

防止電子郵件社交工程攻擊 收信軟體設定建議

電子郵件社交工程攻擊常利用好奇心、興趣來吸引使用者開啟信件，為避免不小心或是誤開啟此類信件，而被植入惡意或後門程式，為讓自己的電腦遠離危險，須調整自己的收信軟體設定，以增加安全性，「**不自動下載圖片**」、「**不開啟預覽視窗**」、「**以純文字開啟信件**」，可有效避免電子郵件社交工程型的攻擊，常見收信軟體之設定建議如下：

- [Apple iOS NEW](#)
- [Android Gmail app NEW](#)
- [Outlook 2007](#)
- [Outlook Express](#)
- [Live mail](#)

參考資料：

- [98年08月12日防範惡意電子郵件社交工程教育訓練投影片](#)
- [教育部98上半年度電子郵件社交工程演練結果說明](#)

-
- [更多防範網路詐騙資料\(See more\)](#)

From:

<https://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:

https://net.nthu.edu.tw/netsys/security:email_setup 

Last update: **2017/09/15 14:30**