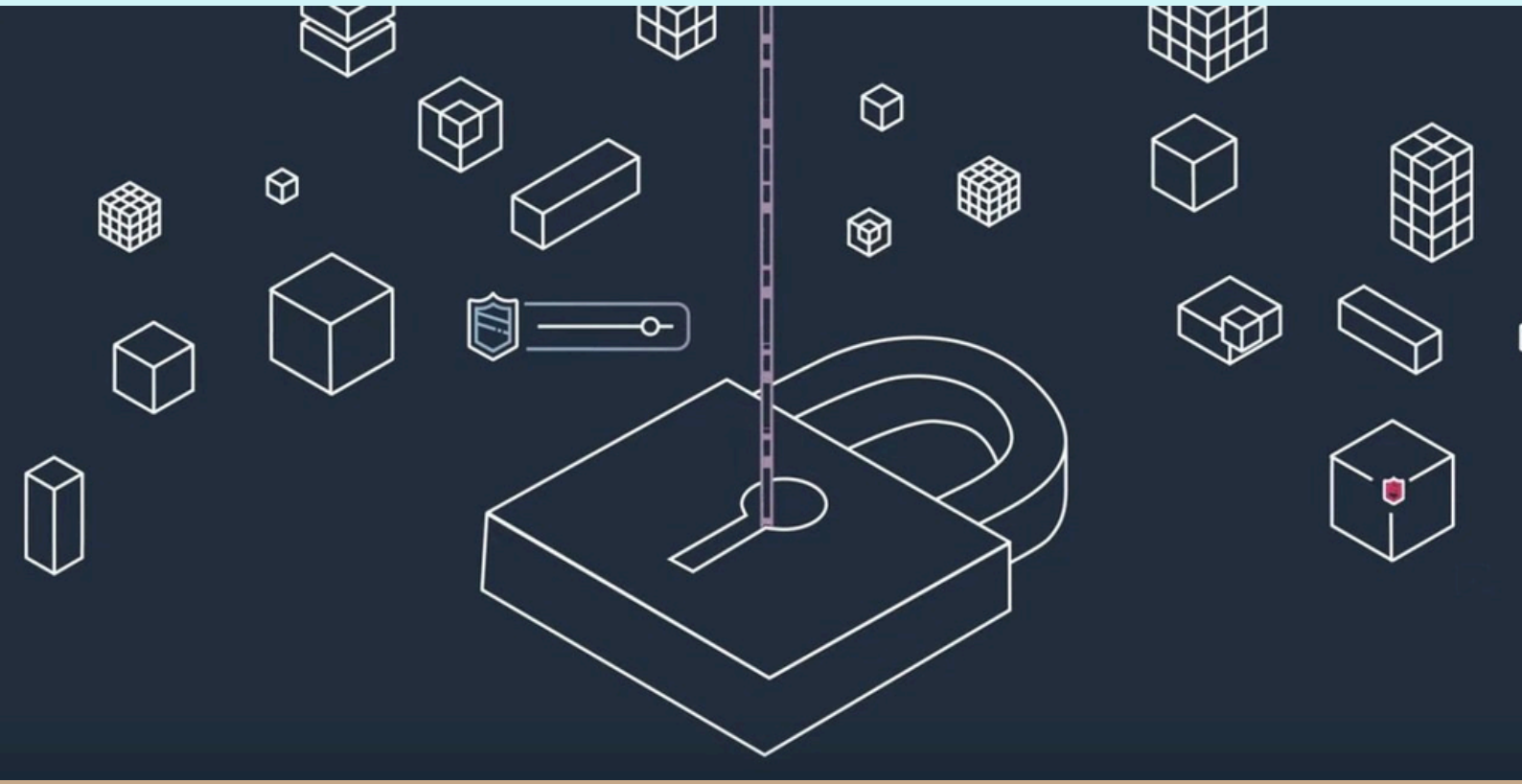
公務機密
資訊安全維護

114年7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

你早就被盯上！台灣個資也難逃毒手　資安崩壞怎麼救？

（示意圖／PIXABAY）

三立新聞網/財經中心／師瑞德報導2025/06/16 19:00:00
近期國際資安團隊在網路上驚見一座未加保護、容量高達631GB的龐大資料庫，內容竟涉及近40億筆中國民眾個人資料，其中包含超過8億筆WeChat用戶ID、逾6億筆銀行與住址等高敏感資訊，外洩規模堪稱史上最大，更令人憂心的是，資料庫中竟出現「tw」標註的子目錄，台灣民眾個資疑似亦遭牽連。

KPMG安侯企業管理股份有限公司董事總經理謝昀澤指出，中國早已形成「資料盜竊技術」加「詐騙行銷話術」的一條龍詐資產業鏈。攻擊者透過網攻、分析、行銷、洗錢、客服甚至假法務等分工，利用各類平台蒐集的巨量資料，從暗網到Telegram乃至實體市場進行頻繁交易。而這次外洩的資料不僅龐雜，更具整合性，透過資料拼圖技術，將社群帳號、住址、銀行資訊結合，可針對目標展開精準詐騙與社交工程攻擊，嚴重威脅個資安全。

KPMG隱私保護專家協理趙慶宏提醒台灣企業，若擁有個資並進行境外傳輸，應依法向當事人明確揭露傳輸地與保護措施，並落實個資法規定的監督機制。他指出，主管機關對個資跨境傳輸日趨關注，近期已有業者因未告知會員其個資儲存於香港雲端而遭糾正，呼籲企業務必審慎應對、即時補強法遵作業。

面對資訊戰時代下的個資風險升溫，民眾應如何提升自我防護力？謝昀澤提供四大實用技巧：
一、多元密碼管理：不同平台設定專屬且高強度密碼，並利用密碼管理工具降低遺忘與重複使用風險。
二、啟用多因素驗證（MFA）：建議加裝指紋辨識、USB金鑰等二階段驗證，即便密碼外洩也能阻擋非法登入。
三、警惕可疑訊息與連結：接獲不明簡訊、來電、郵件要求提供個資或點擊連結時，務必中斷聯繫並撥打165確認。
四、即時更新裝置與應用程式：定期更新手機、電腦與App，以修補潛在漏洞，防範駭客入侵。

此外，他也特別提醒台灣使用者，日後在使用如DeepSeek等中國生成式AI工具時，應注意其將資料儲存於中國境內伺服器的風險。根據其隱私政策，DeepSeek會蒐集用戶的文字、語音輸入、檔案及聊天記錄，恐遭有心人士截取並進行「思想捕捉」與「資訊操控」，個資外洩與意識形態干預的風險不容小覷。

總體而言，面對跨境資料外洩風險不斷升高，不僅企業應強化合規管理與資安防線，民眾也應提升自身的數位警覺與防護習慣，才能在數位社會中確保資訊自主與安全。

資安時事案例

App Store的「免費VPN」真的安全嗎？被爆中國APP有蒐集個資風險

2025-06-17 08:25
聯合新聞網／三嘻行動哇 Yipee!
美國資安 觀察組織 Tech Transparency Project（TTP）最新報告指出，雖然 TTP 在六個星期之前已經提出警告，Apple 與 Google 仍讓多款與中國 企業有關的 VPN APP 留在美國及多國的 App Store 和 Google Play 平台，這些APP多數沒有揭露真實背景，部分甚至與遭美國制裁的資安公司有關聯。

這些 VPN 雖宣稱保障使用者隱私 ，實際上卻可能讓資料流入中國政府手中，而且兩大平台還能從中抽成獲利，因此引發外界對使用者個資安全的關注。

中資 VPN 積極吸金卻不透明
這些 VPN 表面看似無害，多包裝成免費工具吸引使用者，但 TTP 發現，包括 Turbo VPN、VPN Proxy Master、X-VPN 等熱門APP，實際都與中國資安公司奇虎 360 有關，而這家公司則是因為與解放軍合作被美國政府列入制裁名單。

TTP 點名的 13 款具有中資背景的 VPN 目前仍在 App Store ，另外還有 11 款在 Google Play 開放下載，而這些APP開發者的名稱包括「Free Connected」、「Innovative Connecting」等等，多數刻意繞經新加坡登記，掩蓋真正來源。

為何這麼危險？
外媒報導指出，TTP 之所以會說危險，是因為有了 VPN APP等於掌握使用者所有網路活動，一旦 VPN APP背後的公司受中國法規約束，就代表使用者資料可能在未經同意情況下交由政府取得。在強調匿名與隱私的工具中，這無疑成了高風險破口。

Apple 與 Google 雖知情，卻仍從中分潤
這些APP在美國市場吸金能力驚人，其中 X-VPN 至少賺進 1,000 萬美元，Turbo VPN 和 VPN Proxy Master 則各突破 500 萬美元。Apple 則是可以從中抽取最高 30% 的分潤，Google 也能夠從訂閱與廣告中獲利。

這樣的現象被質疑與 Apple 所宣稱的重視隱私立場互相矛盾。

Apple 對報導的回應
根據《AppleInsider》報導，Apple 在這則新聞發布後重申先前的立場：

蘋果 公司表示 App Store 開放所有國家開發者上架，只要遵守 App Review 審核規範與當地法律，並不會因開發者的國籍或公司註冊地而限制上架資格。

對於 VPN APP，Apple 表示他們有額外的嚴格規範，也就是「只有註冊機構才能上架 VPN，開發者也必須在用戶使用前明確揭露資料蒐集與使用方式，且不得任意使用或分享資料」，這些規定需在隱私政策中說明清楚。

Apple 強調公司會執行這些政策，一旦發現違規，就會將APP下架處理。

用戶自己也要多留意
儘管 Apple 與 Google 表示已有機制過濾不當APP，但實際上這些 VPN 多數背景仍不透明，平台審查難以百分百防堵。

若你正在尋找一款 VPN 工具，建議選擇有明確公司資訊、獲得公開信任與驗證，別單憑「免費」與「高評價」就掉以輕心。畢竟，VPN 是網路活動的「守門人」，一不小心，就會把自己的隱私送給別人了。

中國驚傳史上最大規模個資外洩，台灣人也可能受害？專家傳授4招應對

風傳媒/林彥呈 的故事/2025/06/12

近期，國外資安團隊在網路上意外發現了一個高達631GB且未有任何安全防護的資料庫，其中竟存放了將近40億筆中國民眾的個人資料，內容包含WeChat用戶ID超過8億筆、銀行和住址等高敏感訊息高過6億筆，以及其他個資驗證資訊等，堪稱目前為止中國最大規模的資料外洩事件。值得注意的是，外洩的資料庫中，有一名稱為「tw」的資料庫，也不排除與台灣民眾相關的可能性。

KPMG安侯企業管理股份有限公司董事總經理謝昀澤表示，中國由「資料盜竊技術」加上「詐騙行銷話術」的「一條龍詐資鏈」已經非常成熟，透過網路攻擊、資料分析、行銷、洗錢、客服、法務等專業分工，利用來自網購平台、求職網站、醫院、學校、電子支付與電信公司等多元巨量資料，在暗網、Telegram甚至線下，頻繁進行個資交易。

謝昀澤進一步分析，本次事件外洩的資料架構，攻擊者可使用資料拼圖等資料加值技術，整合社群媒體帳號搭配住址及銀行資訊，比起單一平台外洩的個資，更明確掌握個別民眾的背景資訊，這些個資，將會用於精準詐騙、精準行銷、社交工程攻擊或洗錢等用途。

台灣企業需先確認　是否有將個資傳輸到境外

針對企業的個資保護策略，KPMG隱私保護專家協理趙慶宏建議，擁有民眾個資的台灣企業，首先必須確認是否有將個資傳輸到境外，如果有的話，應明確告知當事人如何傳輸到境外。其次，需採取依據個資法適當的安全措施或監督機制以確保當事人個資在境外地區的安全。

趙慶宏提醒，台灣主管機關在近期對於業者在進行個資行政檢查時，特別關注業者針對所保有的消費者或會員個人資料是否有明確告知當事人有跨境傳輸的責任。近期也有業者，因為其所蒐集的會員資料上傳到位於香港的雲端資料庫，但未依法告知會員，而遭糾正的案例。

專家教戰四招　提升數位防護力

而在人人自危的數位空間裡，民眾應如何自保？謝昀澤提供了四大重點技巧提升數位防護力。

一、多元密碼：各平台應使用不同且高強度的密碼。由於高強度密碼不易記憶，建議使用密碼管理工具，避免重複使用或簡單組合。

二、啟用多因素驗證（MFA）：開啟生物辨識、USB Token等強化驗證機制，加強帳號保護。即使密碼外洩，有心人士也無法登入。

三、警覺可疑簡訊、電話與郵件：若突然要求個資、要求點擊連結、提供授權碼等，務必掛斷、回撥或直接撥打165查證。

四、即時更新設備與程式：包括手機、電腦作業系統與行動應用程式，透過及時更新可修復安全漏洞，避免被駭客利用。

Deepseek等中國生成式AI也有風險

謝昀澤也提醒，台灣民眾面對的個資外洩威脅，除了一般網路應用如購物、社群軟體外，未來還將包含使用Deepseek等中國生成式AI的風險。

根據DeepSeek的隱私政策指出，其收集的資訊儲存在中國境內的伺服器上，並可能收集用戶的文本或語音輸入、上傳的文件、聊天記錄等內容。

謝昀澤認為，使用DeepSeek不但有資料跨境安全疑慮，例如特定國家政府或有心人士，透過與AI的互動記錄，進行思想捕捉與資訊誘導，將對使用者的隱私與資訊自由度，將產生更深的侵害。

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

Q15　可依自己的需求任意蒐集或使用個人資料嗎？

A　不能任意蒐集或使用個人資料，蒐集個人資料必須有特定的目的，而利用個人資料的目的，也必須與蒐集的目的有合理的關聯。

文/iThome

LINE瘋傳手機借熱點就會被盜光帳戶！資安專家揭露真相

LINE瘋傳手機借熱點，就會被偷取個資是謠言。（圖／翻攝網路）

自由時報/2025/06/19 15:20文／記者吳佩樺

最近一段影片在LINE上瘋傳，內容聲稱「借熱點竟差點被詐騙，銀行、LINE、身分證資料全外洩」，嚇得不少人不敢再開分享熱點，深怕導致帳戶被駭、戶頭的錢會瞬間被轉光。資安專家出面闢謠，直指這根本是誇大的假劇本。

這段影片描述，一名網友在銀行門口被一位女子借熱點，對方還藉故要求點擊手機上的驗證彈窗、同步裝置。該網友覺得可疑，隨即關閉熱點，事後上網一查，才發現這似乎是「最新詐騙手法」。該影片警告只要點擊驗證，LINE和網銀帳號就會被綁定、盜用。

對此，查核平台MyGoPen表示，這類謠言早在過去就流傳過，只是現在換了劇本，屬於「內容農場式假故事」。

MyGoPen實際詢問台灣數位安全發展協會理事長劉彥伯，他指出，從影片內容來看，描述的場景與說法多為誇大，且與實際資訊安全流程不符。例如銀行與支付工具並不會只透過一個彈窗驗證就授權他人登入，現今大多設有多重驗證機制。

而且單純分享熱點，並不會導致帳戶遭駭，除非使用者被進一步引導開啟可疑網站、下載惡意程式，否則不會有安全疑慮。

刑事警察局預防科科長林書立也補充，這段影片內容極有可能是從中國抖音上流傳來的，藉此博取流量，在台灣的實際環境下，不可能僅憑一個熱點分享就被綁定第三方支付。