# 選舉將屆小心電子郵件遭駭客社交攻擊

因選舉將屆，犯罪集團經常會冒用各政黨、新聞媒體等單位人員名義，以聳動標題與選舉有關之電子郵件，吸引收件者點選相關內容，如「候選人〇〇〇買票即將遭調查」、「FW：〇〇〇特別費案爆發」等，藉以寄送含有惡意程式之電子郵件予不特定之民眾，達到社交攻擊，入侵及掌控被害者電腦系統之目的，若點選郵件中之連結或附加檔案，將致使企業組織、政府機關有被植入惡意程式，並進而遭竊取機密資料之風險。

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。

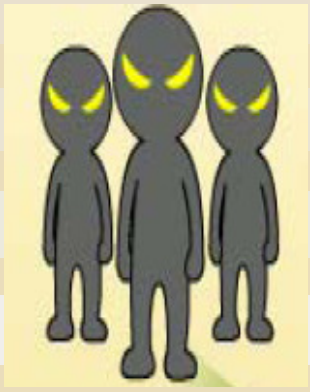
電子郵件社交工程四大類型：

一、假冒寄件者。

二、使用讓人感興趣的主旨與內文。

三、含有惡意程式的附件。

四、利用零時差攻擊。



多想三秒鐘，避開社交工程

臺灣屏東監獄

資訊安全執行小組 提醒您！