

資安月報一月號- 什麼是社交工程

2024.01.23 Nicole編輯

1. 何謂社交工程
2. 社交工程進行的步驟
3. 社交工程攻擊過程
4. 社交工程攻擊類型
5. 社交工程影片賞析
6. 小測驗

何謂社交工程

- 社交工程 (Social Engineering) 係利用人性弱點，應用簡單的溝通和欺騙技倆，以獲取帳號、通行碼、身分證號碼或其他機敏資料，來突破個人、企業或政府機關的資通安全防護，遂行其非法的存取、破壞行為。
- 社交工程這個名詞來自駭客出身的資安顧問 – Kevin Mitnick，它是種引誘人們做出本意不想的行為，或是給出機密資料。欺騙的藝術(The Art of Deception)的作者 (Kevin Mitnick)，更進一步的解釋到

人類的天性就是很希望能幫助別人，因此也相當容易被欺騙。

何謂社交工程 (續)

- 社交工程有兩個基本元件：第一個是詐騙的對象、第二個是詐騙的手法
- 無論再堅強的陣容及防護設備，只要存在「人」這因素，就一定有「漏洞」存在。
- 駭客利用漏洞百出的「人性」，來設計各式各樣的詐騙手法
 - 貪心：撿便宜的個性
 - 情色：食色性也多多益善
 - 好奇：探索八卦訊息的個性
 - 驚恐：威脅恐嚇讓人慌亂
 - 信任：輕易的相信不求實證
 - 不在意：沒那麼倒楣吧的想法
 - 警覺力：無所謂後果的嚴重性

社交工程進行的步驟

搜集資訊



選擇受害者



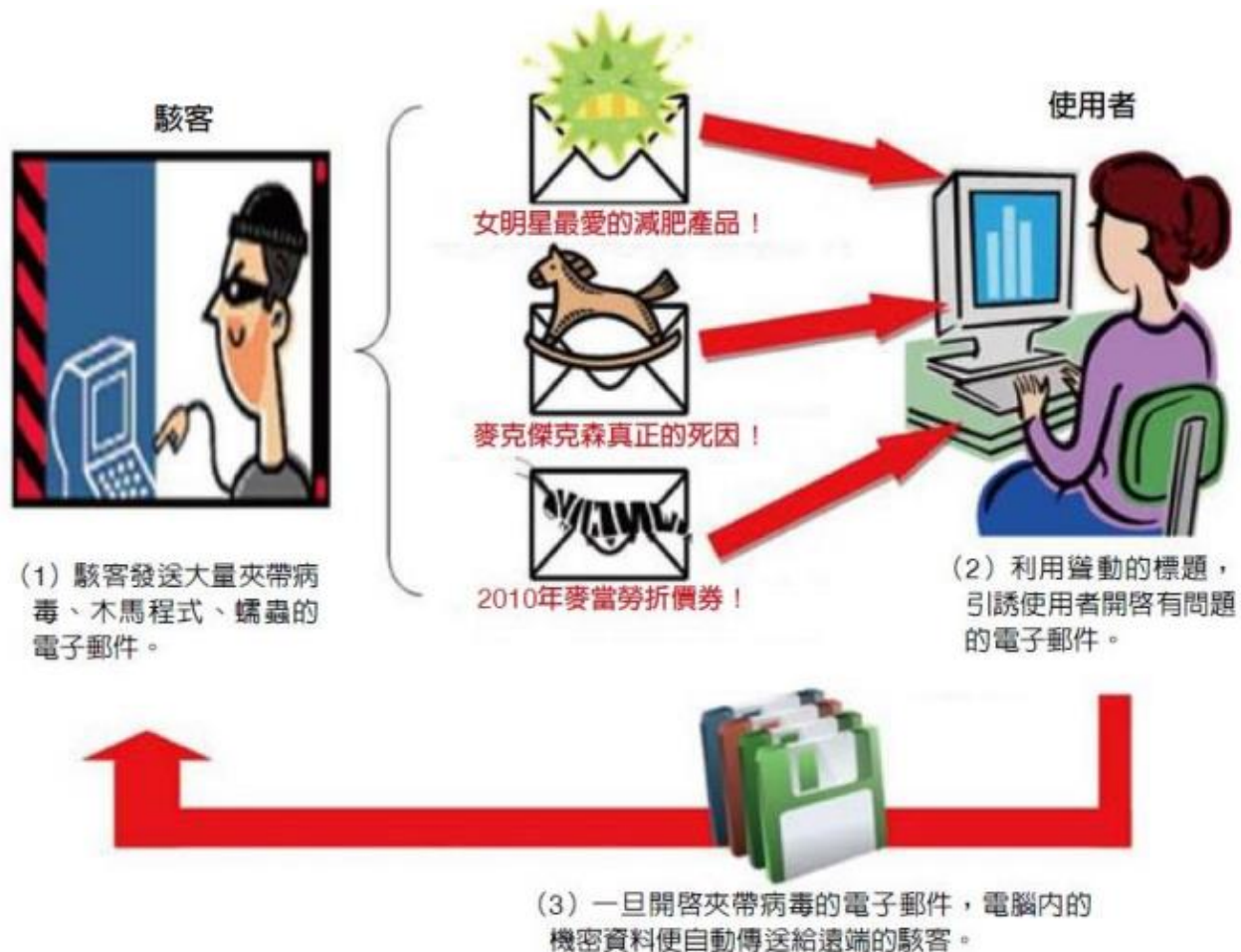
發動攻擊



建立關係

社交工程攻擊過程

- 利用電子郵件進行社交工程的過程



社交工程攻擊類型

- 駭客最愛使用的5大釣魚類型



優惠折扣通知



銀行通知



社交網站通知



網購訊息通知



中獎通知

社交工程影片賞析

- 虎三小之童話變奏 社交工程

<https://www.youtube.com/watch?v=MYQmbNRwzM8>

小測驗

Quiz

- 下列哪一項不屬於「社交工程攻擊」手法？
 - A. 郵件仿冒或偽裝
 - B. 針對帳號密碼採行字典攻擊法
 - C. 網路釣魚
 - D. 電話詐騙個人資訊。





所謂的**字典攻擊法**，用於密碼破解程序，也就是駭客會準備一些常用的字集，先猜這些密碼，而大幅縮短破解密碼的時間。因此字典攻擊法並非社交工程的手法之一唷！

參考資料

- [110年防範惡意電子郵件社交工程演練](#)

下期會讓大家了解如何防範社交工程唷!

敬請期待