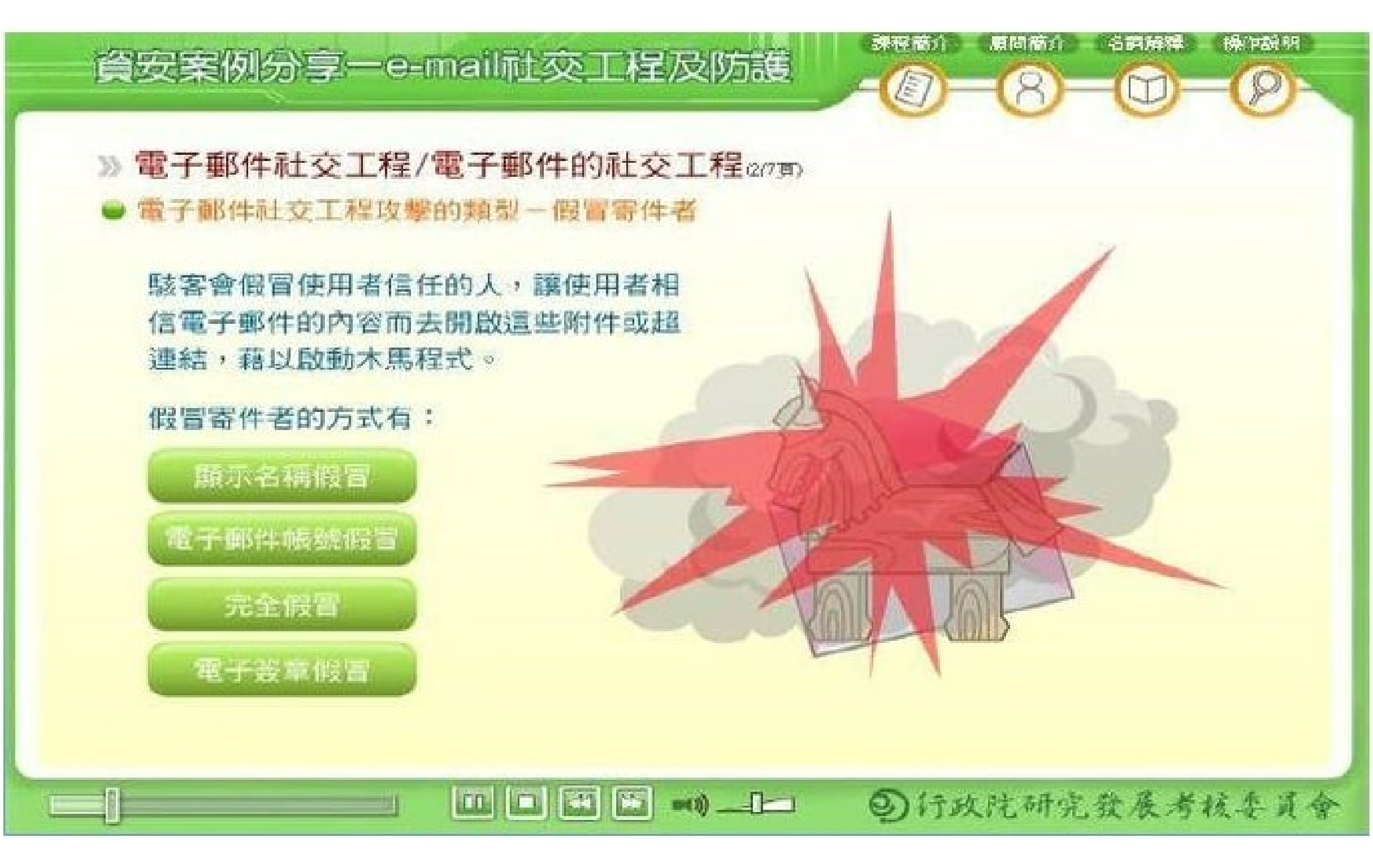
電子郵件社交工程手法

電子郵件社交工程手法

- 假冒寄件者
- 讓人感興趣的主旨或內文
- 帶有惡意內容
- 惡意附件
- 惡意JavaScript
- 惡意連結

假冒寄件者


資安案例分享—e-mail社交工程及防護
課程簡介
顧問簡介
名詞解釋
操作說明
行政院研究發展考核委員會

電子郵件社交工程/電子郵件的社交工程(2/7頁)

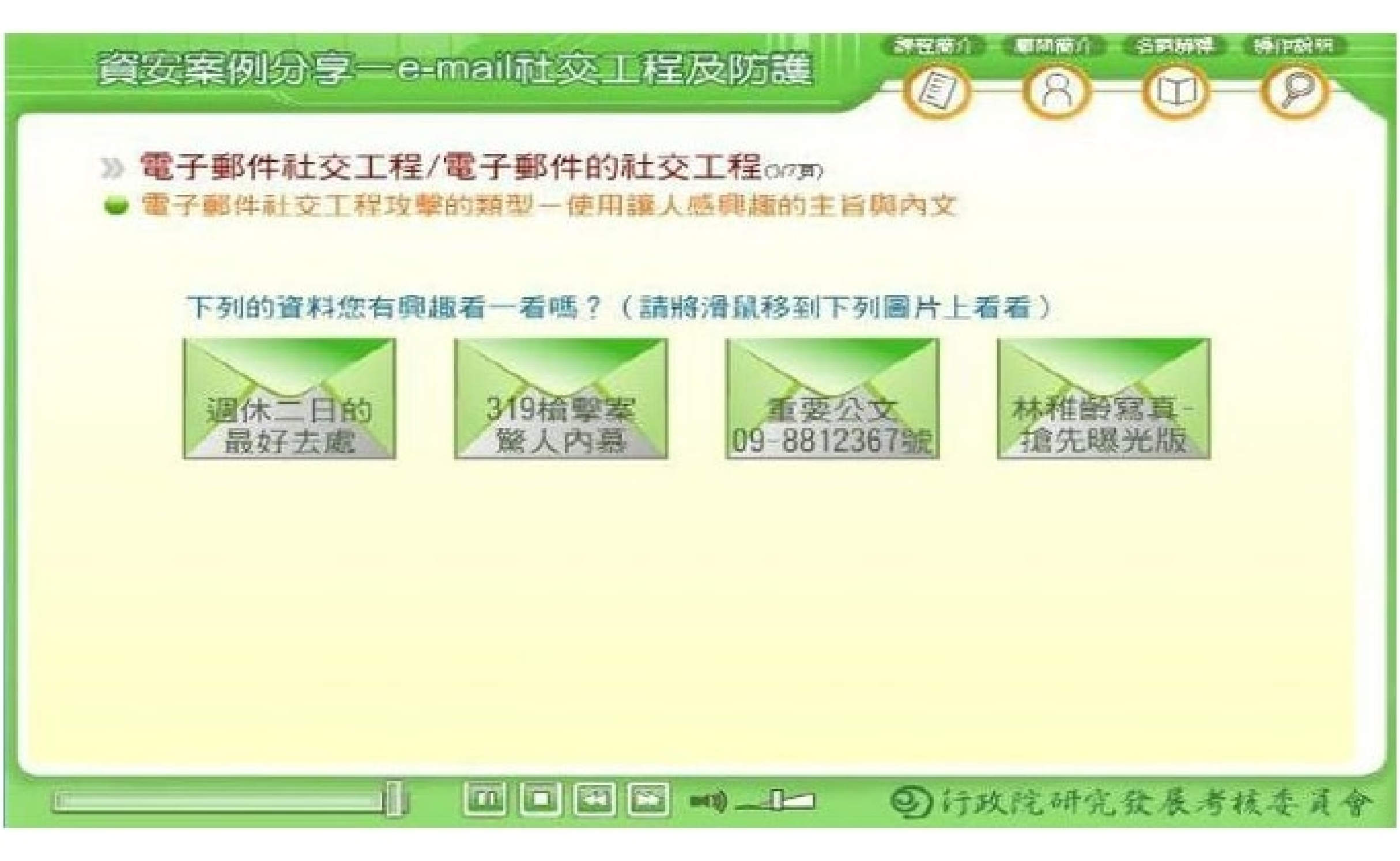
電子郵件社交工程攻擊的類型－假冒寄件者

駭客會假冒使用者信任的人，讓使用者相信電子郵件的內容而去開啟這些附件或超連結，藉以啟動木馬程式。

假冒寄件者的方式有：

顯示名稱假冒
電子郵件帳號假冒
完全假冒
電子簽章假冒

讓人感興趣的主旨或內文

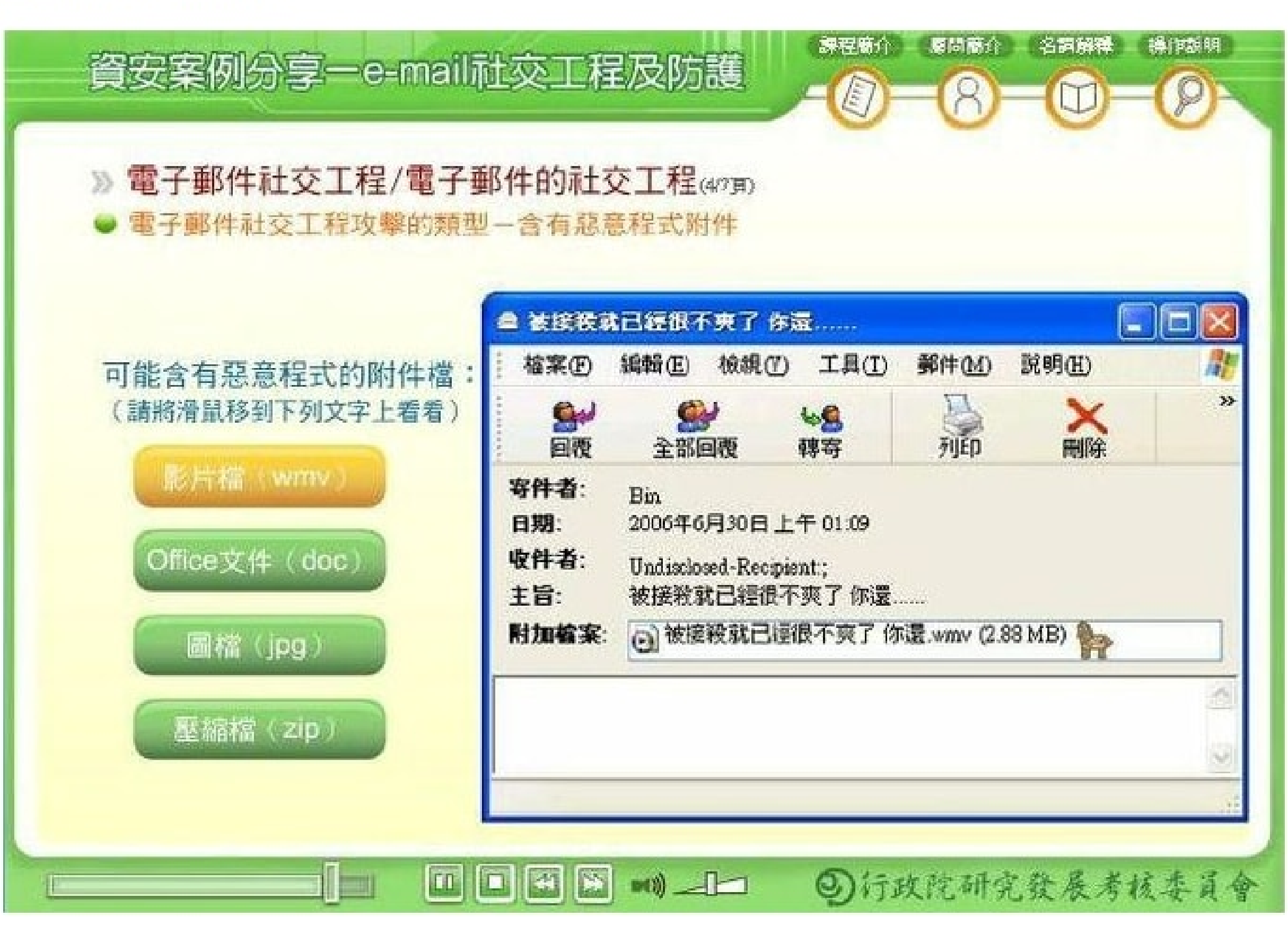

資安案例分享—e-mail社交工程及防護
課程簡介
顧問簡介
名詞解釋
操作說明
週休二日的最好去處
319槍擊案驚人內幕
重要公文09-8812367號
林稚齡寫真-搶先曝光版
行政院研究發展考核委員會

電子郵件社交工程/電子郵件的社交工程(3/7頁)

電子郵件社交工程攻擊的類型－使用讓人感興趣的主旨與內文

下列的資料您有興趣看一看嗎？（請將滑鼠移到下列圖片上看看）

含有惡意程式的附件


資安案例分享—e-mail社交工程及防護
課程簡介
顧問簡介
名詞解釋
操作說明
影片檔（wmv）
Office文件（doc）
圖檔（jpg）
壓縮檔（zip）
檔案(F)
編輯(E)
檢視(V)
工具(T)
郵件(M)
說明(H)
回覆
全部回覆
轉寄
列印
刪除
行政院研究發展考核委員會

電子郵件社交工程/電子郵件的社交工程(4/7頁)

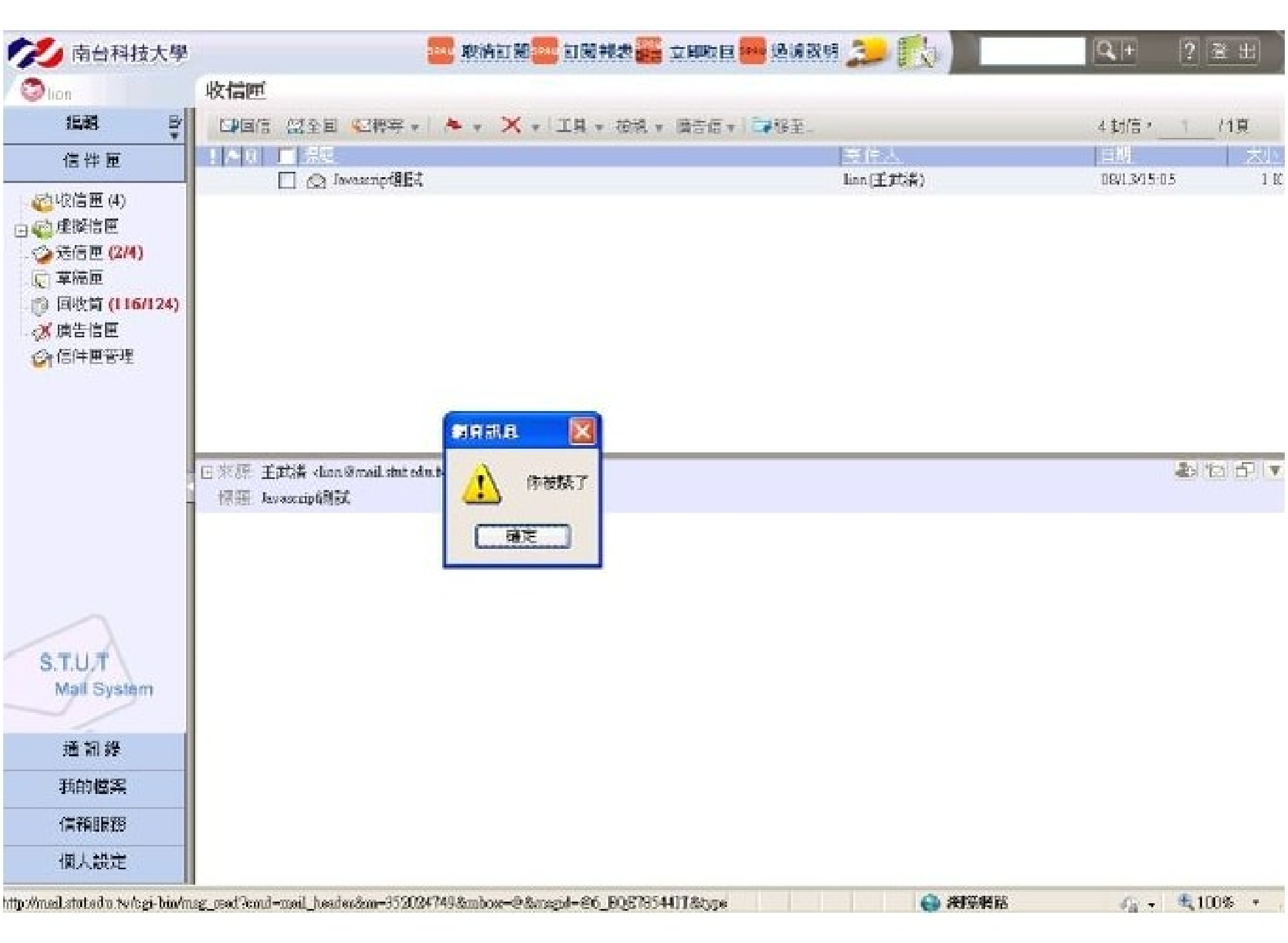
電子郵件社交工程攻擊的類型－含有惡意程式附件

可能含有惡意程式的附件檔：（請將滑鼠移到下列文字上看看）

被接殺就已經很不爽了 你還......

寄件者: Bin
日期: 2006年6月30日 上午 01:09
收件者: Undisclosed-Recipient:;
主旨: 被接殺就已經很不爽了 你還......
附加檔案: 被接殺就已經很不爽了 你還.wmv (2.88 MB)

含有惡意JavaScript


南台科技大學
收信匣
收信匣 (4)
送信匣 (2/4)
草稿匣
回收筒 (116/124)
廣告信匣
信件匣管理
S.T.U.T Mail System
通訊錄
我的檔案
信箱服務
個人設定
網頁訊息
確定

Javascript測試　lion(王武清)

你被騙了

網路釣魚-含有惡意連結

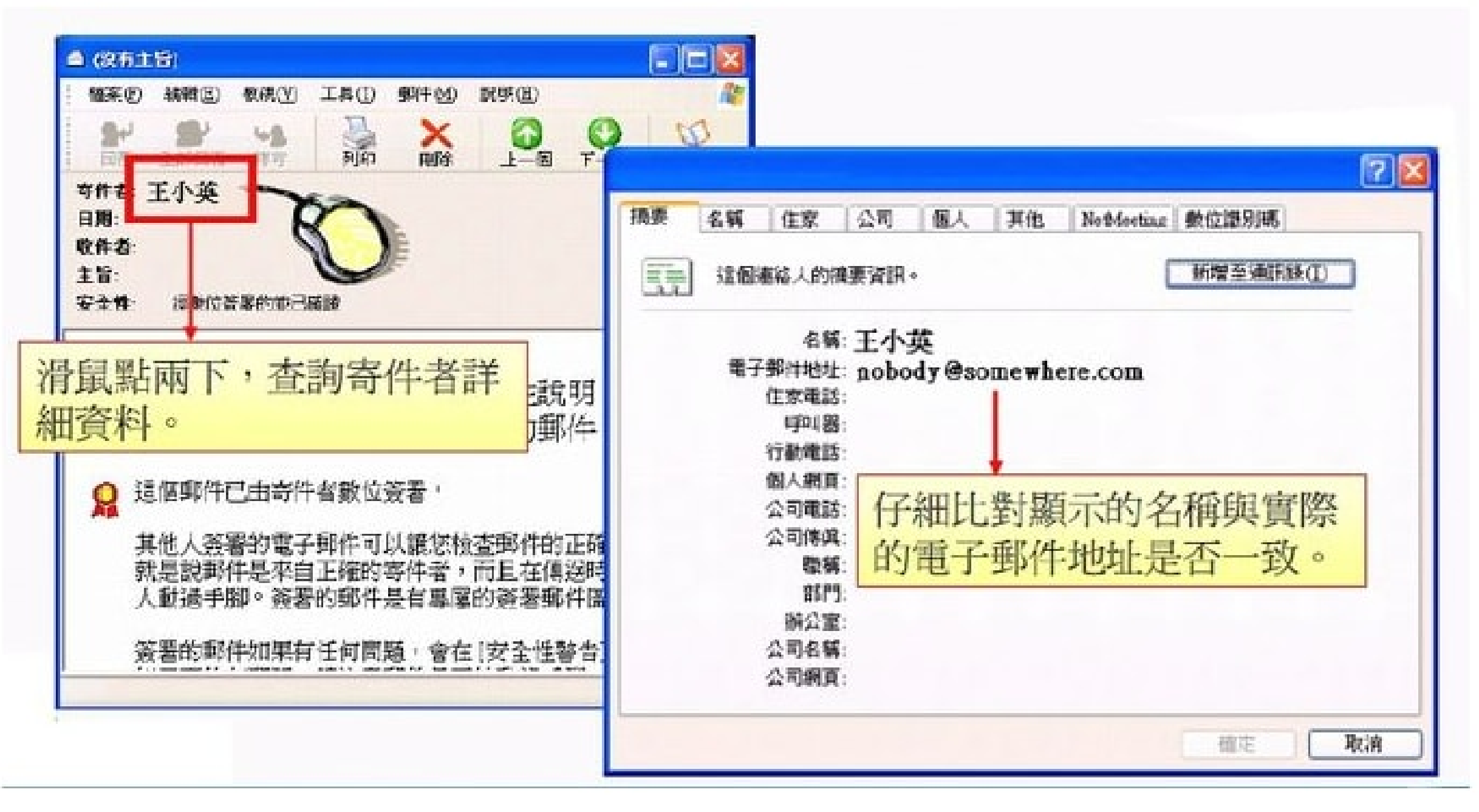
最常見的手法，是駭客架設幾乎與官方公司一模一樣的網站，再透過電子郵件告知使用者資料過期、無效需要更新，或者是基於安全理由進行身分驗證等的理由，騙取個人連線上假冒的網站，進而取得帳號與密碼。

電子郵件社交工之防護

電子郵件社交工之防護

- 分辨電子郵件的真偽
- 分析顯示名稱與電子郵件帳號，檢查寄件者是否正確
- 分析郵件主旨與附件
- 不開啟非公務相關的附件以及郵件
- 不開啟任何寄件者沒有事先知會的附件
- 不要顯示外部img
- 不要點選信件中的連結

檢查寄件者是否正確


(沒有主旨)
摘要
名稱
住家
公司
個人
其他
NetMeeting
數位識別碼
確定
取消

寄件者: 王小英

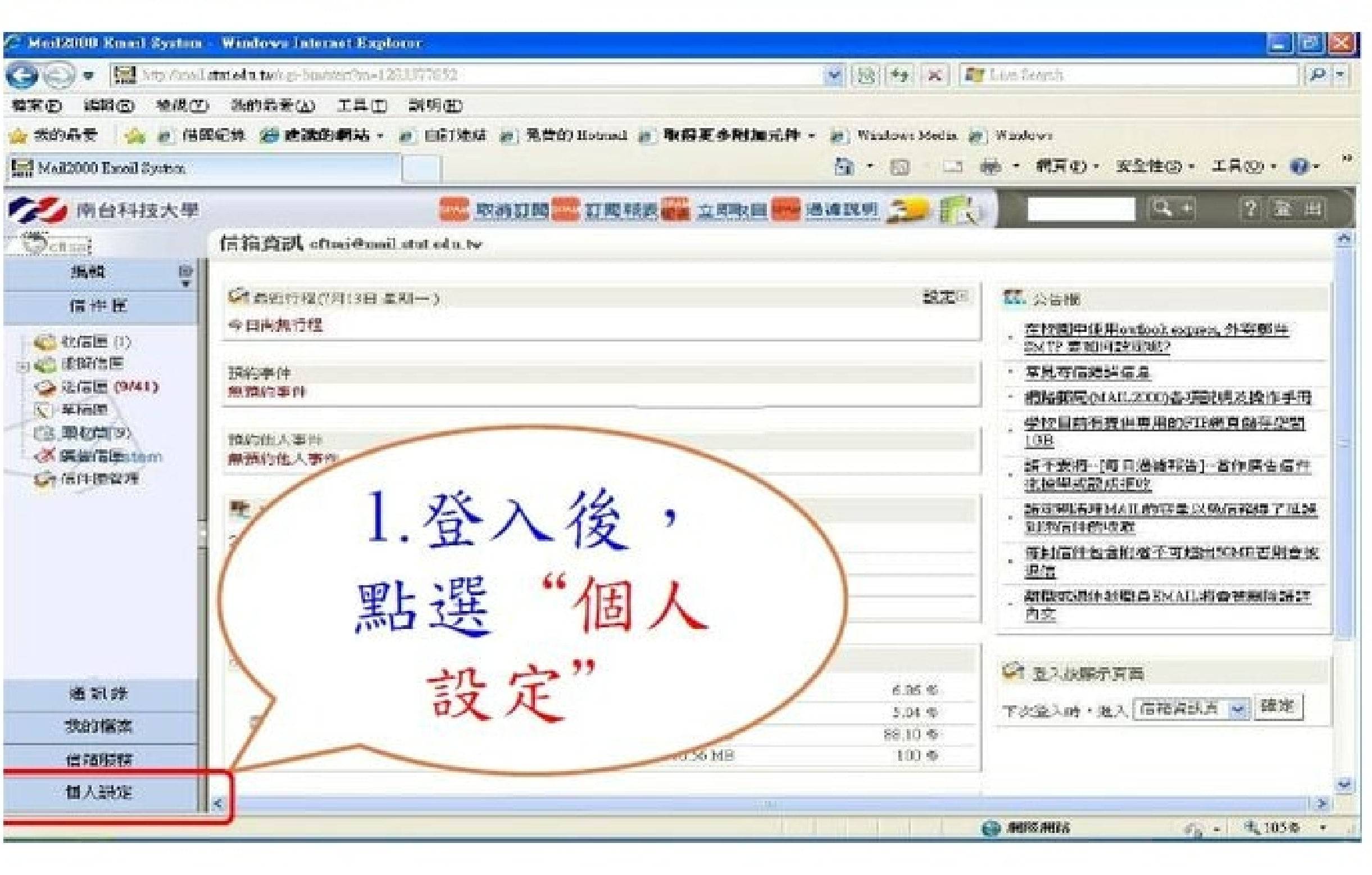
滑鼠點兩下，查詢寄件者詳細資料。

這個郵件已由寄件者數位簽署。

名稱: 王小英
電子郵件地址: nobody@somewhere.com

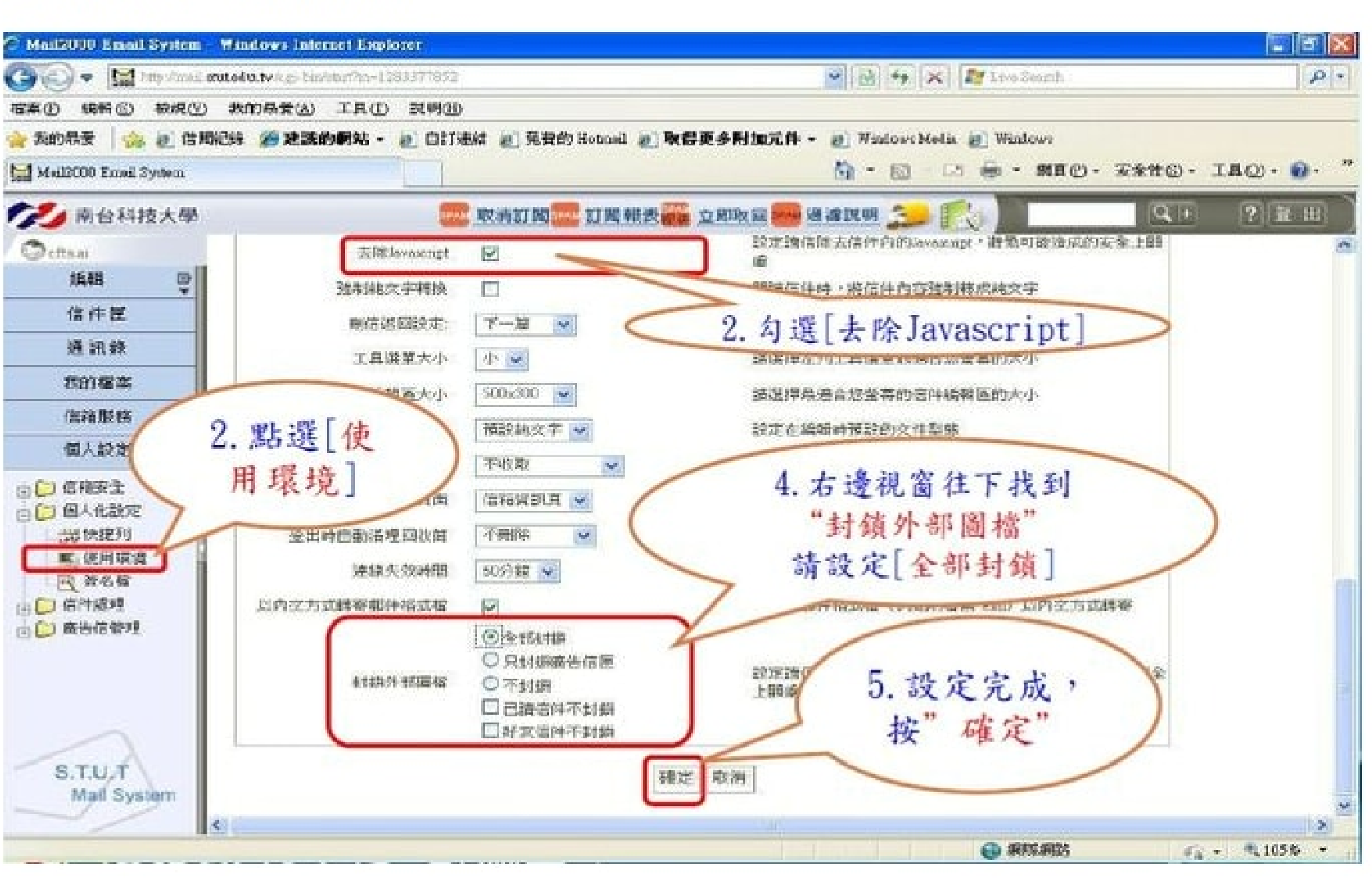
仔細比對顯示的名稱與實際的電子郵件地址是否一致。

Mail 2000之封鎖img設定(1)


Mail2000 Email System - Windows Internet Explorer
南台科技大學
信箱資訊
通訊錄
我的檔案
信箱服務
個人設定

1.登入後，點選“個人設定”

Mail 2000之封鎖img設定(2)


Mail2000 Email System - Windows Internet Explorer
南台科技大學
個人化設定
使用環境
去除Javascript
封鎖外部圖檔
確定
取消

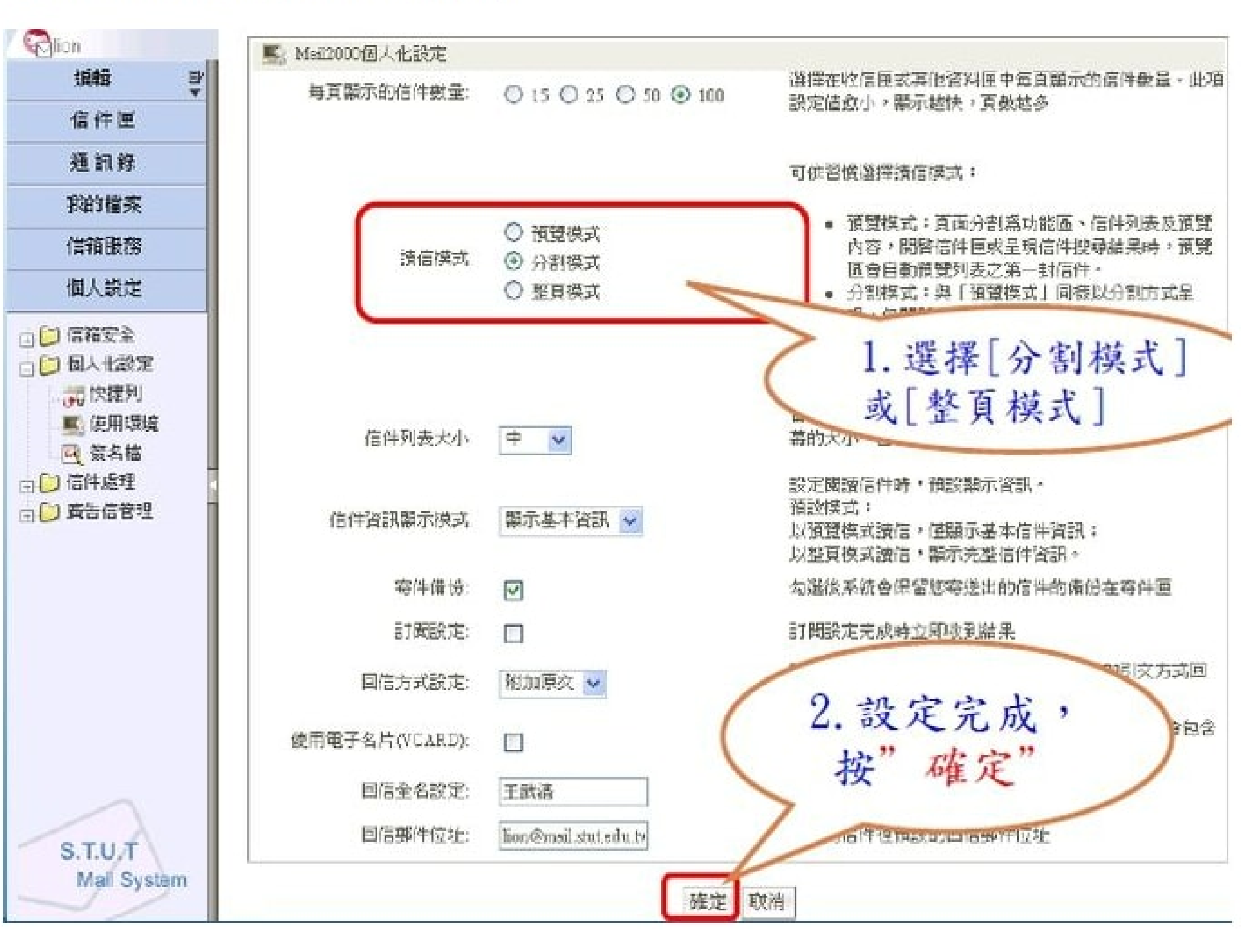
2.點選[使用環境]

2.勾選[去除Javascript]

4.右邊視窗往下找到“封鎖外部圖檔”請設定[全部封鎖]

5.設定完成，按”確定”

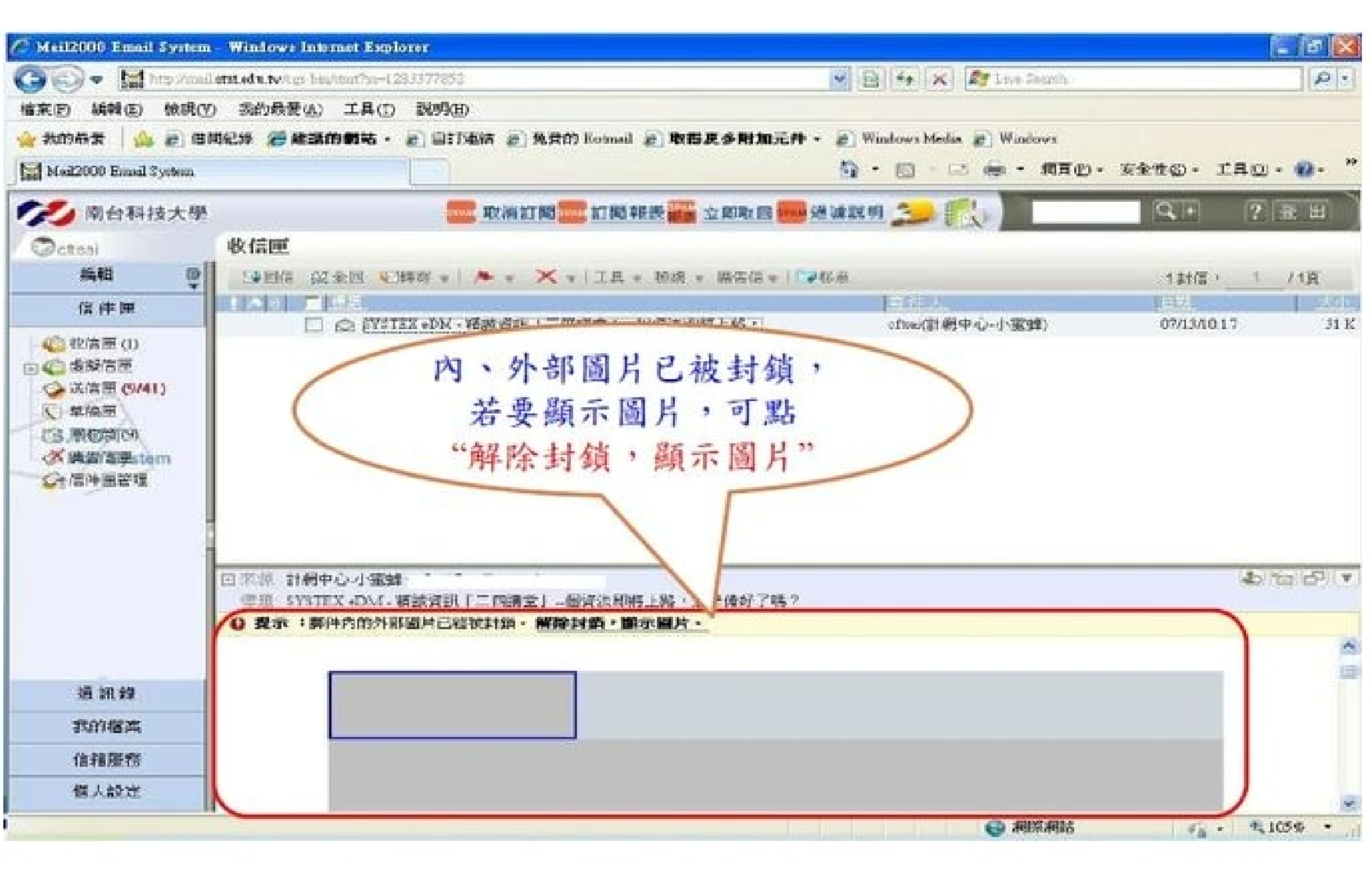
取消預覽-使用[分割模式]或[整頁模式](3)


Mail2000個人化設定
每頁顯示的信件數量
讀信模式
○ 預覽模式
● 分割模式
○ 整頁模式
信件列表大小
信件資訊顯示模式
寄件備份
訂閱設定
回信方式設定
使用電子名片(VCARD)
回信全名設定
回信郵件位址
確定
取消

1.選擇[分割模式]或[整頁模式]

2.設定完成，按”確定”

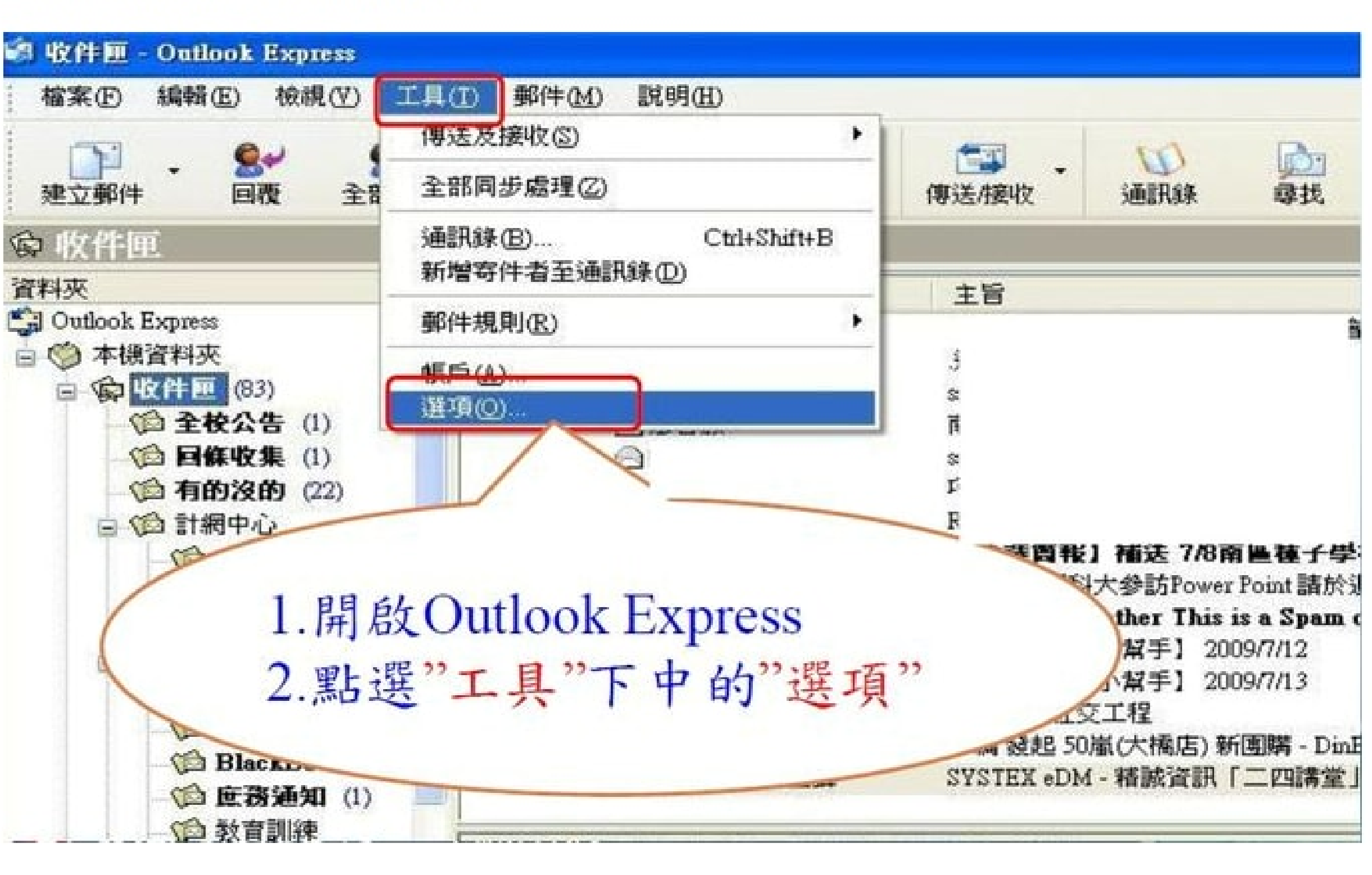
(結果) Mail 2000之封鎖img


Mail2000 Email System - Windows Internet Explorer
南台科技大學
收信匣

內、外部圖片已被封鎖，若要顯示圖片，可點“解除封鎖，顯示圖片”

提示：郵件內的外部圖片已經被封鎖。解除封鎖，顯示圖片。

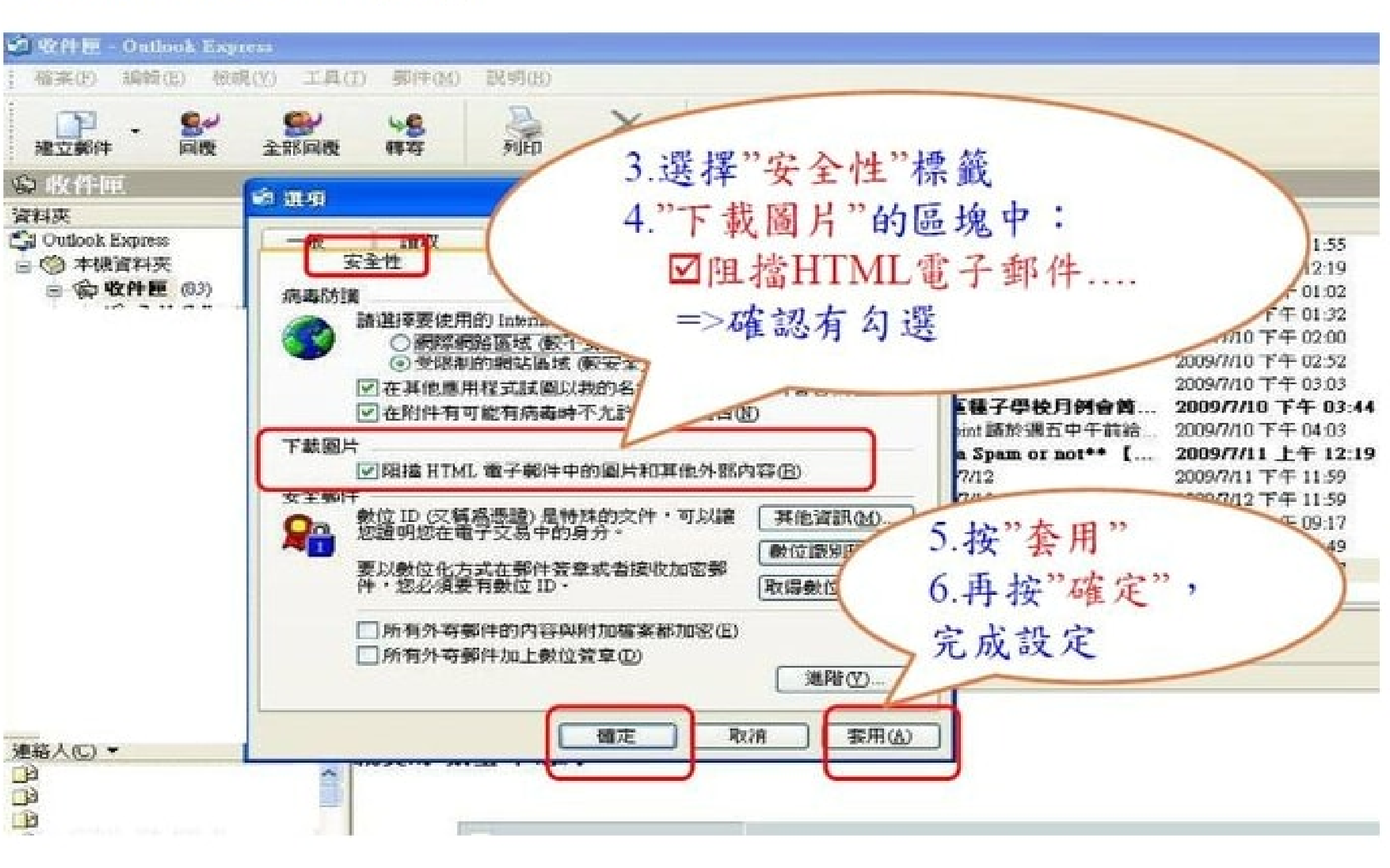
Outlook Express封鎖img設定(1)


收件匣 - Outlook Express
檔案(F)
編輯(E)
檢視(V)
工具(T)
郵件(M)
說明(H)
傳送及接收(S)
全部同步處理(Z)
通訊錄(B)... Ctrl+Shift+B
新增寄件者至通訊錄(D)
郵件規則(R)
帳戶(A)...
選項(O)...
建立郵件
回覆
傳送/接收
通訊錄
尋找

1.開啟Outlook Express

2.點選”工具”下中的”選項”

Outlook Express封鎖img設定(2)


收件匣 - Outlook Express
選項
安全性
病毒防護
下載圖片
☑ 阻擋 HTML 電子郵件中的圖片和其他外部內容(B)
安全郵件
確定
取消
套用(A)

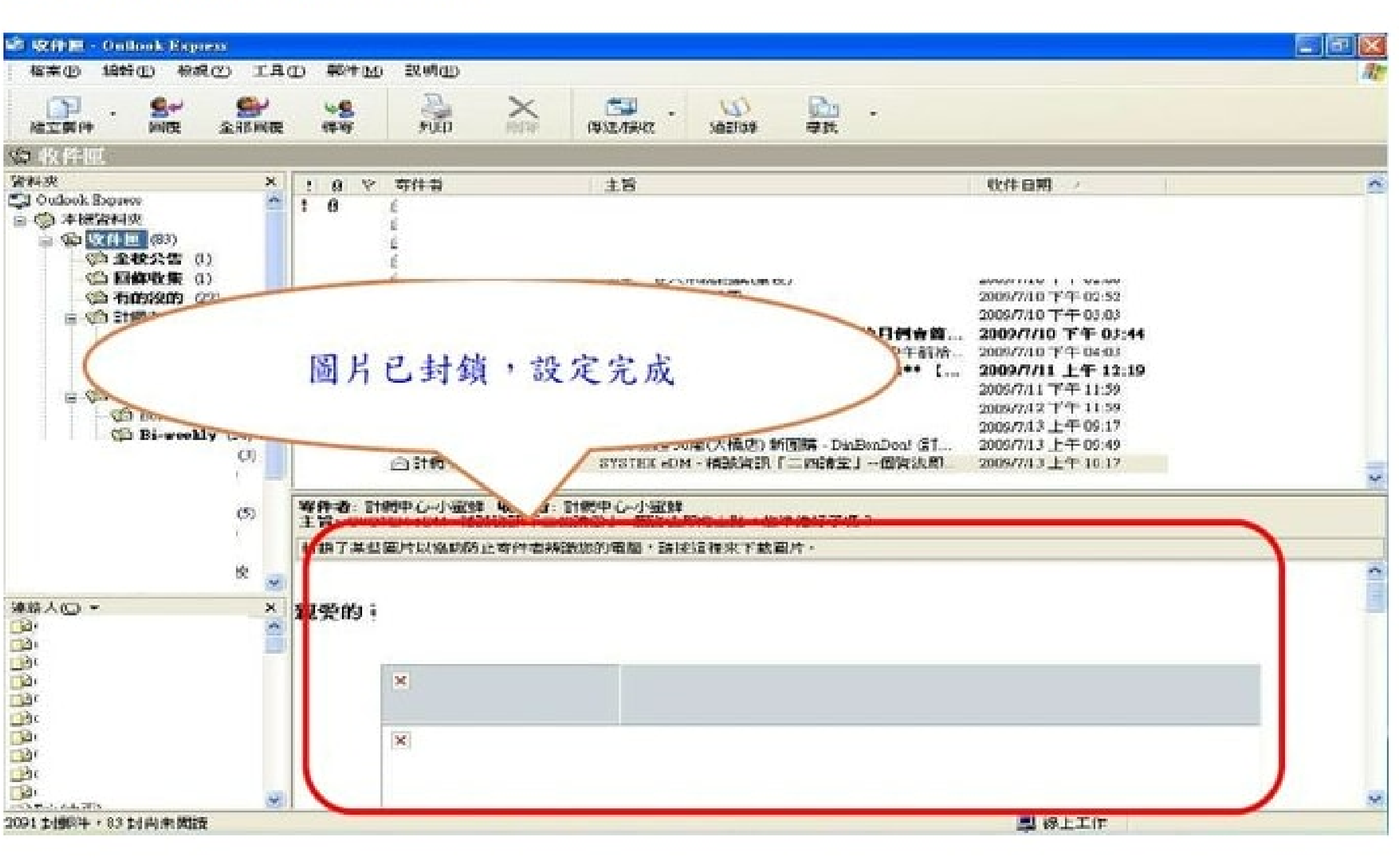
3.選擇”安全性”標籤

4.”下載圖片”的區塊中：☑阻擋HTML電子郵件....=>確認有勾選

5.按”套用”

6.再按”確定”，完成設定

(結果) Outlook Express封鎖img


收件匣 - Outlook Express

圖片已封鎖，設定完成

教育部年度演練計畫

教育部年度演練計畫

- 3~4月進行電子郵件社交工程教育訓練
- 5月進行上半年演練
- 6~8月針對上半年演練結果進行加強教育訓練
- 9月進行下半年演練
- 10月針對下半年演練結果進行加強教育訓練

演練目的

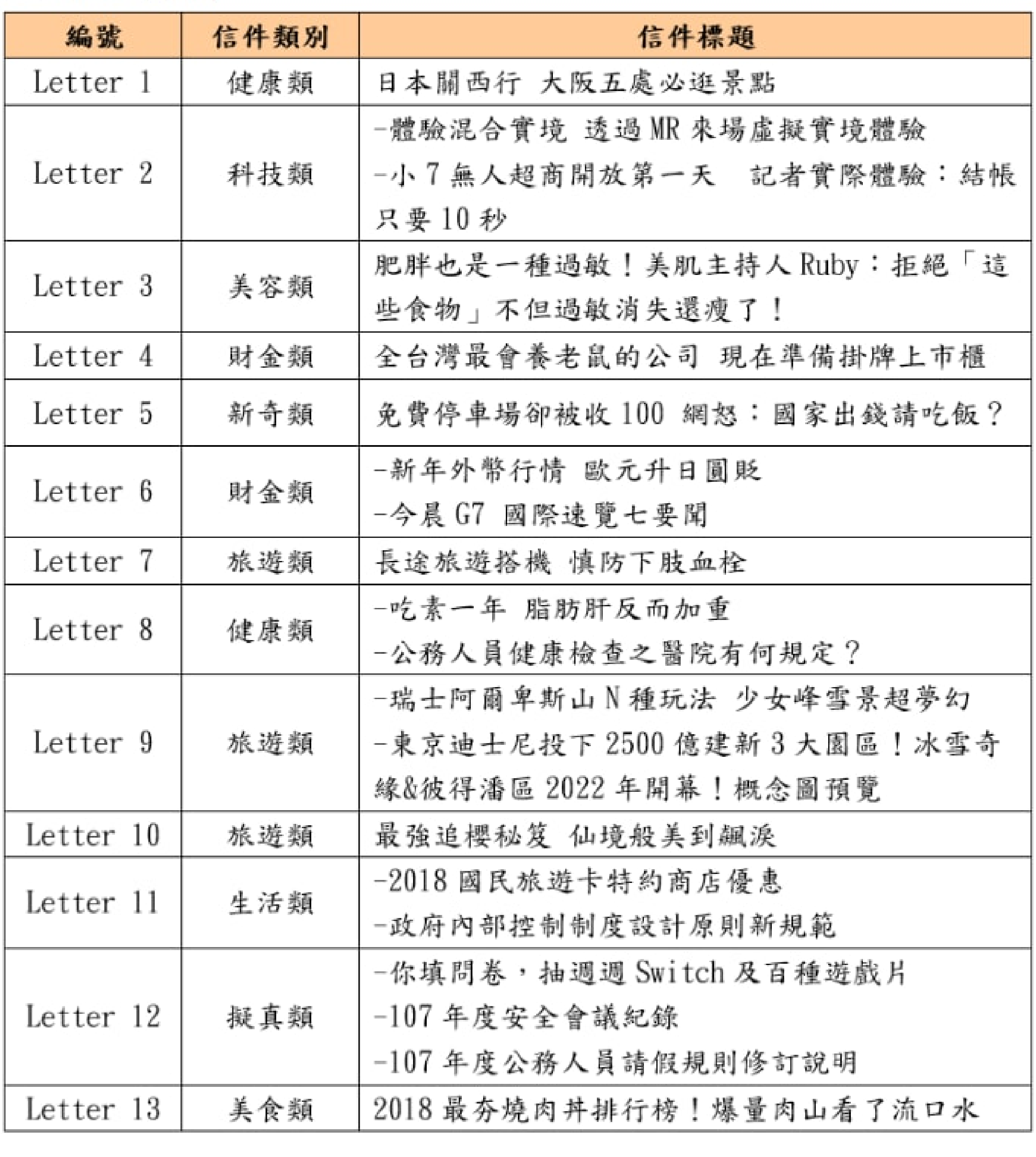
為提高教育機構教職員工警覺性以降低社交工程風險，本測試目的即是藉由模擬駭客寄送各種誘騙信件的手法，測試教職員點選各類誘騙信件的比率。以強化教育機構教職員對資安意識的落實與對社交工程等攻擊行為的資安警覺意識。

演練測試方式

針對每位受測人員寄發 5~10 封不同內容測試測試信件進行統計分析作業，統計受引誘而開啟信件或點選信件內之附件或網頁連結之數量及比率。

測試作業之測試信件寄件人名稱，均為偽造，用來測試受測人對寄件人名稱是否合理的辨識能力。

測試信件主題(範例)



編號	信件類別	信件標題
Letter 1	健康類	日本關西行 大阪五處必逛景點
Letter 2	科技類	-體驗混合實境 透過 MR 來場虛擬實境體驗 -小 7 無人超商開放第一天 記者實際體驗：結帳只要 10 秒
Letter 3	美容類	肥胖也是一種過敏！美肌主持人 Ruby：拒絕「這些食物」不但過敏消失還瘦了！
Letter 4	財金類	全台灣最會養老鼠的公司 現在準備掛牌上市櫃
Letter 5	新奇類	免費停車場卻被收 100 網怒：國家出錢請吃飯？
Letter 6	財金類	-新年外幣行情 歐元升日圓貶 -今晨 G7 國際速覽七要聞
Letter 7	旅遊類	長途旅遊搭機 慎防下肢血栓
Letter 8	健康類	-吃素一年 脂肪肝反而加重 -公務人員健康檢查之醫院有何規定？
Letter 9	旅遊類	-瑞士阿爾卑斯山 N 種玩法 少女峰雪景超夢幻 -東京迪士尼投下 2500 億建新 3 大園區！冰雪奇緣&彼得潘區 2022 年開幕！概念圖預覽
Letter 10	旅遊類	最強追櫻秘笈 仙境般美到飆淚
Letter 11	生活類	-2018 國民旅遊卡特約商店優惠 -政府內部控制制度設計原則新規範
Letter 12	擬真類	-你填問卷，抽週週 Switch 及百種遊戲片 -107 年度安全會議紀錄 -107 年度公務人員請假規則修訂說明
Letter 13	美食類	2018 最夯燒肉丼排行榜！爆量肉山看了流口水