公務機密
資訊安全維護

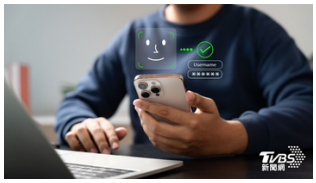
115年5月

林業及自然保育署
臺東分署

目錄

資安時事案例

人臉辨識不安全！21款熱門手機遭照片破解　4萬旗艦機也中招



編輯 沈惟中 報導發佈時間：2026/04/17 15:35 (示意圖／shutterstock 達志影像)

臉部辨識是目前主流手機中，最直覺且安全的解鎖方式之一。但近期有測試指出，60%的手機很容易被照片欺騙。外媒特別列出高風險名單，涵蓋摩托羅拉、諾基亞、一加與 Nothing 等知名品牌，共計21款機型，恐讓用戶的個資與電子錢包遭駭客攻擊。

研究揭露　多數手機可被照片破解

《每日郵報》引述英國產品評測網站Which?指出，臉部辨識看似安全，但實際上不少裝置仍存在漏洞。該機構測試發現，約60%的熱門手機可被簡單的紙本照片騙過，即使是高階機型也不例外。例如售價1099英鎊（約新台幣4萬6889元）的Oppo Find X9 Pro，在測試中也一度將紙張上的影像辨識為真人臉部。Which?警告，若遭不法人士利用，可能導致用戶電子郵件被讀取、敏感帳戶密碼遭重設，甚至存取照片與Google Wallet交易紀錄。

技術限制　2D辨識成漏洞關鍵

Which?測試了自2022年10月以來發布的208款手機，其中133款可被照片破解。數據顯示，這項問題並未隨技術進步而改善。2024年測試中，有72%的手機無法辨識照片偽裝，較前一年的53%大幅上升；2025年雖略降至63%，但仍意味多數設備存在風險。報告指出，許多裝置採用2D臉部辨識技術，只能辨識平面影像，缺乏深度資訊，因此難以區分真人與照片。

專家示警　Android機風險較高

Which?科技編輯芭伯（Lisa Barber）表示，在科技高度發展的時代，手機竟會被平面照片欺騙令人難以置信，但測試結果顯示確實存在此問題。她指出，過去4年測試的大多數Android手機，都可透過2D影像輕易解鎖，且部分製造商未充分提醒用戶相關風險。她建議，用戶應啟用其他更安全的解鎖方式，例如指紋辨識或PIN碼，以提升裝置安全性。

相較之下，部分新款手機在測試中表現較佳。Google Pixel 8、Pixel 9、Pixel 10，以及三星Galaxy S26皆順利通過測試。此外，蘋果的Face ID，以及部分Honor高階Android機型，也較難被照片欺騙。

以下為可被照片破解的高風險機種清單（共21 款）：

1. Fairphone 6
2. Honor Magic6 Lite 5G
3. Motorola Moto G75 5G
4. Motorola Edge 60 Pro, Motorola Edge 60 fusion
5. Motorola Moto G56 5G
6. Motorola G86, Motorola Edge 40 Neo
7. Motorola Moto g35, Motorola Moto g55
8. Motorola Razr 50 Ultra
9. Motorola Edge 50 Ultra
10. Motorola Edge 50 Pro
11. Motorola Moto G73 Nothing Phone (2a) Plus
12. Nothing Phone (3a)
13. Nothing Phone (3a) Pro
14. Nothing Phone (3)
15. Nothing Phone (2a)
16. OnePlus 13R
17. OnePlus 13
18. OnePlus Nord 5
19. OnePlus Nord CE5
20. OnePlus 15
21. OnePlus Nord 3 5G

Google AI平台驚傳「破防」！Antigravity爆發提示注入漏洞

商傳媒

service@sunmedia.tw (商傳媒 SUN MEDIA)2026年4月22日週三 上午9:40
商傳媒｜葉安庭／綜合外電報導

資安研究公司 Pillar Security 日前揭露，谷歌（Google）旗下的人工智慧（AI）程式碼生成平台 Antigravity 存在一項「提示注入」（prompt injection）漏洞，攻擊者能藉此執行惡意程式碼，甚至可繞過該平台最嚴格的安全防護「Secure Mode」。

這項漏洞主要存在於 Antigravity 的檔案搜尋工具 find_by_name 中。該工具在處理使用者輸入時，直接將輸入內容傳遞至命令列公用程式，而未進行充分的驗證。Pillar Security 的研究人員指出，攻擊者可利用此缺陷，將檔案搜尋指令轉化為惡意程式碼執行任務，進而實現遠端程式碼執行。

完整的攻擊鏈路包含兩個步驟：首先，攻擊者需植入惡意腳本；接著，透過看似合法的搜尋操作觸發該腳本，一旦初始的提示注入成功，後續將無需使用者額外互動。研究人員更實際演示，透過此漏洞成功讓系統開啟計算機應用程式，證明了其繞過安全機制的有效性。

Antigravity 是谷歌於 2025 年 11 月推出、旨在協助程式設計師的 AI 開發環境。Pillar Security 已於 2026 年 1 月 7 日向谷歌通報此問題，谷歌當日即確認收到回報，並於 2 月 28 日完成漏洞修復。

提示注入攻擊是指透過隱藏在內容中的指令，使 AI 系統執行非預期行為，恐導致指令在使用者機器上被執行。此前，OpenAI 也曾警告其 ChatGPT 代理程式在連接外部資源時，可能面臨提示注入攻擊導致敏感資料洩露的風險。

Pillar Security 強調，產業應從僅依賴「淨化」（sanitization）的控制措施，轉向採用「執行隔離」（execution isolation）作為 AI 開發工具的安全典範。他們指出，任何觸及 Shell 命令的原生工具參數都可能成為潛在的注入點，因此對此類漏洞進行審計已不再是可選措施，而是安全交付 AI 代理功能的前提。

個人資料保護法

五福旅遊重訊　駭客攻擊「個資外洩」觀光署重罰100萬

五福旅遊遭觀光署重罰。(圖／業者提供)

記者 陳昫蓁 報導

發佈時間：2026/04/14 11:44

最後更新時間：2026/04/14 11:44

五福旅遊1月證實公司資安監控系統偵測到網路駭客攻擊，據了解有23GB的顧客資料外洩，業者也趕緊報案處理。而交通部觀光署經調查後，決定裁處100萬元罰鍰。

五福旅遊遭駭！旅客個資外洩

五福旅遊1月表示，發現異常的第一時間，立即啟動防禦機制與應變程序，同時盤查伺服器紀錄，初步確認受影響之資料包含部分旅客之姓名、護照及行程內容，所有旅客信用卡及金流機敏資料，均採取符合國際標準之加密存儲或委託第三方支付處理，並未儲存於受攻擊之伺服器中。經核實本次事件中旅客信用卡資訊確認安全無虞，不過有部分旅客個資受損，五福旅遊也在盤查後向刑事局報案，同時通報觀光署。

五福旅遊重訊！觀光署重罰百萬

五福旅行社近期發出重大訊息，針對2026年1月27日遭受網路駭客攻擊，致發生該次資安事件，違反《個人資料保護法》第27條第1項規定，觀光署裁處新台幣100萬元罰鍰，強調公司已優化資安機制及強化資訊安全系統，並遵循主管機關相關專業建議進行。

五福旅遊表示，資安強化措施包含導入ISO 27001資訊安全機制、加強資料去識別化與加密技術，強化入侵偵測與預警系統，實現「即時發現、即時阻斷」，今年全面啟動大規模數位轉型，聚焦3大維度，包括：資安升級、電子簽章、導入Google Workspace企業生態系，強化營運韌性。

每月一常識

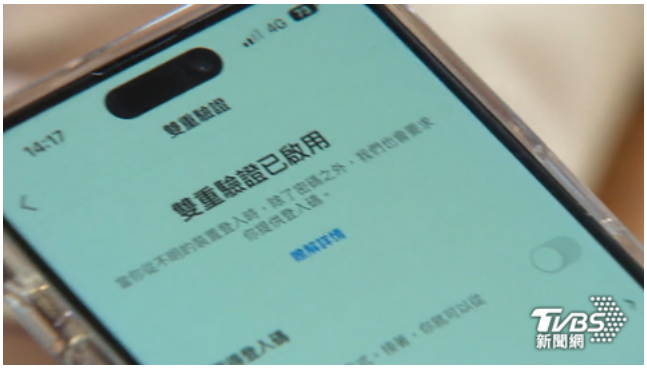
新版個人資料保護法與過去有很大的不同，新法進一步擴大了個人資料的保護範圍，並且讓所有產業一體適用；新法甚至首度增加團體訴訟，而且違法的罰則也加重了，企業老闆要負更大的責任。接下來，我們以60個Q&A，快速帶你認識新版個人資料保護法

Q25　告知只能以紙本型式的書面告知嗎？

A　告知可以採用書面、電話、傳真、電子文件或其他適當的方式。

文/iThome

IG無預警被登出是警訊！她靠AI「隔空廝殺」奪回帳號



責任編輯 新聞中心 報導

發佈時間：2026/04/13 18:16
最後更新時間：2026/04/13 19:43

近期有民眾發現IG無預警被登出，專家指出這其實是駭客盜帳號的警訊。有當事人分享自己求助AI，與駭客隔空交戰最終成功奪回帳號的經歷。資安專家提醒，若在信箱收到帳號密碼登入信，不要隨意填寫，很可能是駭客的假信件，最好定時檢查社群帳號，發現不明位置或裝置應立即刪除，避免帳號被盜用淪為詐騙工具。一名民眾分享自己IG險遭盜用的經歷，她表示那天打開IG發現登不進自己的帳號，才發現大頭貼和帳號都被換掉了。面對天天都在滑的社群軟體被盜，她感到非常緊張，不斷登入改密碼也沒用，最後求救AI，照著GEMINI指示操作才成功登入。

這名當事人描述，她跟對方在空中廝殺搶帳號，同個時間彼此瘋狂登入IG，搶回來之後兩度被對方奪走。當她把帳號移回自己的信箱，第一次順利登入時，信箱卻跳出不明驗證碼。當事人指出，這個應用程式密碼就像一道隱形的後門，能繞過所有密碼直接登入，只要它還在，無論怎麼登入、改密碼都沒有用。她刪掉之後立刻重新設定信箱密碼，再登入IG修改所有密碼與雙重驗證。此外，也有其他人在社群平台發文求助，表示IG無預警被登出，說是為了保護帳號不被盜，所有裝置都被登出了。

資安專家查士朗說明，比如說某些購物網站，如果使用了跟IG相同的帳密，駭客取得購物網站的帳密後，就會用這組資訊去嘗試登入IG，或者直接寄假信件給使用者，讓人以為是在登入，但其實是把帳密交給駭客。查士朗建議，在不同APP軟體最好不要都設置同一組帳號密碼，在陌生裝置登入帳號以及前往不安全的網路位置時，都要特別小心留意。查士朗進一步表示，民眾可以強化自己IG帳號的安全性，例如設定多因子認證，比較簡單的方式就是新增手機，到時候有任何情況，不只是E-mail，手機也可以收到認證訊號，而駭客要直接取得使用者的手機是比較困難的。他指出，最好不定期檢查社群帳號，如果發現有不知名的位置或不知道的裝置，要趕快把它踢掉，避免帳號被盜用，甚至淪為詐騙帳號。