋A之犯行。

(2) 所犯法條：

D明知所屬人員A確實有向廠商收取80萬元現金，僅要求A將該筆現金返還廠商，卻不舉發A貪污犯行之行為，觸犯貪污治罪條例第13條第1項「包庇不舉發罪」。

資料來源: 法務部廉政署刑事責任案例彙編

廉政宣導~3

誣告檢察官收錢

(1) 案情摘要：

A 與甲、乙公司之負責人 B、C 因瓦斯防爆器之專利授權、著作權等糾紛爭執，A 認 B、C 等人製造並銷售瓦斯防爆器違反專利法，爰向丙地方法院檢察署提起告訴，由 D 檢察官承辦。因 A 對於 D 辦案過程有所不滿，明知 D 未曾前往甲公司、C 之住家收取百萬現金，竟基於意圖使 D 受刑事處分之誣告犯意，於某日向臺灣高等法院○○分院檢察署檢察官 E 具狀指稱：「D 於某日夜間親自至甲公司、C 住家收取百萬現金，並令分局偵查員，僅搜索不查扣現場四萬個仿冒品」等語，誣指 D 犯貪污治罪條例之違背職務收受賄賂罪，雖經○○地方法院檢察署以查無事證而簽結，然仍使 D 受有刑事訴追之危險，且徒費司法資源。

(2) 所犯法條：

A 向臺灣高等法院○○分院檢察署檢察官誣指 D 至甲公司、C 住家收取百萬現金之行為，觸犯貪污治罪條例第 16 條第 1 項「誣告他人貪污罪」。

資料來源: 法務部廉政署刑事責任案例彙編

公務機密維護宣導 ~1

保密從守法開始

◎李建宏

乍看之下，「保密防諜」猶如過時的口號。然而事實上，保密防諜不但一直存在於我們 身旁，更在當今激烈的企業競爭中被發揮得淋漓盡致；對於國家來說，當然更是如此。 企業的秘密，關係著他們的獲利來源；國家的秘密，則影響全民的安全，涉及層面之廣， 尤顯得重要。在現今科技日新月異的時代裡，隨著網路不斷發展，人們藉由無遠弗屆的 資訊傳播，能輕易傳送並取得所需資訊，更凸顯保密之重要性與必要性。尤其是國軍部 隊，一旦資訊安全出現漏洞，敵人便可輕易竊取我機密資訊，對國家安全將產生無法估 計的威脅。 儘管臺灣之重要機關多已建置網路實體隔離機制，並訂定完整周延之安全規範，但資安 違規事件仍然偶有發生，究其主要原因，仍以人為因素為主。面對全球資訊戰的威脅， 相關人員如因一時作業疏失，未能確遵通信保密規定，導致機密資訊外洩，或因外在誘 惑而將本身業管內容透漏給外人，將對國家安全與全民利益造成重大損害。 先前媒體曾陸續報導幾件國軍軍官洩密案，多是受到金錢或美色誘惑。是以保密警覺之 提升必須從「守法」開始要求，法令規定的事項，就是規範國人保密的基本責任，不得 恣意違犯。對於違反保密規定者，資安督導人員應秉持「毋枉毋縱，除惡務盡」的原則， 必須依照規定追究其責任，整飭保密紀律，絕不可姑息放縱，進而導致洩密事件一再發 生。至於保密的要旨，是要人人懂得謹言慎行、守口如瓶，懂得拒絕誘惑，任何機密資 訊，少一個人知道，就少一分洩密的顧慮，唯有人人養成良好的保密習慣，才不致使機 密資訊外洩，讓敵人有機可乘。 保密應是自然而為之事，應該視之為一種習慣或素養，並將之融入日常生活中，保持謹 言慎行並處處留心，必能防範洩密之可能。唯有真正從心底遵守，並建立「保密防諜， 人人有責」的觀念及資安防護的正確認知，才能貫徹保密。 審視當前兩岸關係發展形勢，國人

普遍缺乏敵情警覺，輕忽潛藏的危機。國軍肩負國家 安全重責大任，更應有先見之明，不可因兩岸交流頻繁、政治氣氛和緩而錯估形勢。只 要洩密者有心，國防即沒有真正安全的一天。因此，只有養成安全習慣，恪遵保密規定， 在外部的規範及本身習慣的雙重保險下，才能落實保密防諜。

資料來源: 自清流月刊 103年 9 月號

公務機密維護宣導~2

雲端下員工個人行動裝置的管理

◎魯明德

由於網路的普及與行動裝置的功能日益強大，加上雲端運算的推波助瀾，使得企業在資訊基礎建設上，出現兩極化的發展；在 X86 虛擬化技術逐步成熟下，處於後端的機房管理，集中化的趨勢越來越明顯，機房的伺服器是整併再整併，系統也是不斷集中，甚至連原本分散在世界各地工廠的機房，也有收回總部統一管理的趨勢。

但是，前端的客戶端，卻是朝向完全相反的方向發展。由於近年來智慧型手機、平板電腦的風行，前端使用者的裝置類型變得多樣化。未來，讓員工使用私人設備來處理公事，已經被許多大企業採納，即使像美國國防部這樣的機敏單位，都已同意員工使用自己的裝備上班。未來前端的發展趨勢將會日益分散，不再像過去只是 PC 單一平台。

小潘所處的高科技公司也趕上這個潮流，以往公司為了讓工程師 24 小時待命，都會配發一支手機給工程師；小潘就常常自嘲是雙槍俠，左右各配戴一支手機。隨著時代的進步，自己的手機已換成智慧型手機，而公司配發的仍然是傻瓜型手機。這個月開始，公司索性收回公發的傻瓜型手機，開放所有員工使用自己的智慧型手機、平板電腦或筆記型電腦等行動裝置，透過公司建置的無線網路環境，直接存取公司內部網路的資訊。

對於公司的這項政策，小潘有點適應不良，心想：這樣不就門戶大開，歡迎大家來偷機密資料了嗎？趁著這個月的師生下午茶約會，把他的疑慮提出來。司馬特老師喝口咖啡後娓娓道來。

目前國外有一些大型企業，包括 IBM、HP 等跨國公司，都開始開放員工使用自己的行動裝置，在確保資訊安全的前提下，讓員工上班時使

用自己喜歡的智慧型手機或平板電腦，以提升工作效率，這樣的風潮稱之為「員工自帶設備」（Bring Your Own Device，簡稱 BYOD）。

根據英國調查機構 Vanson Bourn 在 2011 年的研究顯示：開放員工帶自己的行動設備上班，有 78%的上班族認為，員工自己帶的電腦一定比公司提供的電腦效能更好。最重要的是，企業若推動 BYOD 的策略，員工會認為公司的管理思維比較先進，可以提高員工對企業的認同感，員工對於工作的滿意度也比較高。

國內的永慶房屋直營或加盟店的房仲經紀人，都是使用自己的 iPad，配合公司「i 智慧經紀人」的系統，提供看屋客戶最即時的服務，因為 iPad 是員工自己掏腰包購買的，也會相對珍惜使用。

小潘聽完司馬特老師的解釋，仍然惦記著資訊安全的問題，看老師都沒有提到，於是繼續追問下去。司馬特老師喝口咖啡接著說：員工自帶設備來上班，對公司的資訊安全確實是一大考驗；但是，如果能做好安全控管，將會是創造員工與公司雙贏的局面。

在員工個人自帶設備的安全控管上，首先要做的是身分認證與存取管理，要求員工的自帶設備上必須安裝公司提供的代理程式或 APP 程式，在登入時可以做身分認證之用，存取資料時，亦可做權限管理之用。其次，要建立行動裝置管理（Mobile Device Management，簡稱 MDM）機制，藉由螢幕的鎖定、遠端鎖定等操作，保護資料不被竊取，甚至在裝置遺失時，可以透過遠端刪除的功能，將公司資料刪除，以防機密資料外洩。

最後，透過虛擬桌面架構（Virtual Desktop Infrastructure，簡稱 VDI），員工日常工作所需的應用程式、資料庫，都是由後端的伺服器提供，操作過程中所產生的資料，也不會留在員工的自帶設備上，統統儲存在後端的伺服器裡；所以，客戶端的行動裝置就像是一個終端機，可以解決機密資料外洩的問題。

小潘聽完司馬特老師的一番解說，也有了另一層心得：原來資訊安全不是一味地防堵即可萬無一失，適當地採取資訊科技與管理措施，也可以化危機為轉機。員工自帶設備上班的現象，對企業來說就像是雙面刃，可以為公司節省採購硬體的成本，也能提升整體工作產能，但也有造成危安的風險。

行動裝置本身不是問題，資訊科技所要關注的，應該是行動裝置取用企業資料過程的安全管理，尤其是裝置的身分識別、網路存取等級和行動應用系統的管理措施，越早部署、效果越好。

資料來源:台中市政府水利局政風室

公務機密維護宣導-3

數位時代的保密防諜

「保密防諜、人人有責」這句口號，對六、七年級生來說，相當的陌生，但是對四、五年級的讀者而言，卻是非常的熟悉，以前不但在社區的牆壁上會看到它，在學校、部隊...等各種重要場合都可以看到這個標語。民國五０、六０年代，兩岸關係緊張，可謂是漢賊不兩立，雙方都有間諜在探視彼此的活動，到了民國九０年代，兩岸交流絡繹不絕，敵我意識漸漸模糊，保密防諜的口號亦漸漸式微。

想必大家都看過 007 情報員或長江一號之類的諜報電影，其中的間諜可能要透過特殊設計的照相機，把所獲得的資料拍下，再放到牙齒或身體的某處做為掩飾，再經過層層的轉送，才能傳回總部。

隨著資訊科技的進步，現在的 007 情報員不需要再用特殊設計的相機，時下的數位相機愈來愈輕薄短小，手機也多附有照相功能，要拍下重要資料是輕而易舉的，而且所有的資訊都資訊化、數位化，透過無線傳輸的技術，更是可以神不知鬼不覺的偷走機密資料，幾乎人人都可以當情報員。

在數位時代裏，不止是政府機關或是軍事部隊需要保密防諜，企業對機密資料的保護更是不遺於力，數位資料的特色是很容易被偷，而且被偷了也不容易被查覺，本文將介紹在數位時代中，企業機密資料的外洩管道，及各個企業如何防止公司的機密資料外洩。

根據微軟內部調查顯示，去年臺灣有近 1000 萬人次申請下載使用 MSN 軟體或申請帳號，35 歲以下的民眾，八成有使用 MSN 的經驗。研究機構 Yankee Group 針對全球即時通訊工具的市場研究報告指出，今（94）年底全球使用即時通訊（包括 MSN、Yahoo Messenger...等）的人數將會超過 3 億人，不少的企業都肯定即時通訊軟體的工作效率，如國內的 3c 大廠 NOVA，很早即利用即時通訊軟體來進行內部溝通。

資訊科技愈來愈發達，照理說使用這類軟體的公司應該也愈來愈多，但是，報載自今（94）年五月四日起，摩根富林明資產管理集團（JPMorgan Fleming Asset Management）全球的 16.4 萬名員工上班全面禁止使用 MSN，這又是甚麼原因？難道是怕員工上班時在網路上聊天？隨著 MSN、Yahoo Messenger…等通訊軟體的普及度越來越高，只要輕輕的敲擊鍵盤，公司機密即無所遁形，大部分企業對於其威都非常恐懼，特別是科技園區、金融單位不少企業明文禁用 MSN、Yahoo Messenger…等通訊軟體，主要都是怕機密的技術資料或者是客戶資料，透過 MSN、Yahoo Messenger…等通訊軟體傳給競爭對手。

除了 MSN、Yahoo Messenger…等即時通訊軟體外，企業洩漏機密的另一管道是電子郵件（E-MAIL），很多的企業為了防止這個洩密管道，都對電子郵件的資訊量及內容做管制，並且在郵件伺服器（Mail Server）上記錄員工傳送的資料，以便後續追查，雖然，此舉曾造成是否侵犯員工通訊隱私權的爭議，但是，為了維護公司機密的安全，各公司仍然採用此方式管制電子郵件。

萬用串列匯流排（Universal Serial Bus，USB）已成為資訊媒體新興的標準介面，只要擁有該介面的電腦週邊設備，都可以透過它來上傳或下載資料，加上行動碟與可攜式硬碟的容量都愈來愈大，一些大的檔案原來透過 3.5 吋的磁碟片不易下載、攜帶，此時都可以經由 USB 介面很容易的被下載、攜帶了。很多的公司為了防止員工藉由 USB 介面下載資料，會在員工的個人電腦上安裝偵測程式，一旦員工藉由 USB 介面傳輸資料，即會啟動網管安全機制，以維公司資訊的安全。

當然，為了釜底抽薪，有的公司甚至於把電腦上所有可傳輸資料的週邊設備全部拿掉，如燒錄器、軟碟機、USB 介面…等，以免員工有機會下載資料，俾能有效管理資訊的安全。

除了以上的防制作為外，很多的高科技公司為了讓公司內部的資訊不易被外界的駭客破壞或竊取，將公司內部的網路與外部網路進行實體隔離，讓外部的人無法接觸公司的資料，但是，這樣有好也有壞，公司

外部的人雖然無法接觸公司的資訊，相對的，公司的員工在外面也不能獲取公司的即時資訊。

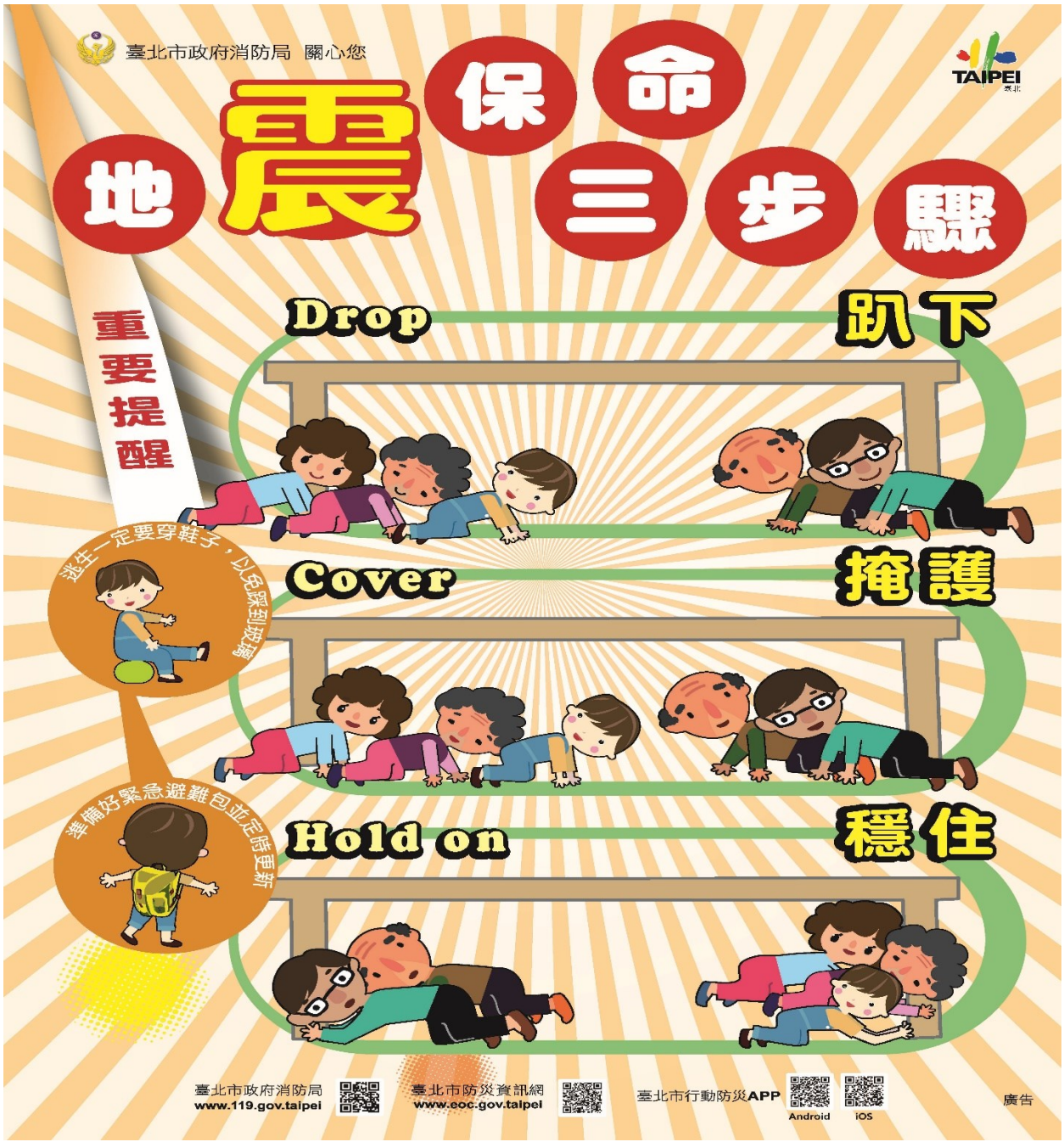
現在的消費性電子產品的功能愈來愈多，也做的愈來愈精巧，如具有照相功能的手機、個人數位助理（Personal Digital Assistant，PDA）...等，都具有儲存影像、資料及錄音等功能，均可能成為洩密的管道，很多科技公司不但管制員工使用，也要求訪客不能帶入公司，必須放在大門由保全人員或警衛先行代為保管，俟離開時再取回。

以上所談的都是企業對內部員工的管制作為及對訪客的限制，其目的不外乎就是維護公司的資訊安全，數位時代中資訊的價值愈來愈高，相對的，機密資料外洩後所需承擔的代價也是不可承受的高，我們在想受豐富資訊的同時，不能不想到保密的重要性。

資料來源:經濟部中小企業處

機關安全維護宣導~1

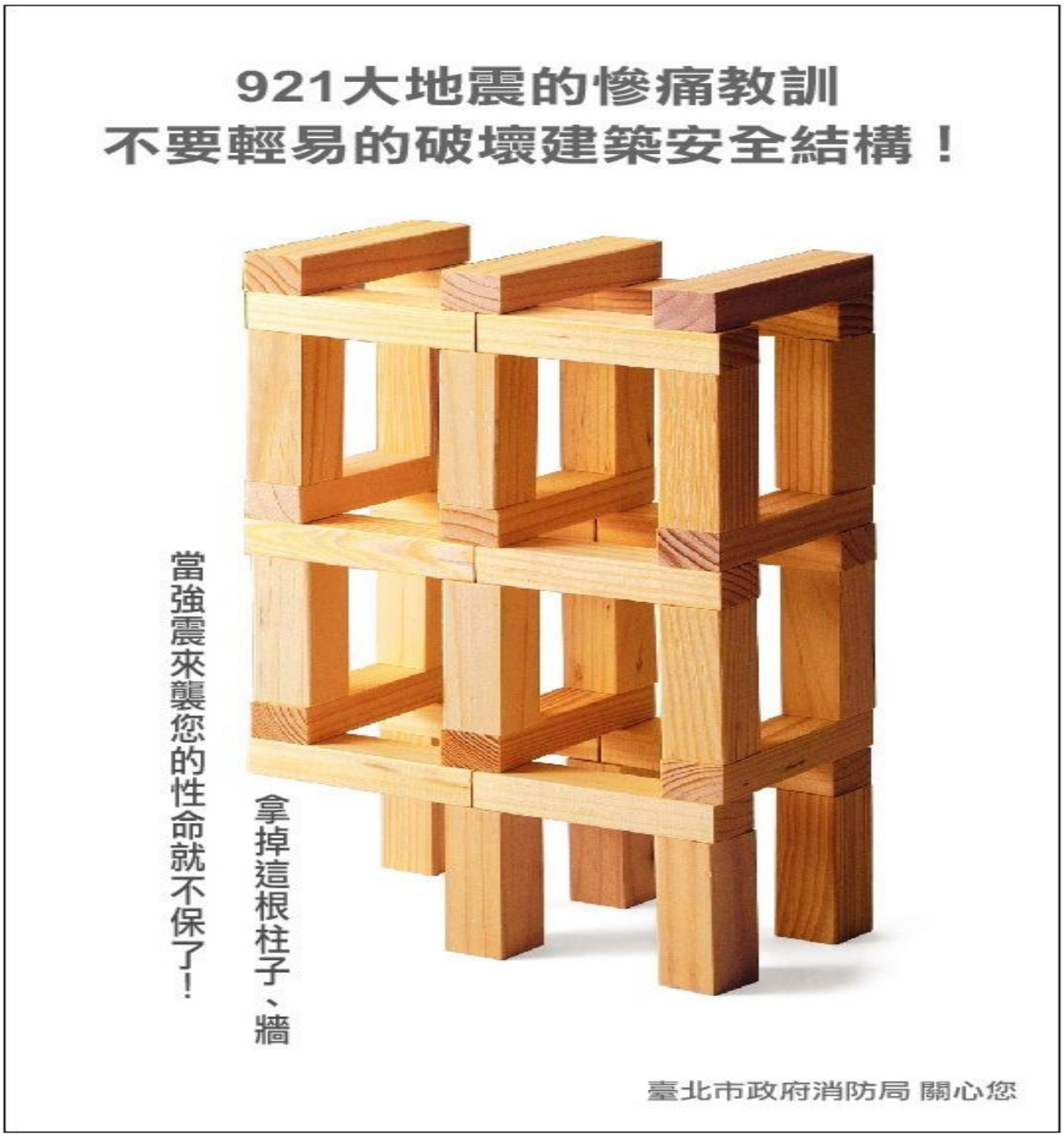
地震保命三步驟



資料來源: 臺北市政府消防局

機關安全維護宣導~2

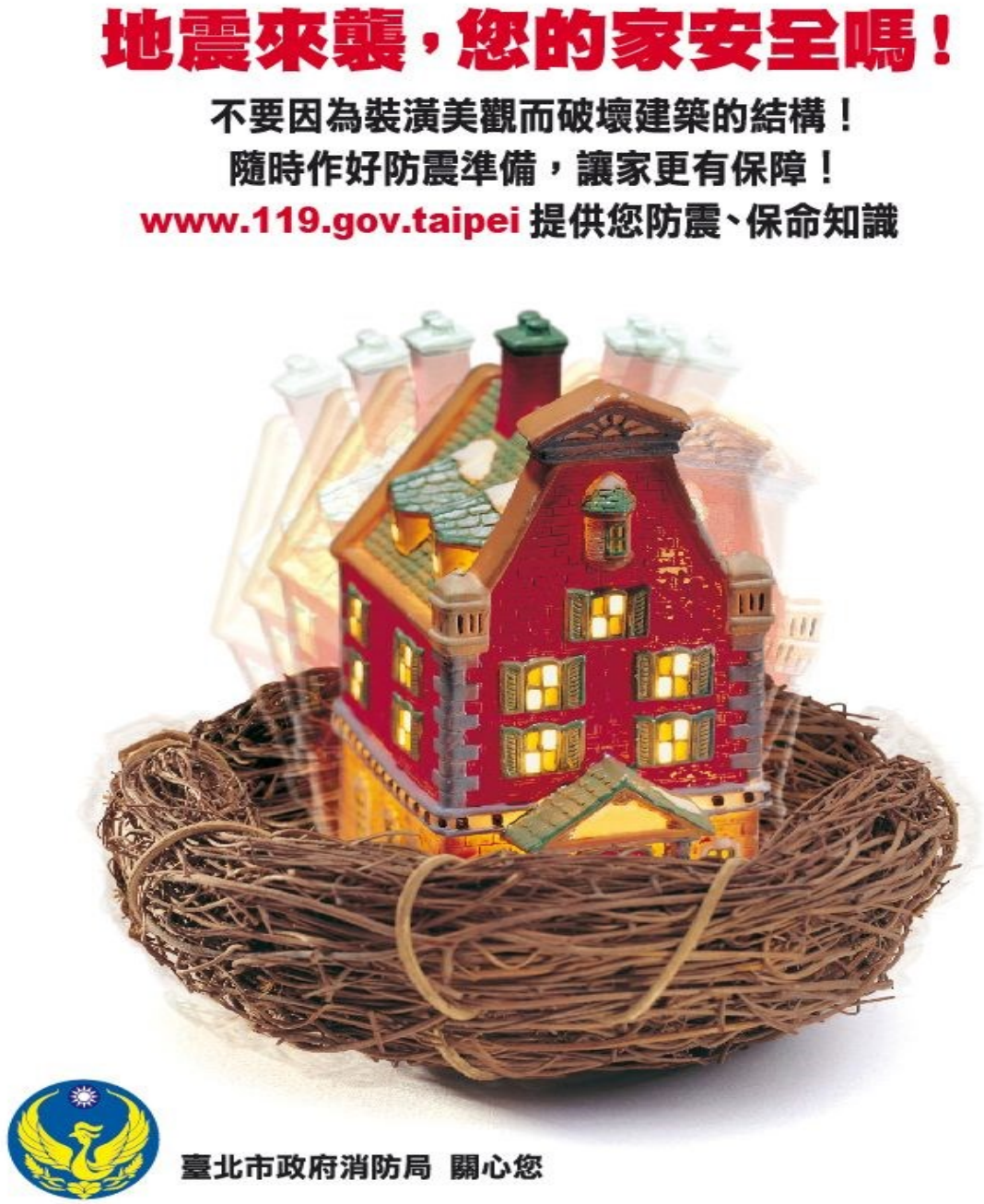
不要輕易的破壞建築安全結構



資料來源: 臺北市政府消防局

機關安全維護宣導~3

地震來襲，您的家安全嗎！



資料來源:臺北市政府消防局

消費者保護宣導~1

搭乘低成本航空，應該注意什麼事情？

低成本航空公司的票價之所以便宜，與業者採取「使用者付費」的經營模式有關，也就是節約可省下的服務成本，直接反應在機票價格上；此與傳統航空公司「包套式」(涵括餐飲及人工作業等)的服務有很大差異。正因如此，消費者易因認知落差而衍生消費爭議。

提醒消費者，在購買低成本航空公司的機票時，應注意下列事項：

一、 通常不能退、改票：訂票後，通常不能退票或改票(如改期)；即便可以，亦需支付高額手續費；此外，有些業者則有提供加購改票費用的選項，以保留日後改票的彈性。建議消費者在購買機票前，務必先確認行程，並進行適切的選擇。

二、 託運行李要加價，事先購買較便宜：若未於訂票時預先購買託運行李服務，在機場會被加收高額超重行李費。

三、 航班上的附加服務要收費：若要選擇機位，或在機上需要餐飲、枕頭毛毯、娛樂設備等，通常需額外付費。此外，有部分業者會在訂票網頁上預設勾選附加服務，行政院消保處已請民航局督導業者應充分揭露，並提供便利的取消預選方法。消費者若不需要附加付費服務，可點選取消。

四、 票價是浮動的，不是天天都超值：票價會依旅遊淡旺季、航班平假日、有無特殊促銷、提早多久買票等因素而不同。若等到出發前才訂機票，可能不見得划算。

綜上，消費者在購買低成本航空公司的機票時，務必睜大眼睛，注意網頁公告的相關規定與限制，才能有一個既省荷包又愉快的旅程。

資料來源：-轉載行政院消費者保護會網站