

飄洋過海來騙你

導論

談到「網路詐騙」，許多人仍停留在早期那種亂槍打鳥的廣告信、中獎簡訊或一頁式購物網站。然而，時至今日，詐騙集團的組織與運作規模早已高度專業化、工業化，甚至跨國分工，形成成熟產業鏈。過去的網路詐騙多屬「非特定對象、一次性接觸、以靜態圖文為主」的模式，往往在初次接觸時便直接引導受害者前往不明網站，要求提供個資或金錢；隨著民眾警覺性提升，這類手法的成功率已大不如前。當前詐騙則轉向「鎖定特定對象、長期互動經營、結合訊息與影音的社交工程」策略，透過持續接觸建立信任關係，待對方卸下心防後，再誘導其提供敏感資訊或資金，如圖 1 所示。

圖 1 網路詐騙的進化



根據內政部警政署「165 打詐儀表板」的統計，「假投資詐騙」常態性地佔據財損金額的第一位，幾乎每天都有超過一億臺幣被騙取，而「網路購物詐騙」則是受理件數的第一位，每天都有上百起的網購詐騙案件；高科技詐騙手法原本是耗費大量時間與人力的，但是在詐騙集團規模擴大，以及 AI 技術的加持下，變得可行而且真假難辨，成功率也大大地提高了，故社會大眾有重新認識現代網路詐騙的必要。

一、假投資詐騙 (財損最高)

典型的假投資詐騙過程中會有圖 2 的四部曲，首先的第一階段，歹徒會在各大社群媒體平臺投放廣告，例如 Facebook 和 YouTube，甚至假冒政商名人建立粉絲專頁，假意分享投資筆記或致富心得，唯一要求是加入特定的通訊群組或留下聯絡方式，以此作為誘餌吸引受害者，此時因為還沒有實際付出金錢，大多參與者只是抱著「看看就好」的心態，警戒心不高。

第二階段是要建立參與者的信任，卸下其心防，於是群組中許多被稱為「托」的暗樁，會在群組中一邊噓寒問暖，一邊感謝群組中的「老師」帶他們賺了錢，而這些「托」甚至可能根本不是真人而是 AI 聊天機器人，一段時日以後，當參與者心癢能耐，就對他提出「投資方案」，慫恿他投入真金白銀。

圖 2 假投資詐騙四部曲



當假投資群組的參與者小額投資之後，就進入第三階段，詐騙集團會假造各種報表騙他已經獲利，也可能會真的讓他領出部分款項，讓他在食髓知味之後決定投入大筆金額。最後是第四階段，詐騙集團收網，假稱參與者的帳戶出了問題、遭到凍結，需要追繳保證金或手續費，最後詐騙帶走所有金錢後人間蒸發，參與者此刻才發現自己受騙。甚至還有更過份者，此時再冒出另一組詐騙者，自稱是律師或有力人士，宣稱能夠追回款項，但是要求受害人先支付律師費或保證金，實則再騙一筆錢。

二、網路購物與拍賣詐騙(次數最多)

如果說假投資詐騙是精心設計的騙局，那麼網路購物與拍賣詐騙就是以簡化騙局衝數量的小額詐騙了。如圖 3 所示，在網購或網拍隔空交換貨物與金錢的過程中，詐騙集團透過偽造各種假商品、假買家、假賣家、甚至是假交易來騙取金錢或貨物，例如隨機寄送「幽靈包裹」並利用「貨到付款」機制以「假商品」騙取金錢；設立俗稱「一頁式網站」的網路特賣會以冒充「假賣家」來銷售劣質仿冒品；也有詐騙集團冒充「假買家」宣稱無法下單，向賣家要求「金流驗證」事實上是導向歹徒自製的假驗證網址，騙得賣家的金融資訊與金錢。

除此之外還有歷久不衰的「解除分期付款」詐騙，歹徒以某種方式取得網購買家的購物紀錄之後，假冒金融或客服人員致電買家，宣稱「分期設定出了問題」要求買家在ATM 或網路銀行上進行指定操作以解除設定，實則是將金錢轉帳給歹徒。

利用了一般人「眼見為憑」的心理，詐騙集團在進行各種手法的過程中，經常會利用深偽技術(deepfake)假冒名人代言商品、假冒親人要求匯款、或是假冒帥哥美女跟受害者談起網路戀愛，最後仍然是試圖誘騙對方拿出金錢投資，由於科技的進步，現在 AI 換臉的即時視訊破綻已經越來越少，除了注意可能的畫面或聲音破綻外，更重要的是無論是跟誰視訊，只要對方「急需用錢」就應該懷疑，此時可以跟對方核對一些通關密碼或私人問題，或是以其他方式聯繫對方查證、例如直接撥打對方的手機號碼，千萬不要「見到本人」就信以為真。

既然網路詐騙如此的猖獗，政府也拿出了一些相應的防詐措施，根據《詐欺犯罪危害防制條例》的源頭打擊措施，網路廣告平臺應該將內容標註為「廣告」並充分地揭露刊播者與出資者，如果內容包含 AI 產物也應該註明，當平臺上的內容或帳號涉及詐欺

的時候，平臺業者應該在司法警察機關或相關的政府主管機關的要求之下，在期限內將平臺移除，此外，無論平臺為國內或國外業者，均應在臺灣設有法律聯絡窗口，配合臺灣政府機構索要資料與追查過程；目前在臺灣營運的絕大部分網路社群與廣告平臺都已經配合此法被納管，包括 Google、LINE、Meta、TikTok，但仍有一些境外的平臺持續拒絕配合，例如小紅書，雖然在其平臺上已經發生大量的在臺詐騙案件，但是該平臺仍然持續忽略臺灣當局的要求，不設立代理人，聯繫也已讀不回，於是臺灣政府依法停止解析與限制接取小紅書的網址。像這樣不配合防詐的境外平臺，一旦發生了詐騙案件，受害者是完全求助無門的，使用者要謹慎考慮使用。

除此之外，根據《洗錢防制法》，金融機構任何國內外的匯款都應該確認客戶真實身分並且保存交易紀錄，此外若有大額交易應主動向法務部調查局申報，這些規定顯然地阻礙了詐騙集團收取金錢的管道，所以歹徒通常會安排車手直接向受害人搬取現金，或是用盡各種話術，促使受害人透過加密貨幣進行投資或付款，例如謊稱「使用加密貨幣進行交易在海外是蔚為風行的」，所以在網路上任何交易或投資場合只要提及「加密貨幣」，你都應該立刻升起警戒心。

五、反網路詐騙的「三不一要」原則

無論男女老幼都想要悠遊網海而不受騙，LINE 官方建議了「三不一要」原則，如圖 4 所示，當你遇到如前所述的網路交友、假冒客服、誘使你投資的疑似詐騙行為的時候，務必謹記「不輕信」對方所述的事情、「不轉帳」付出金錢或個人資料、「不點連結」直接進入對方提供的網頁而是循官方管道登入帳號或查證，高度懷疑或確定對方是詐騙行為的時候「要檢舉」或查證，可以播打「165 反詐騙專線」也可以利用「LINE 訊息查證官網」確認。

圖 4 LINE 官方建議的「三不一要」原則



在網路文章或通訊內容當中一旦出現「臨時急需用錢」、「保證高獲利」、「自稱客服人員」、「要求匯款」等等，尤其是涉及到「加密貨幣(虛擬貨幣)」的時候，就要立刻警覺到這些都是網路內容中常見的「詐騙關鍵字」，務必要查證再查證、小心再小心，千萬別讓那些飄洋過海來騙你的歹徒得逞。

相關報導

1. 2500 萬積蓄全騙光！最新詐騙手法「老師上當 7 次都沒發現」，傾家蕩產連房子也被抵押。(2025，12 月 4 日)。風傳媒。<https://www.storm.mg/lifestyle/11085500>
2. 臺積電澄清張忠謀等無經營公開社群媒體 大眾勿上當。(2025，6 月 2 日)。聯合新聞網。<https://udn.com/news/story/7240/8779693>
3. AI 詐騙成全球主流！趨勢科技揭消費者五大詐騙新趨勢！(2026，1 月 13 日)。趨勢科技。https://www.trendmicro.com/zh_tw/about/newsroom/press-releases/2026/2026-01-13.html
4. 爆紅健康頻道 20 萬粉絲！全是 AI 醫師、假資訊吸粉。(2025，11 月 19 日)。東森新聞。<https://news.ebc.net.tw/news/living/522785>
5. 詐騙集團如何使用深偽技術(Deepfake)變臉？調查官教您破解騙術。(2024，8 月 7 日)。中區養護工程分局。https://thbu2.thb.gov.tw/News_Video_Content.aspx?n=4691&s=252520
6. 【每日揭詐】甜蜜互稱公婆 網戀詐欺師藉口「認領費」金融卡、SIM 卡全騙走。(2024，8 月 7 日)。太報。<https://www.taisounds.com/news/content/96/239323>
7. 2025 最新 QR Code 詐騙手法！餐廳點餐、水電帳單都有詐。(2025，4 月 24 日)。XREX 交易所。<https://xrex.io/tw/zh/blog/anti-fraud-and-anti-money-laundering/2025-latest-qr-code-scams-restaurant-orders-utility-bills-four-common-fraud-tactics-zh/>
8. 臺人一周被騙走 21 億...5 月損失超過 87 億 惡劣詐騙手法前 3 名公開。(2025，6 月 1 日)。CTWANT。<https://www.ctwant.com/article/420817/>
9. 反詐騙三不一要，保持戒心杜絕詐騙。(2023，5 月 1 日)。國軍退除役官兵輔導委員會。<https://www.vac.gov.tw/cp-1100-143983-102.html>