資安月報二月號-
如何防範社交工程

康聯生醫
Healthconn

1. 前言
2. 社交工程攻擊最常利用工具
   - 電子郵件
3. 如何防範社交工程
4. 歸納總結
5. 小測驗

康聯生醫
Healthconn

前言

還記得上期月報提到的社交工程嗎?

這邊簡短的和大家複習一下：

社交工程是一種利用人性的弱點進行詐騙，以達到個人目標的手段。最常利用的工具則是透過電子郵件的方式，誘騙使用者開啟信件或者點擊連結。駭客在這類型的信件中藏有惡意的軟體或連結，使用者如果點擊或開啟之後就讓駭客可以藉此達到操控的目的。

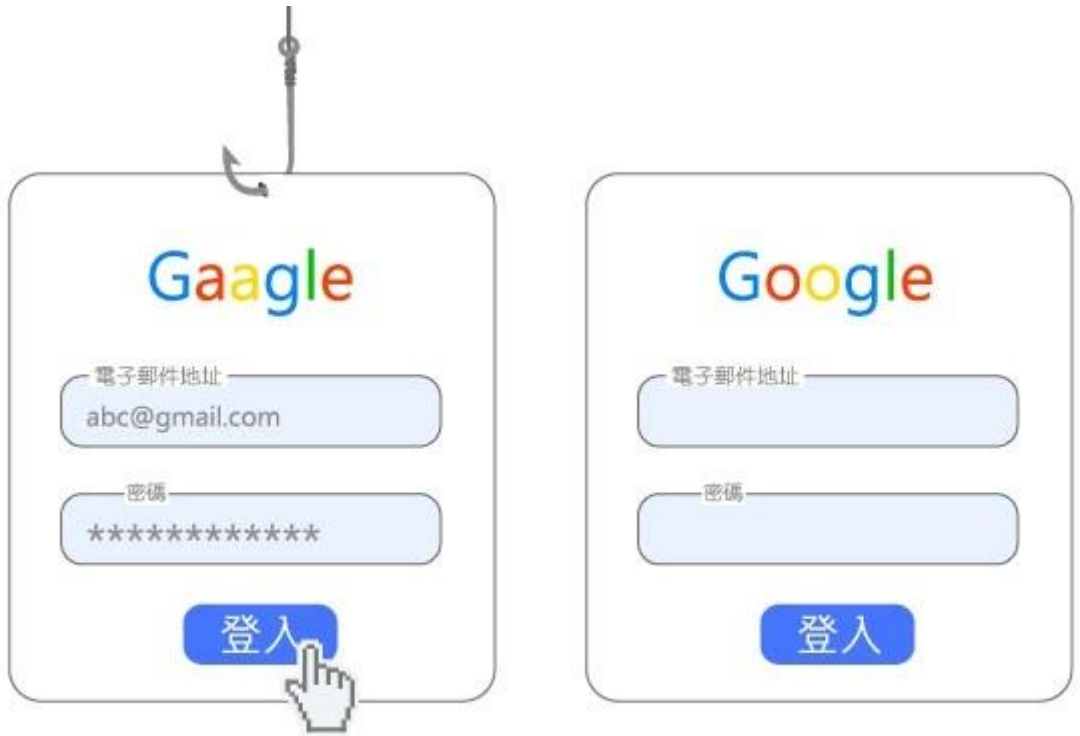
康聯生醫 Healthconn

社交工程攻擊最常利用工具 - 電子郵件

社交工程的手法日新月異，很難一言道盡。
最簡單的應對方式就是：

- 不認識的寄件者來函，不要隨意開啟
- 與自己業務無關的信件，不要開啟
- 寄件者雖然是認識的人，但是寄件地址跟以往不同，開啟前先確認
- 取消收信的媒體之郵件預覽功能

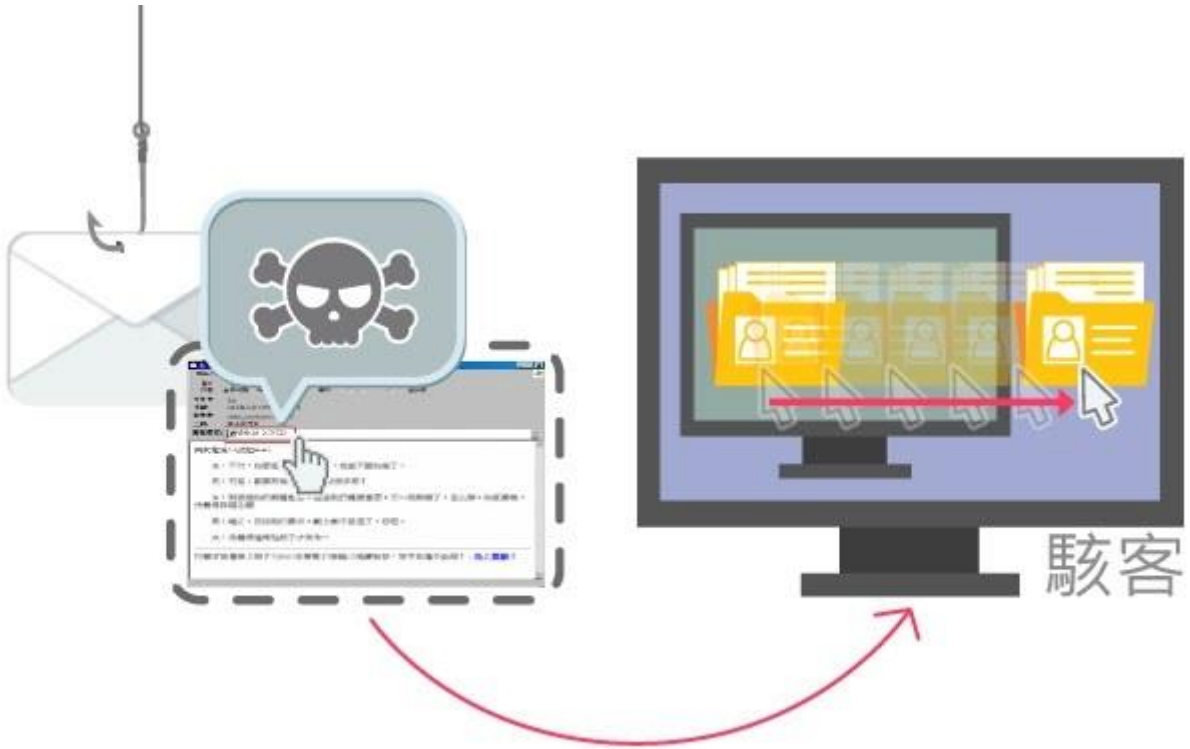
右圖所示, 即為駭客使用假冒的知名網站，偷取你的帳號密碼。如果一時不察，帳號就可能被盜用。



康聯生醫 Healthconn

社交工程攻擊最常利用工具 - 電子郵件(續)

- 信件中的附檔如果有病毒，在不知情的情況點下去就會中木馬等病毒並有機會被駭客盜取個人資料及電腦內的相關訊息。

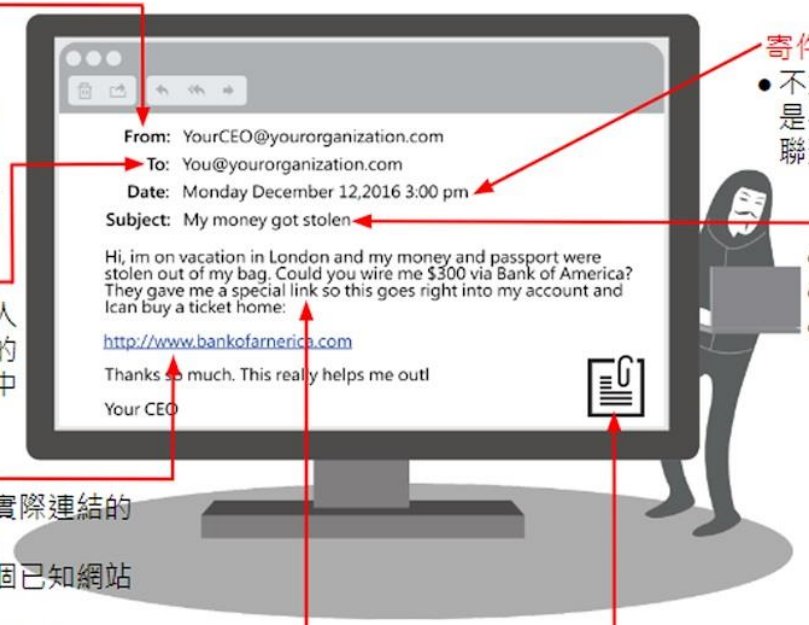


康聯生醫 Healthconn

社交工程攻擊最常利用工具 - 電子郵件(續)

收信時必須要注意

- 寄件者的信箱、寄件時間以及信件的主旨還有附加檔案等等...，發現這些疑點有可能是釣魚郵件，應避免開啟信件附件或點擊信件內的超連結。



寄件人信箱若是.....
- 不認得的人
- 沒有業務往來的人
- 署名某人但他應該不會跟我聯絡的信箱網域名稱蠻可疑的(像某單位的網域又有點不像、或是免費信箱)

收件人群組若是.....
- 還有其他一些不認識收件人
- 看來像是從網站把同頁面的通訊錄都納入收件人名單中

寄件時間若是.....
- 不太正常的寄件時間，像是半夜3點怎麼有人會寄信聯繫業務呢?

信件主旨若是.....
- 主旨看來跟自己無關的
- 主旨與信件內容不相關
- 主旨是回覆什麼，但之前並未寫信去問過什麼啊!

信件內的超連結若是.....
- 滑鼠移到超連結上可看到實際連結的網址與表面上的網址不同
- 超連結網址看得出來是某個已知網站但中間有些微拼錯字的
- 超長的超連結網址就要特別小心

附加檔案若是.....
- 檔案名稱看起來不應該寄給我的
- 檔案名稱與信件內容不相關
- 署名某人來信，但應該不會寄這種檔案給自己啊!
- 除了副檔名.txt，任何檔案都有可能包藏惡意程式在內，有懷疑的話就開啟前先用防毒軟體掃描較保險。

信件內容若是.....
- 不合常理
- 提到為了避免什麼不好的後果
- 提到你中獎了或你獲得什麼好處
- 提到別人或自己可能發生桃色事件或不雅照片等八卦消息
- 內容明顯文法錯誤或錯字不少，不像是一般人會嚴謹擬訂字句。
- 強調快點擊超連結或開啟附加檔案

如何防範社交工程

正確地使用電子郵件

- 關閉郵件預覽功能。
- 除非相當確定信件的來源，否則決不輕易開啟或點擊信件裡的附件檔案或超連結。
- 不要將電子郵件密碼告知任何人，即使是系統管理者。
- 關閉讀信回條功能。
- 不要使用電子郵件傳輸任何不當資訊，包括不法、暴力、 色情、違法交易、侵犯隱私或威脅他人的資料。
- 使用純文字模式瀏覽。
- 轉寄前先將他人郵件地址刪除，避免他人郵件地址傳出。
- 同時寄件給多人時，為保護各收信人資訊，最好使用密件副本方式傳送。

康聯生醫 Healthconn

如何防範社交工程(續)

社交工程的基本防護

- 執行各種作業系統、應用軟體的更新及設定。
- 必須安裝防毒軟體，並確實更新病毒碼。
- 密碼設定要符合複雜度的要求。
- 不要輕易相信電話中任何非經正式授權的請求。
- 不要任意安裝未經授權的軟體。
- 小心釣魚網站、詐騙廣告的陷阱。
- 不使用公務信箱作為登入的帳號。
- 不於社群網路中談論有關公務之相關內容。
- 修改個人資料的隱私設定(提供最少個資為宜)。
- 不要輕易點選陌生的加好友請求。
- 不任意點選社群網路聊天室或電子郵件的連結。

總結歸納 - 三不&三要

- 標題特別吸引人的郵件，開啟前務必再三確認

不上鉤

- 不隨便打開email附加檔案

不打開

- 不隨易點擊email夾帶的網址

不點擊

- 重要資料定期備份

要備份

- 開啟電子郵件前先確認寄件者

要確認

- 安裝的防毒軟體要隨時更新病毒碼

要更新

康聯生醫 Healthconn

小測驗

Quiz

- 下列何者不是防範電子郵件社交工程的「有效」措施？

A. 安裝防毒軟體，確實更新病毒碼

B. 確認信件是否來自來往單位

C. 取消信件預覽功能

D. 制訂企業資訊安全政策，禁止使用非法郵件軟體。

- 單單透過制訂企業資訊安全政策或禁止使用非法郵件軟體並不能有效的防範社交工程攻擊，因為社交工程就是利用漏洞百出的「人性」，即使使用合法郵件軟體也是依然有機會落入詐騙手法裡的！

參考資料

- 社交工程教育訓練-政大
- 110年防範惡意電子郵件社交工程演練
- 元智大學社交工程演練宣導