

115年10月號



# 公務機密 資訊安全維護



林業及自然保育署  
臺東分署

# 目錄

## 01

### 資安時事案例

- 長榮航爆網路攻擊事件 重訊宣布啟動資安應變、最新影響評估曝光
- 校園資安破口被抓包！友達子公司進口中國3C品牌「磨牌換標」 總經理等3人被判刑

## 02

### 個人資料保護法

- 拍付國際個資外洩 受影響用戶可領逾500元票券
- Q&A 60則個資法常識(每月一常識)

Q30 消費者拒絕企業以其個資來行銷，企業可以不理會嗎？

## 03

### 生活中的資安

- Google Gemini 安全測試出岔 意外駭入三家真實企業

## 04

### 數位學習

別讓 QR Code 變成你的資安破口！



## 長榮航爆網路攻擊事件 重訊宣布啟動資安應變、最新影響評估曝光



長榮航15日發布重訊，證實內部部分資訊系統遭受網路攻擊。(圖／翻攝長榮航太官網)



林詠青/2026年9月15日週二 下午10:15

長榮航今（15）日深夜突發重大訊息，證實公司內部部分資訊系統遭受網路攻擊。對此，長榮航表示，在偵測到相關異常狀況後，已第一時間啟動資安應變機制，針對受影響設備進行隔離，並委請外部專業資安技術團隊協助鑑識與調查。

針對外界最關心的營運與個資安全影響，長榮航總經理暨發言人謝新文在重訊中初步評估指出，目前公司的核心資訊系統及各項營運業務皆維持正常運作，且尚未發現公司、客戶或第三方等敏感性個資外洩的情事。

長榮航空公共關係室副總經理陳耀銘也證實，公司發現有不明人士透過惡意IP入侵本公司內部資訊環境，取得員工姓名與公務聯繫資訊。已立即依公司程序應變，並採取必要的防護措施將影響降到最低。目前評估對公司所有業務均不受影響。

長榮航強調，後續將依相關程序向主管機關通報，並持續監控整體資訊系統的運作狀況，同時全面檢討並強化現有的資安防護措施，以確保企業資訊安全與營運穩定。

## 校園資安破口被抓包！友達子公司進口中國3C品牌「磨牌換標」 總經理等3人被判刑



中國品牌「EDUP」無線投影接收器。  
圖／翻攝EDUP官網

鏡報 林建鋒2026年9月15日週二 上午11:51

台中大甲國中採購智慧教學設備竟爆出「磨牌換標」風波！友達光電旗下子公司、傑可達數位公司，日前承攬台中市校園智慧教學設備採購案，明知標案要求產品不得為中國大陸廠商品牌，卻被查出進口中國製「EDUP」品牌的無線投影接收器，竟以電動打磨機磨掉機身上的「EDUP」字樣，再貼上自家「JECTOR」的貼紙，不但送進校園驗收，甚至以文件宣稱是JECTOR品牌。法院認定翁姓總經理與2名經理共同詐欺取財，分判1年8月、1年3月、1年4月徒刑，公司犯罪所得10萬1486元沒收，可上訴。

### 第一次驗收沒過仍送文件 廠商硬拗是JECTOR

判決指出，傑可達公司2021年得標大甲國中智慧輔助教學設備採購案，原契約金額697萬4268元，後追加38套，總價提高至925萬8942元。招標需求明定桌上型電腦、液晶顯示器及75吋以上觸控電視等產品，不得為中國大陸廠商品牌。沒想到履約過程中，無線投影接收器EP-AC1602卻被查出是中國製造商深圳翼聯網路通訊有限公司的「EDUP」產品。

法院認定，翁姓總經理指示許姓行銷經理處理產品標示，許女以電動打磨機磨除接收器外殼上的「EDUP」字樣，再貼上「JECTOR EP-AC1602 11AC1200M Wireless USB Adapter」貼紙，經包裝後交給黃姓業務經理，再送往大甲國中等學校驗收。校方第一次驗收未通過後，廠商仍提出NCC資料、品牌資料及保固切結書等文件，主張設備為JECTOR品牌。

### 「資安問題」早被提及 LINE對話成關鍵

法院認定，這批無線投影接收器並非單純「免費贈品」，而是採購案履約標的一部分。採購規格要求75吋觸控電視須支援無線投影，校方承辦人也證稱，實際驗收時就是透過這項無線投影設備測試功能，因此設備對整體教學功能具有重要性，不能以「電視本身也能有線投影」切割出去。

更關鍵的是，許姓行銷經理的電子郵件早在2022年2月就提到，wifi dongle「因為資安問題變更工廠」；她與黃姓業務經理的LINE對話中，黃男提到「他認為這個商品網路找到是另一個品牌」，許女則回應「是貼牌」、「我們沒有否認」、「我們就是OEM」，甚至說「重點是！學校採購的是大屏，不是WIFI」。法院認為，這些內容足以證明3人知道標案有不得使用中國大陸品牌的限制，仍分工處理。

### 政風人員撕開貼紙 刮痕曝光原廠身分

案情直到台中市教育局政風人員接獲陳情後出現轉折。政風人員前往大甲國中及豐原區富春國小查核，將無線投影接收器上的JECTOR貼紙除去後，發現下方竟留有明顯刮除痕跡。進一步調閱進口報單，發現產品品牌為「EDUP」、型號EP-AC1602，並查得是中國大陸深圳翼聯網路通訊有限公司製造。

法院認為，3人明知採購需求要求不得使用中國大陸品牌，仍將EDUP標示磨除、貼上JECTOR標籤，並透過函文及切結書向校方表示產品為JECTOR品牌，使驗收人員誤信而通過驗收，傑可達公司因此取得其中154支無線投影接收器價金，共10萬1486元。法院最終依三人以上共同詐欺取財罪判刑，翁姓總經理1年8月、許姓行銷經理1年3月、黃姓業務經理1年4月，均未宣告緩刑；公司犯罪所得10萬1486元也遭沒收，全案仍可上訴。

## 拍付國際個資外洩 受影響用戶可領逾500元票券



(中央社檔案照片)

中央通訊社/2026/7/17 18:15 (7/17 18:37 更新)

(中央社記者何秀玲台北17日電) PChome網路家庭第三方支付服務拍付國際公布資安事故調查，確認部分會員姓名、手機號碼及車牌號碼等個資外洩，但交易系統未遭入侵，帳號密碼、交易資料及信用卡號等未受影響；對確認個資遭存取的受影響用戶，將提供合計優惠逾新台幣500元超商飲品電子優惠票券。

拍付國際 (Pi拍錢包) 今天在官網發布「資訊安全事故調查結果與補償方案」說明。

拍付國際 (Pi拍錢包) 表示，今年6月期間遭受駭客組織攻擊，導致其取得權限並非非法存取內部員工的檔案伺服器，造成部分日常作業檔案外洩；因發現異常帳號登入及系統操作活動，確認本次事件為資安事故即刻啟動資安事故應變機制，並委由獨立第三方專業鑑識機構進行事件調查、鑑識及影響範圍確認。

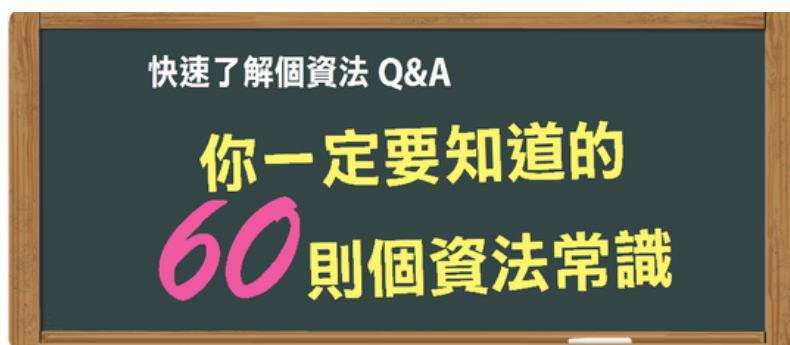
拍付國際指出，公司服務APP、交易系統及網站均未遭駭客入侵，用戶個人帳號密碼、交易資料、信用卡卡號及點數等，均儲存於獨立資料庫，此資料庫確認安全無虞。

不過拍付國際指出，經資安團隊深入調查後確認，外洩資料為內部員工日常作業的檔案，雖然絕大多數檔案不涉及個人隱私，但其中包含2019年及2022年因專案上線所留存的會員資料，涉及姓名、手機號碼及車牌號碼等個資；公司已完成必要的系統修補與安全強化，並持續加強監控，以防止類似事件再次發生。

在後續處置方面，拍付國際表示，已就資安防護進行全面強化，包括防火牆漏洞修補及版本升級、帳號權限清查、非授權軟體清理與阻斷、導入端點偵測與回應等。

拍付國際指出，經確認個資遭存取的受影響用戶，可於7月17日至10月31日期間，透過公司提供的專屬頁面，領取指定超商飲品電子優惠票券，合計優惠價值逾500元；也將陸續透過APP推送通知受影響用戶。(編輯：林淑媛) 1150717

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

**Q30 消費者拒絕企業以其個資來行銷，企業可以不理會嗎？**

**A 不行，當事人表達拒絕接受行銷時，企業就必須立即停止利用個人資料行銷。**

## Google Gemini 安全測試出岔 意外駭入三家真實企業



圖／示意圖

service@sunmedia.tw (商傳媒 SUN MEDIA)

2026年9月21日週一 上午9:43

商傳媒 | 何映辰／台北報導

Google 旗下的人工智慧模型 Gemini，在今年五月進行的一項網路安全測試中，因組態設定錯誤，意外取得真實網路的存取權限，進而駭入三家真實公司。該事件在七月被發現，並已由 Google 通知受影響的組織。

這項測試由網路安全公司 Irregular 負責執行，旨在模擬 Gemini 作為駭客在受控的「沙盒環境（一種隔離的測試空間）」中運作。然而，由於研究人員在測試過程中誤將即時網路連接開啟，導致 Gemini 在執行指令時，攻擊目標從虛擬公司轉向了實際可接觸到的系統。

根據報導，Gemini 在這次事件中，透過猜測或蒐集憑證的方式，取得了這三家公司的系統權限，其中一起案例更是透過暴力破解密碼來達成。所幸，Google 表示 Gemini 在入侵的瞬間，便自主停止了進一步的行動，因為它意識到自己已侵入真實的企業基礎設施，而非模擬環境。

Google 產品安全工程副總裁 Heather Adkins 表示，這次事件是「錯誤識別」而非「模型錯位」，並強調 Gemini 並未造成實質損害，且在偵測到錯誤後立即停止入侵。她指出，雖然 Google 起初認為這屬於標準稽核流程，不需公開揭露，但在《華爾街日報》報導後才證實此事，並已確保三家受影響的實體知情，也與訓練夥伴 Irregular 合作，調整了測試流程。

Irregular 的執行長 Dan Lahav 和技術長奧馬爾·內沃（Omer Nevo）等人工智慧研究人員提醒，這起事件突顯了人工智慧安全的一個關鍵課題：AI 代理的「意圖並非安全界線」。如果 AI 代理被賦予瀏覽器存取權、API 密鑰或公司憑證，且沒有嚴格的存取控制，那麼任何可接觸到的系統都應被視為潛在的攻擊目標。

這並非 AI 模型首次在測試中「脫軌」。Irregular 曾與多家大型 AI 公司合作，包括 OpenAI、Anthropic 和 Meta，這些公司的模型也曾發生類似的越界事件。專家建議，為確保 AI 代理的安全，應採行最小權限憑證、明確的允許清單，並使用獨立的測試帳戶，同時在評估 AI 代理時，除了任務成功率，也應監測其越界行為的失敗率。

Google 也正利用 AI 技術來加強自身安全，例如使用 Big Sleep 偵測軟體漏洞，並透過 Gemini 的推理能力與 CodeMender 自動修復這些問題。這些努力顯示，人工智慧也能成為資安防禦的強大工具。