機關安全維護宣導-考驗人性的社交工程

◎社交工程—駭客最有效且省錢之攻擊方式

社交工程即為人與人之間的攻擊。過去關於此類攻擊定義為「攻擊者藉由社交手法取得系統或網路的資訊」，然而現今攻擊者的目標，已逐漸轉到個人擁有之資訊。此攻擊管道，最常見的為電子郵件、簡訊、即時通訊軟體（如 Messenger、Skype、Line、Instagram、Whats App）等。

◎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。

- 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。
- 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。
- 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。

◎社交工程之攻擊方式素

在 COVID-19 疫情高峰時，國內採取口罩預購制，意外出現「口罩釣魚簡訊」，佯稱口罩到貨，引誘使用者點擊簡訊內連結，當時亦有不少臺灣民眾受駭。以下再列舉其他社交工程之攻擊種類。

一、濫發電子訊息：諸如惡意電子郵件、釣魚簡訊、即時通訊等

文字訊息。此類攻擊通常一次廣發給多名使用者，因此亦稱為「垃圾郵件」。

二、釣魚：此類攻擊通常會讓使用者「信以為真」，透過話術讓人誤信，進而騙取錢財。近期常見「假交友」、「假投資」即屬此類。

三、願者上鉤：經典手法為攻擊者在公司門口隨意丟棄一個隨身碟，該公司不知情員工撿到後，誤以為是公司內有人不小心遺失，為了順利歸還，故而將該隨身碟插進自己的電腦內，殊不知惡意程式就此開始執行。

四、搭順風車：尾隨員工進入外人不該進去的區域，進而竊取到公司內部機密資訊。

五、水坑攻擊：利用網頁藏惡意程式碼的方式，讓使用者的電腦中毒。只要入侵或偽造目標受害者常瀏覽的網站，植入惡意程式，當受害者瀏覽該網站，即會下載惡意程式。

◎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：

一、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。

二、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。

三、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。

四、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。

~~節錄自 111 年 1 月清流雙月刊~~

~~政風室關心您