

個案研討：假冒官網詐騙



以下為數則新聞報導，請就此事件加以評論：

- 詐騙手法再度翻新！本月 10 日起，詐騙集團寄送一卡通 Email 或簡訊，並以更新會員資料、消費回饋等理由，誘騙民眾點選假頁面後，再輸入姓名、身分證字號、一卡通密碼及電話號碼等資訊，再進行盜刷行為；刑事警察局統計，短短 10 天已累積 173 起案件，財物損失近 900 萬元，近日詐騙集團已改用「悠遊付」行騙，民眾切勿受騙上當。

刑事局表示，詐騙集團為了仿冒一卡通官網，遂在網址中放進 ipass 等關鍵字，藉以混淆民眾視聽，但假網址前後皆為亂數字母，與官網「<https://www.i-pass.com.tw/>」的網址並不相同，不過詐騙集團以消費回饋、帳號功能調整或更新會員資料等理由行騙，導致許多民眾被騙走血汗錢，光是本月 10 日到 20 日，至少就有 173 起案件，詐騙總額高達 872 萬元，其中 1 人被查出跨境交易 21 筆，總共盜刷 18 萬 3572 元。

刑事局表示，雖然民眾報案的假網站已被下架，但警方分析資料後發現，從本月 21 日開始，詐騙集團改以「悠遊付」行騙，同樣寄送 Email 或釣魚簡訊，同樣謊稱更新帳戶、儲值回饋等理由，要求民眾填寫個人資料、密碼、手機號碼及 OTP 驗證碼等資料，目前盜刷案件陸續發生中。(2025/10/23 三立新聞網)

- 詐騙手段層出不窮！近日有網友在 Threads 發文表示，收到假冒財政部的電子郵件，內容是要求用戶補全資訊，進行身分認證、更新載具綁

定，輸入信用卡卡號、姓名等資料。對此，財政部表示這類郵件都是詐騙，「平台不會寄 Email 通知載具異常、更不會要求輸入信用卡資訊」。（2025/10/18 鏡報）

傳統觀點

- 刑事局呼籲，公司企業如有建置蒐集個人資料之伺服器，應強化資安、提升防火牆防毒功能，藉以防止客戶資料外洩，造成民眾財損及恐慌；刑事局提醒，民眾接收 Email 或簡訊，應仔細辨明網址，相關操作應至官網查證真偽，而且資料更新與購物消費無關，不應輸入 OTP 驗證碼，如被要求輸入 OTP 驗證碼，皆須留心信用卡遭盜刷。
- 財政部表示，最近出現假冒「財政部電子發票整合服務平台」的電子郵件，以「您在 Yahoo 奇摩購物中心消費所開立的雲端發票已榮幸中獎」為由，謊稱載具歸戶資訊尚需驗證，誘騙民眾點擊信中的連結進入假網頁、輸入個資，這實際上是詐騙網頁。
- 財政部強調，平台的信箱及網址結尾都是政府專用「.gov.tw」，且不會寄 Email 通知載具異常，更不會要求輸入信用卡資訊。財政部呼籲，「不明網址不點擊、信用卡等個資不輸入，如有接獲類似訊息，立即撥打 165 反詐騙專線或平台客服詢問」。

管理觀點

台灣的詐騙案件非常猖獗，以上只是一種新的詐騙手法。以本個案來說，針對這些詐騙事件，刑事局和財政部呼籲的防詐方法，同學們認為會有用嗎？效果如何？你認為有多少人會注意收到的訊息是來自什麼網址？你能辨別政府或機構官網的網址、網頁的首頁設計嗎？如果看得出是假網頁還會上當嗎？為什麼大家會相信「政府機關」發送的訊息？為什麼民眾會相信政府機關說的：還要再驗證、資料要更新，還要求輸入個資、密碼……？為什麼對方要冒用警察、調查局、檢查官、法院、國稅局、海關……等身分，這些身分為什麼會令民眾感到害怕？再加上「偵查不公開」、「代管帳戶」……等等，為什麼年長者更容易相信並受騙？要解決問題，這些才是會上當的根本原因，不是嗎？

平台有客服嗎？連絡方便嗎？打了有用嗎？有多少%是因民眾打了 165 反詐騙專線才破案的？165 專線為什麼不想辦法主動出擊，等著別人來檢舉？平

台沒辦法發現自己被利用了嗎？這些用來詐騙的網址訊息流動量和方式會有什麼共同特性嗎？防範和清查虛假網頁是誰的責任？在詐騙案件中，平台有責任嗎？為什麼好像反詐完全沒有他們的事？當民眾發現或收到可疑訊息時，有管道可立即轉知平台嗎？政府可以強制要求每個平台都要提供設立反詐據點，隨時接受並即時處理民眾轉來的可疑訊息嗎？……

還有，為什麼詐騙分子能有受害者的個資？能將民眾在金融機構的存款轉移出去？帳戶主人知道嗎？請不要推托說是符合內部規定，這不是明擺著有漏洞嗎？就算是帳戶主(本)人自己的操作，難道不能規定某些特別的異動，一定要本人攜帶證件，親自到分行辦理嗎？為什麼政府本是為了「反洗錢」規定的措施，反而可以因而破獲詐騙案？……

目前的防詐措施重點好像重點都是放在受騙者身上，是不是這正是效果不彰的原因所在？我們要知道，有警覺心的精明人當然是不會受騙的，容易受騙的都是那些不熟悉政府作業或各機構網站運作方式的人，他們不會查詢網址、不會懷疑、不知道平台上竟會有這麼多假網頁、分不出機構名稱或網站首頁上的些許差異、不知道怎麼查證真假、自己貪便宜或貪方便、沒有年輕人可以問……，難怪打詐效果會不彰。我們為什麼不改變矛頭，從要求平台上的防詐設計、大數據分析、實名管制註冊網址、讓有疑問的民眾更方便的舉報問題訊息、重罰詐騙犯……來著手？思考為什麼民眾會相信詐騙分子冒用的機構、冒用的名義、冒用的執行方式……？個資是怎麼流出的？為什麼詐騙犯這麼容易得手？為什麼不在乎被抓一犯再犯？…這些難道不是打詐的防堵重點嗎？

同學們，你收到過可疑的詐騙資訊嗎？你知道什麼詐騙的手法或案例嗎？對於防詐你還有什麼點子或補充？請提出分享討論。