『社交工程，英文為 Social Engineering，是以影響力或說服力來欺騙他人以獲得有用的資訊，這是近年來造成企業或個人極大威脅和損失的駭客攻擊手法。

社交工程造成極大威脅的原因，在於惡意人士不需要具備頂尖的電腦專業技術，只要企業員工對於防範詐騙沒有足夠的認知，就可以輕易地避過了企業的軟硬體安全防護，而騙取到各項帳號密碼、個人資料、財務資料或公司重要資料等資訊，對企業所造成的損害與威脅，完全不下於網路上的各種駭客攻擊。

企業員工對安全防護認知的不足與輕忽，造成了企業資通安全的一大漏洞，公司即使投資了各種網路防護的軟硬體，並訓練員工正確的系統操作步驟、資料儲存程序，再加上良好的保全系統保護機房安全，結果仍可能不堪一擊，因為社交工程利用人性容易相信而上當的弱點，避開了不容易破解的網路防火牆，選擇容易跨越的人性防火牆，只應用了簡單的溝通和欺騙技巧，便突破了企業的安全防護，而突破這些耗資千萬的層層安全防護，所花費的成本竟然只有一、兩通電話的費用。

## 應用社交工程的各種攻擊方法

除了利用電話詐騙之外，常見的社交工程攻擊還包括：

（1）電子郵件隱藏電腦病毒

駭客利用社交工程的概念，將病毒、蠕蟲與惡意程式等隱藏在電子郵件中，這些看似朋友所寄來的郵件，卻是應用社交工程的電子郵件陷阱， 例如過去造成重大損害的 I LOVE YOU 蠕蟲，就是一種利用社交工程散播的電腦病毒。

（2）網路釣魚

有一種偽裝知名企業或機關單位寄發的電子郵件，通知收件人必須重新驗證密碼或登入某網址輸入個人資料等，這種詐騙稱為網路釣魚。收件人若無小心求證而連結了郵件中的鏈結，可能就下載了惡意程式；或者在假網頁上輸入了帳號密碼或信用卡資料等，造成銀行戶頭被盜領或盜刷等的嚴重後果，這是近年來造成個人與企業極大損害的犯罪手法，而 1 網路釣魚就是一種典型的社交工程攻擊。

（3）圖片中的惡意程式

明星或色情圖片也是許多惡意程式慣用的社交工程技巧之一，這些都是利用使用者的好奇心來散佈惡意程式，之前 Sobig 網路病毒出現在某個含有色情內容的網路討論群組，網友點選了其中像是裸照的內容就會感染病毒，而該病毒總共導致了約 10 億美金的損失。

（4）偽裝修補程式

另一種社交工程的欺騙手法，就是偽裝成微軟的修補更新程式，因為一 般使用者不會覺得這是來路不明的程式，卻沒有防範社交工程也會利用這個漏洞，而將惡意程式隱藏其中。使用者若安裝了這個檔案，不但不會修補作業系統的任何漏洞，還可能被安裝了遠端竊取資料的木馬程式。

## 社交工程攻擊四步驟

社交工程攻擊首先取得一個攻擊目標的背景資訊，透過交談與受害人建立信任，然後向受害人要求資訊，再利用這些資訊向其他或更高層人員欺騙，不斷重覆這些步驟，以達成最後目標。

## 常見的社交攻擊手法與目標

不管是純粹使用詐騙技巧，或是利用電腦專業技術製造詐騙機會，常見的詐騙與攻擊手法相當多元，包括：假冒為同事；假冒新進員工；假冒廠商、客戶或政府單位；假冒具有權威的人；假冒系統廠商，表示欲提供系統修補程式或更新程式；假冒好心人士，告訴對方如果電腦發生問題可以找他，然後製造問題，讓受害人打電話來求援…等。其中，某些職務人員是社交工程攻擊常鎖定的目標，尤其是基層庶務人員，當其對 23 於公司主要業務較無直接關係時，往往對於資訊

保密的警覺性較低，常常成為社交工程攻擊常鎖定的主要目標。

## 有效防範社交工程攻擊的方法

在了解社交工程的攻擊手法後，應建立正確防範社交工程的觀念，包括人員的教育訓練與平常的宣導。

（1）認識常見社交工程的可疑徵兆

首先，隨時具備危機意識，惡意人士可能以任何角色或形式出現，在沒有適當的認證情況下，不應輕信他人，只要出現社交工程攻擊警訊，都應保持小心求證的戒心。認識幾個社交工程的可疑徵兆，例如對方強調是緊急事件；提出不尋常的請求；威脅對方如果不照辦會有嚴重的後果；拒絕告知回電號碼…等，遇有上述情形時應提高警覺心。

（2）遵守公司安全政策與程序 確認要求者的身分

另外，平時亦應遵守公司安全政策與程序，例如依資料分級制度流通資訊，不開啟來路不明的電子郵件等，在任何資訊釋出時，都要確認要求者的身分及對方經過授權。

（3）通報作業

最後，遇到疑似攻擊事件時應向資訊單位通報。

## 總結

社交工程其實就是一種利用人性弱點的詐騙技術，它避開了嚴密的資通安全技術防護，是一種非常難以防範的攻擊模式，只有具備高度的

危機意識及警覺心，才能減少社交工程攻擊傷害。

【資料來源：載自 I Security 邱瑩青 著】