# 公務機密宣導

防範
網路社交工程

# 前言

**社交工程（Social Engineering）**是目前十分常見的駭客攻擊手法，係指駭客在網路上假冒熟人（例如：主管、好友、親人等）或其他任何角色（推銷員、網路商店等），以電子郵件、Facebook等聯絡管道，散佈詐騙訊息，**誘騙個人開啟含有惡意程式的檔案或造訪惡意網頁，藉以將惡意程式植入受害人電腦，以獲取帳號、通行碼、身分證號碼或其他機敏資料**。

攻擊的第一步是誘騙使用者打開含有惡意程式的檔案或電子郵件，猶如上演木馬屠城記，使用者自願開啟後門後，讓駭客輕而易舉地入侵使用者電腦，再透過長時間地潛伏尋找最佳時間出手竊密或進行破壞。

# 前言

比起直接攻破網路閘道器的外部攻擊，**電子郵件詐騙是屬於最常見的社交攻擊手法之一**，因採取社交攻擊成本最低、效果最好，這種針對資訊系統中最弱的一環——「人性」發動攻擊的手法，也成為駭客最愛利用的方式。

除了常見的EXE檔、COM檔及BAT檔等執行檔能夠藏病毒外，開啟 PDF 檔、Word 檔等文件檔案也都有可能遭到社交工程之攻擊！

# 案例說明

法務部調查局為討論兩岸交流及統戰因應防處作為等議題，故舉辦國安研討會，邀請國內各情治單位中堅幹部參訓。

承辦科B科長提早數月著手進行邀請研討會來賓等事宜，為求研討會盡善盡美，B科長上網搜尋了相關領域的專家並得到了A君之公務郵件信箱，隨後以電子郵件詢問A君是否能夠蒞會指導。

經多次電子郵件往來後，A君因有要職分身乏術，只能婉拒參加本次國安研討會。數日後，B科長的信箱卻收到另一位官員C君的來信，信件內容涉及本次國安研討會討論之機密事項，且為B科長十分重視急需之資料！

# 案例說明

此時B科長腦中卻冒出了幾個問號，觸動了雷達警報：

1. 平日未使用之公務信箱，為何在寄信給A君後，就收到C君的回信？
2. B科長與C君素昧平生，不相識且未曾聯繫，C君如何得知本次國安研討會之資訊？

更重要的是，因平日的社交工程演練，讓同仁皆有資安防護的危機意識，B科長首先**利用了防毒軟體掃毒**，而C君之來信安全通過掃毒軟體的檢驗。

但為求謹慎，**B科長再透過管道聯繫C君，不料C君卻表示未曾發過此封郵件**，顯見此封信件應是冒名傳送的社交工程郵件！

# 案例說明

B科長隨後致電資通安全處的電腦偵辦科請求協助，經過電腦偵辦科的鑑識後才發現，這確實是一個不折不扣的社交工程郵件，只要一開啟附件資料，就會開啟電腦的後門，拱手歡迎敵對勢力進入內部網路，恣意瀏覽機密。

從這個例子中可以發現，即使自己的電腦再安全，駭客仍可利用入侵A君電腦，抑或是在網路上中途攔截封包，藉以進行社交工程。

# 案例分析

資訊安全的大原則是**「整體資安水平取決於全體最低的水準」**，即使機關內的資安設備再先進，人員訓練再優良，只要有一位同仁輕忽資安的重要性，讓駭客有機可乘，整體的資安防護也隨之瓦解，因此每個人都應隨時保持資安意識，面對這種針對「人性」弱點的攻擊手法，千萬不可掉以輕心，時時都須將資安意識放在心裡！

社交工程所造成的資安事件層出不窮，釣魚攻擊手法時時翻新，身處危機當中的我們，務必提醒自己小心防範。

# 改善及策進作為

1. **定期執行病毒碼更新與資安監控**，以維護資安防護有效性。
2. **不開啟來路不明之郵件**，以免遭社交工程攻擊。
3. 若已點開可疑的電子郵件後，**切勿直接下載或開啟附加檔**，也不隨意點擊郵件中夾帶的網址連結。
4. **不安裝來路不明的軟體、不瀏覽不明網站**，遇可疑訊息或信件請先查證。

# 改善及策進作為

5. 如不慎開啟了惡意郵件的附加檔，務必**利用防毒軟體**掃除植入電腦的惡意程式。
6. 如與對方不相識且未曾聯繫，以電子郵件進行交流時，請先行確認對方有寄出信件後再開啟，並**避免將郵件帳號提供給無關人員**。
7. 提醒**系統委外維護廠商強化**及重視自身**資安作為**，並嚴禁私設遠端維護機制。

# 資料來源：


1. 清流月刊-中華民國106年5月號「資安木馬屠城記—論社交工程與APT駭客攻擊手法」
   https://www.mjib.gov.tw/FileUploads/eBooks/1c6ffab1dc9e4209be994652f934bab7/Section_file/8fed11b510d9465ea3e996e065f00dae.pdf

2. 桃園市政府都市發展局政風室-「請注意防範社交工程攻擊」
   https://urdb.tycg.gov.tw/home.jsp?id=107&parentpath=0,2,103&mcustomize=onemessages_view.jsp&dataserno=201406130002&aplistdn=ou=data,ou=ethicsclass,ou=chdevelopment,ou=ap_root,o=tycg,c=tw&toolsflag=Y


——花蓮縣政府政風處關心您！