資策會科法所TPIPAS講座：個資外洩不容忽視 企業應強化資安意識

科技與網路的進步，牽動全球跨境購物模式。眾多企業建構虛實整合的通路，為消費者提供便捷的網購服務與取貨管道，包辦大眾的生活大小事，改變現代人的思考和□為模式。但網購平臺造成駭客攻擊、資安事件、個資外洩衍生詐騙案頻傳，資策會科法所為重視此問題，邀請刑事警察局警務正林君豫以「個資外洩事件之防護暨應處作為」為題，與學員講解165反詐騙諮詢專線高風險賣場趨勢、詐騙話術關鍵字、詐騙手法與管道等個資外洩跡象，並分享日常防詐的因應之道，有助於提高大家對網路活動的警覺心和資安意識。

近年來社會上層出不窮的新形態詐騙手法，如駭客假借政府機關名義寄發惡意釣魚郵件，使收件者誤載惡意程式，而致個資外洩的風險。林君豫更進一步舉出「165反詐專線」遭不明人士偽冒名義的案例，以此例教導大家辨別釣魚信件，並從疑似官方信件中追查事實，下為防範可疑電子郵件的注意事項：確認寄件信箱帳號與郵件伺服器，是否為可疑的國外電子信箱的註冊網站；留意內文單位名稱，是否誤植其他單位之聯繫資訊；查詢可疑網址，是否在網域查詢工具 (Domain Tools) 上為境外的IP 位址；檢查信件內文的字體與網路常用語，是否為兩岸差異用詞（如用網路寫成網絡）或簡體字。使用者依這四處細節，自行查證信件來源，分辨其真偽，才能減少社交工程的傷害，避免個資外洩。

講座尾聲，林君豫宣導個資外洩的處置作為，特別說明公司組織接獲詐騙的基本程序（來源─法規依據─報案單位─報案資料─完成報案），有助於提高企業於個資外洩事件應變能力，林君豫更指出，企業應於日常業務妥善留存個資的軌跡，以配合外洩調查的需求。當企業接獲詐騙，建立適當的處理流程，第一步：接獲「來源」，來自系統異常的警示，或是經由客戶反應。第二步：適用「法規依據」，由於企業為詐騙被害者非直接受害者，此類行為法規涉及刑法妨害電腦使用罪、妨害營業秘密罪。第三步：聯繫「報案單位」，受理機關為各地刑警大隊科技偵查隊、刑事警察局偵查第七、九大隊、電信偵查大隊。第四步：準備「報案資料」，提供相關設備受攻擊電磁紀錄（後臺異常帳戶、社教郵件、第三方資安廠商資案事件報告），及受詐騙客戶資料（詐騙話術、金額、報案佐證）。第五步「完成報案」，留存受（處）理案件證明單，提高資安防護機制（如多因子驗證、IP白名單、reCAPTCHA），定期更換帳號、密碼複雜度。資策會科法所提醒各企業改善資安環境，並強化反詐騙宣導等措施，希冀阻斷駭客持續入侵業者資料庫，斷絕詐騙集團獲取民眾個資管道，削弱詐騙犯罪發生的可能。

本年度TPIPAS個人資料隱私講座課程，由產、官、學、研等不同領域的專業人員擔綱講師，提供法規、管理及技術領域，最新發展趨勢及管理實務解析等課程。3月14日將於資策會科法所行遠講堂舉辦下一場講座「以去識別化達到個資最大的利用價值」，歡迎您透過TPIPAS官方網站活動報名頁面（https://www.tpipas.org.tw/），查詢相關課程及報名時間。

中央社

上稿時間： 2023年03月09日

新聞來源： https://www.cna.com.tw/postwrite/chi/336461