防範惡意電子郵件社交工程 8 大步驟

1. 關閉"預覽信件"功能。

這是最重要的一步。使用 Windows Live Mail、Outlook Express 或本校 CIP 內 Web mail 的信件預覽功能，系統即認定為讀取信件。若 Outlook Express 本身弱點沒有修正，這有中毒的風險。高度建議關閉"預覽信件"功能。(請參閱: 資訊中心首頁 ->FAQ ->電子郵件類。
http://fs3.just.edu.tw/~cc/02_service/closeview/closeview2.pdf)

2. 來路不明的寄件者、不明的附件檔，請不要開啟，應立即刪除。

寄件人跟本不認識或很像認識的人，但跟之前寄來的名稱不一樣，請不要開啟，應立即刪除。來路不明的附件檔，亦請不要任意點開，以免中毒

3. 主旨太八卦，請不要開啟亦不要轉信，應立即刪除。

主旨太八卦，通常是吸引收信者開信，但這些多是垃圾郵件或惡意郵件。例如：網路上最好笑的一則笑話；如何提高中獎機率；昔日玉女紅星坦承吸毒；iPhone 便宜賣等。

4. 跟本身業務無關的信件，請不要開啟亦不要轉信，應立即刪除。

本校使用 E-mail 主要以傳遞收取公務相關使用，若跟本身業務無關的信件，請不要開啟亦不要轉信，應立即刪除。

5. 寄件者及主旨有符號、亂碼、怪字、一堆英文等，請不要開啟，應立即刪除。

主旨常有●、▼、☆、◆、■、↖或一堆英文等，通常是吸引收信者開信，但這些多是垃圾郵件或惡意郵件，請不要開啟，應立即刪除。

6. 仿冒信件，特別要小心。

由於電子郵件系統的特性，寄件者的名稱很容易被仿冒或偽裝。例如:偽裝政府機關或其它學校來信。這類的信件很難防範，只能小心判斷。若平時跟本沒有收過這類信件，忽然收到，通常就是有異，請不要開啟，應立即刪除。

7. 不要點擊信件內具有超連結內容的圖片或文字

另一個中毒的高度風險，即是你開啟不明信件後，又再點擊信件內的超連結。例如: 好康在這裡、取消訂閱請按此、第一銀行網站(但事實上不是連至第一銀行)等，這通常都不懷好意。請不要點擊

8. 不要任意解除外來圖片封鎖功能

外來圖片即是信件內的圖片由 internet 網路上某個 server(伺服器)提供的，而不是信件本身內嵌的。簡單來說，若你的電腦沒有接上網路，外來圖片就不會下載回來。這是最新的放毒方式，就是使用者主動下載惡意網站內容，導致中毒。Outlook express 及本校的 CIP Webmail 均會出現警告文字加以封鎖這種類型的圖片，對於不明的信件，請同仁留意不要任意按"解除"封鎖，並立即刪除此封信件。