安全維護宣導

《如何維護機關同仁人身與設施之安全》

由於社會型態的快速轉變，在愈趨複雜的環境下，各類犯罪及意外災害頻傳，以機關危安事件而言，不僅造成同仁人身或機關財物等損失，更影響機關形象及整體公務運作，故落實各項安全維護作為，係有效確保機關內部安全的不二法門。以下將舉出數個機關危安事件肇生的主要原因及策進作為，以為防護。

注意電器設備之安全使用：針對老舊設施應將電線設備重新拉線更新，同仁使用電器設備亦應謹慎，勿長期使用、勿超過負荷、以維護電器設備安全。另重要電機房應保持通風，嚴禁堆置物品，以免發生危險。如果不慎起火，應使用**乾粉滅火器**滅火，不能使用水或泡沫滅火器，否則會因為水的導電特性，不小心觸電。

非上班期間加強管制，加強留意是否有民眾逗留：雖然許多機關係開放式空間，惟單位同仁下班前仍應做好管制 措施確認已無洽公民眾於非上班時間仍逗留於機關內，以免發生辦公設備失竊或公文書遺失事件。下班後及例假日則應執行出入管制，以員工識別證進行驗證通行。

設定保全系統並確保保全公司能夠即時派員處理突發狀況：辦公廳舍遭人侵入，卻因機關未設定保全系統或保全公司未即時派員處理，最後導致設備遭竊之情況時有所聞。建議定期加強值班人員教育訓練、定期測試保全公司反應能力及防護效率。

注意辦公廳舍周遭有無遭置放易燃、爆裂物或其它危險物品：辦公廳舍周遭通常停放有不少汽機車，如遭縱火或類似意外，可能發生嚴重後果，應加強巡查並透過全體員工共同維護。若知將有大型抗議活動時，應請求警察單位支援警力並通報政風單位，降低抗議者因情緒失控而置放危險物品之可能。

平時即應注意辦公廳舍安全狀況，定期辦理安全檢查：平時即應注意「滅火器是否仍在有效期限內」、「是否有定期辦理電梯安全檢查」、「機關出入門口、樓梯、走廊及逃生通道上禁止堆放雜物」等辦公廳舍內之設備安全降低災害發生機率。

培養員工安全意識，密切注意可疑之人、事、物：多數行政機關為開放式服務機關，民眾進出頻繁，實施門禁管制不易，惟仍可請服務臺或保全人員加強辨識可疑人物，例如：疑似攜帶危險物品、穿著不合時宜、詢問特定人員位置、嘗試進入非洽公區或其他形跡詭異行為，並適時詢問洽公事由藉交談過程中初步判別是否有不良意圖，提高警覺 。

充實機關監視設備系統：發生糾紛時，雙方往往各說各話，為有客觀證據還原事實，充足的監視設備不可或缺；此外，監視影像亦可用於預先發現洽公民眾有無異常舉動，以為因應。

結論：機關內部安全防護主要作為在於「防災」、「防竊」、「防破壞」、「防資料失散」以及「做好重要器材設備的維護」等，換言之，可說是一切為「人安」、「事安」、「物安」、「地安」而密切執行之作為，此皆須仰賴全體機關同仁共同配合。注意周遭的一切，便是幫了機關安全一個大忙，也為自己的上班環境表達出一份關心與愛護。

資料來源：法務部行政執行署

滅火器使用方式：提起滅火器→拉開安全插梢→握住皮管，朝向火苗→用力握下手壓柄→朝向火源根部噴射→左右移動掃射→熄滅後澆水將餘燼冷卻→保持監控確定熄滅

機密維護宣導

《考驗人性的 社交工程誘惑》

自從人們可以利用網際網路互通有無，每個人至少都擁有多個網路服務帳號，包括個人或其所屬單位的電子郵件帳號；正因如此，利用資訊科技便利之社交工程犯罪行為層出不窮，且趨勢逐年上升。社交工程即為人與人之間的攻擊。過去關於此類攻擊定義為「攻擊者藉由社交手法取得系統或網路的資訊」，然而現今攻擊者的目標，已逐漸轉到個人擁有之資訊。此攻擊管道，最常見的為電子郵件、簡訊、即時通訊軟體（如 Messenger、Skype、Line、Instagram、WhatsApp）等等。為何此種攻擊趨勢會逐年上升？因為對駭客而言，這是最有效、最省成本的攻擊方法。

社交工程郵件之包含要素

以電子郵件來詐騙至少已有十年歷史，然至今仍有民眾上當，因為民眾輕忽或無知，易讓駭客達到欺騙目的。社交工程電子郵件不乏利用聳動的郵件主旨、偽造受害者熟悉的寄件者、以假亂真的郵件內容等等，試圖吸引使用者上鉤。社交工程電子郵件中會有幾個要素，包含超連結、附件、圖片、郵件內容內嵌程式碼。

◆ 超連結：有可能會讓受害者連至攻擊者所架設之惡意網站，藉此收集受害者相關資訊。

◆ 附件：多含惡意程式，開啟並執行後會潛藏在受害電腦裡，直接將電腦內資料對外傳輸、偷偷側錄用戶使用電腦的任何行為、接續下載惡意程式至受害電腦再執行各項行為等。

◆ 圖片及郵件內容內嵌程式碼：能回報給攻擊者表示「登陸成功」，更甚者直接讓受害者電腦自動從中繼站下載小程式（諸如鍵盤側錄工具、螢幕側錄工具等），記錄受害者使用電腦行為，再進行下一步攻擊。

以上要素不一定會同時出現，亦可能交互搭配使用，曾有僅憑單一內容即欺騙成功的案例，造成受害者損失。例如，假冒會議邀請信函，成功欺騙到受害者出門參加會議，加害者利用這段時間闖空門等。

社交工程之攻擊方式

只要個人一時疏忽，即使只是小小電子郵件，就有很大機會對企業、群體，甚至國家安全造成危害。另外，即時通訊軟體也成為社交工程攻擊管道之一，以下再列舉其他社交工程之攻擊種類：

一、濫發電子訊息：諸如惡意電子郵件、釣魚簡訊、即時通訊等文字訊息。此類攻擊通常一次廣發給多名使用者，因此亦稱為「垃圾郵件」。

二、釣魚：此類攻擊通常會讓使用者「信以為真」，透過話術讓人誤信，進而騙取錢財。近期常見「假交友」、「假投資」即屬此類。

三、願者上鉤：經典手法為攻擊者在公司門口隨意丟棄一個隨身碟，該公司不知情員工撿到後，誤以為是公司內有人不小心遺失，為了順利歸還，故而將該隨身碟插進自己的電腦內，殊不知惡意程式就此開始執行。

四、搭順風車：尾隨員工進入外人不該進去的區域，進而竊取到公司內部機密資訊。

五、水坑攻擊：利用網頁藏惡意程式碼的方式，讓使用者的電腦中毒。只要入侵或偽造目標受害者常瀏覽的網站，植入惡意程式，當受害者瀏覽該網站，即會下載惡意程式。

社交工程攻擊之防範措施

社交工程攻擊防不勝防，面對攻擊，可行的防範措施包含：

一、使用垃圾郵件過濾器：現行的郵件伺服器（包括 Gmail）皆有此機制。

二、定期更新：隨時更新防毒軟體、防火牆與電腦及手機的作業系統，以防任何安全性漏洞被利用。

三、仔細確認：確認訊息與自己是否相關，並查證訊息來源，有必要時打電話向來源確認。倘於公務信箱發覺有惡意郵件切勿開啟或點閱惡意郵件所附連結或檔案，並請同仁按「關閉預覽功能取消方式」及自行檢視是否已取消「自動轉寄功能取消方式」。

資料來源：法務部調查局清流雙月刊第37期