第三章

社交工程

社交工程

- **There is No Patch to Human Stupidity !**
- 資安最大的問題就是「人」。

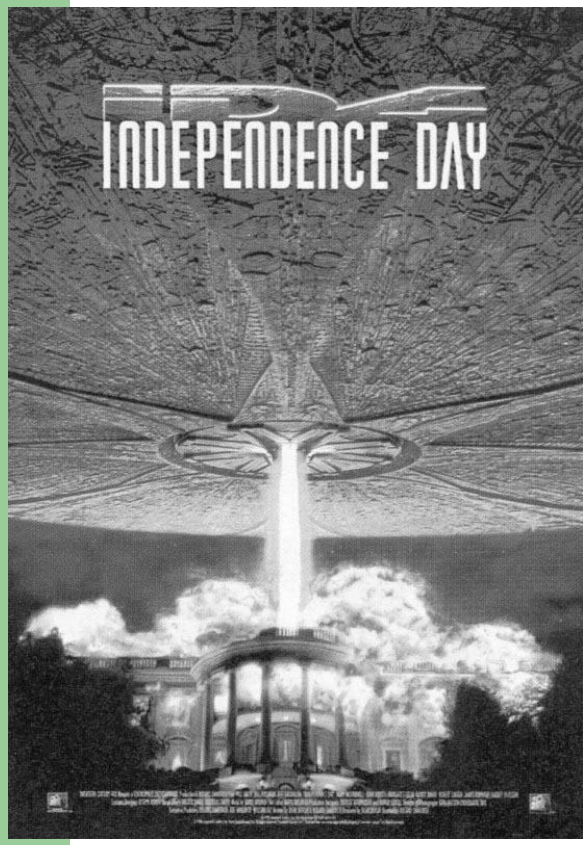
社交工程

- 社交工程（Social Engineering）使用的方法並不是依靠資訊技術，而是一種利用人性弱點的詐騙技術，可以藉由與他人之間的互動，或是利用某些組織內部的人員去違反組織的政策，最後的目的就是獲得有價值的敏感資訊，社交工程屬於犯罪行為的一種。

社交工程

- 和善的聲音、假冒的能力、誘惑人的內容...等都是社交工程的武器，社交工程攻擊的是整個安全鍊中最脆弱的一個環節：人類。沒有任何硬體或軟體可以防禦社交工程。

電影情節



星際終結者（Independence Day）

- 地球人對於外星人的攻擊束手無策。由於外星人的攻擊都是由母船控制，最後人類利用一架俘虜的外星戰機，進入外星人的母船並且上傳病毒，使外星人母船停止運作。這種進入母船並上傳病毒的手法，就類似社交工程。

真實的世界

- MIS人員接到一通電話，自稱是該公司的財務長，你從未聽過財務長的聲音。對方表示他正在前往開會的途中，目前正在另一個國家。打電話的人說了個悲慘故事：他的筆記型電腦在機場被偷了，而公司各個系統的帳號密碼都在那部筆記型電腦中，他馬上要去見一個重要客戶，需要公司系統中的資料。
- MIS人員會不會如他所願，告訴他想要知道的資料？

社交工程分類

社交工程可以被分成兩種分類：

- 「以人為基礎」
- 「以電腦為基礎」

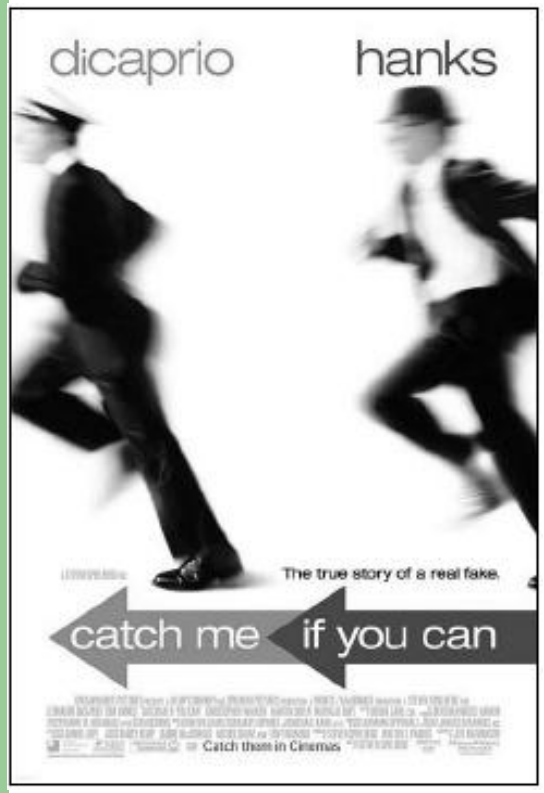
社交工程以人為基礎

- 偽裝成合法使用者
- 偽裝成重要的人物
- 偽裝成技術支援
- 列印的紙中找資料
- 背後偷窺

社交工程以電腦為基礎

- 郵件附檔
- 彈出視窗
- 中獎網頁
- 垃圾信（Spam Mail）與釣魚
- 即時通訊軟體
- 假的（Fake）網站

電影情節



神鬼交鋒

此片改編自真人真事法蘭克二世的同名自傳，他是一個連高中都沒畢業的青少年，卻能假扮成航空公司機長、醫生、律師和大學教授，最離譜的是，他還用偽造支票兌現了數百萬美元的鉅額。最後，他付出了牢獄的代價，出獄後改邪歸正。

社交工程施行階段

- 先對目標組織進行研究
- 選擇目標人員
- 與被害者發展關係
- 利用關係獲得目標

目標組織

- 組織的員工或成員人數眾多
- 分支辦公室地點眾多
- 教育訓練不足
- 組織缺乏適當的安全政策
- 組織內的資訊很容易被獲得

目標人員

- 接待處或服務中心人員
- 技術支援人員
- 目標組織的業務人員
- 具有特殊權力者
- 基層庶務人員

心理弱點

- 信任
- 忽略
- 害怕
- 貪婪
- 道德責任

案例 1

從某公司網頁上發現XX部有一個人員叫做Iris，也可以看到該公司的總機號碼。於是攻擊者依據電話號碼，撥電話進行社交工程：

總機：「XX公司你好。」
駭客：「請轉XX部Iris，我不知道她分機號碼是幾號。」
總機：「她分機是110，我幫您轉接，請稍等。」
助理：「你好，XX部。」
駭客：「請找Iris。」
助理：「她不在，她外出了，您要留電話嗎？」
駭客：「不用了，我有一個Case急著找她，不在就算了。」
助理：「請等一下，我給你她的手機號碼。」
駭客：「好，請說…。」
助理：「……」
駭客：「好，我知道了，謝謝你。」

案例 2

在地上撿到一支隨身碟，上面標明容量有512M，你會怎麼做？

- A.撿起來。
- B.不理它。

回答若是A.撿起來，則繼續往下看。

案例 2

你會怎麼處理這隨身碟？

- A.拿回家，自己用。
- B.插入電腦看看裏面的檔案，有沒有原持有者的資料，以物歸原主。
- C.送給別人。

不論回答哪一個，都繼續往下看。

USB 社交工程法

- 利用Windows預設會跑 autorun 的特性，在USB隨身碟裡面設定一些間諜軟體（SpyWare）。
- 當這USB插入電腦時，系統就會被植入病毒，並且會開始蒐集這部電腦內的各種資料。

對策

1.教育與訓練。

- 教育組織的員工，認識社交工程有哪些常見的可疑徵兆。
- 教育組織的員工了解並遵守公司安全政策與程序。
- 實際模擬演練與測試。

對策

2.密碼政策。

- 週期性的更換密碼。
- 避免使用容易猜到的密碼。
- 帳號在輸入數次失敗後，會有一段時間暫時不准輸入。
- 要求使用者密碼的長度與複雜度（使用「強密碼」）。
- 不要將密碼保存於紙張上或電腦中。
- 禁止將員工個人密碼告訴他人。

對策

3.完整運作指引。

- 確認身分（員工編號，身份字號，出生日期...）。
- 確認在職狀況（是否仍在職，單位部門，職稱...）。
- 確認對方有取得資訊的需求及權限。

對策

4.實體的安全政策。

進入具有資訊安全顧慮的空間，是否具有實體的管控。例如：進入機房是否需要刷卡，只有指定的人員進入機房可以開啟門禁。

對策

5. 資訊的分類 。將文件等級區分為

- 極機密
- 特權使用
- 內部使用
- 公共使用
- …

對策

6.員工背景檢查。

7.適當的事件反應系統。

對策

8. 政策檢查表。

- 帳號的設定。
- 密碼改變的政策。
- 存取權限。
- 紙張文件。
- 實體存取限制。
- 病毒控制。

練習

- 假設你是機房工程師，接到一通電話，在前面敘述的 MIS 事件真的發生在你身上，很不幸的你公司沒有訂定任何安全程序。
- 如果打來的人自稱是「總經理」，而你正好也跟「總經理」不熟，你該如何？
- 如果打來的真的是總經理，你會採取哪些步驟？
- 注意：這些步驟必須讓你既不得罪上層主管，又可以達到防止社交工程的目的？
- 將對話與步驟寫下。