Hackers are ready, Are you?

# APEXSYS 電子郵件社交工程演練系統

電子郵件散佈力非常驚人，而駭客們利用惡意郵件，攻破使用者心防
即可輕易竊取各式重要資料，造成政府機關、企業或個人極大的安全威脅與損失！

而電子郵件可夾帶各式文字、影片、圖檔、壓縮檔、Office 文件… 已成為傳送資訊之主要工具，駭客也藉此寄發八卦、情色、科技、保健、娛樂、新知…含有惡意目的之郵件，誘騙使用者開啟、進而安裝木馬程式！

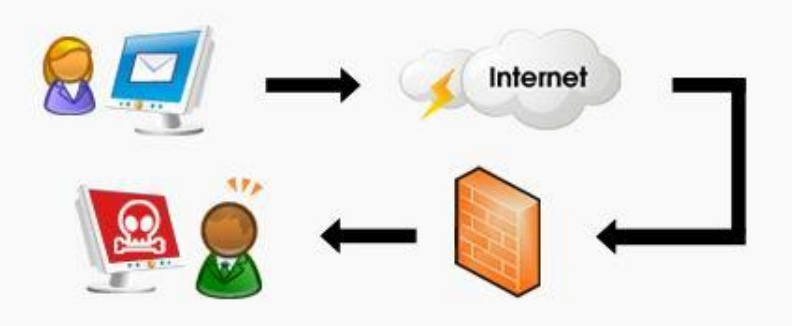
駭客之入侵手法，已由過去之盲目攻擊，轉為可鎖定特殊目標之方式。而此種手法，即使具備高階防火牆或防毒閘道器，也無法完全阻擋駭客威脅！

## 演練目的：

- **提昇使用者對郵件入侵手法的警覺性**
- **避免使用者因開啟惡意郵件，影響網路安全、發生個資洩漏事件**
- **強化使用者之資安意識，檢驗宣導社交工程防治之成效**
- **演練結果可成為導入 ISMS 時，對 MAIL SERVER 之風險評估**

## 惡意郵件攻擊模式：

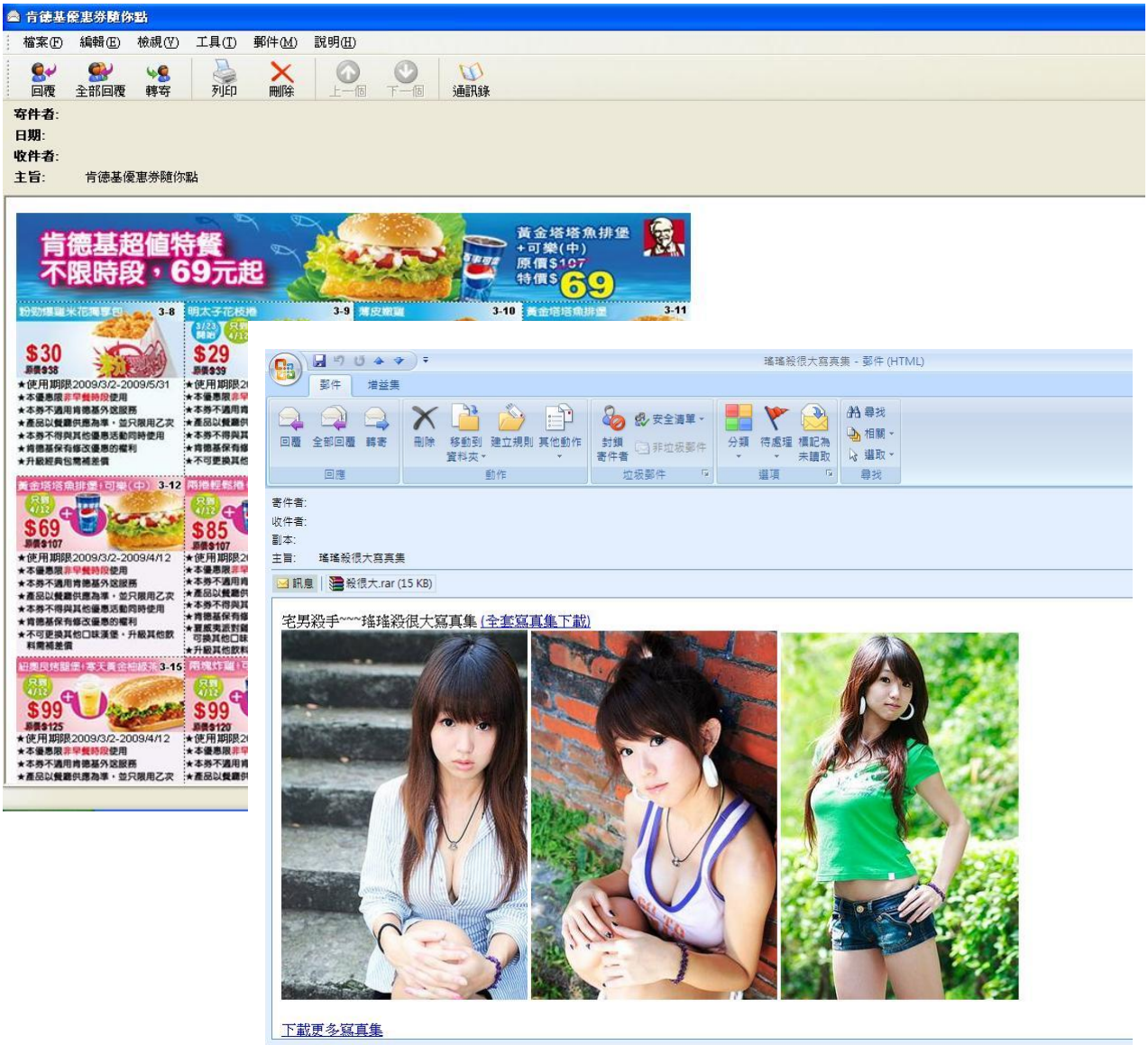
1- 駭客設計攻擊陷阱程式
(特殊檔案或惡意連結)
2- 將攻擊程式置入電子郵件
3- 寄發電郵給特定目標使用者
4- 使用者開啟郵件、啟動陷阱
5- 使用者電腦被植入後門程式
6- 後門程式逆向連接、向遠端駭客報到




## 社交工程演練流程：

## 系統優勢：

＊產出中文化報表，解讀無門檻
＊報表將計算開啟率、點選率，符合資通安全會報格式
＊可依單位需求，自行於系統調整演練內容
＊可依單位需求，自行設計攻擊電郵

＊可依單位需求，自行排定演練時間與頻率

## 惡意郵件範本：