全民防詐　打造安全台中
識詐及資安宣導

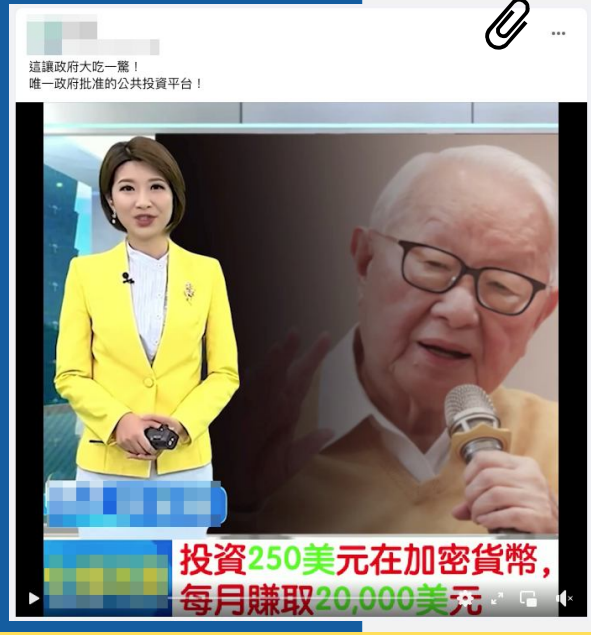
報告機關　臺中市政府 數位發展局 DIGITAL AFFAIRS BUREAU of Taichung City Government

報告人　局長 林谷隆

報告日期　114年4月8日

臺中市政府114年度4月份市政會議專案報告

AI 驅動社交工程攻擊



後製新聞片段並用AI深偽技術冒用張忠謀，並利用中視主播畫面模擬聲音合成，製成投資社群詐騙貼文。

網路/郵件釣魚詐騙（偽冒連結）

透過偽造官方網站的網址（URL）或發送帶有惡意連結的簡訊、電子郵件，引導受害者點擊，進而盜取個資、帳號密碼或誘導匯款。

深偽技術（Deepfake）

不法分子利用AI深偽技術假冒政治人物或知名人物製作假影片，聲稱有高回報的投資機會，並通過社交媒體廣泛傳播，誘騙民眾投入資金。

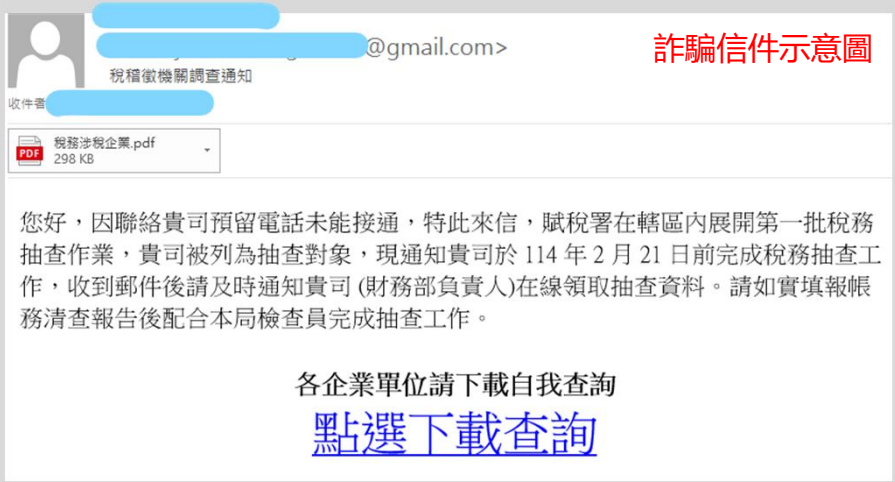
AI 變聲技術詐騙

詐騙者通過AI仿聲技術可在幾秒內生成假音頻，冒充受害者親友、主管聲音直接與受害者通話，難以分辨真偽，誘騙受害者相信。

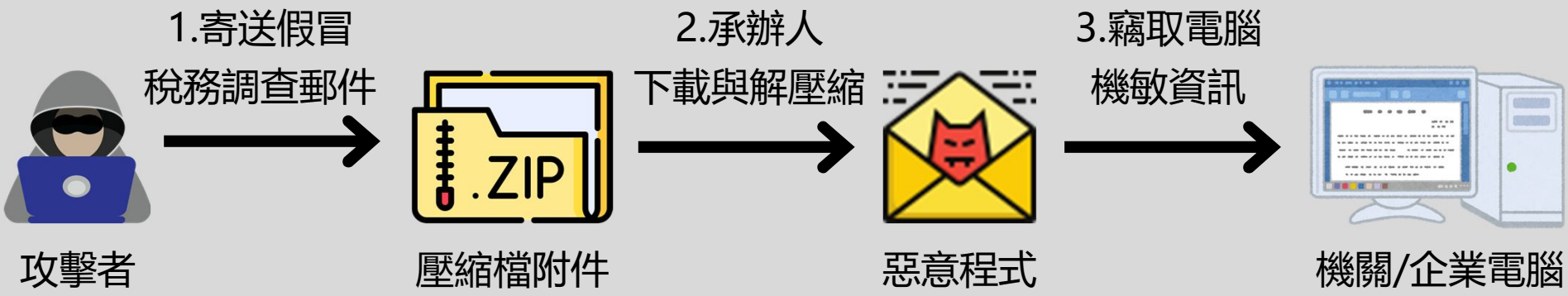
近期社交工程案例

資料來源：數位發展部資通安全署資安月報

- 駭客偽冒財政部名義並以稅務調查為由，對政府機關與台灣企業機構發動社交工程電子郵件攻擊，針對具敏感資訊存取權限之財務人員，誘導開啟並點擊附檔內含之惡意連結，誘騙收件人開啟惡意附檔以植入後門程式，進而竊取電腦機敏資訊。

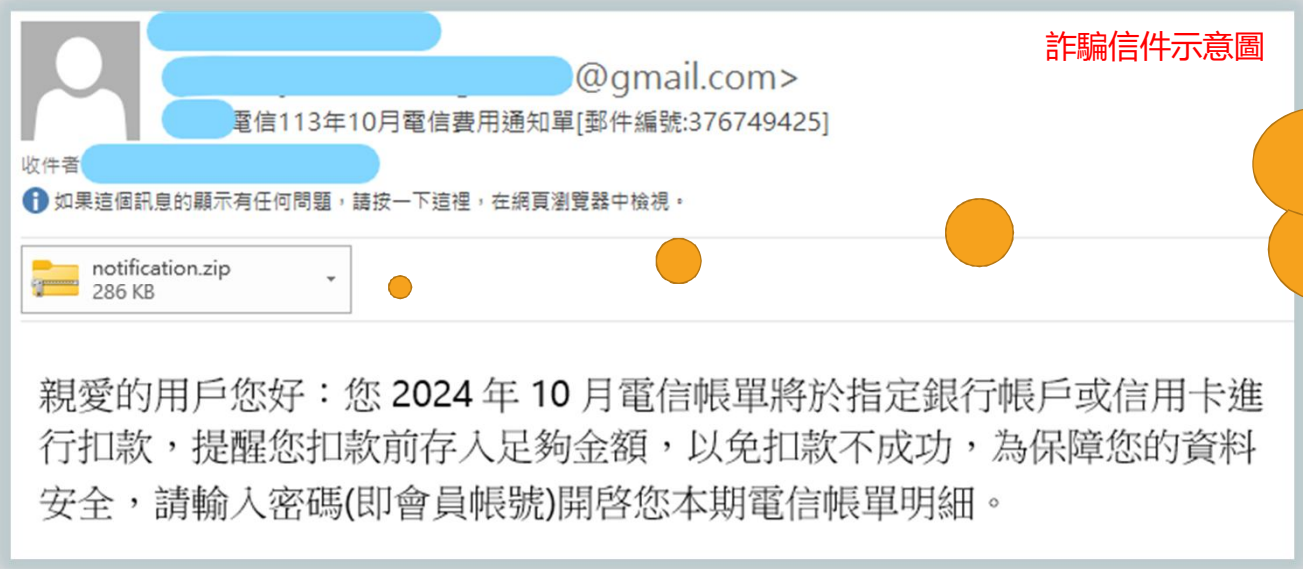


詐騙信件示意圖



近期社交工程案例

- 駭客偽冒某電信公司，利用當月電信費用通知單為主旨，寄送社交工程郵件攻擊政府機關與一般民眾。駭客偽冒某電信公司發送之電子帳單郵件內文做為誘餌，附上惡意附檔，並大量散布含惡意程式的郵件進行社交工程攻擊



詐騙附件
(附件為ZIP壓縮檔，開啓檔案可能導致電腦受駭)

資料來源：數位發展部資通安全署資安月報

本府電子郵件防護系統113年攔截成果

檢測	381萬5,963封信
隔離	855封中高風險郵件
類型	惡意連結、釣魚網站、惡意檔案及病毒等
主旨	付款失敗、帳號到期、發票確認、驗證卡片等，都與日常生活、消費相關

本府社交工程與防詐措施

上下半年
各1次
社交工程演練

開信信件、點擊連結、開啟附件
(1.09%)　(0.61%)　(0.03%)
3項指標皆符合目標值

113年辦理
2場
防詐活動

數位局與政風處攜手
邀集防詐領域專家、檢察官
聚焦AI防詐與實務應用分享

防詐種子教師
培訓>**400位**

識別社交工程及 AI 詐騙

識別假冒訊息與網站

詐騙訊息通常包含「限時優惠」、「法院傳票」、「帳戶異常」等恐嚇字眼。

政府官方網站通常使用「gov.tw」，避免點擊來路不明的連結。

收到疑似詐騙簡訊、Email，可透過企業或政府官網查證。

強化登入安全

透過多因子2階段驗證，降低遭撞庫攻擊之風險。

於不同網站使用相異之高強度密碼，並定期變更。

警覺誇大內容

檢查網址

官方管道驗證

啟用2階段驗證

密碼使用原則

識別社交工程及 AI 詐騙

防範 AI 詐騙技術

檢查影片細節，如眼睛眨動不自然、嘴型與聲音不同步，可要求對方揮手測試。

若接到疑似親友來電要求匯款，可掛斷後撥打對方號碼確認。

深偽影片識別

AI 變聲技術識別

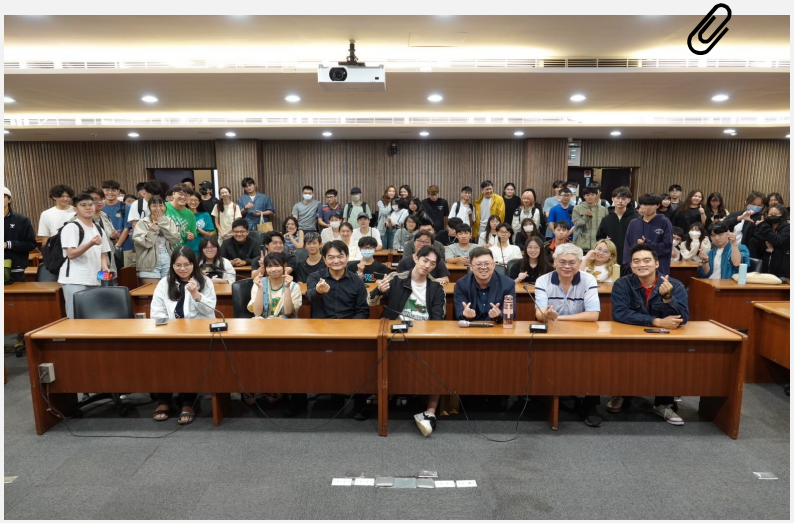
本局已建立「資安宣導專區」宣導防詐資訊

保持懷疑心態
面對財務異常、高額投資等訊息應先查證，不點擊可疑信件

提升數位素養
了解最新詐騙手法，提高識別詐騙技巧

防詐宣導進校園
邀防詐網紅「Bump」談破解詐騙，加強防範意識

全民防詐舉報
鼓勵民眾向165專線檢舉可疑案件



「不明來電不輕信、不明連結不點擊、可疑資訊多查證」

簡報結束　敬請市長指導

臺中市政府數位發展局
DIGITAL AFFAIRS BUREAU of Taichung City Government