



# 公務機密 資訊安全維護

114年4月號



林業及自然保育署  
臺東分署

## 目錄

01

### 資安時事案例

- 資安議題嚴峻！AI輔助攻擊盜取數僅需25分鐘
- 一天網攻240萬次！國安局揭大陸網駭政府與企業最新手法

02

### 個人資料保護法

- Line又有新型詐騙！看到1連結千萬別點，否則個資恐全被騙光荷包空空
- 快速瞭解個資法Q&A 60則個資法常識(每月一常識)  
Q12 任何類型的個人資料都可以蒐集嗎？

03

### 生活中的資安

- 網購1習慣很致命！專家：盜刷、個資外洩風險大增

04

### 數位學習

3D五力全開 

## 資安議題嚴峻！ AI輔助攻擊盜取數僅需25分鐘



駭客示意圖。路透社資料照片

陳俐玟

2025年3月13日 週四 上午6:45

資安議題嚴峻！AI輔助威脅與多重入侵等手段、攻擊速度、複雜程度和規模都達到前所未見的水準，在一小時內盜取數據的案例達到20%。Palo Alto Networks Unit 42威脅情報小組發現，AI輔助攻擊可將盜取數據時間縮短至僅25分鐘。

Palo Alto Networks 的Unit 42威脅情報小組發布最新報告，2024年發生的重大網路事件中，86%導致了企業營運中斷、聲譽受損或經濟損失。以財務為動機的攻擊者已將重點轉向蓄意破壞營運，優先進行破壞行動，例如：摧毀系統、封鎖客戶帳戶、造成長時間當機，以此造成更大的影響並迫使企業支付贖金。

報告顯示，網路攻擊達到空前的速度，在25%的事件中，攻擊者在5個小時內就盜取數據，相較於2021年快了三倍。更令人擔憂的是，在一小時內盜取數據的案例達到20%。

2024年與北韓相關的內部網路攻擊增加三倍。北韓國家級駭客被發現以IT專業人士身分滲透企業，獲取就業機會後，逐步植入後門、盜取數據甚至修改原始碼。

多管齊下的攻擊成為新常態，在70%的事件中，攻擊者同時利用三種或更多攻擊面進行入侵，迫使安全團隊不得不同時防禦端點、網路、雲端和人為因素。

2024年網路釣魚再次成為主要攻擊入口，佔所有初始入侵的23%。在生成式AI的助力下，網路釣魚活動的複雜程度、可信度和規模都達到空前的水平。

而雲端攻擊也持續增加，近29%的網路事件涉及雲端環境，其中21%直接對雲端環境或營運造成損害。攻擊者利用錯誤配置的環境，掃描廣泛的網路以尋找有價值的數據。

報告也顯示，AI正在加快攻擊週期：攻擊者利用AI技術提高網路釣魚活動的可信度、自動開發惡意程式和加快整條攻擊鏈的進展速度，使網路攻擊更難被偵測且執行速度更快。在一項受控實驗中，Unit 42威脅情報小組發現AI輔助攻擊可將盜取數據時間縮短至僅25分鐘。

由於駭客已經改變了攻擊手法，利用AI、自動化和多重入侵的工作手法繞過傳統防禦系統，從入侵到造成全面影響的時間正大幅縮短，因此快速檢測、回應和修復變得至關重要。

Palo Alto Networks指出，企業如果希望能在2025年領先於攻擊者，關鍵在於提前保護網路、應用和雲端安全，同時透過AI驅動的檢測和回應獲得全面地可見性並加快遏止威脅的速度，以此提高自身安全營運能力。



## 一天網攻240萬次！國安局揭大陸網駭政府與企業最新手法



國安局揭大陸網駭政府與企業最新手法。  
(圖:shutterstock/達志)

2025/01/05 /中時新聞網/戴志揚

針對中共網軍對我國網路空間攻擊、竊資及侵擾不斷，且駭侵手法不斷翻新。為讓國人瞭解網安威脅趨勢，國安局近期完成「2024年中共網駭手法分析」報告。其中顯示，大陸網軍平均每日攻擊政府網際240萬次，同時結合民間駭客，破壞基礎關鍵設及勒索金融企業，危害日益嚴重。

國安局分析，大陸網攻趨勢發展，依據政府網際服務網「入侵偵測指標」統計，我政府網際服務網去（2024）年每日平均侵擾數為240萬次，較2023年日平均侵擾數120萬次增加逾2倍。其中多數為中共網軍所為，雖多已有效偵阻，惟仍凸顯整體網駭侵擾態勢愈趨嚴峻。

另國安情報團隊去年掌握我國政府及民間網駭案件計906案，相較2023年752案，增長比率逾二成，其中以政府機關比率最高，占整體總數逾八成。經分析中共網軍駭攻目標，以通訊傳播領域（650%，主要為電信業）、交通（70%）及國防供應鏈（57%）增長最為顯著，顯見該等領域已成為中共新興網駭重點。

國安局也表示，在駭客入侵手法部分，中共網軍鎖定我政府機關網通設備漏洞設伏竊資，以「離地攻擊」（Living off-the-land）手法，躲避網防系統偵察，並針對我公職人員電子郵件，發動社交工程等攻擊，企圖竊取機敏資訊。此外，中共以多元手段，對我國防供應鏈及資服業者駭侵竊資，並透過進階持續性滲透、釣魚郵件、零時差漏洞、木馬病毒、後門程式等方式，駭攻設伏我公路、港務等關鍵基礎設施，企圖影響我國交通運輸秩序。

國安局更查出，在中共軍演期間，其網軍對我交通及金融機構，發動「分散式阻斷服務攻擊」（DDoS），期強化騷擾效果，並擴大軍事威懾。值得注意的是，中共亦結合民間駭客協力組織，運用勒索軟體等網路犯罪手法，對我製造業廠商遂行駭攻，以及對各國高科技新創產業竊取專利技術，圖謀獲取經濟利益。另中共網軍以網駭手段竊取我國人個資，於暗網及駭客論壇公開販售獲利，遂行「駭侵及洩漏」（Hack & Leak），同時藉由社群網路論壇發文批評網防不力，打擊我國家威信。

國安局強調，中共持續加大對我網路攻勢，並結合多元網路駭侵手法，對我政府、關鍵基礎設施及重要民企，進行偵查設伏及網駭竊資。我國政府透過資通安全聯防機制，運用多元情報來源管道，掌蒐網安威脅預警情資，即時分享權責部門應處；同時提醒國人重視資安防護，警覺中共對我網駭威脅，共維我國整體網路安全。

## Line又有新型詐騙！看到1連結千萬別點，否則個資恐全被騙光荷包空空



王品遭不肖人士陷害，詐騙集團誤導民眾回應個資。(圖／王品集團提供)

風生活綜合報導2025-03-11 11:24

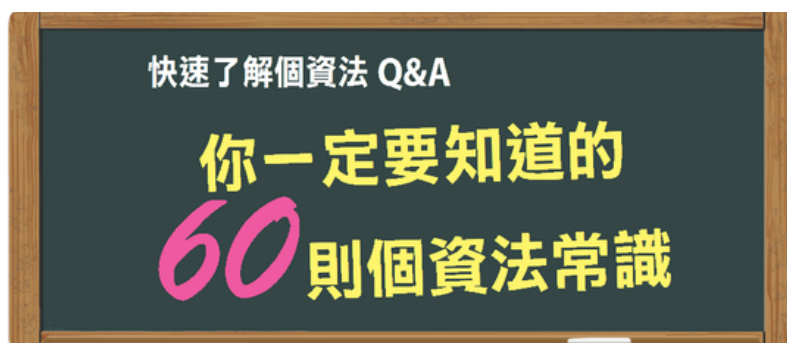
近來詐騙案件層出不窮，王品旗下西堤、陶板屋、夏慕尼、原燒、和牛涮...等各品牌，遭不肖人士宣稱租借場地舉辦「小小廚師」體驗活動，並製作廣告圖文於Facebook、Instagram等社群渠道投放廣告，意圖誤導民眾點擊連結、加入Line群組進而騙取個資。王品集團請民眾多加留意，請勿加入任何不明群組，並提供任何重要個資，以免遭不肖人士利用。

詐騙集團利用民眾對王品集團信任，宣稱租借品牌場地舉辦「小小廚師」活動，在Facebook、Instagram等社群投放廣告，誤導民眾點擊連結、加入Line群組，以報名活動話術誘導民眾騙取個資。像是在群組中提供姓名、手機號碼或電子郵件等個資，恐遭不肖人士用來詐騙或其他犯罪活動。

### 王品集團沒有舉辦「小小廚師」活動

王品集團提醒，集團旗下各品牌皆無舉辦「小小廚師」活動，也無租借場地給任何單位，請民眾小心提防各種詐騙手法，保護個資，遠離不明LINE群組邀約。如有相關疑問，請撥打165反詐騙專線，杜絕不法詐騙。對於層出不窮的詐騙案件，王品集團針對詐騙廣告展開蒐證、檢舉，向警方報案，並將追究相關民刑事責任，絕不寬貸。集團官網、王品瘋美食App、各品牌官方社群平台發布防詐騙公告，提醒民眾提高警覺，切勿相信詐騙廣告，點擊任何蒐集個資的連結、加入來路不明的Line聊天群組，避免上當受害。

## 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

**Q12 任何類型的個人資料都可以蒐集嗎？**

**A** 新版個資法引進「特種資料」的概念，對於敏感性資料不得蒐集，包括醫療、基因、性生活、健康檢查及犯罪前科的個人資料，都不得蒐集。在沒有法律明訂可以的前提下，要求任何人提供不得蒐集的特種資料，就會違法。

## 網購1習慣很致命！專家：盜刷、個資外洩風險大增



專家警告，網購時在網站上儲存信用卡資料，很容易被盜用。  
(示意圖：shutterstock／達志)

網購方便，讓許多人懶得出門購物、愛叫外送，但資安危機也跟著增加，網路安全服務公司「Fortalice Solutions」戰略長歐蕾莉近日警告，網購時儲存信用卡資料的習慣，很容易成為網路犯罪下手的目標，並教6招反制，包括停止儲存信用卡資料、用加密工具儲存密碼、啟動雙重驗證等。

根據外媒《HuffPost》報導，前白宮行政辦公室負責人兼首席幕僚、資安公司「Fortalice Solutions」戰略長歐蕾莉表示，網購時儲存信用卡資料是很方便，但網路犯罪最難防的就是他們不只有一種方法來竊取信用卡資訊，等受害者發現情況不對時，大多為時已晚，已經被盜刷。

歐蕾莉表示，網路犯罪人士主要是用偷走電子產品，像是手機、電腦、筆電；利用公用Wi-Fi入侵；在App植入惡意軟體或間諜軟體，以及駭客入侵、接管帳號、資料外洩、利用憑證填充攻擊等方式竊取信用卡資料。而「憑證填充攻擊」也叫撞庫攻擊，是駭客從某個網站獲得使用者的帳號密碼，再編寫程式把這些帳密拿到其他網站一個個嘗試登入，企圖從不同網站找到相同的使用者，盜用其帳號、信用卡、個人資料等，看準了用戶喜歡使用同一組帳密的資安漏洞。

對此，歐蕾莉教6招反制措施，避免信用卡、個人資料等被盜用。

1. 停止儲存信用卡資料
2. 使用加密工具儲存密碼、使用Apple Wallet
3. 定期檢查銀行帳單
4. 啟動雙重驗證（2FA）
5. 安裝口碑好的防毒軟體
6. 下載或點擊不明檔案、連結之前要多加留意

歐蕾莉指出，若民眾仍覺得網購時儲存信用卡資料比較方便，記得最多只存一張信用卡，這樣較容易偵測到可疑交易，並利用信用卡的安全性，避免銀行帳戶被掏空。