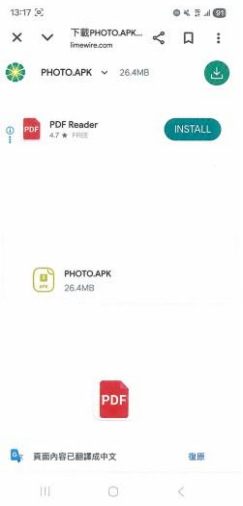
「幫忙投票」竟讓電信帳單爆增　刑事局提醒慎防惡意 APK

近期詐騙集團透過常見之社群平臺，以「幫忙投票」等話術，誘使民眾點擊不明連結，甚至下載、安裝來源不明的應用程式（Android Package Kit，簡稱 APK)。這看似舉手之勞的投票動作，背後卻可能暗藏惡意程式，不僅可能造成社群帳號遭盜用、個人資料外洩，更可能使手機支付或電信帳單代收功能遭冒用，導致財產損失。

日前北部一名 20 餘歲楊姓男子在 Facebook 結識一名自稱模特兒的網友，對方隨後提供 LINE 聯繫方式，要求楊男加為好友。雙方聊天一段時間後，該名網友聲稱正在參加模特兒票選活動，並傳送一個不明連結，要求楊男下載名為「PHOTO APK」的 APP，以便每天協助投票。楊男安裝後發現手機頻繁當機，使用不久便將該 APP 刪除；惟隔日中午，手機仍陸續收到電信帳單代收的消費通知簡訊。由於楊男未曾使用電信帳單代扣功能，隨即向電信業者查詢，才得知已產生共計新臺幣 8 萬 4,000 元的消費金額，始驚覺遭到詐騙並向警方報案。

刑事警察局表示，釣魚連結常是詐團誘導民眾上鉤的起手式，凡收到網友傳送的不明連結或下載來路不明檔案，均應提高警覺。然而詐騙集團為降低被害人的戒心，也會先盜用親友 LINE 帳號，再冒充本人傳送「幫忙投票」的釣魚連結，或以臨時急需用錢為由要求匯款。因此，即使訊息來自熟識親友，仍應透過電話或其他方式向本人查證。另安裝來源不明的 APK 檔，可能使手機遭植入惡意程式，進而攔截刷卡或交易時所傳送的簡訊驗證碼（One-Time Password，簡稱 OTP)，甚至竊取網路銀行帳號、密碼等重要資訊，使民眾在毫無察覺的情況下遭到盜刷、盜領或冒用電信帳單代收。刑事警察局提醒，APP 應用程式應透過官方管道下載（如 App Store 或 Google Play 商店)，切勿任意點擊不明連結或安裝來路不明的 APK 檔。如有疑慮，請立即撥打 165 反詐騙諮詢專線或 110 查證。另亦可洽詢內政部警政署「165 打詐儀錶板」(https://165dashboard.tw）及 AI 智能客服

小幫手，或加入 LINE 官方帳號（目前於 115 年 10 月 29 日前可下載最新防詐貼圖），查詢最新防詐資訊，協助民眾快速辨識情境式詐騙風險及參考具體處置建議。



不明應用程式安裝檔 APK 暗藏惡意程式

