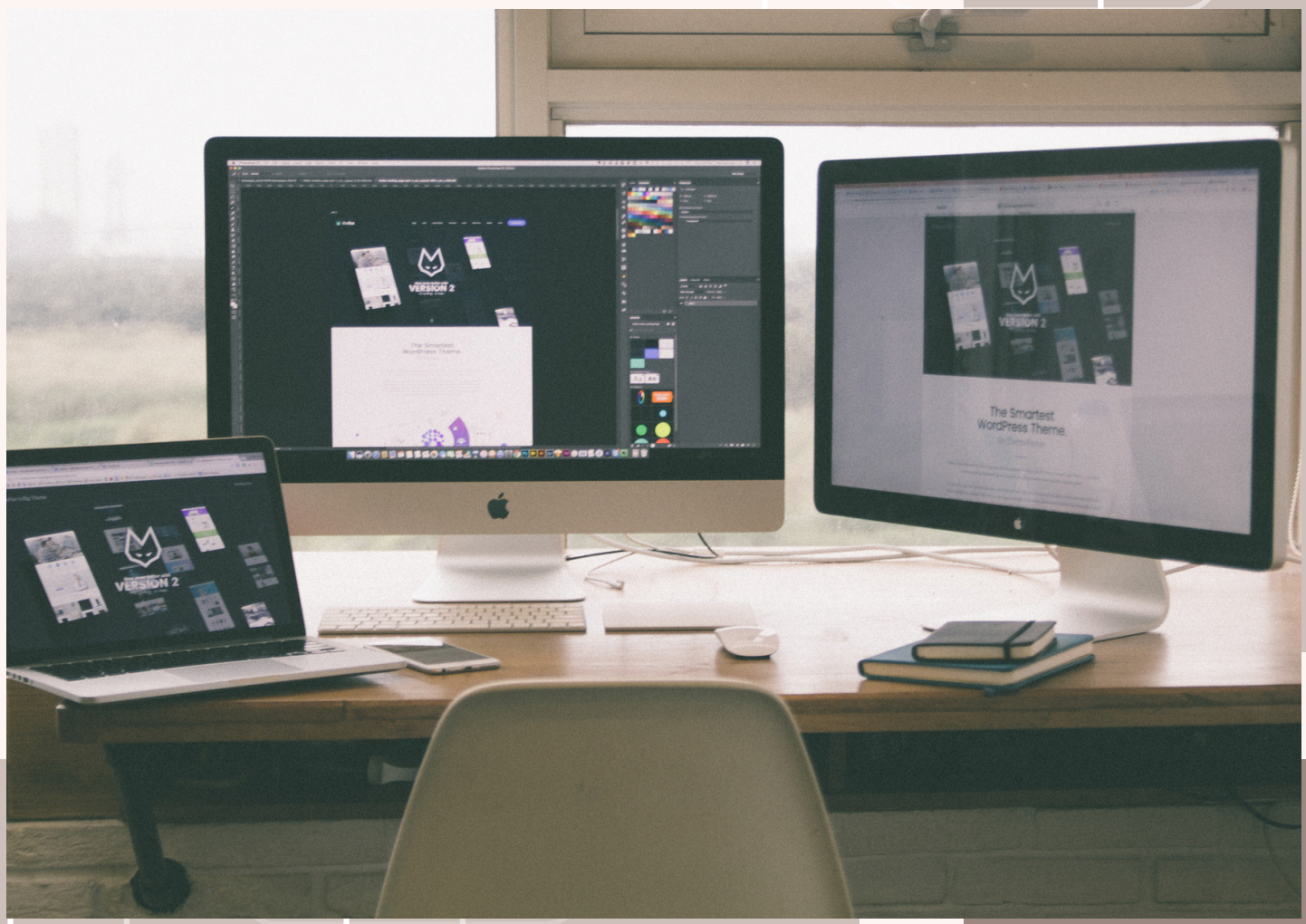
114年1月 號

# 公務機密
# 資訊安全維護




林業及自然保育署
臺東分署

# 公務機密 資訊安全維護

# 目錄

# 11月資安聯防情資達9.6萬件 創逾2年新高

The Central News Agency 中央通訊社
2024年12月17日 週二 下午8:22

（中央社記者蘇思云台北17日電）根據數發部資安署11月資安月報顯示，11月政府機關資安聯防情資共9萬6175件，創下2022年9月以來、逾2年新高。資安署提醒，也有駭客以商業報價或發票為由，寄送惡意程式垃圾郵件攻擊公部門，呼籲各機關多留意。

所謂資安聯防情資，就是偵測是否有壞人在門外徘徊，壞人可能嘗試開門，看是否有門沒鎖好、伺機闖入，而這些測試都可能留下異常的紀錄。資安月報顯示，11月政府機關資安聯防情資共9萬6175件，月增5417件。

分析可辨識的威脅種類，第1名為資訊蒐集類（52%），主要是透過掃描、探測及社交工程等攻擊手法取得資訊；其次為入侵嘗試類（19%），主要是嘗試入侵未經授權的主機；以及入侵攻擊類（18%），大多是系統遭未經授權存取或取得系統或使用者權限。

資安署指出，進一步彙整分析聯防情資資訊，發現近期駭客以商業報價或發票為由，大量寄送惡意程式垃圾郵件攻擊政府機關，惡意郵件會夾帶壓縮檔作為郵件附檔，藉此躲避掃描偵測，附檔內藏XRed木馬程式，企圖欺騙收件人以竊取資訊，相關情資已提供各機關聯防。
至於事中通報應變，11月資安事件通報數共53件，月減26件，年減38%。資安署指出，11月有多個機關發現資訊設備異常連線、執行異常指令或存在惡意程式，占總通報數的37.74%。

資安署觀察，社交工程攻擊屬於常見攻擊手法，近期發現駭客以申訴或舉報等議題，在申訴內容附上加密壓縮檔或外部下載連結，規避資安防護偵測，提高攻擊成功機率。

資安署建議，機關應加強民意信箱安全防護機制，像是檢視檔案前以防毒軟體掃描，不點擊外部不明連結，或強化內部人員資安教育訓練，提升對社交工程攻擊手法辨識能力，避免因檔名或圖示誤導而執行惡意程式。

此外，資安署指出，機關應檢視並強化民意信箱處理機制，如禁用或標記外部連結，限制民眾上傳檔案格式，在隔離環境處理外部高風險檔案，降低系統遭入侵風險。（編輯：林興盟）1131217

# 11月駭客假商業報價、發票或申訴舉報夾帶惡意程式多

2024.12.17 18:08 工商時報 呂俊儀

數發部資安署11月月報資料，本月蒐整政府機關資安聯防情資共9萬6,175件，月增加5,417件，資安事件通報數量共53件，比10月減少26件，為去年同期減少0.62倍，11月多個機關發現資訊設備異常連線、執行異常指令或存在惡意程式，占總通報數量37.74%。

分析可辨識的威脅種類，第1名仍是資訊蒐集類（52%），主要是透過掃描、探測及社交工程等攻擊手法取得資訊。第2名的威脅種類為入侵嘗試類（19%），主要嘗試入侵未經授權的主機；以及入侵攻擊類（18%），大多是系統遭未經授權存取或取得系統／使用者權限。

另外，彙整分析聯防情資資訊，近期駭客以商業報價或發票為由，大量寄送惡意程式垃圾郵件攻擊政府機關，惡意郵件夾帶壓縮檔作為郵件附檔藉此躲避掃描偵測，附檔內藏XRed木馬程式，企圖欺騙收件人以竊取資訊，資安署指出，相關情資已提供各機關聯防監控防護建議。

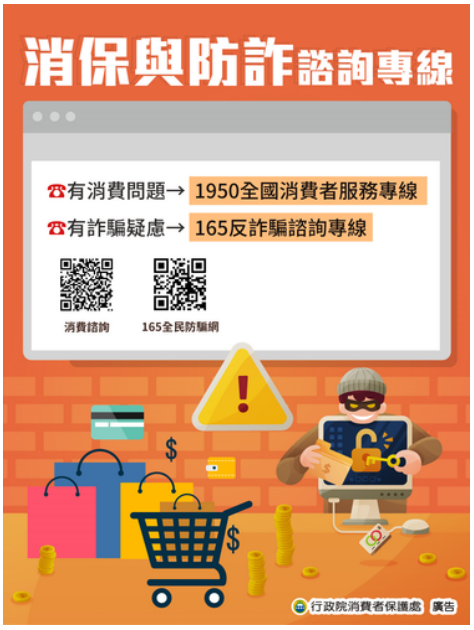
月報中也分享，某機關Endpoint Detection and Response （EDR）偵測資訊設備執行異常指令，經查發現該惡意程式來自官網民意信箱申訴內容，該內容要求自Google Drive連結下載檔案，並提供壓縮檔密碼，以規避民意信箱檔案上傳檢查機制。

由於承辦人員因業務所需，下載並解壓縮檔案，點擊偽裝成PDF文件的捷徑檔（LNK）後，遭載入並執行惡意程式，因此遭EDR偵測發現告警。
報告中提到，社交工程攻擊為常見攻擊手法，近期發現駭客以申訴或舉報等議題，於申訴內容附上加密壓縮檔或外部下載連結，規避資安防護偵測，提高攻擊成功機率。

建議機關加強民意信箱安全防護機制，如檢視檔案前以防毒軟體掃描，不點擊外部不明連結，或強化內部人員資安教育訓練，提升對社交工程攻擊手法辨識能力，避免因檔名或圖示誤導而執行惡意程式。

此外，應檢視並強化民意信箱處理機制，如禁用或標記外部連結，限制民眾上傳檔案格式，於隔離環境處理外部高風險檔案，降低系統遭入侵風險。

個人資料保護法




## 想騙身分證文件 詐團冒用高市府人員

2024-12-17 18:09 中央社／ 高雄17日電

高雄市社會局表示，近期接獲民眾來電，稱有人假冒市府人員藉核對申辦福利身分名義，企圖取得個資，提醒民眾若遇類似狀況，應洽社會局詢問或撥打「165」反詐騙專線以免受騙。

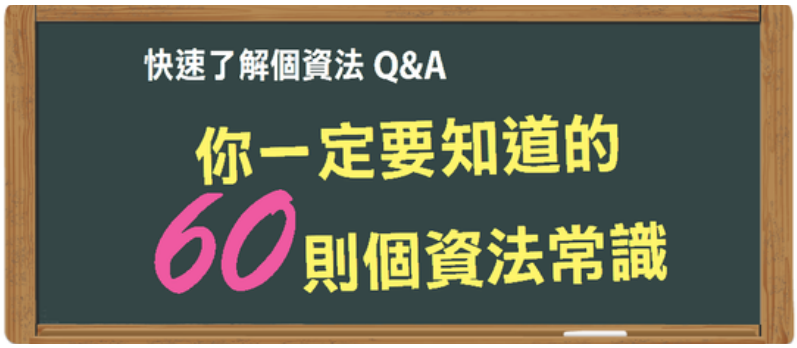
高雄市政府社會局今天發布新聞稿指出，近日接獲多起民眾來電及陳情，指有詐騙集團以社會局人員名義，欲協助申辦低（中低）收入戶補助，或告知有他人持民眾身分證明文件申辦社福補助要核對個人資料等狀況。

社會局提醒民眾留意，勿輕易洩漏個資以免受騙，若接獲來電顯示號碼「334-4885」，該電話為社會福利諮詢專線，僅有受話功能無法撥出，若接到來電顯示此號碼說明申辦福利補助需核對個資等即為詐騙電話。

社會局表示，各項社會福利申請需由民眾持相關證件洽戶籍地區公所或至社會局提出申辦，若委託他人辦理則需填妥委託書並攜帶委託人及受託人雙方身分證件。社會局及區公所不會主動派人協助津貼申辦，也不會透過電話取得申請人身分資料及帳戶資訊或要求簽署不明文件等。

社會局指出，若民眾遇到類似狀況，應提高警覺確認個人證件是否遺失，並洽詢區公所或高雄市政府電話「07-3368333」轉社會局詢問，或撥打「165」反詐騙專線、「110」報案，切勿將個人身分證明等相關資料交付不明人士，讓詐騙集團有機可乘。

## 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

**Q9 何謂個人資料蒐集？**

**A「蒐集」是指以任何方式取得個人資料，因此不論是以紙本方式記錄個人資料，或是透過網站的註冊系統蒐集，都算是在蒐集個人資料。而且即使是以非法手段蒐集個人資料，亦算是蒐集。**

文/iThome

# AI讓詐騙更猖狂！趨勢科技公布2025資安預測 中小企業恐成駭客首要目標

2024-12-16 16:51 聯合報／ 記者黃筱晴／即時報導

生成式AI應用在2024年的被大幅應用在各行各業，對網路趨勢敏感度極高的駭客也跟著轉型，更多的AI應用將催生出全新攻擊手段，駭客因應情勢變化調整攻擊目標，將形成更加詭譎難測的資安態勢。

趨勢科技今公布2025年資安年度預測報告，指出駭客將持續利用AI技術加速攻擊效率、擴大攻擊規模、產出更擬真的文字與影音內容進行AI詐騙，並尋找阻力最小、最容易取得的入侵途徑，如濫用合法工具、攻擊可公開存取的資料。此外，AI代理成為駭客覬覦的目標，AI系統漏洞可能將被用來誘騙AI執行有害或未經授權的動作甚至假冒身分，企業與個人皆需警戒任何AI可能帶來的資安風險。

趨勢科技台灣區總經理洪偉淦表示：「生成式AI的進步將讓駭客的攻擊更隱匿、高效，預期2025年，駭客將全力開發AI的應用範疇使網路犯罪更具毀滅性。面對不可逆的AI進程，全球資安風險和壓力勢必加劇，企業應化被動為主動，採用一套風險導向的資安方案做整體風險評估與管理；而作為AI世代的公民，人人皆需強化資安意識，以期能負責任並安全地使用AI。」

趨勢科技預期，利用AI持續發動新的社交工程詐騙將是駭客的發展重點之一，如運用Deepfake深偽技術讓社交工程詐騙更逼真、更個人化，只需利用個人公開的貼文來訓練LLM大型語言模型，就能模仿其寫作風格、知識及性格並針對目標對象精準攻擊，企業尤須留意變臉詐騙及假冒員工的AI變臉詐騙。而非蓄意暴露的生物辨識資訊、外流或遭人竊取的個人身分識別資訊，以及日益強大的AI功能，也讓KYC認證迴避服務（Bypass-KYC-as-a-service）近年也相當受地下市場歡迎，金融保險產業需對此謹慎防範。

另一方面，企業為提升營運效率所頻繁部署的AI代理系統將成為駭客更具吸引力的目標。駭客可能挾持AI代理或藉由發掘AI系統的漏洞，誘使其執行未經授權或有害的動作，例如處理惡意指令、協助外洩敏感資料，或生成假數位身分欺騙AI系統。趨勢科技建議，企業必須更加著重漏洞與攻擊面管理，並善用基礎資料情報，同時也需留意AI軟體供應鏈攻擊，避免AI代理或供應商出現缺失而連帶受害。

趨勢科技觀察，勒索病毒集團經營模式改變，他們減少對釣魚郵件的依賴，轉而利用被竊取的帳戶資料直接進入受害者系統，並頻繁地結合惡意廣告進行資訊竊取，將來自企業網路的數據應用於後續的勒索行動。除此之外，根據趨勢科技台灣的資安事故應變服務案件統計，2024年目標式勒索資安事故有將近9成來自中小企業，原因是網路犯罪服務CaaS的興起，也讓勒索病毒策略轉型，瞄準更容易下手的中小企業，恐將持續成為駭客攻擊的目標。

隨著國際政治局勢、地緣政治的變化，國家級駭客集團如Lazarus、Turla和 Pawn Storm等，預計在2025年將繼續活躍並加大攻擊力度，並針對那些與其理念相牴觸的組織發動攻擊。這些駭客集團的目標依然集中在外交資訊、軍事技術及其供應鏈。趨勢科技提醒，企業組織必須預先建立強健的防禦，認知自身在供應鏈中所扮演的角色，並採取積極的風險管理策略來保護關鍵基礎設施與資訊。

2025年，AI加劇了傳統攻擊：產出更逼真的假訊息與更客製的網路釣魚強化APT攻擊、生成惡意程式碼散播惡意程式或瞄準AI平台/工具來發動勒索攻擊；同時助長新型態攻擊手法：利用AI幻覺進行攻擊、利用AI代理或AI漏洞製造資料外洩、從事未經授權惡意活動等問題，網路犯罪更難以防範。