「某機關網際網路公務電子郵件遭社交工程攻擊事件」資訊安全案例宣導

資料來源：法務部政風小組

某機關人員於 103 年 3 月某日收到以承攬該機關系統建置及維護廠商之工程師名義，寄送之電子郵件，內容附帶一壓縮檔，經該機關查獲該壓縮檔解壓縮後，內含副檔名為 pptx 之簡報檔，開啟後除會顯示出正常簡報檔案外，另將分離出經註冊為自動執行惡意程式檔案，且簡報檔經開啟後電腦會自動造訪位於泰國之未知網站。經分析該郵件內容，具有檔案加密規避防毒偵測、檔案字元反轉引誘開啟、自動植入後門及逆向連線回報功能，確認屬於惡意郵件。復經該機關向該名工程師查證後，該工程師表示並未寄出該封郵件，疑似駭客以該系統建置及維護廠商為身分掩護，針對該機關為釣魚郵件攻擊行為。

防處作為：

(一)坊間多數掃毒軟體對於本案相關檔案已可有效偵測，應定期執行病毒碼更新與資安監控，以維護資安防護有效性。

(二)持續強化機關同仁資安教育訓練，避免因開啟來路不明郵件或連結，致遭社交工程攻擊。

(三)與廠商郵件往來，應先行確認後再開啟，並避免將郵件帳號供給無關人員。

(四)機關應管控公務電子郵件帳號使用情況，發現異常情形應即時通報處理。

(五)提醒承商重視及強化自身網安作為，並嚴禁私設遠端維護機制，落實現地維護要求，避免成為駭客入侵管道。

臺中監獄政風室關心您

廉政檢舉專線 0800-286-586