

# 公務機密維護宣導 - 考驗人性的 社交工程誘惑

## 社交工程 - 駭客最有效且省錢之攻擊方式

自從人們可以利用網際網路互通有無，每個人至少都擁有多個網路服務帳號，包括個人或其所屬單位的電子郵件帳號；正因如此，利用資訊科技便利之社交工程犯罪行為層出不窮，且趨勢逐年上升。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、WhatsApp）等等。為何此種攻擊趨勢會逐年上升？為對駭客而言，這是最有效、最省成本的攻擊方法。

### 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。

超連結

附件

圖片及  
郵件內容內嵌程式碼

※ 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。

以上要素不一定會同時出現，亦可能交互搭配使用，曾有僅憑單一內容即欺騙成功的案例，造成受害者損失。例如，假冒會議邀請信函，成功欺騙到受害者出門參加會議，加害者利用這段時間闖空門等。

## 社交工程之攻擊方式

只要個人一時疏忽，即使只是小小電子郵件，就有很大的機會對企業、群體，甚至國家安全造成危害。另外，即時通訊軟體也成為社交工程攻擊管道之一，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。倘於公務信箱發覺有惡意郵件切勿開啟或點閱惡意郵件所附連結或檔案，並請同仁按「關閉預覽功能取消方式」及自行檢視是否已取消「自動轉寄功能取消方式」。

資料來源：法務部調查局清流雙月刊第37期

資料發佈日期:111/04/20