社交工程防護教學

一、何謂「社交工程」?

社交工程(Social Engineering)為利用人性的弱點進行詐騙，是一種非”全面”技術性的資訊安全攻擊方式，藉由人際關係的互動進行犯罪行為。駭客通常由電話、Email或是假扮身份，問些看似無關緊要的問題來進行社交工程。

二、最常見的社交工程手法

1. 釣魚電子郵件
   利用的郵件標題誘騙使用者開啟郵件的目的進而點選郵件內的網址或圖片。如：八卦、情色、健康、旅遊、折扣、團購...等。

2. 各種IM軟體
   利用已被入侵的電腦，竊取使用者IM軟體帳號，並傳送惡意連結給使用者好友名單，利用假冒好友的身分誘騙使用者點擊傳送的連結。
   如：MSN、YAHOO…等。

3. 假冒資訊設備廠商
   製作假的識別證，選其承辦負責人不在或離開時，假冒工程人員至重要資訊設備前操作並植入木馬或病毒達到入侵手段。

4. 電話
   利用各項可輕易查詢的公開資訊，去電騙取其他更多的資訊，最終使決行人員相信並失去戒心以達到目的。

三、釣魚電子郵件預防方法

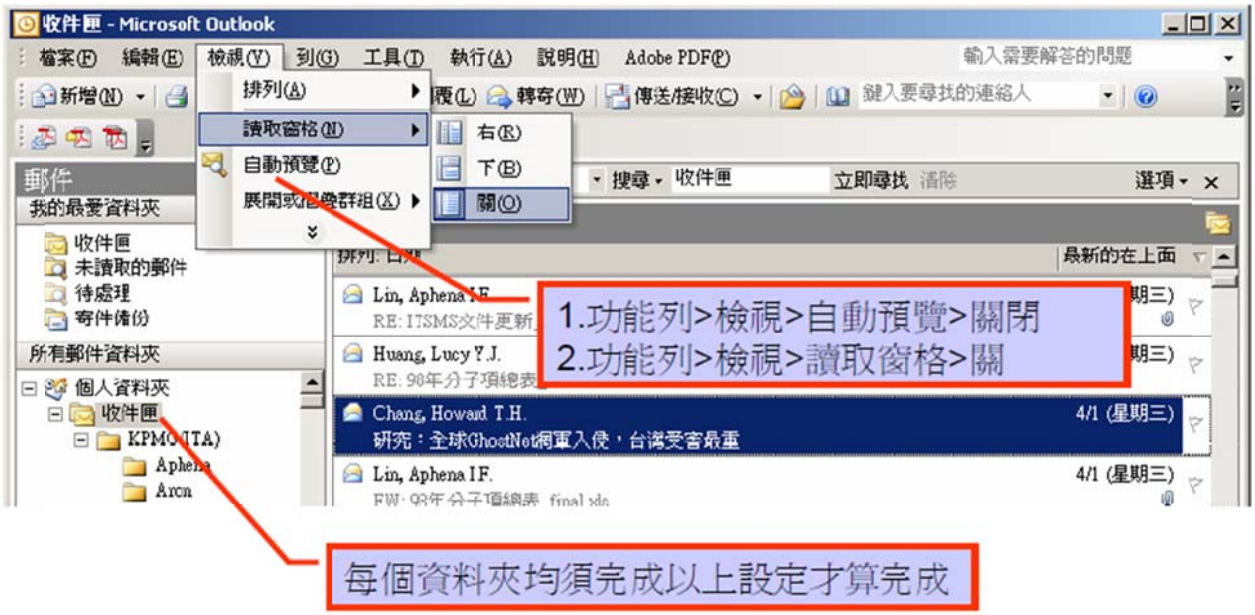
1. 使用者對於可疑的電子郵件應提高警覺，不點選寄件者不明的郵件。
2. 確認郵件主旨是否與本身業務相關，並判定是否可直接刪除。
3. 若無法確認，可打電話詢問寄件者。
4. 可判定與業務無關的信件直接刪除。
5. 使用OUTLOOK內安全性設定，如：不自動下載HTML圖片、關閉自動預覽、以純文字模式開啟郵件。
6. 不回覆來源不明之郵件。
7. 區分公司及個人使用之信箱。
8. 不隨意留下郵件地址予他人。

四、Outlook2003郵件相關設定

(一) 關閉預覽設定說明。

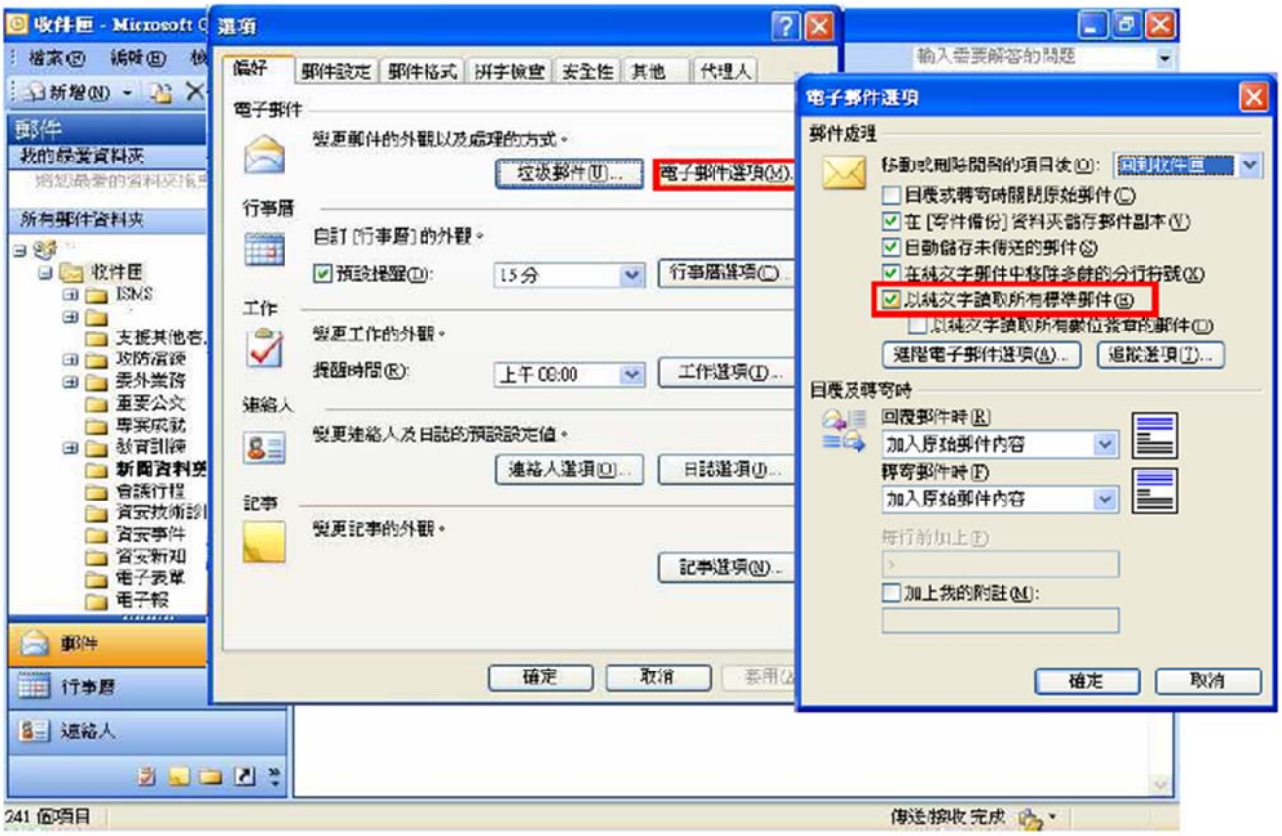
1. 功能列→檢視→自動預覽→關閉。
2. 功能列→檢視→讀取窗格→關閉。

※每個資料夾均須完成以上設定才算完成。



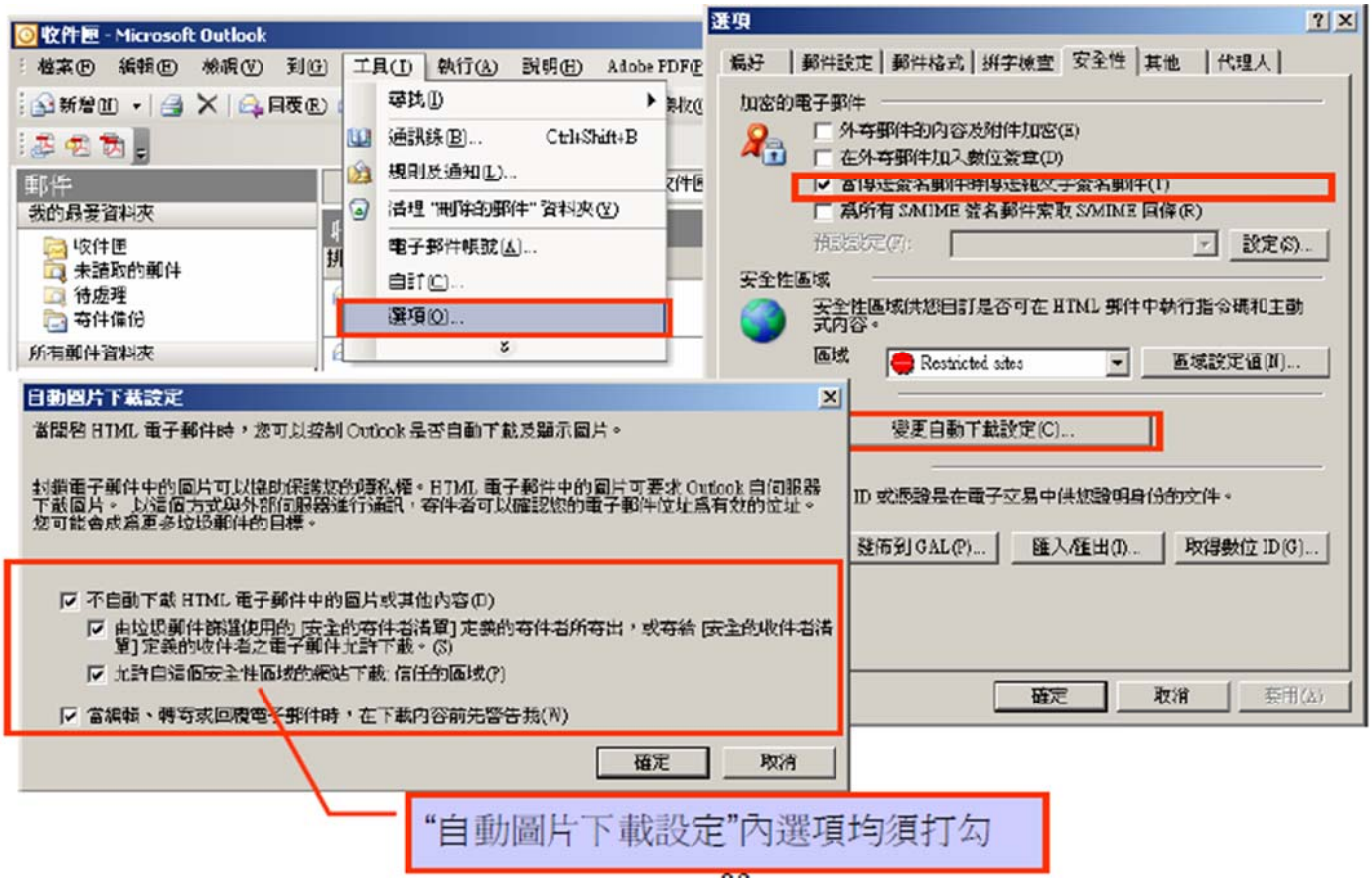
(二) 設定使用純文字模式。

1. 工具→選項→偏好→電子郵件選項→勾選”以純文字讀取所有標準郵件”。



(三) 設定關閉HTML圖片自動下載。

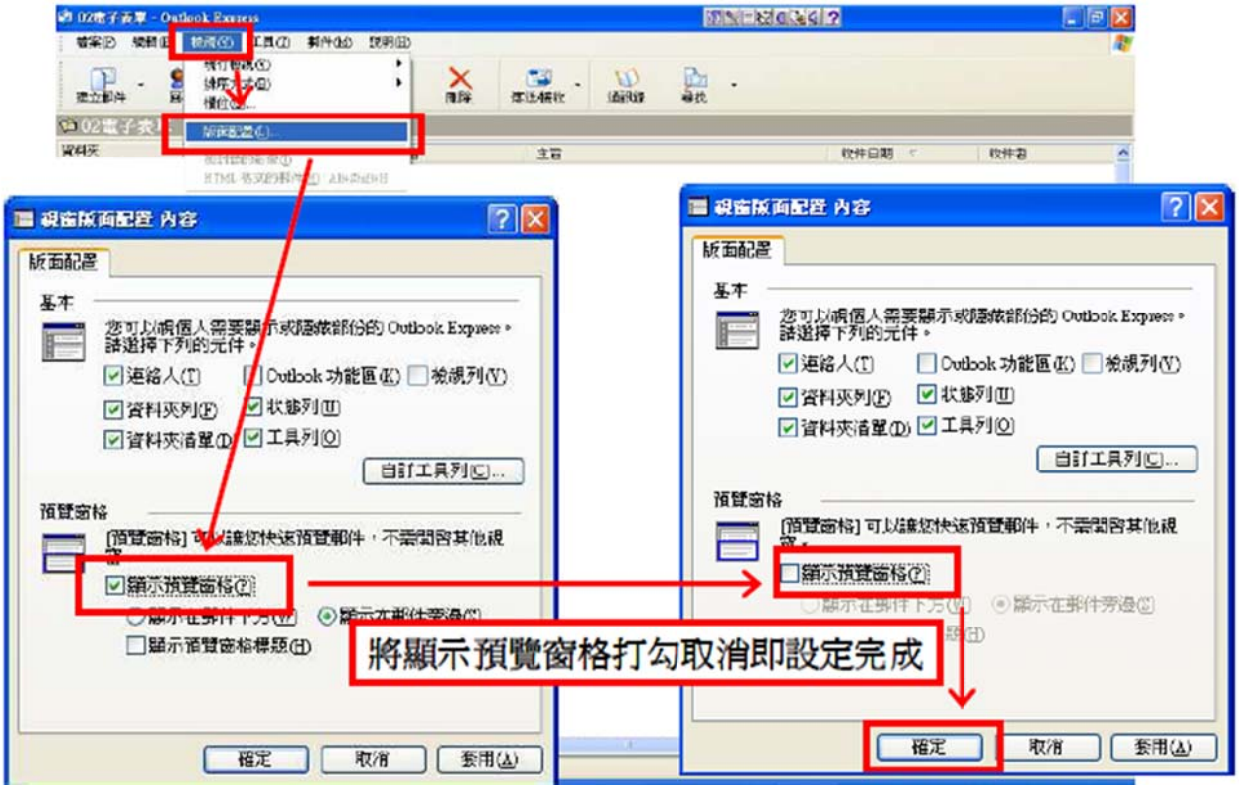
1. 工具→選項→安全性→勾選”當傳送簽名郵件時傳送純文字簽名郵件”
2. 變更自動下載設定→”自動下載圖片設定”內選項勻須打勾。



五、Outlook Express郵件相關設定

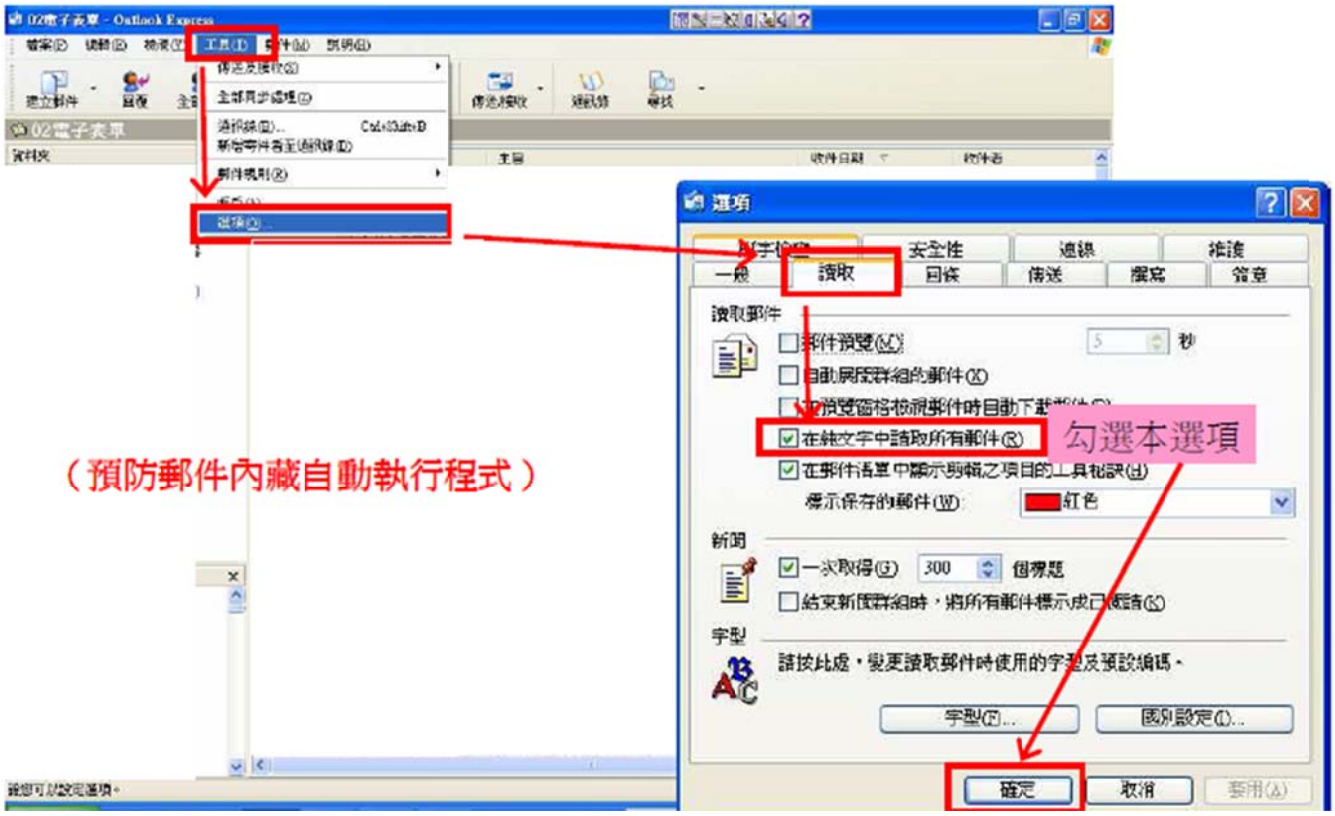
(一) 關閉預覽設定說明。

1. 檢視→版面配置→預覽窗格→取消勾選”顯示預覽窗格”→確定。



(二) 設定使用純文字模式。

1. 工具→選項→讀取→勾選”在純文字中讀取所有郵件”→確定。



(三) 設定關閉HTML圖片自動下載。

1. 工具→選項。
2. 安全性→勾選”阻擋HTML電子郵件中的圖片和其他外部內容”→確定。