◎資訊安全宣導

—考驗人性的社交工程誘惑—

社交工程郵件之包含要素，以電子郵件來詐騙至少已有十年歷史，然至今仍有民眾上當，因為民眾輕忽或無知，易讓駭客達到欺騙目的。社交工程電子郵件不乏利用聳動的郵件主旨、偽造受害者熟悉的寄件者、以假亂真的郵件內容等等，試圖吸引使用者上鉤。社交工程電子郵件中會有幾個要素，包含超連結、附件、圖片、郵件內容內嵌程式碼。

1. 超連結：有可能會讓受害者連至攻擊者所架設之惡意網站，藉此收集受害者相關資訊。
2. 附件：多含惡意程式，開啟並執行後會潛藏在受害電腦裡，直接將電腦內資料對外傳輸、偷偷側 錄用戶使用電腦的任何行為、接續下載惡意程式至受害電腦再執行各項行為等。
3. 圖片及郵件內容內嵌程式碼：能回報給攻擊者表示「登陸成功」，更甚者直接讓受害者電腦自動從中繼站下載小程式（諸如鍵盤側錄工具、螢幕側錄工具等），記錄受害者使用電腦行為，再進行下一步攻擊。

社交工程攻擊之防範措施，社交工程攻擊防不勝防，面對攻擊，可行的防範措施包含：

1. 使用垃圾郵件過濾器：現行的郵件伺服器（包括 Gmail）皆有此機制。
2. 定期更新：隨時更新防毒軟體、防火牆 與電腦及手機的作業系統，以防任何安全性漏洞被利用。
3. 仔細確認：確認訊息與自己是否相關，並查證訊息來源，有必要時打電話向來源確認。
4. 提高警覺：個人應提防不明電子郵件，並且勿任意點選附檔及超連結。

【文章擷取-法務部調查局清流雙月刊】

臺中榮民總醫院提醒你!也關心你!