115年3月號
林業及自然保育署
臺東分署

公務機密
資訊安全維護

目錄

資安時事案例

智生活App爆16項資安漏洞
300萬用戶恐個資外洩、交易遭駭客攔截

ETtoday新聞雲/2026年02月12日 11:38/記者許敏溶／台北報導

宣稱用戶數達300萬住戶的「智生活App」，今（12日）遭消基會指出，經送國家資通安全研究院檢測，竟高達16項不合格，涵蓋「個資外洩、交易攔截、管理缺失」等3大類資安與隱私風險，衍生駭客可輕易竊取用戶敏感資訊等問題。消基會提醒用戶不要綁定高額信用卡，也呼籲政府建立更完善的後市場治理架構。

為打造智慧社區，不少廠商開發出非常便利的手機App，提供住戶和社區大樓管委會成員使用。其中「智生活（SmaDay）App」由智生活科技（原今網智慧科技）公司開發，在官方網站宣稱用戶數已達1萬個社區、300萬住戶，更宣稱應用軟體已經通過MAS L3最高等級資安標章。

不過，消基會今天召開記者會指出，將智生活App的安卓版送到國家資通安全研究院進行兩次檢測，發現智生活App高達16項檢測未通過，包括9項L1（最低等級）、4項L2和3項L3項目不通過。

消基金會董事長鄧惟中指出，檢測16項不合格涵蓋「個資外洩、交易攔截、管理缺失」等3大類資安與隱私風險。在「個資外洩」部分，由於程式碼與日誌檔未落實加密或清理，駭客可輕易從手機暫存中竊取敏感資訊；在「交易攔截」部分，因缺乏交易時的再次驗證與防覆蓋保護，攻擊者可透過偽裝介面誘導入坑，或在背景側錄用戶的輸入動作來盜取金流權限；至於「管理缺失」，因為隱私宣告不全且連線識別碼（Session）容易被預測，增加帳戶連線被劫持的風險。

消基會監察人卓政宏分析，「智生活App」的商業模式沒收費，但又想賺錢，所以透過蒐集客戶個資來進一步利用，讓廣告主願意投資，但該公司要蒐集個資，卻連儲存與保護能力都沒有，就可能產生資安風險，「這件事蠻嚴重的！」他呼籲政府要以動態方式進行管理，而且政府對洩漏個資沒有嚴重罰則，這是非常離譜的。

因此，鄧惟中提醒用戶，不綁定高額信用卡，也不要開啟自動儲存密碼功能，提高對「金流與交易」的防護，並頻繁清理該App的「快取資料」，避免「敏感資料殘留」，以及盡可能最低限度的打開該App的存取權。

對於數發部等政府與標準制定單位，消基會呼籲建立更完善的後市場治理架構，包括針對高風險（L3 等級）App 實施年度不定期抽測，並強化實驗室課責，若App 在通過檢測後短時間內爆發重大已知漏洞，應追究實驗室檢測不實之責，還有建立類似 CVE 的「App 漏洞通報平台」，強制開發商在時限內修復並公告，否則應撤銷其資安標章。

資安時事案例

日航「行李配送服務」系統驚傳遭駭客攻擊 2.8萬旅客資料恐外洩

日本航空昨（10）日發布緊急公告，其「當日行李配送服務」預約系統遭第三方非法入侵。（圖／翻攝日本航空臉書）

FTNN新聞網2026年2月11日 週三 下午3:24

[FTNN新聞網]實習記者陳又綺／綜合報導

日本航空昨（10）日發布緊急公告，其「當日行李配送服務」預約系統遭第三方非法入侵，受影響人數恐高達2萬8千人，目前已暫停預約功能並全力調查資料是否外洩，同時也引發旅客資安疑慮。

日航表示，此次事件的受害對象為2024年7月10日之後曾預約或使用該服務的所有旅客。可能遭竊取的個資範圍包含旅客姓名、電子郵件信箱、聯絡電話以及JAL哩程俱樂部會員編號等資料，旅客搭乘的航空公司名稱、班機編號、飛行日期、起飛與降落機場等細節，通通在風險名單內。

除了個資與航班資訊外，行李配送的相關紀錄也疑似外洩，旅客在哪個機場寄存行李、指定配送到哪間飯店、支付多少服務費用、何時提出申請等資訊，全都有外洩的可能性。不過日航特別澄清，旅客的信用卡號碼和系統密碼並未存放在受影響的資料庫中，因此這2項資料目前確認安全無虞。

根據日媒報導，日航指出，機場第一線工作人員9日上午9時率先察覺異狀，發現配送服務系統無法正常運作，立即向公司總部回報。日航接獲通知後，在當天上午10時20分果斷關閉預約功能，避免災情擴大。資訊系統部門檢視系統存取紀錄後發現，系統早在8日傍晚6時18分就曾出現預約故障，當時可能已是駭客入侵的前兆。9日凌晨0時40分，系統明確記錄到非法入侵的痕跡。

目前日航已與外部專業資安機構合作，全面清查資料是否流出企業外部。日航內部強調，這次資安事件僅限於行李配送服務的單一系統，其他服務項目的運作一切正常，並未受到波及影響。

個人資料保護法

包括社區門禁密碼！酷澎逾3300萬用戶個資外洩 歹徒瀏覽近1.5億個資

南韓政府10日公布對電商酷澎用戶個資外洩事件的初步調查結果，認定逾3300萬用戶個資遭到洩露。（路透資料照）

自由時報2026/02/11 07:59

〔即時新聞／綜合報導〕南韓科學技術資訊通信部（科技部）10日公布對電商酷澎（coupang）用戶個資外洩事件的初步調查結果，認定逾3300萬用戶的個資遭到洩露，歹徒非法瀏覽的個資更達近1.5億項。

酷澎去年11月通報發生大規模用戶個資外洩事件，外流資料包括姓名、電話、電郵地址及配送資訊，似乎波及酷澎絕大部分用戶。當時，酷澎公布公司內部調查結果，宣稱僅3000個帳戶的個資外洩。

韓聯社報導，南韓科技部調查小組對酷澎伺服器去年11月29日之後的25.6TB網站存取紀錄進行了分析。結果顯示，酷澎「我的資訊修改頁面」中，約3367萬用戶的個資遭洩露，包括用戶姓名、電子郵件等。在「收貨地址列表頁面」，涉案人員累計非法查詢約1.48億項個資，包括姓名、電話號碼、收貨地址，甚至包含社區門禁密碼等。

考量部分酷澎用戶在為家屬、朋友等第三方下單後登錄其資訊的狀況，且上述調查結果尚未包含酷澎上週另被爆出的16.5萬個受害帳戶，預計受害規模將進一步擴大。

調查小組掌握的個資外洩規模明顯少於酷澎1名前中國籍員工最初主張的數字。該員工曾於去年11月25日向酷澎發送恐嚇電郵，稱其已掌握1.2億項以上的收貨地址、5.6億項以上的訂單資訊，以及3300萬項以上的用戶電郵資訊。

調查小組指出，該中國籍人員在酷澎任職期間，曾負責設計用戶驗證系統。其自去年1月起發現酷澎伺服器認證系統存在漏洞並測試可攻擊性後，於同年4月14日至11月8日非法收集用戶個資，但相關數據是否被傳輸至外部雲端尚不得而知。

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

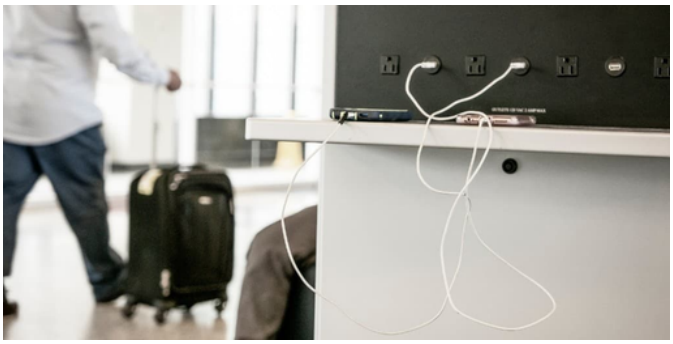
Q23　間接取得個人資料時，什麼情況下可不必告知當事人？

A　除非有下列情況之一，可以不必告知：

1.直接自當事人蒐集個資時，可免告知的情況之一。
2.當事人自行公開或其他已合法公開的個人資料。
3.不能向當事人或其法定代理人告知。
4.基於公共利益而需要的統計，或是學術研究上有必要，而且資料須經處理過而無從識別出特定的當事人。
5.大眾傳播業者基於新聞報導公益目的而蒐集個人資料。

文/iThome

租借行動電源遭駭？台灣專家示警沒做3招恐被駭客狂盜刷信用卡



3C新聞與科技生活 / 2026-02-10 / 作者: 瘋先生 / USB, 手機充電, 機場, 資安, 駭客
現在人出門手機沒電超緊張，不過現在到處都有「行動電源租借站」也變得超方便，就連便利商店也都能租借行動電源。但你知道嗎？中國最近傳出有人用租借行動電源，結果手機的個資竟然被偷走，連信用卡號、支付密碼都外洩，就算把行動電源拔掉也無法阻止駭客繼續操控你的手機事件發生。

租借行動電源藏木馬？一插線駭客就能控制手機
根據中國媒體報導，開始有詐騙集團會在租借行動電源裡偷偷裝上惡意晶片，只要有人把手機插上去，手機裡的資料像是銀行帳號、支付密碼、甚至信用卡資訊，全都一覽無遺，最可怕的是，就算拔掉電源，駭客也可能已經植入程式，還能遠端控制你的手機。

台科大資安專家查士朝就提醒，這類資安問題在台灣也不排除發生，因為現在大多數的充電線都支援資料傳輸功能，只要你連到被改裝過的行動電源，對方就可能偷偷拷貝你手機裡的資料。

他特別提到，如果在充電時看到手機跳出「是否信任此裝置」或「是否同意資料傳輸」這類訊息，一定要點「不同意」！這一個小動作，可能就能避免被入侵。

不只行動電源！機場、百貨的免費USB插座也要當心
別以為只有行動電源有問題，其實美國聯邦調查局（FBI）早就警告過大家，公共空間內的免費USB充電站可能潛藏惡意程式植入風險，無論是機場、飯店、購物中心提供的USB或Type-C插座，駭客可能透過微型硬體裝置或修改插座韌體來竊取資料，使用者若未察覺手機自動與插座進行資料交換，重要資訊恐已在不知不覺中遭竊。

不論是USB或Type-C插孔，只要駭客偷偷改過硬體或插入晶片，只要一接上手機，惡意程式就能入侵，會把手機裡的資料偷個精光。

3招如何防範手機充電被竊取資料技巧
1. 定期更新系統：修補漏洞是防範駭客的第一道防線
2. 拒絕資料傳輸：出現「是否信任此裝置」或「是否同意資料傳輸」請選擇不同意
3. 自備設備充電：儘量使用自帶的行動電源與插頭，避免使用公共USB插座與不明設備