張貼日期：2023/10/24

【資安訊息】針對近期熱門時事議題，請加強資安防護宣導！

- 主旨說明：針對近期熱門時事議題，請加強資安防護宣導！
- 內容說明：
  - 轉發 國家資安資訊分享與分析中心 NISAC-400-202310-00000033□
  1. 社交工程攻擊：利用總統大選等熱門時事為主題 資安院近期接獲情資，發現駭客組織利用總統大選或台積電等時事議題，鎖定政府機關與半導體業者進行社交工程攻擊，並運用google等雲端服務隱藏惡意連結或程式，引誘收件者下載惡意工具。
  2. 偽冒手機應用程式：資安院近期接獲情資，駭客組織於APK.TW台灣中文網論壇，張貼已植入間諜程式之手機應用程式□whoscall□□誘導民眾下載使用，以竊取手機資料，經發現特定版本將連線中繼站下載惡意程式。
  3. 生成式AI相關應用程式之資安威脅：使用生成式AI相關應用程式，如□ChatGPT□□□文心一言」等AI聊天軟體等，應注意其是否提取高風險權限，例如使用者地理位置、讀寫手機檔案、讀取手機設備訊息或開放遠端偵錯等，避免洩露敏感資訊；此外，使用生成之文案或影像，亦應避免導致惡、假、害之不當應用。
- 影響平台:無
- 建議措施:
  1. 請加強社交工程宣導，包含留意可疑電子郵件、注意郵件來源正確性，以及勿開啟不明來源之郵件與相關附檔，以防範駭客透過電子郵件進行社交工程攻擊。
  2. 加強提升人員資安意識，宣導勿使用來路不明或非法取得之手機應用程式，以防範手機資料外洩。
  3. 使用生成式 AI 時，應秉持負責任及可信賴之態度，掌握自主權與控制權，並秉持安全性、隱私性與資料治理、問責等原則，不得恣意揭露未經公開之公務資訊、不得分享個人隱私資訊及不可完全信任生成資訊，詳細請參照「行政院及所屬機關（構）使用生成式AI參考指引」。
- 參考資料:
  - 行政院及所屬機關（構）使用生成式AI參考指引：https://www.nstc.gov.tw/folksonomy/detail/f9242c02-6c3b-4289-8e38-b8daa7ab8a75?l=ch

---

計算機與通訊中心
網路系統組 敬啟