112年7月號

公務機密

資訊安全維護

- 資安時事案例
- 個人資料保護法
- 生活中的資安
- 數位學習

HTTPS://WWW.YOUTUBE.COM/WATCH?V=NEHTD-AP74I

資安時事案例

YOUBIKE遭境外網攻 遭境外網攻 週五提補償機制

〔記者蔡亞樺、黃良傑／綜合報導〕全國各縣市公共自行車YOUBIKE系統上週遭境外攻擊，全國逾四萬筆會員的手機號碼、卡號、密碼及交易資料遭竊取，微笑單車公司除通報各縣市政府，也報案追查元兇。北市府交通局昨表示，經要求，業者將在本週五提出補償機制與資安防護改善計畫。

微笑單車公司昨說明，五月十七日晚間六時至十時、廿一日凌晨二至五時遭到駭客以不同技術手法進行網路攻擊，均屬惡意人士自不明來源取得會員的手機號碼，於其他平台慣用密碼，藉此嘗試登入YOUBIKE會員帳號。統計全台共計四萬○五九三筆會員帳號遭駭客登入，盜取電子票證卡號及其騎乘紀錄。微笑單車已主動變更遭惡意登入的會員密碼，並發簡訊通知上述會員變更密碼。

為抵禦駭客可能再次發動攻擊，微笑單車公司指出，五月廿一日關閉會員登入功能，所有會員強制登出，完成修改密碼強度規則及新增防堵機器人的驗證功能。廿二日下午三時恢復開放會員登入功能，所有會員需先以「忘記密碼」功能重新設定密碼。新密碼須包含八至廿碼英文大小寫與數字，建議勿採用生日、電話號碼，或與其他平台相同等較易遭人破解的密碼當新密碼。

高雄交通局昨指出，高雄有一四九○筆遭竊，依據個資法規定，微笑單車公司保有個人資料檔案，應採行適當的安全措施，防止個資被竊取、洩漏，已要求業者限期改善，並提出會員補償方案，逾期未改善則依契約罰款。

誠品疑似個資外洩案 數位部2週內做出處分

〔記者徐子苓／台北報導〕誠品疑似個資外洩，有讀者在誠品書店網購書籍，卻接到「統戰市調」電話，數位發展部數位產業署今（16日）邀集國家資通安全研究院、警政署及專家等人組成行政調查小組，共同前往誠品進行實地行政調查，預計2週內做出行政處分。

唐鳳上午出席活動受訪表示，做為綜合性電商（無店面零售業）的主管機關，數位部產業署在第一時間就有請誠品前來說明之外，今天也率隊實地做重大矚目案件的行政調查。她強調，數位部不會只了解發生什麼事情，而是會找出根本原因，透過導入「零信任」、「隱碼」技術等，確保未來不會再發生。

數位產業署平台經濟組副組長說明，依照行政院「打詐行動綱領1.5版」，產業署會在時限內提出完整報告，再看報告有沒有違反個資法，若有違反個資法，會依法處理、不排除開罰，期待2週內能夠做出處分。

對於民間企業個資外洩的處置，根據行政院訂定的作法，3天內由行政檢查小組會同資安院進行行政檢查，10天內針對個資外洩作成調查報告，2週內要做成處分決策。

至於媒體報導，有白帽駭客反映使用營利事業預設密碼，即可登入財政部電子發票整合服務平台，導致使用電子發票的營利事業或國家單位採購資訊外洩的資安疑慮。唐鳳表示，數位部資安署接獲通報後，就和財政部聯防，也督促財政部進行資安通報。

歹徒冒名申請更改地址竊個資 郵政局提醒每日查看信箱、信用卡帳單

世界日報／ 記者許君達／紐約報導

民眾在搬家後會通知美國郵政局(USPS)更改郵寄地址，但該局近日提醒紐約居民，有不法分子利用此機會盜竊身分，冒用受害人姓名假借申請更改地址；郵政局呼籲民眾每日應即時查看信箱、信用卡帳單和信用報告等，以免在不知情的情況下個資外流。

根據美國郵政局，通常人們在填寫地址變更表後，郵局會寄出一個確認地址變更的通知，近日有不法分子假借以受害者名義，向郵政局填寫地址變更表，在提交申請後，伺機盜竊寄到受害者原地址郵箱的變更通知。

如果受害人沒有每日即時查收郵箱，或將地址變更通知當作是垃圾廣告而忽略，不法分子在成功取得通知並確認後，受害者名下的所有郵件都會被轉至不法分子提供的地址，包括信用卡帳單、水電費帳單，甚至由政府寄來的郵件等。

郵政局建議，民眾應該每天查看郵箱，若發現收到地址變更通知但過去從未提出申請，且變更後的地址陌生，就很可能遭到盜竊，應立刻前往附近郵局，向郵政檢察部門報告。

若民眾有較長時間未收到任何信件，也有可能是地址已被不法分子轉出，恐遭到身分盜竊；即時查看信用卡帳單和信用報告，也能夠在第一時間察覺到身分盜竊。

對於利用變更地址盜竊個資，郵政局表示，當局目前正在研擬增加額外身分驗證的方法，以加強該服務的安全性；民眾若發現上述問題，可在美東時間上午8時至下午4時30分，致電聯邦郵政督察局(U.S. POSTAL INSPECTORS)，電話(877)876-2455；另外關於身分盜竊，還可致電聯邦貿易委員會(FTC)，電話(877)438-4338。

個資外洩訴訟 消基會籲修消保法要企業負責舉證

中央社 記者楊淑閔

個資外洩詐騙氾濫，消基會副董事長徐則鈺表示，樂見個資法條文修正後提高罰鍰，將設獨立監督機關個資保護委員會，並呼籲最好再修消保法全面轉換舉證責任，由企業負舉證之責。

網路化個資外洩數量龐大，影響層面廣，非法使用方式也多元化，不僅詐騙錢財，近期還有報導指出，疑因個資外洩，消費者買「阿共打來怎麼辦」一書後，接到統戰電話。

屢次幫消費者打團體訴訟的消費者文教基金會副董事長徐則鈺，過往曾為雄獅旅遊個資外洩事件打團訟，他表示，樂見立法院16日三讀通過「個人資料保護法」第1條之1、第48條，及第56條修正條文。

依據修正條文，他說，行政院將設置個資保護獨立監督機關個資保護委員會，讓事權統一，這有助於現況發生個資外洩時，究竟是哪個是主管機關的問題獲得解決，很期望儘速完成其組織法的立法。

舉例來說，他說，日前電商、網路書店的客戶個資外洩時，各部會都認為主管機關是數位發展部，但數發部不一定同意，若是經濟部或數發部，也有爭議；未來將有主管機關，這也是呼應去年8月12日憲法法庭第13號判決，要求3年內完成個資保護獨立監督機制之意旨。

其次，個資法修法提高個資外洩罰鍰上限最高台幣1500萬元。徐則鈺說，原本罰鍰2萬元以上、20萬元以下，使得企業對於個資保護「有點沒那麼重視」，未來新法要執行，才能讓企業有所警惕、落實個資保護。

他並說，個資保護委員會成立後，應對目前個資外洩的企業經營者，加強指導改善個資保護業務，不能只有開罰，其組織法應具體規範未來的職權、主責內容。

徐則鈺更主張，應修正消費者保護法有關消費訴訟的條文（第47到55條），他認為，規定消費者只要證明業者的違法事實即可，由業者舉證其行為對消費者未造成損害，而非消費者證明業者的行為損害消費者權益。

他說，團體訴訟對原告（消保團體）僅有裁判費有點優待，審理速度沒較快，舉證責任也沒較輕鬆，如果能夠 修正消保法，對個人、團體訴訟都有幫助，否則舉證問題會讓訴訟糾纏很久。

以實例來說，徐則鈺說明，消費者根本不知道接到詐騙電話，怎麼可能當下會錄音，他個人認為消費者事後知道被騙，報了案即可證明業者有違法的事實，但現況是法院認為不算，問題是明明已經很多人去報案，「這些人何須無緣無故去報案稱某公司客服去電詐騙？」

他重申，修消保法的訴訟舉證責任在企業，可同時解決個資外洩之外的消費者權益受害的訴訟問題，包含食安議題，例如只要冷凍莓果檢出A型肝炎病毒就算是違法事實，消費者只需提出發票證明有購買，然後由企業舉證吃了也沒事、沒損害。

他也說，當然個資保護委員會只能提案修正個資法，將個資外洩的受害者與企業的舉證責任轉換；不過消基會仍期待修消保法，以徹底解決消費者權益團訟勝率低、賠償金少等問題。

徐則鈺特別提及，政府怕人民濫訴，在個資法第32條，對提起團體訴訟的財團法人、公益社團法人設了登記財產、社團法人社員人數、章程目的需含保護個資事項及許可設立3年以上等要件，但是現在詐騙氾濫，問題是濫詐而非濫訴，應修法調整貼近事實。

WHATSAPP會偷聽？ 杜奕瑾分析現代人資安意識

〔即時新聞／綜合報導〕推特（TWITTER）執行長馬斯克（ELON MUSK）日前在推特PO文表示，通訊軟體WHATSAPP不可信，PTT網路創世神杜奕瑾分析現代人應該要有的資安意識，因為人們的隱私與認知往往就是商品。

杜奕瑾在臉書PO文表示，APP會偷聽使用者講話是真的，因為ANDROID新功能PRIVACY INDICATOR，可以知道APP有沒有偷開麥克風，有多個使用者回報臉書的WHATSAPP會偷開麥克風即使在背景執行。也驗證了APP會偷聽使用者的傳說。

杜奕瑾指出，現代人資安意識，智慧型音箱只有喚醒時在聽？一般持續聽；商用視訊軟體只有開鏡頭麥克風錄？部分軟體會持續錄即使按關閉，不要關閉鏡頭後做壞事；客服對話文字只有送出才會被看到？即使沒送出客服可以看到你的編輯過程，作為情資，想好再打；你在公共場所看螢幕廣告是單向的？其實廣告公司也藉由設備上的小鏡頭在看你對廣告反應，遠離計程車上、梯間廣告螢幕；躲在車後面上廁所？很多智慧車如特斯拉停車時仍持續錄下車子四週影像。

杜奕瑾在文末直言，為什麼能有免費服務？因為你的隱私與認知往往就是商品。

TIKTOK美聽證會 執行長閃躲提問

編譯林雨萱／綜合報導〕中國短影音社群程式「抖音」國際版「TIKTOK」安全疑慮難消， TIKTOK執行長周受資廿三日出席美國國會聽證會，兩黨議員針對資安和有害內容管理砲火猛攻。面對種種尖銳問題，周受資僅以「事情很複雜」匆匆帶過，並極力撇清與中國政府的關聯。民主黨籍聯邦眾議員卡德納斯指出，周受資善以言辭閃躲問題，顯示近六小時的質詢最終無能緩解對於TIKTOK的憂慮。

美議員猛攻資安與有害內容管理 質疑淪中共工具

共和黨籍聯邦眾議員羅傑斯表示，TIKTOK屢次選擇加強控制、監控和操縱路線，「應該被禁」，指控中共利用一億五千萬名美國用戶來蒐集敏感資訊，控制他們看到、聽到、相信的內容。他還說，在創建TIKTOK帳號之後的短短數分鐘內，演算法便宣傳自我傷害和飲食失調的內容，慫恿用戶從事種種可能對孩童生命安全構成風險的危險挑戰。民主黨籍聯邦眾議員帕隆也說，TIKTOK的內容加劇孩童的情緒壓力。新加坡籍的周受資告訴眾議院能源和商業委員會，TIKTOK將年輕用戶的安全置於首位，否認其為國家安全構成風險，並重申公司計畫透過移轉資料至甲骨文公司的伺服器內等作法，保護用戶個資。他還說，TIKTOK母公司「字節跳動」並非為中國或任何一個國家所有，是私人企業，並提及字節跳動六十%股份由凱雷投資集團等外國企業持有，表示所有權並非解決這些擔憂的核心。

撇清與中國關聯 否認內容審查共享資訊

至於與字節跳動的關係，周受資表示，僅與字節跳動首席執行官經常接觸，否認與字節跳動的中共黨委書記有所往來。被問及字節跳動員工是否能夠查看美國資料，周受資並未直接否認，僅說在推動「德州項目」之後，只有美國員工才能看到。不過，帕隆認為，北京仍能控制、影響所作所為。

對於中共是否有權要求共享資訊，周受資回答，已經調查此事，並無證據顯示中方有權查看，同時否認TIKTOK進行內容審查，可在平台找到天安門事件等敏感內容。鑑於中國商務部廿三日表態，反對美國強迫要求TIKTOK出售中方股東股份，以脫離北京母公司，專家指出，這讓拜登政府面臨若要查禁TIKTOK，就得面對升高中美衝突的風險。

又一國跟進 法公務員禁在公用手機使用

與此同時，法國公務員部部長蓋里尼廿四日宣布，為了確保政府機構和公務員的網路安全，國家決定即日起禁止全國二百五十萬名公務員在公用手機使用TIKTOK等「娛樂性」軟體。據法國數位部解釋，該禁令不僅針對TIKTOK，也包括網路串流影音與網路遊戲平台如NETFLIX或CANDY CRUSH等。