113年8月號

公務機密
資訊安全維護

農業部林業及自然保育署臺東分署

公務機密 資訊安全維護

目錄

首長及將官座車傳用到中國製行車紀錄器恐洩密 軍方下令全面大清查

（取自憲兵指揮部臉書）

〔記者羅添斌／台北報導〕2024/07/07
在野立委先前指控軍方多個部隊單位安裝的光電設施及電腦設備，得標廠商竟然違約使用中國製產品設備，國防部軍備局則公布部分清查結果，表示已立即拆除停運，將諮詢法務懲處作為。但包括將官座車、指揮官戰備督導車在內的各式軍用行政車輛，車上的行車紀錄器，也被立委質疑可能使用到中國廠牌再貼牌偽混為台灣產品，將會使得高階軍事首長的行蹤有外洩之虞。

國防部今天表示，現已對各單位安裝之行車紀錄器實施全面調查，如查獲中國品牌設備則立即停止使用，防杜資安罅隙。

國防部指出，國軍車輛出勤使用行車紀錄器等攝錄影設備，係為確保駕駛行車安全及道路行駛權利。國防部各式公務車輛安裝行車紀錄器均依「國軍營內民用通信資訊器材管理要點」辦理申請及管制。

儘管軍方三令五申，要求得標廠商不得使用中國廠牌產品及設備，但仍有不肖廠商心存投機，在光電設備、電腦系統的部分零組件設備上，違約使用中國設備，軍方人士說，有關軍用行政車輛使用的行車紀錄器是否使用中國生產設備，或是以貼牌方式混裝為台灣品牌設備，日前已下令全面大清查，只要查到任何一件有此情事，一律先行更換，並追究失職人員及違約廠商責任。

軍方人士說，軍用行政車輛包括將官行政用車、各級指揮部指揮官的戰備督導車在內，由於是由重要軍職指揮官、參謀業務主管在使用，廠商若是違約使用中國製的行車紀錄器，很可能會因為行車紀錄器有後門的系統裝置，造成軍事首長、各級指揮官的行蹤外洩，遭到有心人士掌控。

民眾黨立委黃國昌6月底揭露，陸軍蘭陽地區指揮部光電標租案，被聯合再生集團旗下的永梁公司違約裝上中國製太陽能逆變器。7月4日再爆料稱，聯合再生不只逆變器，甚至連接網路的路由器及控制用工業電腦，全都是中國製造，其中還包含中國華為生產的路由器。國防部軍備局公布部分清查結果，表示已立即拆除停運，將諮詢法務懲處作為。

科技防詐！
資安院發表AI技術 每天偵測平台萬筆詐騙

數位發展部今天舉行「資安院AI打詐技術發表會」。（記者徐子苓攝）

〔記者徐子苓／台北報導〕2024/06/19
打詐是新政府首要任務之一，隨著AI技術日益成熟，資安院運用機器學習、自然語言處理等技術，研發出更高效率的詐騙識別工具，每天偵測網路平台近1萬筆的可疑詐騙貼文，通報平台業者後的下架比率達9成，平均約8小時可成功下架。未來資安院將和平台業者協調下架的「自動化」流程，盼在最短時間內移除詐騙廣告。

數位產業署委託資安院研發「詐騙關鍵字提取、資料探勘深化、訊息溯源」等系列打詐技術，由資安院9位成員參與，經費2000多萬，除了快速協助相關單位識別詐騙訊息，並能透過持續觀測，提前預測並防範潛在的詐騙行為，提升詐騙識別的效率和準確性。

數位發展部今天舉行「資安院AI打詐技術發表會」，資安院前瞻研究籌獲中心經理江禹賢分享詐騙廣告的「變臉術」，根據資安院統計，詐騙廣告出現最多的關鍵字竟是「詐騙」，這些貼文多強調自己不是詐騙，甚至主打幫民眾追回詐騙財損。

江禹賢說，今年5月時資安院發現，光一個月就有超過20萬篇詐騙廣告出現在平台上，其中有97%的詐騙廣告刊登不到2天，因為刊登時間太長，就容易被偵測到並下架，提高詐團的詐騙成本，因此對詐團來說，廣告刊登1到2天是最有效益的。

資安院副院長林盈達表示，資安院透過AI辨識詐騙廣告的特徵，進行「末端清掃」，例如偵測帳號是否有藍勾勾、貼文中的LINE連結有沒有動手腳等等，目前準確度已經達到93%，只要再加上一點點人工確認，就能得到完整的名單，再通報請平台業者下架。

林盈達表示，數發部在3個月內會建置「打詐通報查詢網」，把資安院主動用AI偵測到的詐騙廣告、投放的詐騙粉專等等，匯入查詢網的資料庫。也就是說，未來除了民眾通報以外，數發部也會主動透過AI匯入可疑內容，民眾就能查詢到詐騙貼文或有疑慮的LINE ID。

風傳媒

不小心侵權了？
詐團冒名「釣魚信件」最新手法曝 一點開「個資全外洩」怎補救？

陳怡穎 2024年7月5日 週五

近期詐騙猖獗，其中「釣魚信件」成為最常見手法之一，近期有不肖分子竟仿冒《風傳媒》法務名義寄送通知，聲稱「版權被侵害」，接獲郵件的民眾一旦點開連結，恐怕會造成個資外洩！

近期有不少民眾收到一封自稱是來自《風傳媒》法律代表的通知信，告訴收件者「非法使用我們的圖片及視頻，在Facebook的臉書專頁上宣傳產品」，要求立即在24小時之內刪除相關資訊，甚至語帶威脅的警告「如果您在24小時內不遵守這些要求，可能會面臨嚴重後果」，同時附上一則來源不明的連結以及密碼，要求收件者開啟。

《風傳媒》近期遭到不肖人士冒名寄送侵權通知，實為「詐騙釣魚信件」，收件者千萬別點！

然而事實上，仔細看看這封內容，除了字裡行間使用「視頻、信息」等非台灣用語，字型粗細更是錯落不一，破綻百出。據了解，近期已有多家企業行號、媒體公司遭冒名，《風傳媒》強調，類似的信件內容皆為有心人士的冒名惡意釣魚信件，並非集團所發出。

要怎麼辨認釣魚信件？不小心點開怎麼辦？

刑事局近期也針對類似的「釣魚詐騙信」提醒民眾，詐騙集團經常以假冒他人、知名企業、公司高層等方式，發送偽造郵件，內藏釣魚連結或是木馬程式，以此騙取個資。
民眾平時發現含有不明連結之信件，可多加檢視電子郵件信箱地址，是否有相似的字母或數字加以混淆，千萬不要輕易點選信件內的任何檔案或連結，以免個資通通外洩。

萬一民眾已點選連結開啟，資安專家建議，可立刻將手機的雙重認證開啟，並盡快修改手機裡儲存的密碼，就能盡量減少個資外洩的風險。

每月一常識

新版個人資料保護法與過去有很大的不同，新法進一步擴大了個人資料的保護範圍，並且讓所有產業一體適用；新法甚至首度增加團體訴訟，而且違法的罰則也加重了，企業老闆要負更大的責任。接下來，我們以60個Q&A，快速帶你認識新版個人資料保護法

Q4 以紙本記錄的個人資料，會受到新版個資法的規範嗎？

A 新版個資法擴大對於個人資料的保護，不論是經由電腦處理的個人資料，或是手抄記錄的個人資料，都受到規範。

文/iThome

資安宣導—盤點 7 種常見的資安風險，看看你犯了哪些錯？

民眾別以為駭客對於一般人個資不感興趣，事實上，有大量個資內容在網路黑市以高額價格販售給包含色情集團等不肖業者。資安攻擊，其實時時刻刻存在，以下盤點 7 種日常生活中常見的資安風險。

風險一：網路釣魚

網路釣魚可說是最常見的攻擊手法。網路釣魚時常搶搭熱門時事話題，如疫情、三倍券、雙 11 購物等，透過各種管道偽裝，如釣魚簡訊、釣魚郵件、一頁式網頁等，企圖欺騙消費者個資。這種手法常以釣魚郵件將使用者引導至偽裝成真實購物網站、銀行、信用卡公司或網路服務等之合法登入頁面的假網站，藉以竊取使用者在該網站所輸入個資。

風險二：連接公共 Wi-Fi 要考慮

由於 Wi-Fi 是以電波進行通訊，若是民眾連接到安全措施不完備的 Wi-Fi 或是駭客故意設置的假 Wi-Fi，例如駭客創造與公共 Wi-Fi 名稱相似的假熱點，讓使用者在不知情的狀況下登入 Wi-Fi，以竊取個資。換言之，民眾在使用公共 Wi-Fi 的過程中，可能面臨遭受第三方惡意偷窺、通訊內容被監視的風險。

風險三：惡意 App

一般民眾普遍認為手機不會中毒，但是目前非法應用程式已是智慧型手機的主要威脅之一，在應用程式商店上也可能有非法應用程式，駭客會利用惡意網址或惡意 App 盜取手機上的重要資料，民眾用手機遭到詐騙的機率很高。

風險四：軟體漏洞攻擊

因軟體漏洞而遭受攻擊，惡意軟體或惡意應用程式會針對作業系統等安全漏洞進行攻擊，例如駭客利用瀏覽器漏洞植入病毒，或是駭客透過網路直接攻擊系統漏洞（類似像 WannaCry 勒索病毒）。

風險五：瀏覽被入侵的網站或惡意連結，被導向下載惡意程式

民眾一旦瀏覽遭受惡意入侵的網站或是點擊惡意連結，可能會導致裝置被下載惡意程式，而遭受勒索或重要資訊外洩。

風險六：詐騙訊息

詐騙訊息也是十分常見的手法，駭客透過電話、網站導向、彈出式視窗廣告、釣魚郵件等發送詐騙訊息，接觸潛在目標。像是在社群媒體上散播假免費服務電話、假技術支援網站連結等，用來誘騙在線上搜尋技術支援資訊的使用者點入網路釣魚網站或撥打免費服務電話，取得受害者個人身分資料或讓受害者為其「服務」付費。

風險七：不安全的家庭路由器或 IoT 設備

隨著家庭聯網設備越來越多，除了為生活帶來更大的便利性，卻也為駭客提供更多的入侵節點。智慧家庭生活日趨便利，家用網路潛在資安風險也持續升溫，一旦家中路由器安全性遭破解，駭客可以隨意入侵各式連網裝置，使家中成員的資訊安全暴露在高風險下，導致智慧連網裝置遭竊聽、誘導至非法網站而遭詐騙或感染病毒，使得民眾隱私外洩，進一步造成財產損失。

資料來源:雲林縣斗六市公所