電子郵件社交工程

一、何謂電子郵件社交工程

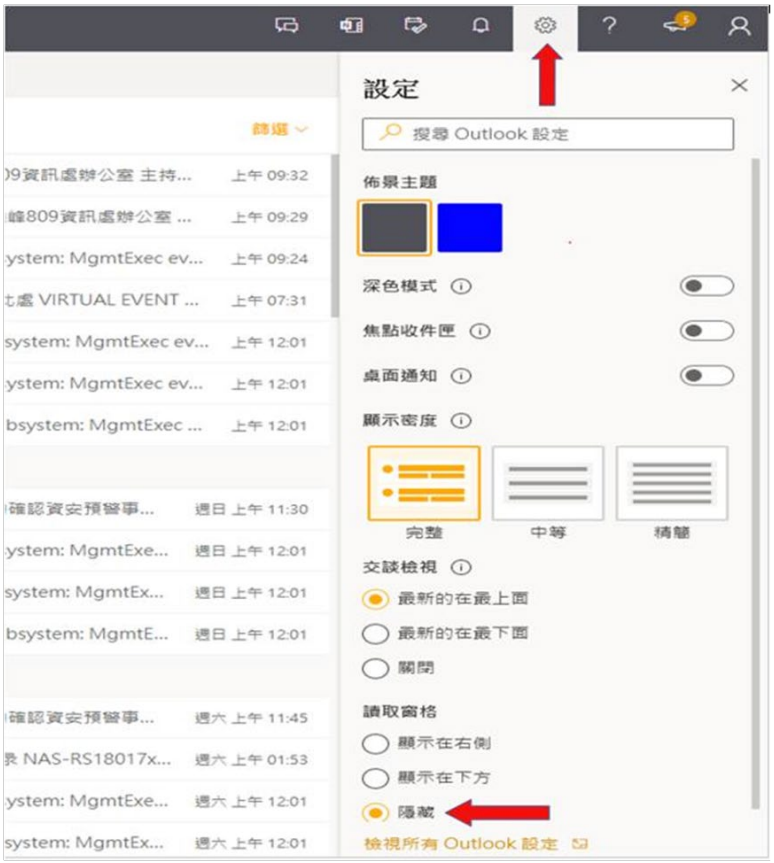
電子郵件社交工程 (Social Engineering) 係利用人性弱點， 引誘使用者開啟來路不明的惡意電子郵件，暗中進行不法情事，對資安危害極大。

二、常見的社交工程攻擊方式：

1.利用人類好奇的天性，誘騙使用者點擊惡意網站連結，以騙取帳號密碼。
2.誘騙使用者開啟檔案、圖片 ，以植入惡意程式、暗中收集機敏性資料。
3.利用提供工具、檔案、圖片為幌子，誘騙使用者下載，如偽裝的修補程式 、 p2p 下載軟體、工具軟體。
4.利用即時通訊軟體如 Line，偽裝親友來訊，誘騙點選來訊中之連結後中毒。

三、防範社交工程攻擊方式：
其實很簡單，**若收到任何不明來源信件一定一定一定不要隨便開啟，請立即依下列方式關閉郵件預覽功能，如不關閉收信後極易自動點閱，亦會中招，請立刻檢查您的設定是否如下:**

1. 若使用 ulive web 界面請依照下圖紅色箭頭關閉預覽功能，先按上方齒輪，再選下方隱藏，請參考附件圖示



2.若使用 outlook 請依照下列說明檔關閉預覽功能

如何關閉郵件預覽功能 outlook.pdf

四、台灣電腦網路危機處理暨協調中心(TWCERT/CC)相關社交工程教育影片

社交工程因應之道

https://www.youtube.com/watch?v=XNg8WNByShs

https://www.youtube.com/watch?v=YLHho7GsVwU