115 年 8 月公務機密維護宣導

旅遊 eSIM 真方便，當心資料全都露！

美國東北大學研究團隊2025年針對市面上數十款主流eSIM進行實際測試，發現多數eSIM的網路流量並不會直接從使用者所在國家連上網際網路，而是會先繞送至背後真正電信業者（包括中國電信業者「中國移動」）的境外網路處理，且使用者通常完全不知情。即使傳輸內容經過加密保護或認為資料不重要，該業者在流量傳輸途中仍可看到使用者連上了哪些服務、何時連線、從哪個位置連線，可能增加個資遭不當蒐集的風險，若涉及行動支付或網路銀行等功能使用，更可能造成財務損失。對政府機關人員而言，若以流量路徑未揭露的eSIM存取公務信箱或內部系統，風險層級更高。

☆☆ **防護措施建議** ☆☆

1.購買前確認背後的實際電信業者與流量出口：

若業者未主動揭露，可直接向賣家查詢，或參考其他使用者的實測紀錄加以確認，不應以能否使用特定服務作為安全與否的唯一判斷依據。

2.依使用情境採取對應防護措施：

若需存取公務信箱、內部系統、雲端儲存或視訊會議，應避免使

用背後電信業者及流量路徑未經揭露的 eSIM，並透過機關核准的 VPN 連線。

3.留意帳號異常通知並強化登入防護：

若收到帳號異常登入通知，或發現登入地點顯示為非所在地區，應立即檢查登入紀錄、變更密碼，並確認多重要素驗證（MFA）已正確啟用。若為公務帳號，應依資安通報程序回報。

資料來源：摘錄自 國家資通安全研究院 2026/7/9 公告訊息