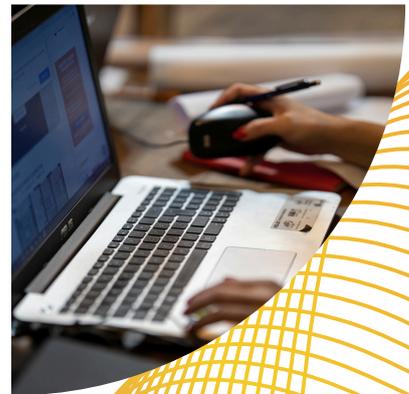


114年10月號

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

- 1.1萬臺物聯網裝置、路由器遭綁架，發動每秒15億個封包的DDoS攻擊
- 一票人險上當！這封email千萬別點 網址「2字結尾」100%是詐騙

02

個人資料保護法

- 林姓調查員涉違個資法與洩密罪 台南地院裁准10萬元交保
- 快速瞭解個資法Q&A 60則個資法常識(每月一常識)

Q18 在國外蒐集個人資料，仍須遵守個資法規定嗎？

03

生活中的資安

- 壽司郎出包！他狂收600封信「會員個資全看光」業者急道歉曝賠償方案

04

數位學習

資安大作戰



1.1 萬臺物聯網裝置、路由器遭綁架，發動每秒15億個封包的DDoS攻擊



iThome/文/周峻佑|2025-09-15發表

資安業者FastNetMon揭露專門鎖定DDoS流量清洗服務業者的DDoS攻擊行動，駭客綁架1.1萬臺物聯網裝置、路由器，發動每秒發出15億個封包的UDP洪水攻擊

9月初資安業者Cloudflare揭露峰值達到11.5 Tbps的DDoS攻擊，封包速率最高達5.1 Bpps，持續約35秒，一開始認為攻擊流量來自Google雲端，後續確認同時來自物聯網裝置及多家雲端服務供應商，如今有其他資安業者發現新一波攻擊行動，但這次主要是針對緩解相關攻擊的服務業者而來。

英國資安業者FastNetMon於9月9日指出，他們發現專門針對西歐一家DDoS流量清洗服務業者的DDoS攻擊，封包的速率每秒達到15億個（1.5 Gpps或1.5 Bpps），惡意流量主要是UDP洪水攻擊，由全球1.1萬臺物聯網裝置及路由器等用戶端設備（Customer-Premises Equipment，CPE）產生。由於這起事故發生在Cloudflare揭露的事故數天之後，代表攻擊者現在已經將攻擊流量和封包的規模，提升到另一個境界。

針對這樣的現象，FastNetMon認為，當數以萬計的CPE設備被挾持用於如此大規模DDoS攻擊，網際網路服務供應商（ISP）的資安風險就會呈現指數級成長，因此，業者必須在ISP層級實施相關偵測，才有機會在流量膨脹到如此規模之前，攔阻這類攻擊。

一票人險上當！這封email千萬別點 網址「2字結尾」100%是詐騙



交通部提醒，網址以「gov.tw」結尾的才是政府官方網站。(圖／翻攝自交通部臉書)

三立新聞網

2025年9月7日

生活中心／張尚辰報導

詐騙事件層出不窮，許多詐騙集團為了達到目的，甚至還會冒充政府機關的名義，就有不少網友差點中招。對此，交通部提醒網址以「gov.tw」結尾的才是政府官方網站，警政署也補充說明，詐騙集團的網址經常會用數字「0」或是英文字母「O」做結尾，請民眾千萬不要上當受騙，如遇可疑訊息，可以撥打「165」查證。

交通部近日在臉書發文，指出近期有不肖人士冒用「公路局」的名義，寄送詐騙Email，要求民眾繳納欠款。對此，交通部提醒，只有網址以「gov.tw」結尾的才是政府官方網站，遇到可疑訊息，請記得撥打165反詐專線查證。

交通部提醒，切勿點擊來源不明電子郵件、簡訊或連結，以免遭受詐騙，監理機關雖有交通違規罰單到期簡訊提醒通知服務，但需要車主主動提出申請，且此服務僅限於「提醒通知」，不會附上網址供下載及點選。

另外，警政署也在臉書「165全民防騙」中轉發交通部的貼文，補充說明詐騙集團的網站通常是以數字「0」或是英文字母「O」做結尾，請民眾務必看清楚，不要上當受騙。

林姓調查員涉違個資法與洩密罪 台南地院裁准10萬元交保



台南地院審理林姓調查員違反個資法及洩密案，裁准以10萬元具保後釋放。(記者林東良攝)

ETtoday 新聞雲2025/9/16/記者林東良／台南報導

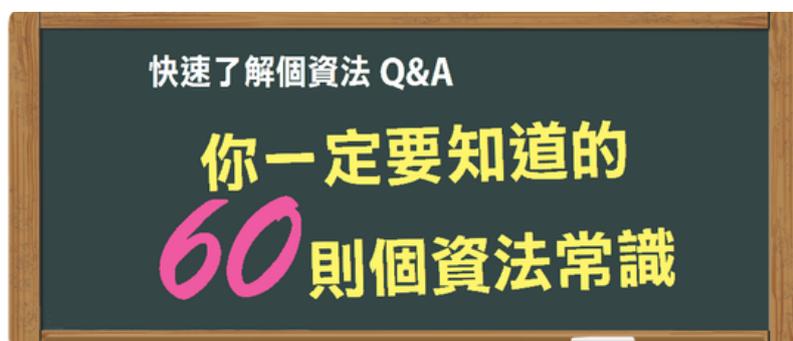
一名林姓調查員涉嫌違反個人資料保護法及刑法洩密案，台南地檢署提起公訴，案經15日移審台南地院，合議庭審酌相關情節後，認為林員雖有湮滅、串供之虞，但可能性已降低，最終裁定以10萬元交保並限制行為，案件將進入審理程序。

起訴資料指出，林姓調查員涉嫌利用職務機會非法取得並使用個人資料，涉犯《個資法》第44條、第41條公務員假借職務機會非法利用個資罪嫌，另依《刑法》第132條第1項，涉犯公務員洩漏國防以外祕密罪嫌。

台南地院審理時，針對林員與同案被告交接電子檔案供述存有歧異，仍待進一步調查。合議庭認為，林員確有湮滅、偽造、變造證據或串供風險，符合刑訴法第101條第1項第2款規定。不過，考量被告已具體供述、羈押原因降低，並兼顧司法權行使與被告防禦權，裁定准予10萬元具保停押。

另台南地明令，林員不得再與共犯或證人聯繫，不得湮滅或變造證據，亦禁止與同案被告接觸，以確保後續審判順利。

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

Q18 在國外蒐集個人資料，仍須遵守個資法規定嗎？

A 不論是在國內或國外，只要蒐集個資的對象是中華民國國民，在個資蒐集、處理或利用，就必須受個人資料保護法的規定。

文/[iThome](#)

壽司郎出包！他狂收600封信「會員個資全看光」 業者急道歉曝賠償方案



壽司郎品項眾多，是不少壽司控的心頭愛。(圖／資料照)

三立新聞網/2025年9月16日 週二 上午11:53/生活中心／張尚辰報導

知名連鎖店「壽司郎」是不少壽司控的心頭愛，菜單品項豐富，常常讓人選擇障礙。近日，壽司郎卻爆出資料外洩的問題，有網友爆料他總共收到64封的「點數到期通知」裡面包含會員姓名、剩餘點數以及會員email信箱等，甚至還有人收到高達600封的通知郵件。對此，壽司郎緊急致歉，並祭出應對措施，為表示歉意還提供新台幣500元的折價券給受影響的顧客。

一名網友14日在Threads上發文，指出他收到壽司郎的點數到期通知，沒想到一次收到64封，仔細一看才發現上面是不同會員的名字，還包含會員的email信箱，「現在我家巷口阿伯手上有幾點我都知道」。

貼文曝光後，吸引43萬人瀏覽、4千多人按讚、1千多人轉發，不少網友紛紛留言，「姓名和電郵都是個資，壽司郎這出包好像有點嚴重」、「看到有人收到六百封，慘了他們，只能說好險只有姓名，其他都沒有，不然多一個資訊他們都死定」、「就算只是mail應該也會造成不小的困擾」。

壽司郎官方小編在貼文下緊急道歉，表示經查證後，是因為系統發信程序出現異常，技術團隊已介入處理，並釐清問題根源，「造成的不便與困擾，我們深感抱歉」。

壽司郎也向用戶寄出道歉信，對於這次的誤植事件壽司郎採取4點緊急措施，包括立即停止異常的發信功能，防止影響範圍擴大、與第三方專業單位合作完成檢測，確認未有持續性外洩風險、啟動內部稽核權制，全面檢討對委外廠商之監督流程，加強資訊安全管控、對於受影響顧客，持續提供必要協助與專屬客服支援。

另外，針對此次事件，壽司郎也向受影響顧客提供價值新台幣500元的電子折價券，將於本月19日以前陸續配送至會員的APP帳戶中。