

【追星圈的假面怪客】延伸學習文章

■ 教學對象：國小五至六年級

■ 主題：社交工程

什麼是「社交工程」？想像一下，你擁有一個裝滿寶藏的保險箱，壞人想取得裡面的寶物，他不必費力敲壞鎖頭，只要扮演成你的好朋友或是管理員，讓你自已心甘情願地把「鑰匙」交給他，這就是社交工程。這種手法利用了我們的好奇心、信任感，甚至貪小便宜的心態，讓我們在不知不覺中成為詐騙的受害者。那麼，有社交工程有哪些常見的形式呢？

【網路釣魚】

有些詐騙者會假裝成知名公司、遊戲平臺、銀行或政府單位，寄信或傳訊息通知你「帳號有問題」、「要重新設定密碼」、或「要補填資料」。如果你急著點開連結，可能會進到假的網站，把帳號密碼輸入給壞人。遇到這種情況時，不要直接點對方提供的連結，也不要急著下載附加檔案。最安全的方法是自已搜尋官方網站，或請家長或老師幫忙確認。

【假冒身分】

假冒身分是社交工程裡最常見、也最容易讓人放下戒心的手法。詐騙者會假扮成專業人士、銀行專員、客服或政府人員；或是偽裝成熟識的人或社團成員來取得信任，例如在追星社群裡則可能冒充資深粉絲、後援會成員（例如站姐）或工作人員，接著再以「帳號異常、核對資料、退款、領福利、抽明星小卡」等理由騙取個資、帳密與驗證碼。遇到這種情況時，先不要回答對方的問題，也不要使用他提供的連結。應該改用官方網站、官方 APP 或客服電話查證。

【誘餌攻擊】

透過「限量周邊免費送」、「保證中獎」或「免費貼圖」等誘餌吸引人上鉤。一旦點擊連結、加入群組或下載檔案，帳號就可能被盜用或被植入惡意程式。我們應隨時提醒自己當網路上的優惠好到讓人難以置信時，通常就是陷阱的開始。特別是私下交易時，如果對方一直催你快點決定、要求先付運費或訂金，甚至還要你提供帳號密碼或驗證碼，就一定要提高警覺。

如果不確定對方是不是詐騙，除了詢問家長與老師，還可以用「內政部警政署 165 打詐儀錶板：AI 智能客服」來協助快速判斷：

1. 先搜尋「打詐儀錶板」網頁。（<https://165dashboard.tw/>）
2. 進到網頁後，點右下角的「防詐客服」圖示。
3. 在對話框輸入你遇到的狀況、對方傳的訊息，或直接貼上可疑網址，讓它協助判斷是否可能是詐騙網站，並提供處置建議。