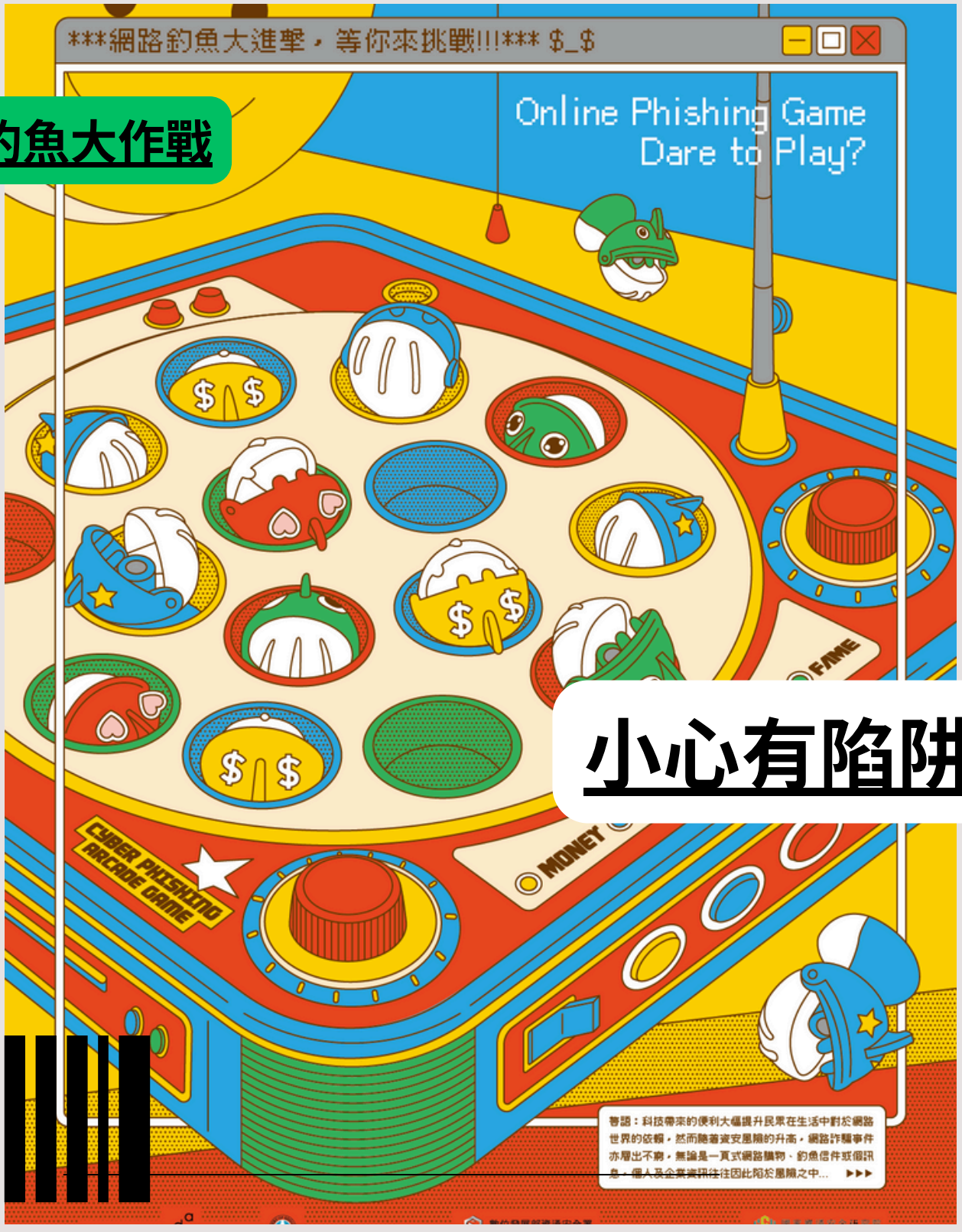
林業及自然保育署
臺東分署

公務機密
資訊安全維護

網路釣魚大作戰



小心有陷阱

公務機密 資訊安全維護

目錄

【資安週報】0707~0711，駭客打造上萬個投資詐騙網站，Deepfake偽冒政府官員

iThome/文/羅正漢|2025-07-14發表

在2025年7月第二星期的資安新聞，涉及身分偽冒的詐騙、Deepfake事件，是我們首要關注的焦點，顯示攻擊者不僅用好康、冒名與假消息來騙不懂求證的人，加上Deepfake門檻變低，因此，越來越多攻擊者採用語音網釣加上AI語音偽冒的手段，讓受害者明知陌生電話或帳號來聯繫，也可能因為聲音很像誤信而忽略求證，下列兩起事件，是我們認為這個星期最重大的資安危機。

（一）橫行全球的網路投資詐騙活動BaitTrap，被資安業者CM360揭露，駭客架設逾1.7萬個誘餌新聞網站，中東有1萬個最多，亞太地區3,400個次之，不僅偽裝成知名媒體散布假消息，並假借知名公眾人物或銀行名義來建立信任，宣稱意外發現透過加密貨幣致富秘密方法來進行投資詐騙。

（二）AI偽冒政府官員的事件正引發全球關注。在美國，繼5月白宮幕僚長Susie Wiles遭偽冒後，美國國務院7月也警告，有人偽冒美國國務卿盧比奧（Marco Rubio）發送文字與Signal語音訊息。國務院警告，歹徒可能企圖透過AI生成的文字與語音操控特定人士，目的在於取得資訊或存取帳號。

此外，駭客也持續利用不同社交工程手法來欺騙上網的大眾，散布釣魚網站、釣魚郵件，或是散布假瀏覽器套件，近期有3起重要事件揭露，意圖讓目標上當，導致信用卡資訊被竊或電腦被安裝惡意程式。

●墨西哥記者發現當地出現各種仿冒熱門品牌的釣魚網站，有逾700個，網路情報平臺Silent Push循線追查，揭露是中國駭客所為，封鎖後仍有數千個釣魚網站活躍，當中多是以假亂真的網址，誘拐消費者購買並輸入信用卡資訊。

●18款惡意瀏覽器延伸套件被下載230萬次，資安業者Koi Security揭露相關攻擊行動RedDirection，指出這些偽冒的套件類型包括：Emoji符號鍵盤、天氣預報、影片速度控制器、音量放大、YouTube解鎖工具等。

●中國駭客Mustang Panda持續鎖定圖博人士從事攻擊，IBM X-Force指出該組織寄送釣魚郵件，利用6月圖博大會、達賴喇嘛新書等時事議題作為誘餌，意圖引誘開啟郵件中的雲端檔案連結，下載包含惡意的ZIP或RAR壓縮檔。

在資安威脅事件與態勢方面，這星期國內有一起上市公司資安事件的揭露，還有四大議題值得特別留意，涵蓋OT安全、紅隊演練工具遭濫用，以及Linux、macOS遭鎖定的態勢。

●專注無線通訊模組及數位影像處理方案的海華科技，屬於和碩集團的成員，他們發布資安事件重訊，揭露資訊系統遭受駭客攻擊。

●挪威媒體揭露今年4月有駭客入侵Lake Risevatnet水壩控制系統，閘門開啟數小時無法關閉，而原因是弱密碼釀禍，幸好當時河床足以因應龐大水流。

●出現駭客濫用新的資安演練工具從事攻擊的狀況，Elastic發現駭客濫用迴避偵測框架Shellter來散布竊資軟體，企圖迴避防毒軟體與EDR偵測。

●韓國資安公司AhnLab揭露，Linux伺服器因密碼強度不足或管理疏忽，逐漸成為駭客鎖定目標。

●近期針對macOS用戶的竊資軟體接連被揭露，包括Atomic Stealer（AMOS Stealer）、北韓駭客打造的NimDoor，以及先前揭露的Odyssey Stealer，突顯攻擊者鎖定macOS攻擊的狀況是越來越多。

在漏洞消息方面，這一星期微軟、Adobe、SAP等多家廠商發布7月例行更新，需要大家儘快修補與因應，還有4個老舊已知漏洞遭利用的消息需要留意，已被美國CISA列入已知漏洞利用清單（KEV）。

其中1起漏洞利用值得電信ISP業者或大型網路業者重視，是開源TCP/IP路由軟體Multi-Router Looking Glass（MRLG）的漏洞CVE-2014-3931，駭客仍鎖定這個10年前的漏洞來利用。其他還包括：PHP開源郵件寄送函式庫PHPMailer的漏洞CVE-2016-10033，Ruby開源Web應用框架Ruby on Rails的漏洞CVE-2019-5418，以及整合式企業郵件與協作平臺ZCS的漏洞CVE-2019-9621。

還有3個漏洞需要密切關注，因為已發現駭客掃描的跡象，可能是攻擊前兆，這些漏洞是3月Tomcat修補的RCE漏洞（CVE-2025-24813），以及同樣3月Camel修補的RCE漏洞（CVE-2025-27636、CVE-2025-29891）

至於資安防禦上，有兩起重要消息，一是美國司法部在義大利米蘭逮捕一名中國駭客，此人涉嫌於2020年2月至2021年6月間，受中國政府指使竊取COVID-19疫苗研究成果；另一是臺灣資安業者奧義智慧切入AI Guardrails領域，並攜手AI業者APMIC推出AI模型XecGuard，以及Safety LLM安全評測服務。預計第三季將推出閘道端的AI防火牆產品。

資安時事案例

HR大廠Workday CRM系統資料外洩

圖片來源: Workday

iThome/文/林妍溱|2025-08-19發表

HR雲端平臺大廠Workday上周公告，近日公司使用的客戶關係管理（CRM）系統遭駭客存取，導致資料外洩。

Workday說明事件起於員工遭社交工程攻擊。駭客冒充IT或HR部門人員利用文字簡訊或電話聯繫員工，誘使他們提供帳號密碼或是個人資訊。之後該公司發現駭客成功存取Workday的第三方CRM系統。他們很快就終止了駭客活動，也新增防護措施。

但Workday說，沒有跡象顯示客戶租戶或是儲存的資料遭駭客取得。

根據Workday網站，該公司全球客戶超過1.1萬家，涵蓋全球7000萬使用者。

Bleeping Computer看到Workday發送給受影響客戶的信件，顯示事件發生在8月6日。

最終駭客存取了Workday部份CRM系統資料。該公司強調外洩資料主要是常見的企業聯絡資訊，像是姓名、電子郵件信箱、電話號碼。但該公司未透露被竊的是員工或客戶資料，也未說明受影響資料的幅度。廠商也呼籲用戶留意外洩資料可能導致社交工程詐騙攻擊。

Workday事件是近來多家知名企業客戶資料被駭客竊取後的最新一起。這些企業包含LV、香奈兒（Chanel）、安聯人壽、澳航、法航與荷航、以及Google與思科。其中除了Google坦承被存取的系統是Salesforce，其餘受害企業皆未說明。

Google將攻擊者命名為UNC6040，即業界稱的ShinyHunters。資安業者相信這組織已經和另一組織Scattered Spider合作或整併。他們利用手上的資料勒索受害用戶，有的則是企圖賣給其他團隊。上周有不明人士在暗網公開280萬筆安聯人壽的客戶及合作夥伴資料，以作為販售更大宗資料的樣本。

這封郵件千萬別點！他籲「小心個資被盜光」 一堆人差點中招

三立新聞網 的故事/生活中心／許智超報導/2025/8/8
詐騙手法層出不窮，讓人防不勝防，之前就有不法分子冒充財政部發送「雲端發票整合」詐騙郵件，謊稱「雲端發票載具」與信用卡綁定的載具不同，並誘使民眾點擊假網址並輸入信用卡資訊。近日，又有許多人收到「歸戶核對」信件，內容稱雲端發票中獎，但因無法正常驗證，要求點擊連結更新資料，藉機盜走個資。

原PO日前在Threads貼出截圖畫面，標題為「票務同步－電子雲端發票郵件」，內容指他在電商平台購物的發票已中獎，但由於載具信息核實有誤，中獎發票將無法正常驗證，請及時更新資料。

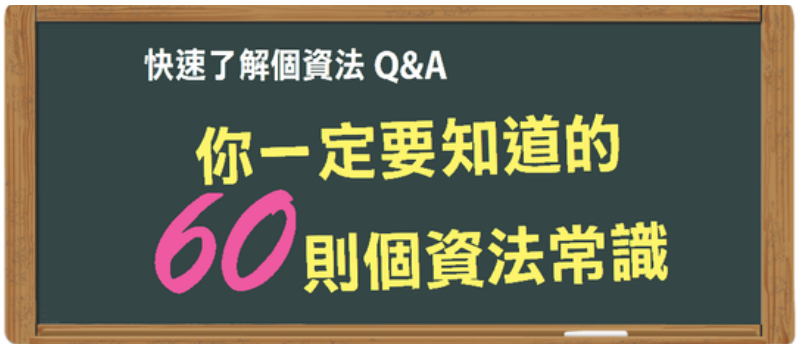
信件內容接著要求進行3步驟，首先點擊載具歸戶更新「頁面鏈接」，再來輸入手機號碼和驗證密碼，最後選擇「更新載具歸戶」並完成操作。原PO則發文呼籲「這是假的」，若大家有收到這種「信件」，不要點選裡面的連結，它是釣魚網站連結，個資可能因此被竊走。

貼文曝光後，網友也紛紛回應，「我看到覺得很怪，後來去電商查，明明就有匯入雲端發票」，還有人一看就知道是詐騙，「頁面鏈接露餡了」。另外，有網友透露，自己不慎點進連結，直到頁面要求輸入信用卡資料，就沒繼續填寫，立即撥打165反詐騙專線檢舉，而原PO也建議不要再繼續操作了。

財政部曾提醒，平台不會寄信要求輸入信用卡資訊，也呼籲當民眾收到來自「財政部電子發票整合服務平台」的電子郵件時，必須先確認信件來源是否合法，若發現郵件來自不明的電子郵件地址，或網址中包含可疑字符或簡體字，應立即刪除，避免上當受騙。

此外，民眾可以通過查詢官方網站、撥打官方熱線等方式，核實任何關於電子發票的疑問。財政部也會持續監控詐騙行為，並與相關單位合作，打擊這些不法行為，保護民眾的個人資訊安全。

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

Q17　若符合特定目的，就可以蒐集個人資料了嗎？

A　蒐集個人資料除了要有明確的目的，不得蒐集特種資料之外，還要符合以下事項，才可以合法蒐集個資。
企業必須符合其中一個項目：
1．法律明文規定。
2．與當事人有契約或類似契約之關係。
3．當事人自行公開或其他已合法公開之個人資料。
4．學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。
5．經當事人書面同意。
6．與公共利益有關。
7．個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。

文/iThome

學生要注意！專家揭露5大常見詐騙手法，租屋、打工、追劇都有陷阱

風傳媒/2025-08-18 12:58林彥呈

暑假邁入尾聲、新學期將至，學生們開始整理課業用品，準備迎接新生活，不論添購新用品、找租屋處、找資訊、學習、娛樂等，網路與學生生活形影不離。全球網路資安領導廠商趨勢科技彙整5大「詐騙陷阱題」，不肖份子經常透過假交易、假補助、假投資等手法鎖定學生族群，一旦遭遇駭客攻擊、勒索病毒或點進詐騙連結，將可能造成數位與財務資產「人財兩失」的窘境。

陷阱題一：小心「無卡分期」陷阱與假賣家手法

工欲善其事，必先利其器。開學前夕是汰舊換新3C產品的高峰期，過去曾有詐騙份子以「簽約立刻拿5000元佣金」為誘餌，誆稱協助代辦無卡分期，實則藉由不平等合約誘騙購買高價3C產品，導致學生背負龐大債務。如果簽約後無法證明其為詐欺共犯，即使未拿到商品也須付款，甚至可能被提告詐欺罪。

此外，詐騙集團也經常透過二手交易平台假冒為賣家，並以「付款錯誤」、「系統驗證」等話術發送惡意連結誘使消費者點擊，導致洩露個資或財損。

趨勢科技提醒，若欲購買電子產品、線上進修課程，都應透過合理正當管道。無論進行付款或提供個人資料時，也務必確認交易網站真偽，並核實交易方的身份。在選擇店家時也應特別注意其合約價格是否透明、條款是否清楚，以及對方是否具備實體營業據點，避免誤入詐騙陷阱。

陷阱題二：打工存錢想投資？小心誤入假投資陷阱

近期不少學生利用打工累積資金嘗試小額投資。然而，根據警政署165全民防騙網，假投資平台常透過社群投放廣告吸引被害人加入LINE投資群組，並提供假投資網站或App給被害人，要求受害者入金投資。當被害人要求提領獲利時，便會以各種理由拖延拒絕「出金」。

趨勢科技呼籲，投資應選擇金管會核准的合法金融機構進行操作，切勿輕信網路廣告推薦的投資資訊，以免誤入詐團圈套。

此外，建議運用與刑事警察局165合作的專業資安工具PC-cillin，透過業界領先的AI防詐技術與龐大資料庫即時封鎖詐騙連結，守護使用者的財務與個資安全。

陷阱題三：租屋補助也能詐？學生在外租房須謹慎查證

外地學子通常在開學前尋覓租屋處，是否具備租屋補助也是學生選擇租屋考量的重點之一。近期已有案例是不法分子假冒政府單位致電給受害者，謊稱受害者的證件已遭他人冒用申請「租屋補助」，並涉嫌詐騙案件，進而誘騙其提供身份證、銀行帳戶等敏感資訊。

趨勢科技提醒，政府機關不會主動致電要求個資或匯款，如接獲不明來電，應立即掛斷並主動致電官方查證。若需申辦租屋補助，也應直接前往政府官方網站窗口。

陷阱題四：線上遊戲中的「隊友」可能是詐騙集團

線上遊戲常為學生課後休閒娛樂，然不肖份子看準網路遊戲平台難以監管的特性，透過私訊、語音方式騙取信任，受害者易在無防備情況下透露遊戲帳密、個資或金錢交易，嚴重者更可能捲入詐騙犯罪鏈，淪為共犯。
趨勢科技提醒，駭客常透過遊戲平台聲稱可販售虛擬貨幣或提供優惠道具，實則夾帶惡意連結以達到竊取個資等非法目的。學生在享受遊戲娛樂的同時，應避免點擊來路不明的支付連結，更不要輕易交付個人機敏資訊。

陷阱題五：上網追劇看影片也有陷阱？留意免費影音網站暗藏惡意連結

許多學生習慣透過免費影音網站追劇，隨著串流平台盛行，網路上也充斥大量來路不明、未經授權的免費影音網站。這類平台表面上提供免費內容，實際上卻暗藏風險，不僅可能夾帶釣魚連結或色情廣告，還常透過假登入頁面或彈跳視窗，誘導使用者誤點。若為了一時搶快而忽略查證來源，極有可能誤觸惡意連結，導致裝置感染病毒或個資遭到竊取。

趨勢科技提醒，免費影片觀看連結可能產生的風險在公共Wi-Fi環境下尤為嚴重，駭客可趁機攔截資料，進而竊取帳號密碼或入侵裝置。建議學生在外追劇時，不僅應選擇合法平台，也可搭配使用PC-cillin所搭載的安全VPN功能，能有效保障上網連線安全，安心追劇，避免落入陷阱。