

安全的開啓電子郵件的方式(簡國璋 撰稿)

教育部每學期都會施行「社交工程演練」，對各校關於電子郵件的資訊安全作檢測；如果同仁們開啓不明來源的信件，次數超過訂定的上限(惡意郵件開啓率需在 10%以下，惡意郵件點閱率需在 6%以下，點閱率是指信件開啓之後，又再點選信件內容中的連結，或開啓附件)，則該校必須針對這些特定使用者，進行加強管理，及事後律定具體的改善措施。往往總是有些同仁，不經意地點開(或是 Outlook 設定開啓閱讀窗格)，而讓教育部電算中心接收到不該點閱的訊息。

一個漫不經心的動作，可能使得您的個人電腦感染電腦病毒，或駭客刻意存入的後門程式，導致電腦裡的檔案損毀，或是機密資料外洩；在整個學校的網路環境中，一個人的電腦中毒，可能連帶導致其他人的電腦被攻擊；若後果嚴重，甚至會癱瘓掉整個網路。因為，我們是德明健康資訊環境內的生命共同體，確保團體成員安全地使用資訊相關設備，是每個人的責任。請大家共同維護校園內的資訊安全，並配合教育部的「社交工程演練」，關閉郵件預覽功能(預覽就等於是開啓信件)，以免信件一經寄達，即被開啓，使得其內含的惡意內容，立即被執行；若是這樣，您的麻煩就大了，因為您的電腦就被惡意入侵了。

為避免誤開惡意電子郵件，簡易的判斷方式如下：

- 一、凡校內同仁寄出的郵件，在寄件者處都會出現中文姓名；所以一旦出現英文的寄件者，除非是您已確認為安全的來源，否則請將其列入不明來源。
- 二、「好奇心殺死一隻貓！」，惡意郵件常偽裝成一般人有興趣或是聳動的標題，如：時事、新聞、八卦、購物、優惠卷...等，吸引好奇的人開啓。

不明來源的信件，若經判斷為不重要的信，基於安全著想，請即刻刪除；若是不確定是否不重要，可依以下方式處理：

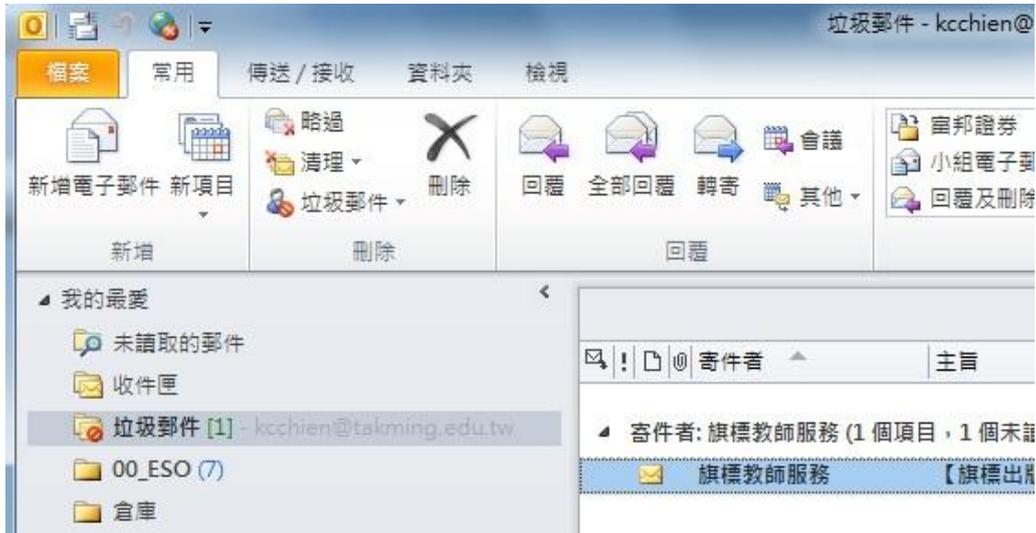
1. 在資料夾中選取不明來源信件，如下圖所示。



2. 將不明來源信件拖曳至「垃圾郵件」資料夾中，如下圖所示。



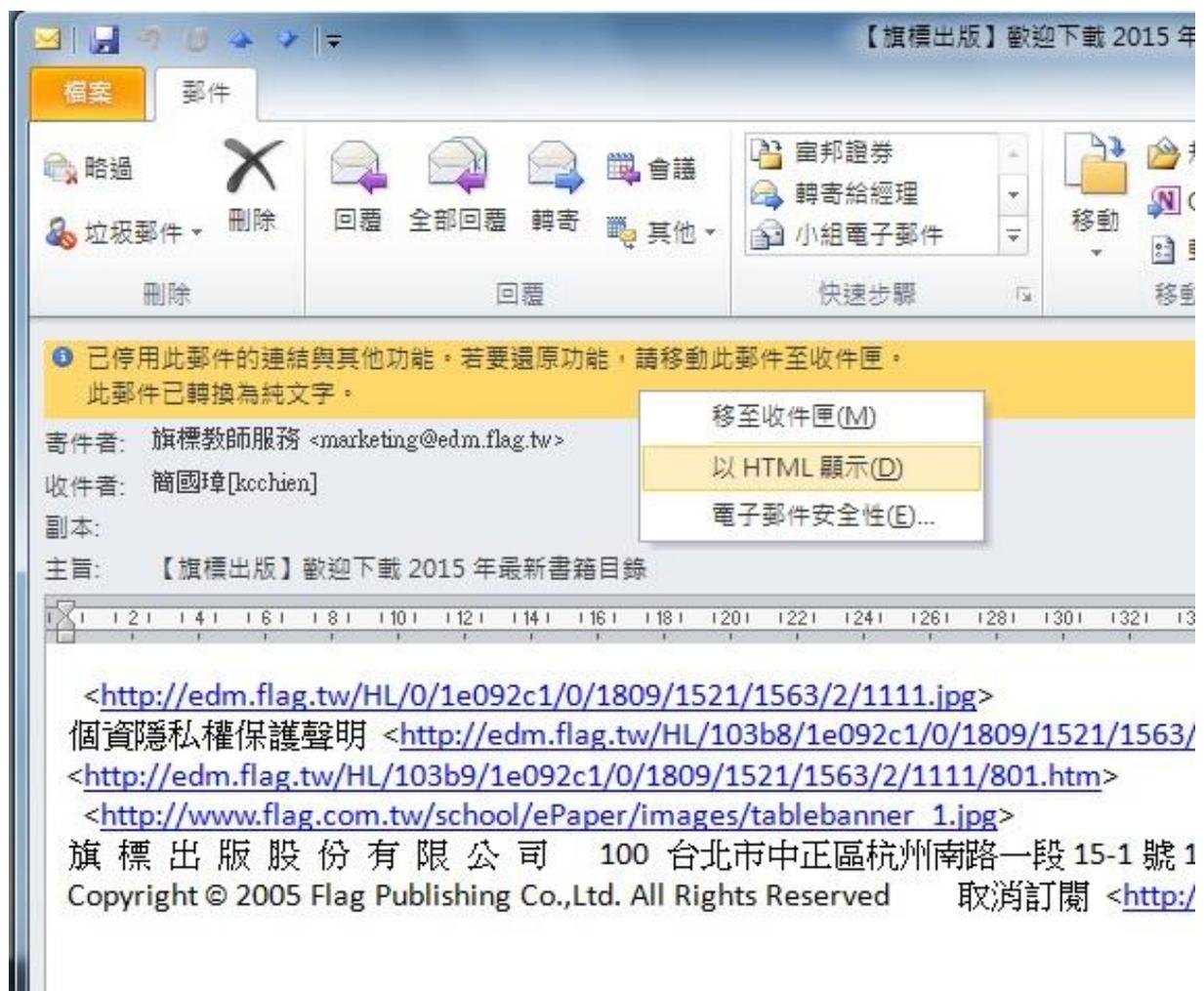
3. 到「垃圾郵件」資料夾中，點選該不明來源信件，如下圖所示。



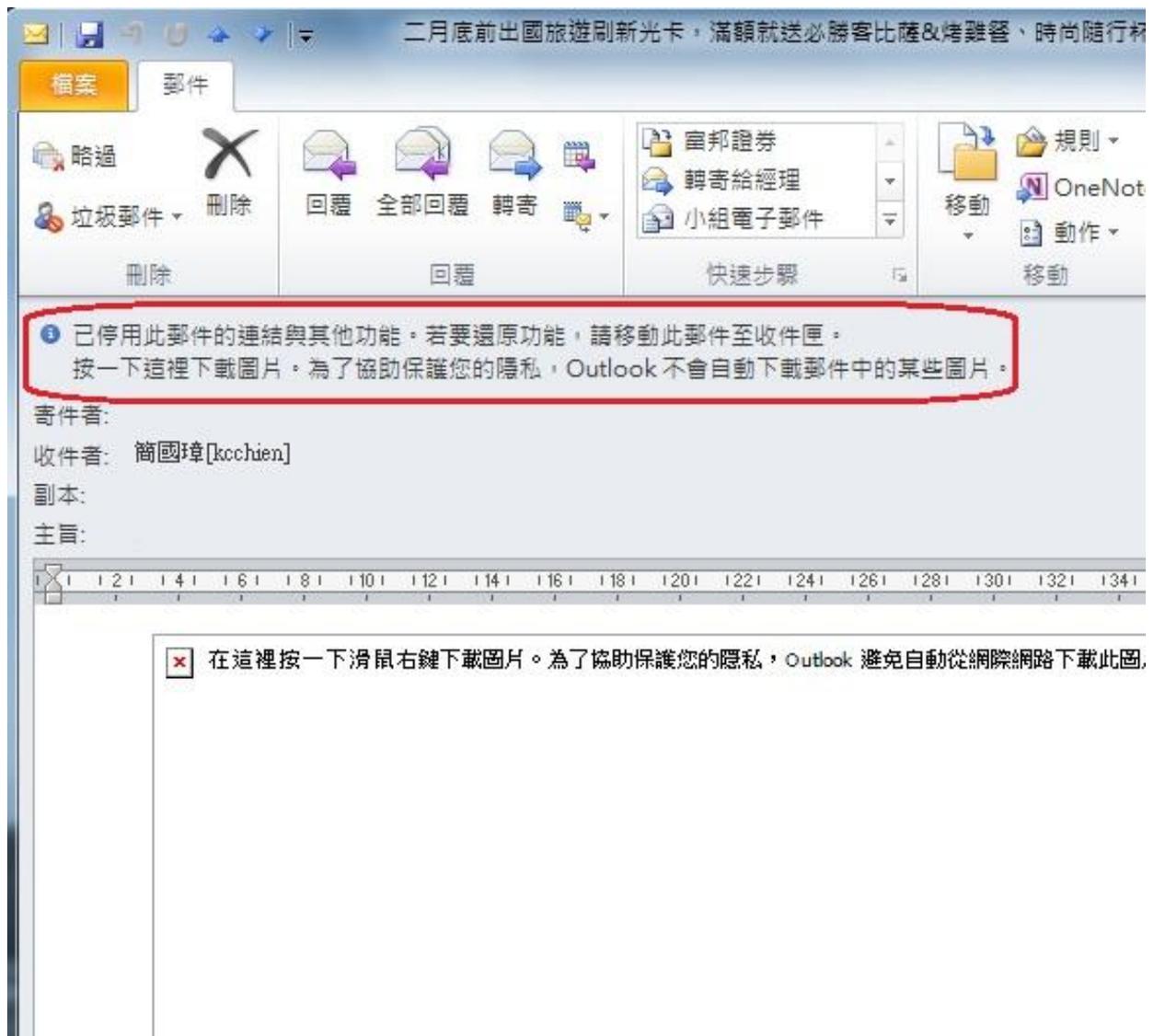
4. 在「垃圾郵件」資料夾中的信件，預設的開啓行動會先以「純文字」格式開啓，因此不會自動執行惡意的程式或連結，如下圖所示。



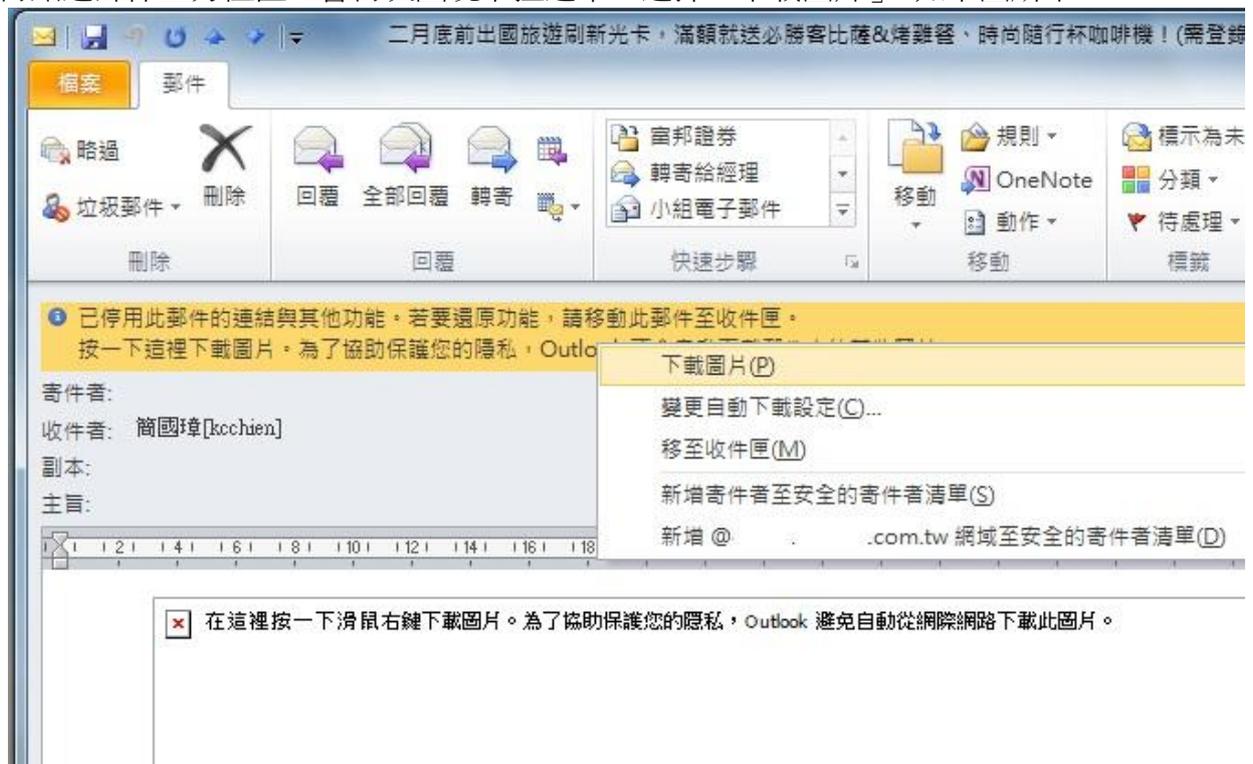
5. 在純文字郵件中，如果檢查確認為安全的信件，想以原網頁格式開啓，可點選信件上方的「已停用此郵件的廉潔與其他功能。若要還原功能，請移動此郵件至收件匣，此郵件已轉換為純文字。」，則會出現下拉選單，請選擇「以 HTML 顯示」，如下圖所示。



6. 此時信件會呈現網頁格式，但是為安全起見，尚且不會下載圖片，如下圖所示。



7. 再點選郵件上方位置，會再次出現下拉選單，選擇「下載圖片」，如下圖所示。



8. 完成後，信件則會完整呈現原來的面貌。