# 麥寮鄉公所政風室112年8月機關安全維護宣導

## 1.機關安全維護宣導－－砸窗疑雲

前言

公務機關屬於開放式服務場所，範圍廣闊且通常無圍牆防護，且出入口、死角眾多，假日巡邏門禁管制不足，民眾可在廳舍周圍自由進出或逗留，惟可規劃增設監視器及辨識警報效能、強化死角區域安全、請保全人員加強巡邏頻率，並關心非上班時段逗留、徘徊、行為舉止異常的民眾，將可能的危險因子降低，確實保護機關安全。

案例摘要

正值母親節假期，正午的太陽照得路面熱氣蒸騰，公園、廣場裡嬉鬧的孩子窩在家中吹冷氣，人們都躲到百貨公司、大賣場、餐廳與家人歡聚母親節，周邊道路塞的水洩不通，有位機車騎士頂著大太陽行經快樂市市政府車道，突然拿出一塊石頭猛力砸向市政府帷幕玻璃，「砰」的一聲砸出一個大洞，顯然他過得不快樂。這聲響並沒有引起巡邏的警察注意，該騎士一溜煙跑了。下午三點，巡邏員警發現一樓快樂館的玻璃被砸破，緊急通報警察隊長及相關部門到場處理，經調閱周遭監視器，發現該機車騎士涉有嫌疑，迅速將相關資料送交警察局調查。隔日，快樂派出所來電「男子阿泰因工作不順遂，領不到薪資，目前人在派出所陳情，且表示他心情很差，將再到市政府砸玻璃洩憤，若再找不到工作且相關機關不積極協助處理，將帶汽油和番仔火至市政府門口自焚，目前人由派出所離開，請勤務同仁落實勤務，加強巡邏管制。」至此，砸毀玻璃真相始大白。由上述案例研判，疑係勞資糾紛使民眾心生不滿，乃砸玻璃引起注意，希望政府相關機關介入關心。機關玻璃帷幕未裝設警報器、未有護欄或圍牆等阻絕設施、警察維安巡邏頻率不足、中央監控室未有危安預警等，致廳舍假日安全出現漏洞。為避免類似情事，各級機關及學校應建立假日安全維護控管制度為妥，不因假日而鬆懈管制。另各機關並應建立完善之監視系統及人員辨識管理機制，加強安全維護宣導事宜。

結語

機關安全猶如飄渺的空氣，時時環繞在機關同仁四周，承平時期安全維護工作似乎微不足道，在危安發生時是能有效降低機關損害的作用。防範危安事件之發生，貴在「弭禍於未萌、防患於機先」，除各機關應積極掌握狀況事先通報外，全體員工並應發揮協助處理的功能。安全維護是具有層次變化的工作，而潛在危安

人員之生理、心理等情狀頗為複雜，可能會因機關人員的及時介入，使危安事件不會發生或不再擴大。對辦公廳舍之巡邏安檢應予重視，並提升廳舍死角及高風險區域之管控，多一分預防就少一分損害。本案凸顯機關維安巡檢問題，值得作為機關安全維護工作之借鏡。

## 2.生活中的資安

在網路資訊發達的年代，駭客偽裝成一般使用者來散播惡意鏈結進行釣魚已是常態，因此資安意識對於民眾而言已是必修課題之一。防範作為有：

(一)提升潛在威脅警覺性：當收到陌生訊息、開啟未知網址、下載非官方軟體時，人們其實難以辨別其中是否夾帶惡意行為或攻擊，應提高警覺性，避免落入駭客陷阱。

(二)陌生訊息：當使用者瀏覽社群媒體上陌生人所發布的訊息時，應時刻保持懷疑的態度，在進入網址前要先查證訊息的正確性。如 NFT 遭盜取事件中，在社群網站看到 NFT 鏈結時，應先去向官方求證，而不是相信社群網站的訊息。只要使用者對內容產生懷疑並查證，就可以有效避免釣魚事件發生。

(三)未知網址：收到朋友傳遞的未知網址時，使用者應先確定該消息為本人傳遞，才點擊鏈結。如案例 FB Messenger 點擊網址詐騙中，使用者在收到可疑鏈結後，可透過打電話的方式來確認朋友身分的真偽，避免朋友的個人帳號遭到駭客利用而不自知。

(四)使用威脅檢測軟體：使用檢測軟體可以有效偵測惡意鏈結和惡意程式，大幅降低使用者被釣魚的風險。當使用者遇到必須點擊陌生鏈結或執行來歷不明檔案的情況時，可以利用 Virustotal 檢測軟體，使用者將鏈結或檔案上傳後，該軟體會自動偵測其是否被資安廠商認證為惡意鏈結或檔案，並產出相應的報告。使用者可自行評估該檔案所伴隨的風險。基於安全考量，倘若有任一廠商對該鏈結報有疑慮，建議使用者不要點擊。