114年3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

一通電話AI仿聲國防部長！竟讓富商被詐3000萬 詐騙手法曝光

三立新聞網
2025年2月11日 週二 上午8:47
國際中心／施郁韻報導

▲有詐騙份子假冒義大利國防部長的聲音，有富商上當匯了百萬歐元。（示意圖／翻攝自Pixabay）

人工智慧（AI）迅速發展，如今卻有詐騙集團利用AI模擬語音，騙取不法現金。有詐騙份子假冒義大利國防部長的聲音，向義大利多名富商聲稱「我國記者在中東被綁架」，需要籌措贖金，亂槍打鳥下，至少1位富商上當，匯了百萬歐元（約3385萬元新台幣）。

據《金融時報》報導，警方表示，詐騙份子利用AI模擬出國防部長克羅塞托（Guido Crosetto），再假冒其幕僚致電給富豪們，模仿克羅塞托的聲音，稱總理梅洛尼（Giorgia Meloni）政府需要幫忙解救在中東被綁架的義大利記者。

接到來電的富商不只一位，包括輪胎大廠倍耐力（Pirelli）董事長普洛維拉（Marco Tronchetti Provera）、時尚設計師亞曼尼（Giorgio Armani）、普拉達（Prada）董事長貝特里（Patrizio Bertelli），甚至還有義大利軍火商貝瑞塔（Beretta）家族。不少人接到電話驚覺不對勁，仍有一人匯款了100萬歐元到海外銀行帳戶。目前已有3名米蘭的富商報案，其中一人正是受害者本人。

克羅塞托日前也在社群平台上呼籲，「有嚴重詐騙正在發生」，提醒大家保持警覺，希望不要看到有人上當。

病歷資料打不開！馬偕醫院遭駭客勒索 資安專家進駐搶救

（本刊資料照）

鏡週刊/謝文哲2025年2月11日 週二 下午9:46

台灣首度有醫院遭受勒索軟體大規模攻擊，衛福部今（11）日證實，北部醫學中心馬偕醫院的門診與急診系統9日開始陸續遭受駭客攻擊，導致超過500台電腦當機，病歷資料被加密無法開啟。由於駭客揚言下午5點將進行第二波攻擊，衛福部緊急啟動應變機制，聯手數位發展部資通安全署派遣專家進駐馬偕醫院，全力防堵。

馬偕醫院於2月9日發現系統異常，立即啟動資安緊急應變作業並通報衛福部資安聯防平台（H-ISAC），同時報請法務部調查局台北市調查處進行調查。此次攻擊手法為駭客利用勒索軟體加密醫院內部病患資料，導致醫療人員無法存取病歷，嚴重影響診療作業。

初步調查顯示，攻擊影響範圍主要集中在馬偕醫院台北與淡水院區的急診室，所幸醫院在發現異常後迅速應變，當日已完成系統修復，醫療作業已恢復正常，目前尚未發現病人個資外洩。

針對此次資安事件，衛福部資訊處長李建璋表示，這是台灣首次發生醫院遭駭客大規模攻擊的事件，衛福部已經採取三項應變措施。首先，衛福部立即聯繫數位發展部資通安全署，並請該署派遣資安專家進駐馬偕醫院，協助防禦可能發生的第二波攻擊。這是台灣醫院首次有資安專家直接駐點應對駭客攻擊。

其次，衛福部已迅速公告攻擊病毒碼，通知全國醫療機構提升資安防護，並協調國內資安廠商更新防毒軟體，以攔截類似攻擊。此外，衛福部也已加強醫院的主動防禦能力，針對系統老舊且資安防護較弱的醫院，提供臨時免費的主動防禦方案。

據李建璋表示，這次駭客攻擊疑似來自過去俄羅斯等地，但真正的意圖尚不清楚。駭客揚言若未滿足其要求，將在今日下午5點進行第二波攻擊，為此，政府與資安單位高度戒備，全力確保醫院系統安全。

馬偕醫院則強調，醫療行為不得受到威脅，並嚴厲譴責任何非法攻擊行為，未來將持續強化資安防護，確保醫療環境安全。

DeepSeek 爆紅引發山寨域名潮，逾 2650 個釣魚網站伺機竊取個資

T客邦/KKJ發表於 2025年2月08日 10:30
隨著中國 AI 新創公司 DeepSeek的 AI 模型在全球爆紅，網路上湧現大量仿冒 DeepSeek 品牌的山寨網站，數量已超過 2650 個，且持續快速增加中。這些釣魚網站正伺機透過多種詐騙手法，誘騙使用者上當，竊取個人資訊、散播惡意軟體，甚至進行金融詐欺，使用者務必提高警覺。

AI 新星 DeepSeek 崛起，山寨網站如影隨形
DeepSeek 是一家中國人工智慧新創公司，近期因推出效能直逼 OpenAI GPT-4 的大型語言模型而聲名大噪，吸引全球科技界的目光。然而，如同過往爆紅的科技產品如 ChatGPT 等，DeepSeek 的快速竄紅也引來了網路犯罪集團的覬覦。不法份子看準 DeepSeek 的高人氣，大量註冊與 DeepSeek 品牌名稱相似的域名，架設仿冒網站，企圖魚目混珠，誘騙使用者點擊造訪。根據資安公司奇安信 XLab 實驗室的最新報告指出，自 2024 年 12 月 1 日至 2025 年 2 月 3 日期間，已偵測到高達 2650 個仿冒 DeepSeek 的網站域名。從域名註冊趨勢分析可見，大規模的仿冒域名註冊潮始於 2025 年 1 月 26 日，並在 1 月 28 日達到高峰。儘管後續成長幅度稍緩，但仿冒域名數量仍在持續攀升，顯示此一網路詐騙現象已形成規模，且有擴大蔓延之勢。

釣魚詐騙手法翻新，使用者個資與財產面臨威脅
根據奇安信 XLab 對當前 DeepSeek 仿冒域名解析結果的分析，這些山寨網站的主要用途可歸納為以下幾類：

- 釣魚詐欺： 這是最常見的仿冒網站用途。不法份子利用與 DeepSeek 官方網站極為相似的域名和網頁設計，企圖誤導使用者，誘騙使用者輸入帳號密碼等登入憑證，藉此竊取使用者個資。部分釣魚網站更會進一步誘騙使用者購買虛擬資產或訂閱付費服務，直接進行金融詐騙。
- 惡意軟體散播： 部分仿冒網站暗藏惡意程式碼，使用者一旦不慎點擊連結或下載檔案，電腦或手機裝置可能因此感染病毒或木馬程式，導致個資外洩、裝置效能降低，甚至成為駭客遠端操控的「殭屍電腦」。
- 域名搶註與流量導引： 另有部分仿冒域名被註冊後，並未立即用於釣魚詐騙，而是被不法份子囤積，企圖伺機高價出售，或作為未來其他網路詐騙行動的跳板。此外，部分仿冒域名也可能被用於惡意流量導引，將使用者導向廣告網站或惡意網站，藉此牟取不當利益。
-

值得注意的是，奇安信 XLab 的分析報告指出，這些仿冒 DeepSeek 的域名，有高達六成解析 IP 位址位於美國，其餘則分散於新加坡、德國、立陶宛、俄羅斯和中國等地。仿冒域名呈現全球化分佈的特點，意味著使用者可能面臨來自世界各地不同類型、手法更加複雜多樣的網路攻擊，潛在安全威脅不容小覷。

防範山寨網站釣魚詐騙，使用者應提高警覺
奇安信集團針對此波 DeepSeek 山寨域名潮發出安全預警，呼籲廣大網路使用者提高警覺，切勿輕信來路不明的網站連結。奇安信建議使用者應採取以下防範措施，認明官方網站： 瀏覽 DeepSeek 相關資訊時，務必認明官方網站域名，避免點擊或瀏覽域名可疑的山寨網站。DeepSeek 官方網站網址為deepseek.com。

DeepSeek 山寨域名事件，再次凸顯了科技爆紅現象背後潛藏的網路安全風險。每當熱門科技產品或技術問世，往往伴隨著各種仿冒、詐騙亂象。不法份子總是能迅速搭上熱潮，利用使用者對新科技的好奇心與資訊落差，設計出各式各樣的詐騙陷阱。

每月一常識

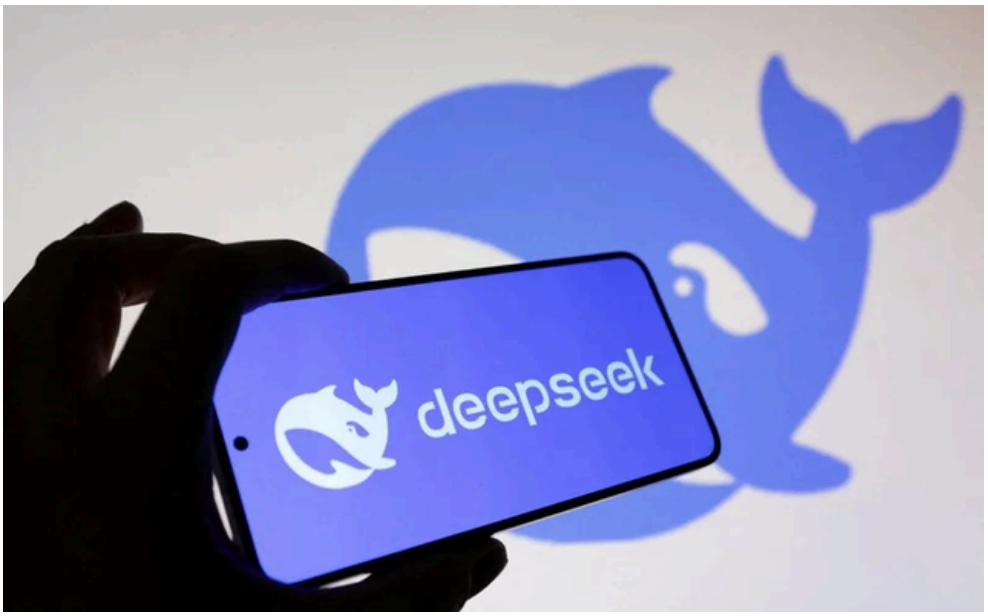
新版個人資料保護法與過去有很大的不同，新法進一步擴大了個人資料的保護範圍，並且讓所有產業一體適用；新法甚至首度增加團體訴訟，而且違法的罰則也加重了，企業老闆要負更大的責任。接下來，我們以60個Q&A，快速帶你認識新版個人資料保護法

Q11 何謂個人資料利用？

A 「利用」，是指將蒐集的個人資料做「處理」以外的使用，例如將蒐集的個資做為行銷、統計調查等等。

文/iThome

數發部：未禁止民間使用DeepSeek 僅公務機關全面禁用



DeepSeek。（路透）

2025-02-20 15:51 經濟日報／ 記者余弦妙／即時報導

基於防範公務機關資安風險等考量，行政院已宣布公務機關立即全面禁用DeepSeek AI服務，包含雲端服務、APP及地端下載等方式，公務機關皆不得使用。惟考量適法性與可行性等影響因素，目前未進一步限制業者提供民眾下載及使用，數發部並提醒使用時應注意可能之資安及隱私風險。

數發部表示，有關中國「杭州深度求索人工智慧基礎技術研究有限公司」所發布DeepSeek AI服務產品，觀察目前世界各國採取之應對趨勢，包括民間與公務機關全面禁止及公務機關全面或部分禁止使用，其中多數又以限制公務機關使用為主要應對措施。目前有2個國家限制民間使用特定服務類型。

數發部強調，台灣是法治國家，政府機關依法行政是法治國家的基本原則，未來是否進一步限制業者提供民眾下載及使用，將視有無違反個資法等相關法規規定 。政府將持續關注DeepSeek議題，並提醒民眾要注意相關風險。