電子郵件社交工程防制

2009–4–17 Jerry

Contents

何謂社交工程

- 社交工程(Social Engineering)爲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爲。 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等各種方法來進行社交工程。
- 以人爲本騙術爲主
- 技術門檻較低
- 貪心：撿便宜的個性
- 好奇：探索感興趣的事務
- 缺乏警覺：有那麼嚴重嗎？

案例分析：社交工程幽默


CALTECH CANNON
April 6, 2006
MIT hackers posing as the Howe & Ser Moving Company appropriated this cannon on March 28, 2006. It later appeared on MIT's campus with the addition of a large brass rat made of gold-plated aluminum. In honor of its previous owners, the cannon points towards Pasadena, CA.


Vancouver
Seattle
Spokane
Washington
Portland
Salem
Oregon
Boise
Idaho
Montana
North Dakota
Minnesota
Minneapolis
South Dakota
Wisconsin
Michigan
Wyoming
Milwaukee
Chicago
Fort Wayne
Detroit
Toronto
Ottawa
Montréal
Québec
New Brunswick
Nova Scotia
Prince Edward Island
Maine
New York
Vermont
New Hampshire
Massachusetts
Rhode Island
Connecticut
New Jersey
Delaware
Maryland
District of Columbia
Pennsylvania
Philadelphia
New York
Ohio
Indiana
Illinois
Iowa
Nebraska
Lincoln
Kansas City
Salt Lake City
Utah
Denver
Colorado
Nevada
Reno
Sacramento
San Francisco
California
Las Vegas
Bakersfield
Los Angeles
Riverside
Phoenix
San Diego
Tucson
Arizona
New Mexico
El Paso
Albuquerque
Amarillo
Lubbock
Dallas
Texas
Shreveport
Oklahoma
Kansas
Wichita
Springfield
Missouri
Louisville
Kentucky
West Virginia
Virginia
North Carolina
South Carolina
Tennessee
Arkansas
Mississippi
Alabama
Atlanta
Georgia
Mobile
Tallahassee
Jacksonville
Orlando
Florida
Naples
Miami
Louisiana
Houston
San Antonio
Corpus Christi
Gulf of Mexico
Mexico
North Atlantic Ocean

網路釣魚

- 網路釣魚(Phishing)是網路上在常見的社交工程，特別是利用Email來欺騙，對於此類攻擊的最佳對應方法就是在預覽前就刪除所有類似的郵件，如此亦可同時避免會在背景觸發不良程式的惡意郵件攻擊。
- 只要使用者警覺性不足，點選網頁連結或是開啓來路不明郵件的附加檔案，都可能被植入惡意程式。
- 當收到不尋常或太好康的訊息時，應思考訊息內容的可行性，千萬不要下載附件或是連結網頁，並依循資安通報管道進行通報。

網路釣魚方法

- 砍站程式
- 首頁植入惡意程式
- 將DNS名稱更改其中一個英文字母
  - 用數字1取代英文l
  - 或用數字0來取代英文O
  - xxx.com.tw 或 xxx.com
- 發E-mail、廣告或簡訊
- Google搜尋排名
  - 向Google買關鍵字廣告
  - 偽站已存在很久

網路釣魚之媒介

- 搜尋引擎與入口網站
  - Google
  - Yahoo
  - ．．．
- IM軟體
  - MSN
  - 即時通
  - Skype
  - ICQ
  - ．．．
- E-Mail
- 手機簡訊
- 廣告

網路釣魚目的

- 廣告目的(不斷開啓惡意廣告)
- 攻擊目的(植入後門程式)
- 金錢目的(詐騙行爲)
  - 花旗銀行(mail)
  - 旅遊網站
  - 拍賣網站
- 竊取帳號密碼與個人資料

IM詐騙


MSN Messenger
檔案(F) 連絡人(C) 執行(A) 工具(T) 說明(H)
msn Messenger
:: Sarana :: 天氣真不好.... (線上)
電腦壞了誰能幫我?
我的分享空間(S)
MSN 今日焦點(Y)
按一下這裡了解客戶經驗改進計畫的相關資訊
:: 好用的工具 :: (2/3)
我幫你修電腦好不好？ (網路/線上)
(粘守裕)--寶貝等我，我來幫你修電腦了
Tama~!? Sarana軍曹我愛妳 (離線)
[用過的工具回收箱] (7/25)
賤女人最好不要被我過到你！(封鎖)
═慎世嫉俗的本命・女人是這樣的生物═ (封...
Jeff--原來我是自作多情 (封鎖)
TARYN 糟糕 莎拉拉爲什麼不理我了.....? (封...
人的一生 也許就是過往 妳都不記得那點點滴滴 (封...
我的第一次就莫名奇妙地飛了 (封鎖)
情不自禁 (封鎖)
收到好人卡的感覺.....唉.... (封鎖)
莎拉拉 妳是我的 (封鎖)
茫茫人海 卻不見妳的踪影 我好想妳妳知道嗎 (封...
新增連絡人(O)
搜尋網頁...
搜尋(R)
msn 搜尋 結果更精確 功能更強大
海外遊學
搜尋

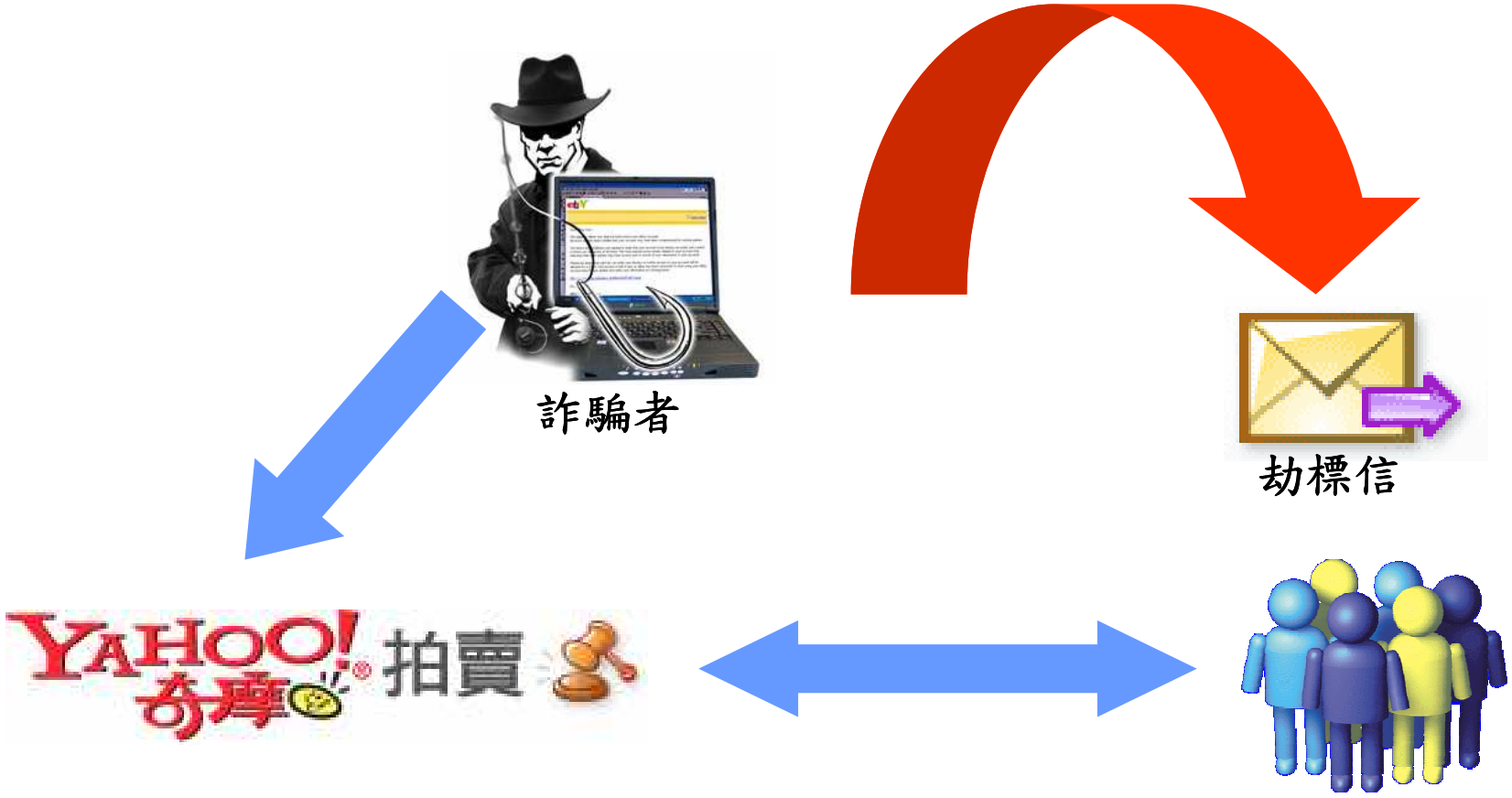
案例分析： **MSN卡到陰**


Windows Live(TM) Messenger Service 工作小組 <messenger@microsoft.com>
相片
檔案
遊戲
活動
邀請
封鎖
Windows Live(TM) Messenger Service 工作小組 (離線)
Windows Live(TM) Messenger Service 工作小組 不在您的連絡人清單中。新增至連絡人清單
Windows Live(TM) Messenger Service 工作小組 說 (08:08):
重要服務宣告: 因應近期系統增強的需要，您必須變更您的電子郵件地址以登入 Windows Live(TM) Messenger Service。
若要確保您的存取權限不被封鎖或了解更多相關資訊，請移至
[redacted]
[redacted] 說 (08:22):
這啥鬼...
下列訊息無法傳送給所有收訊者:
這啥鬼...

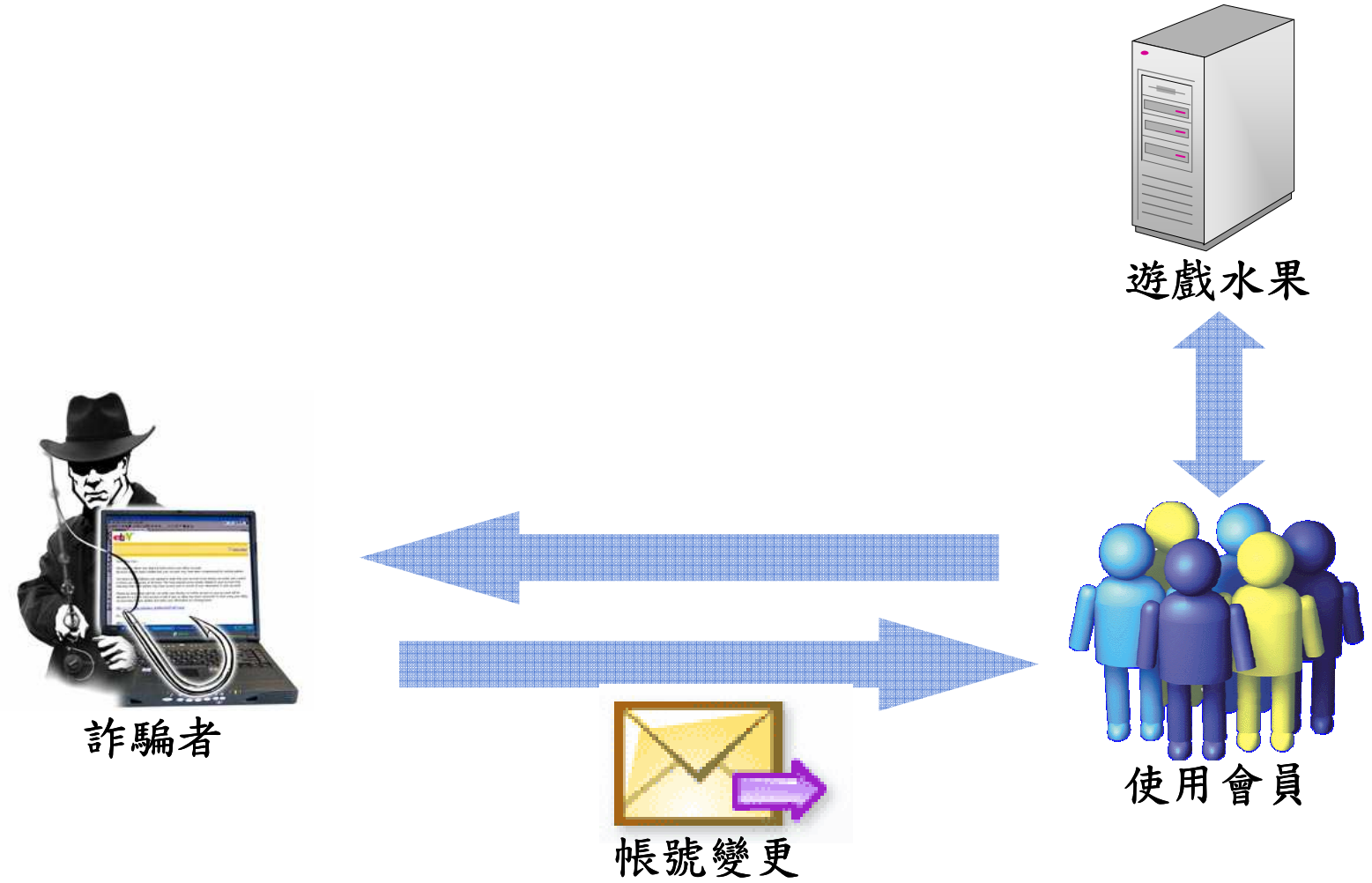
「我的最愛」是釣魚台?

- 合作金庫www.tcb**c**-bank.com.tw/
- 土地銀行www.**1**andbank.com.tw/
- 中國商銀www.**1**cbc.com.tw/
- 宏碁電腦 www.ac**c**er.com.tw

案例分析：YAHOO拍賣



案例分析：遊戲橘子



案例分析：偽冒網站


真
偽
Google
所有網頁 圖片 新聞 網上論壇 更多 »
"翠湖水草網站"
搜尋
所有網頁
翠湖網頁
翠湖水草網站
真
偽
www.tbs-aqua.com.tw
www.tbs-aqua.com.tw/encyclopaedia/plantShow
www.tbs-aqua.com/index.htm - 56k
www.tbs-aqua.com/researchList-Pid=1&Cid=56.htm - 34k
歡迎光臨翠湖水草網站
水族辭典 Aquarium dictionary

教育部資訊安全演練－電子郵件社交工程

- 演練目的：檢測單位之資安防護能力或執行成效
  - 演練方式
    - 模擬入侵攻擊 - 技術性演練
    - **社交工程 - 資安認知與警覺**
- 電子郵件社交工程執行方式
  - 透過電子郵件寄發附帶word、圖檔、網頁等類型

惡意網頁攻擊(八卦主旨)

收件者... center11 <center11@cc.ncu.edu.tw>;

副本(C):

密件副本(B)...

主旨(J): 賈靜雯外遇眞象

賈靜雯外遇真象

孫志浩舅舅劉正中爆賈靜雯3年前在南京拍戲時「發生不堪的事情」，曾與賈傳緋聞的黃磊昨以「見鬼了」形容自己無奈的心情。他說他與賈靜雯的緋聞純屬無稽之談，「我的為人大家也知道，怎會扯出這麼一筆爛帳。」

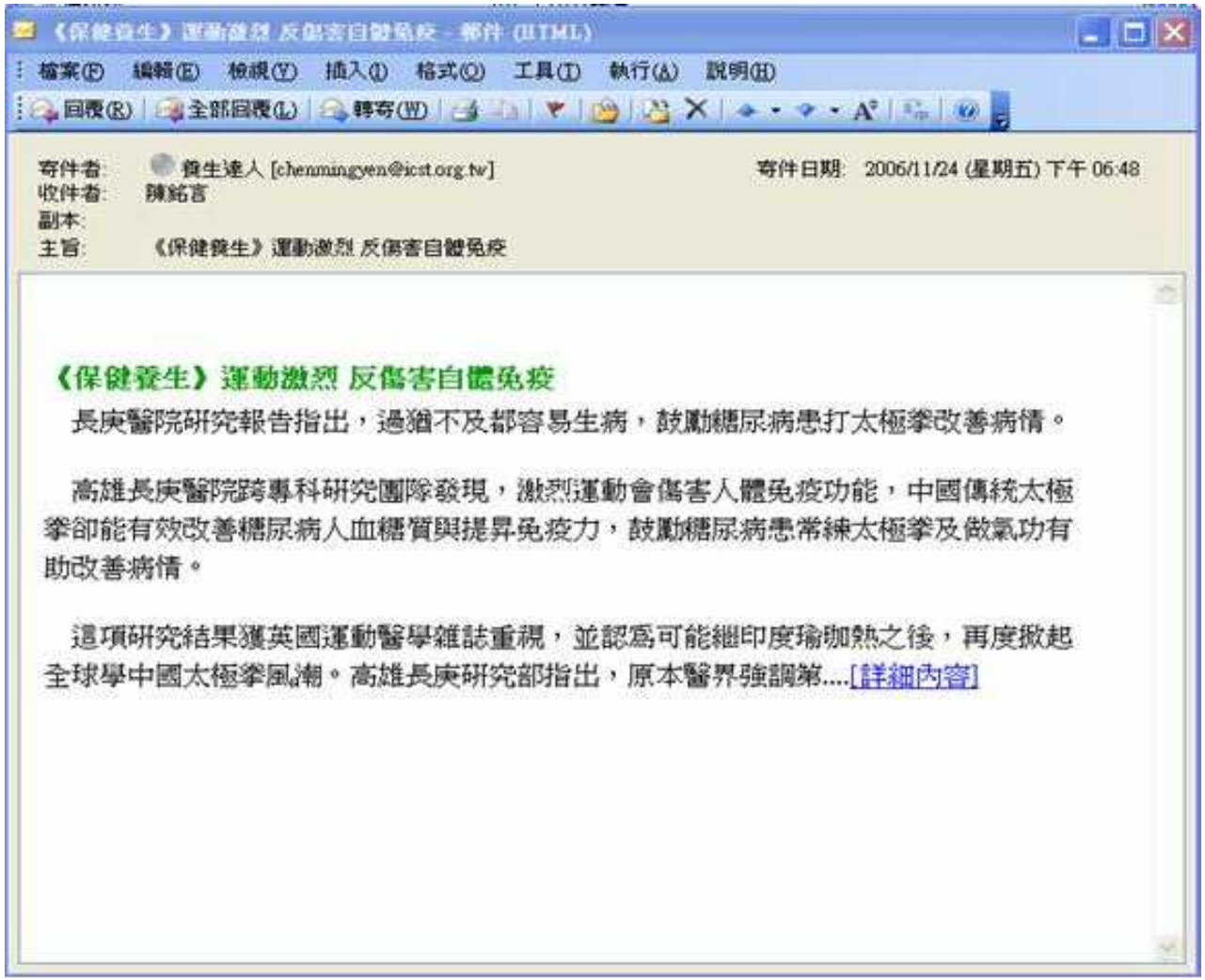
http://udn.com/NEWS/ENTERTAINMENT/ENT1/4837510.shtml

惡意圖檔攻擊(情色主旨)


收件者...
center11 <center11@cc.ncu.edu.tw>;
副本(C):
密件副本(B)...
主旨(J):
瑤瑤殺很大寫眞集
附件...
殺很大.rar (78 B);
附件選項(M)...
宅男的最愛~瑤瑤殺很大寫真集

惡意word檔攻擊(休閒娛樂主旨)

惡意網頁攻擊(養生保健主旨)



案例分析：愚人節電子郵件可能包含病毒

即時新聞 》愚人節電子郵件可能包含病毒
Breaking news

【美通社／美通社-PR Newswire】 2009.04.01 05:32 pm

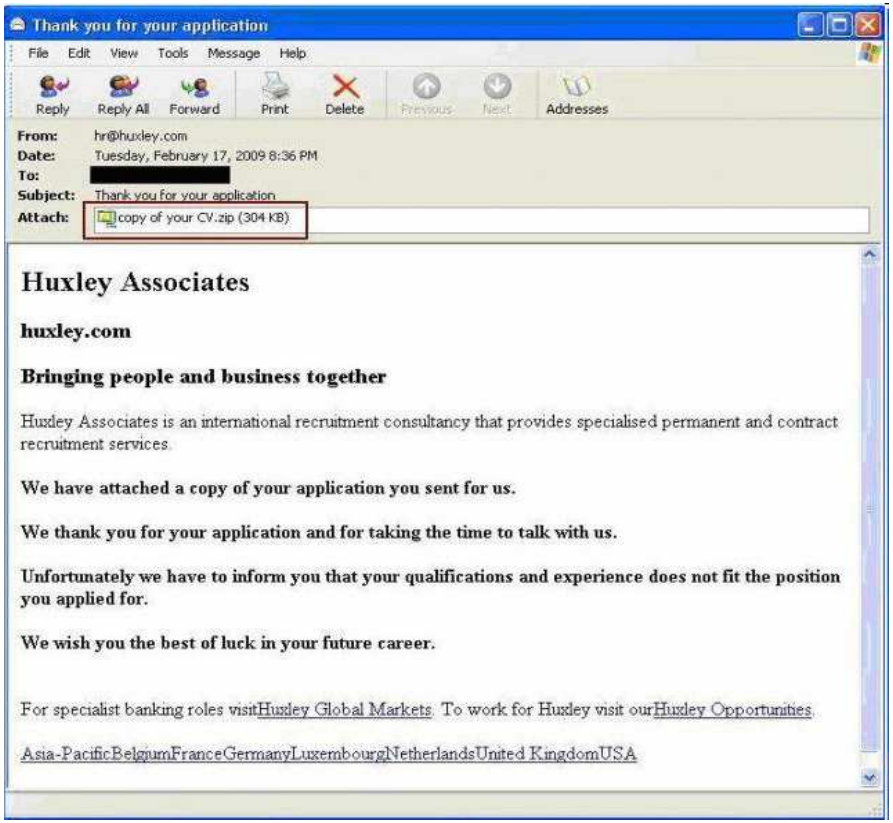
亞特蘭大, 3月31日 /美通社-PR Newswire/ -- 在過去的兩年裏，愚人節給全球各地數以百萬計的電腦用戶帶來了技術困擾。2007年4月1日，蠕蟲病毒 ANI 利用 Windows 中的漏洞在全球各地肆虐，而去年 Storm 蠕蟲病毒利用發送愚人節主題的電子郵件大肆傳播。爲在今年愚人節搶先打擊任何可能的威脅，網路安全供應商 Stonesoft 建議電腦用戶們在打開愚人節的郵件時要特別謹慎。

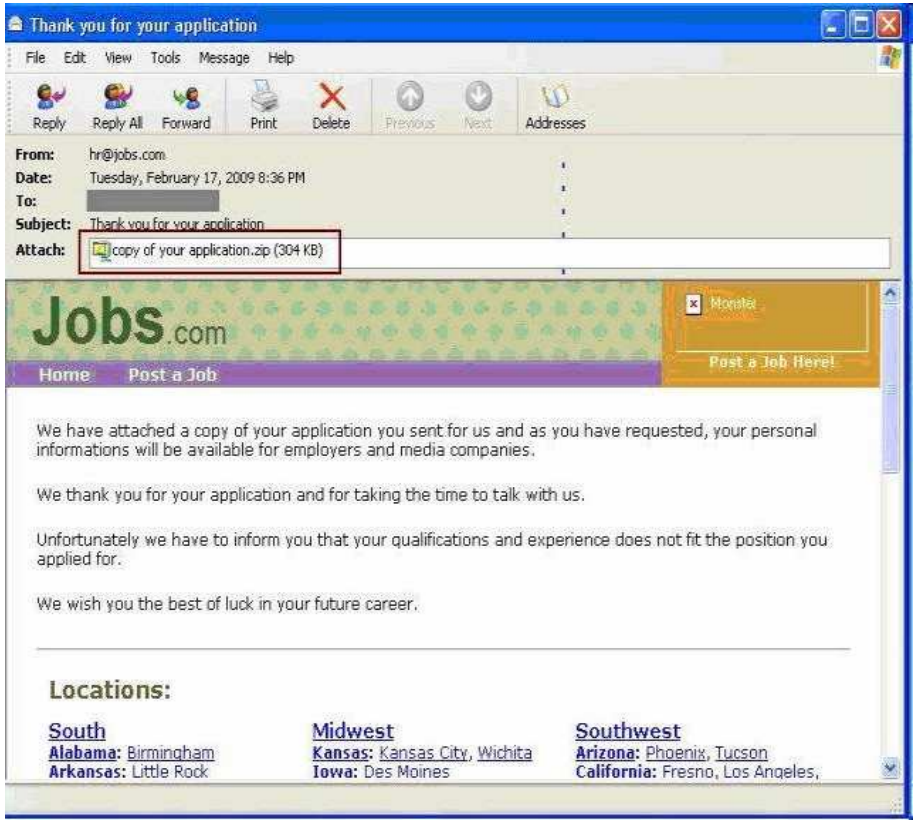
眾所周知愚人節是新的資料安全威脅出現和舊的威脅重現的日子。今年，人們已經圍繞 Conficker 網路蠕蟲的預期更新進行了許多討論，該病毒更新被認爲是病毒歷史上破壞力最強的。然而，該更新將產生怎樣的破壞仍有待觀察。

Stonesoft 漏洞專家 Olli-Pekka Niemi 表示：「之所以資料安全威脅在愚人節前後出現是完全可以理解的，同樣的事情也發生在絕大部分的公共假期或者情人節等。即使人們從陌生位址接收到電子郵件，他們往往也會輕易地打開這些問候郵件寄希望於看到有趣的愚人節玩笑。」

案例分析：駭客也在求職網找工作

- 下面電子郵件樣本是冒充jobs.com發送的信件：
  - 信件來源看似來自人力資源部門:hr@jobs.com
    信件標題是：「Thank you for your application」
    附件是：copy of your application.zip





案例分析：假強風真病毒

小心！ 假強風特報 真電腦病毒

2009-03-18 | 中國時報 | 【李宗祐／台北報導】

「中央氣象局緊急通知─強風特報」？最近幾天如果接到上述主旨的電子郵件，最好直接刪除掉，千萬不要開啓，以免電腦病毒趁機入侵！氣象局昨日發布通訊安全緊急公告，呼籲民眾提防駭客假冒該局名義發送電子郵件，散播電腦病毒。

氣象局前天發現該局網站設置的民眾意見箱（webqry@cwb.gov.tw）發送出去的電子郵件中，有四、五十封電郵被莫名退回，信件主旨都是「中央氣象局緊急通知─強風特報」。追查發現，原寄信者的ＩＰ位址並非氣象局，且該局最近未傳送電子郵件給這些收件者，懷疑有駭客假冒該局名義發送電子郵件。

氣象局資訊中心爲追查冒名信件來源及駭客企圖，逐一打開被退回信件，赫然發現附件檔夾帶電腦病毒。

由於駭客冒用氣象局名義傳送電子郵件，並非針對該局電子報訂戶，而是發送垃圾郵件「散彈打鳥」，不知情民眾看到信件主旨及寄件者電子郵件帳號爲代表政府單位的「.gov」，多會不疑有它、打開信件。氣象局爲避免無辜民眾慘遭毒手，昨日發布資通安全緊急公告。

--

案例分析：引毒上身？五成網友主動下載有毒影音檔、電子郵件

記者蘇湘雲／台北報導

調查顯示，有五成網友是主動下載有毒影音檔、開啓電子郵件，讓自己曝露於網路毒駭的問題中。（圖／Yahoo！提供）

總是抱怨網路毒駭事件層出不窮的使用者聽到以下消息，可能要先檢討自己爲何如此「手癢」囉！入口網站最新調查顯示，網路中毒原因的前三名分別爲「**下載有毒的音樂或影音檔案」（27.6%）、「帳號被盜」（26.7%）及「收到夾帶有毒檔案和連結的電子郵件」（24.2%）**，除了帳號被盜，有五成 以上的網友都是「**主動被駭**」，主因來至網路安全知識的不足，而誤入「毒」徑。

網友最容易點選「跟搜尋結果相關的網站」（42.3%）及「好友寄的信件或訊息」（29%）而上了有毒程式的釣鉤，誤入電腦被 駭的危機。而另外依序還有「免費試玩或下載」（13.9%）、「火辣性感圖」（7.3%）及「折扣好康」（5.7%）等誘人資訊也會讓網友忍不住點選。

透過交叉分析也發現有趣的現象，**會被「折扣好康」內容吸引的女性網友爲男性的三倍，而「火辣性感圖」的內容吸引者則大多數爲男性網友**。

惡意word檔攻擊(公務人員相關主旨)

案例分析：來自資通安全會報技服中心的通知

- 近日國家資通安全會報技術服務中心發現，有不明駭客假冒國家資通安全會報技術服務中心之客戶服務信箱名義發送含有惡意程式之電子郵件，請使用者若收到此類信件時，切勿開啓電子郵件之附件檔案，以免遭受攻擊。若使用者開啓此項惡意設計之電子郵件副檔，即被植入後門程式。

案例分析：來自資通安全會報技服中心的通知

- 目前已知該假冒信件訊息如下:
  - 寄件者：service@icst.org.tw
  - 主旨爲「W32.Timeserv@mm 病毒通告」
  - 附件有3 筆名稱分別爲「安全防護.ppt」、「病毒原理.ppt」、「解決方案列表.xls」。

案例分析：來自資通安全會報技服中心的通知

- 事件說明
  - 此事件爲一起「零時差攻擊」（ Zero-day Attack ），因此附檔使用的弱點所使用的未公開的 Office 漏洞目前尚無更新程式可修補。
  - 經調查，駭客大量寄發經特殊設計的電子郵件，顯示此次大規模入侵事件並非個案。
- 解決之道
  - 若有收到類似不明信件，請勿開啓以避免其他攻擊，發生造成更嚴重之後果。

同仁對於可疑電子郵件應有警覺性

- 「爲何我會收到這封郵件」
  - 應確認寄件來源及寄件者。
- 「我是否應該收到這封郵件」
  - 應確認郵件主旨及郵件內容。
- 「我是否應該開啓這封郵件」
  - 是否與業務工作相關。
  - 不開啓(點選)連結是否有影響。
  - 審慎查證（寄件者或資訊中心）。

判斷網路釣魚郵件方式

- 發信人的名稱或郵件地址
  - 是否有異常？需確認發信者的身分
- 電子郵件的主旨與內容
  - 與本身的工作、業務是否有關連
- 網頁連結或夾帶附件檔案是否可疑
  - 郵件內異常網址連結判斷
    - www.microsoft-mis.com
    - www.hinet1.net , www-hinet.net
    - www.paper-pchome.com , www.pchorne.com
    - 使用不明IP 代替URL（如：http://220.33.444.12/）

判斷網路釣魚郵件方式

- 附加檔案之檢查
  - 與接收者的日常工作是否有關
  - 往往帶有惡意攻擊碼的檔案不易察覺
  - 常見病毒附件檔案副檔名
    （.bat、.pif、.exe、.zip、.src、.cmd、.rar等）
- 對於切身相關的電子郵件，若內含威脅、利誘、警告、提示等訊息內容，先思考後再行動作，應考慮詐騙之可能性

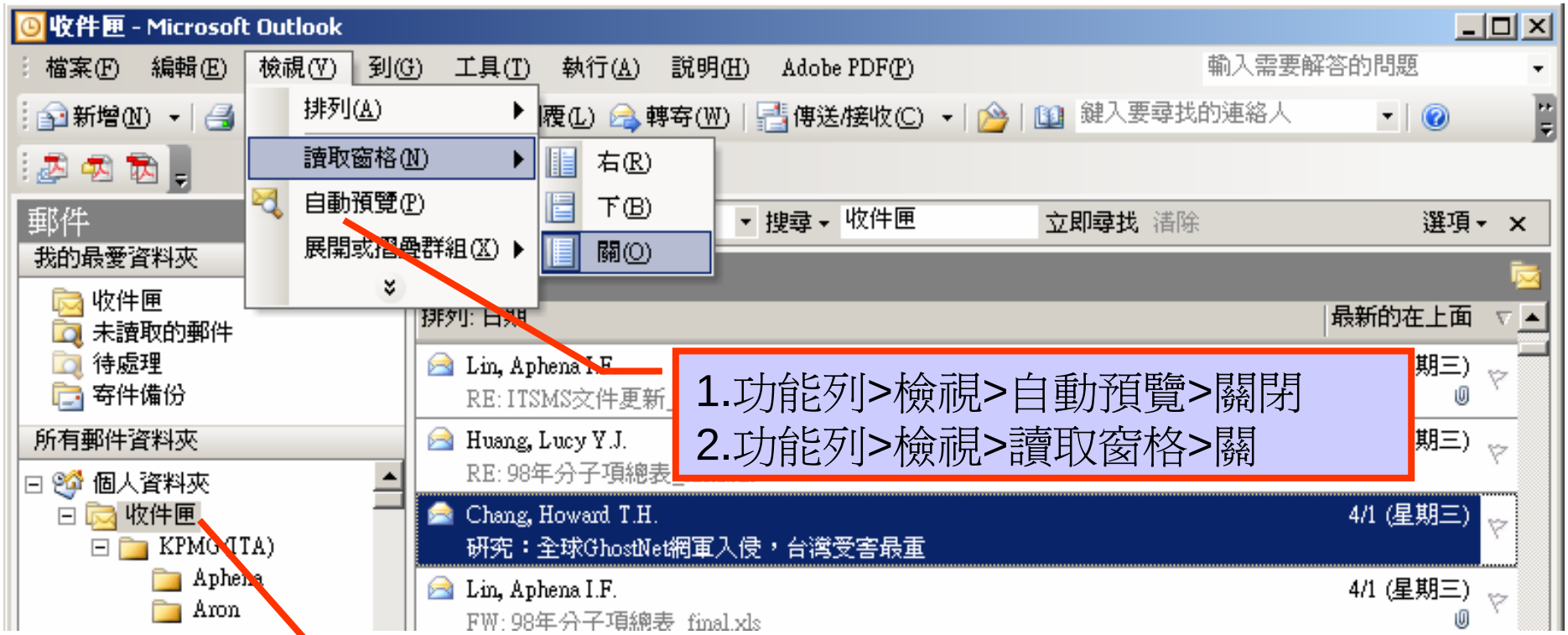
防範惡意程式與詐騙

- 個人資訊勿隨意登錄於不明網站
  - E-mail 管理
    - 區分公司及個人使用之信箱
    - 在外登錄註冊之信箱，容易收到許多垃圾郵件，使用時務必小心
- 不回覆來源不明之郵件
- 即時更新軟體修補程式
- 即時更新防毒軟體及病毒碼
- 經常對系統進行檢測
  - 定期安檢作業
- 實體隔離
  - 機敏資料應於實體隔離主機上作業

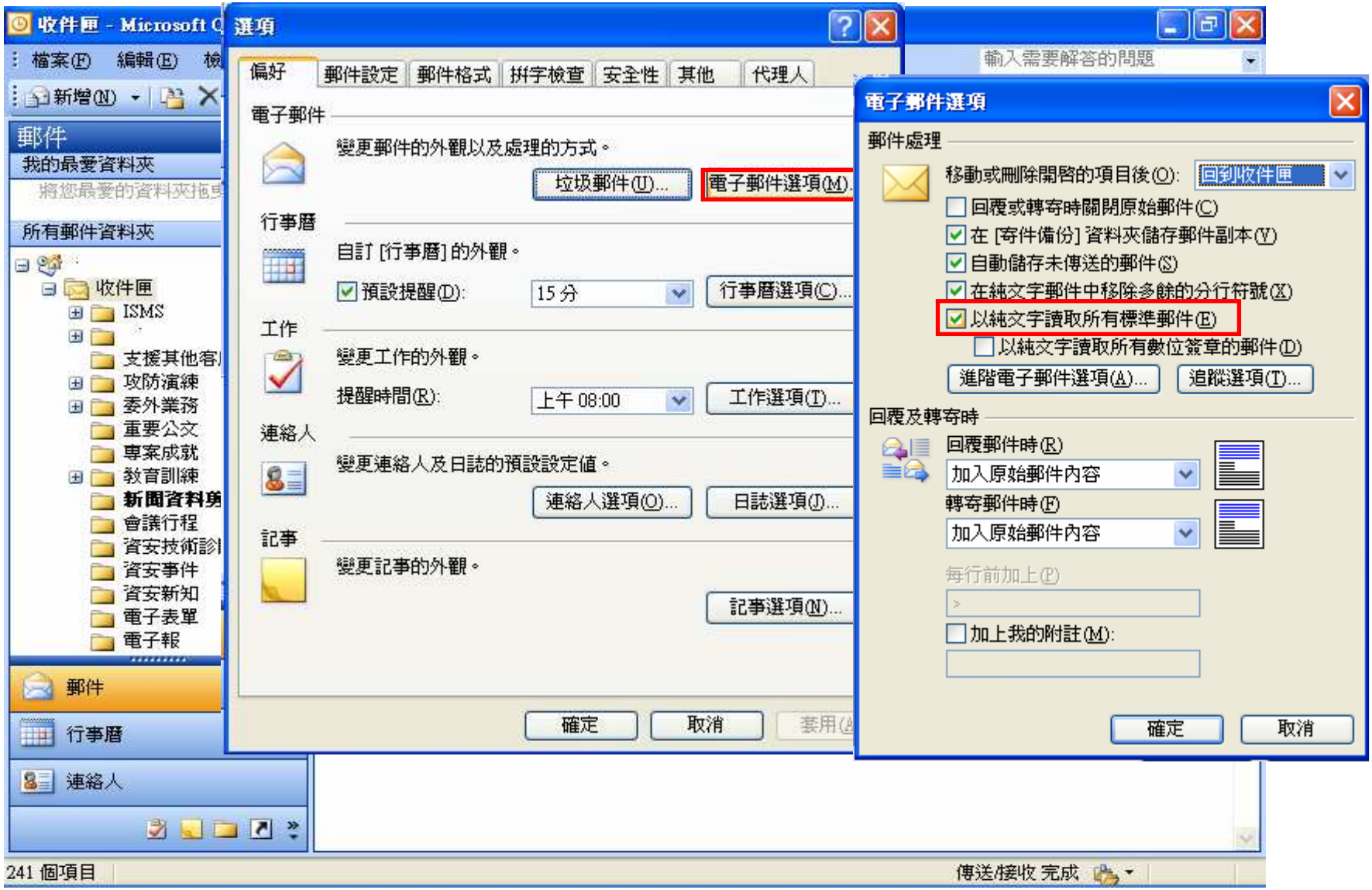
電子郵件安全防制措施

- 同仁之電子郵件應「關閉預覽郵件」設定。
- 同仁之電子郵件應設定爲「以純文字模式」開啓郵件。
- 不隨意開啓及轉寄與業務無關之電子郵件及網站。
- 如發現爲不明來源或疑似網路釣魚之郵件應直接刪除。
- 不隨意點選或下載郵件內之連結與附件檔案。
- 如發現可疑信件應先與寄件者確認其真僞或通報資訊單位查證。
- 不隨意開啓郵件（確認寄件人）
- 不隨意開啓或下載附件
- 善用密件收件人
- 非必要不設自動回覆
- 不隨意留下郵件地址予他人
- 注意陌生之寄件者
- 了解組織傳送郵件規定

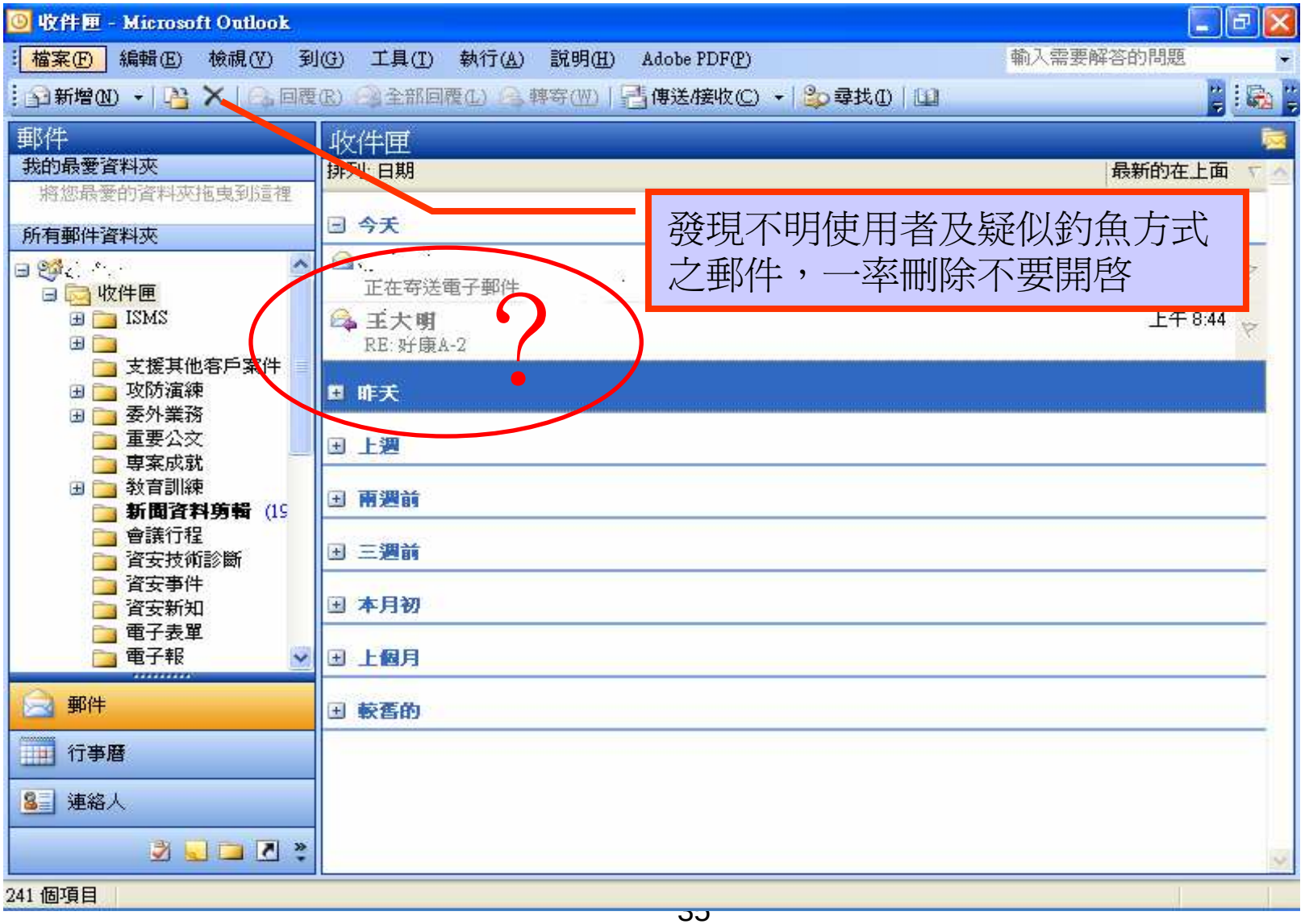
一、Outlook取消郵件預覽



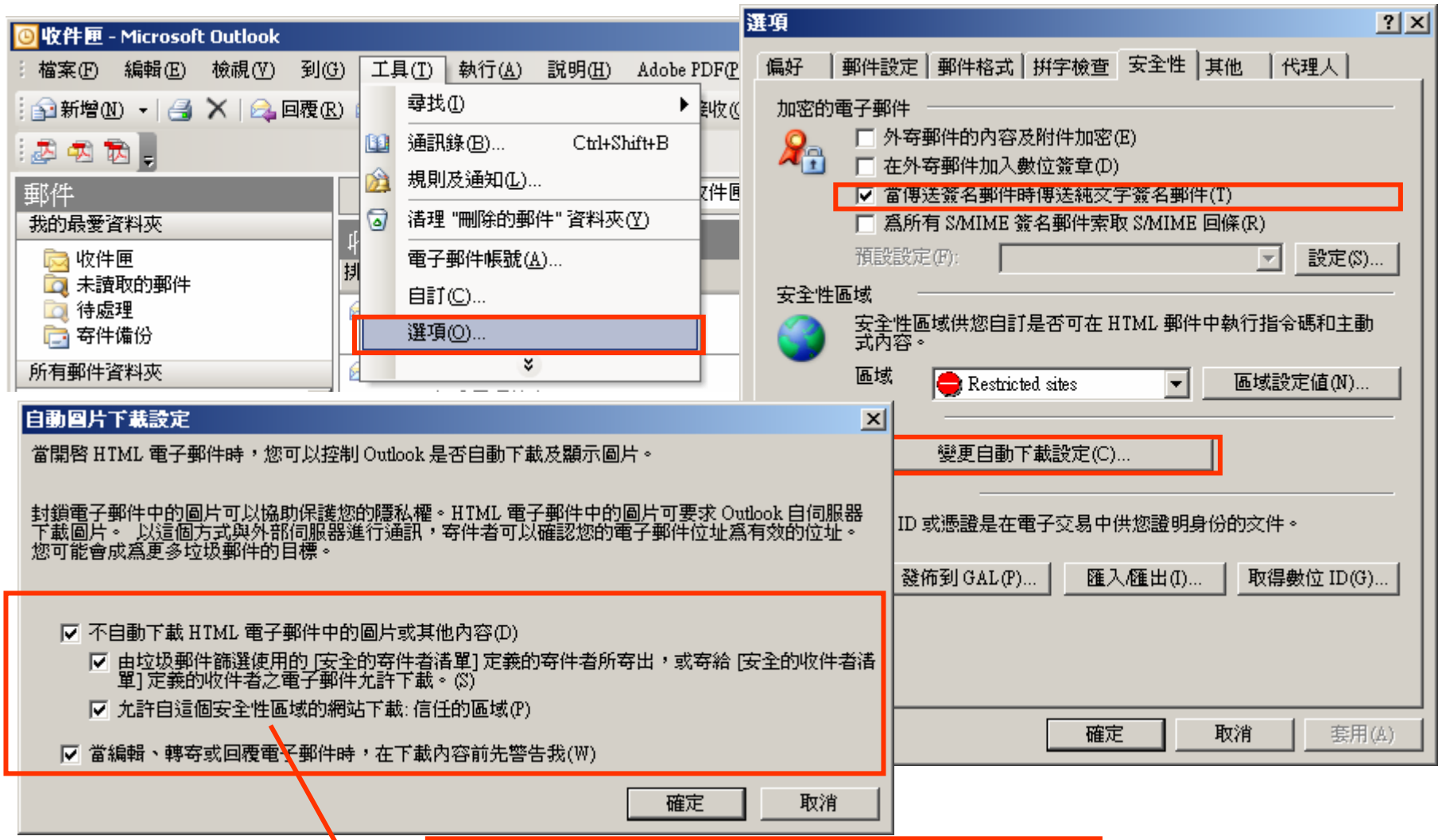
二、Outlook設定純文字模式開啓郵件



三、Outlook刪除不明來源郵件



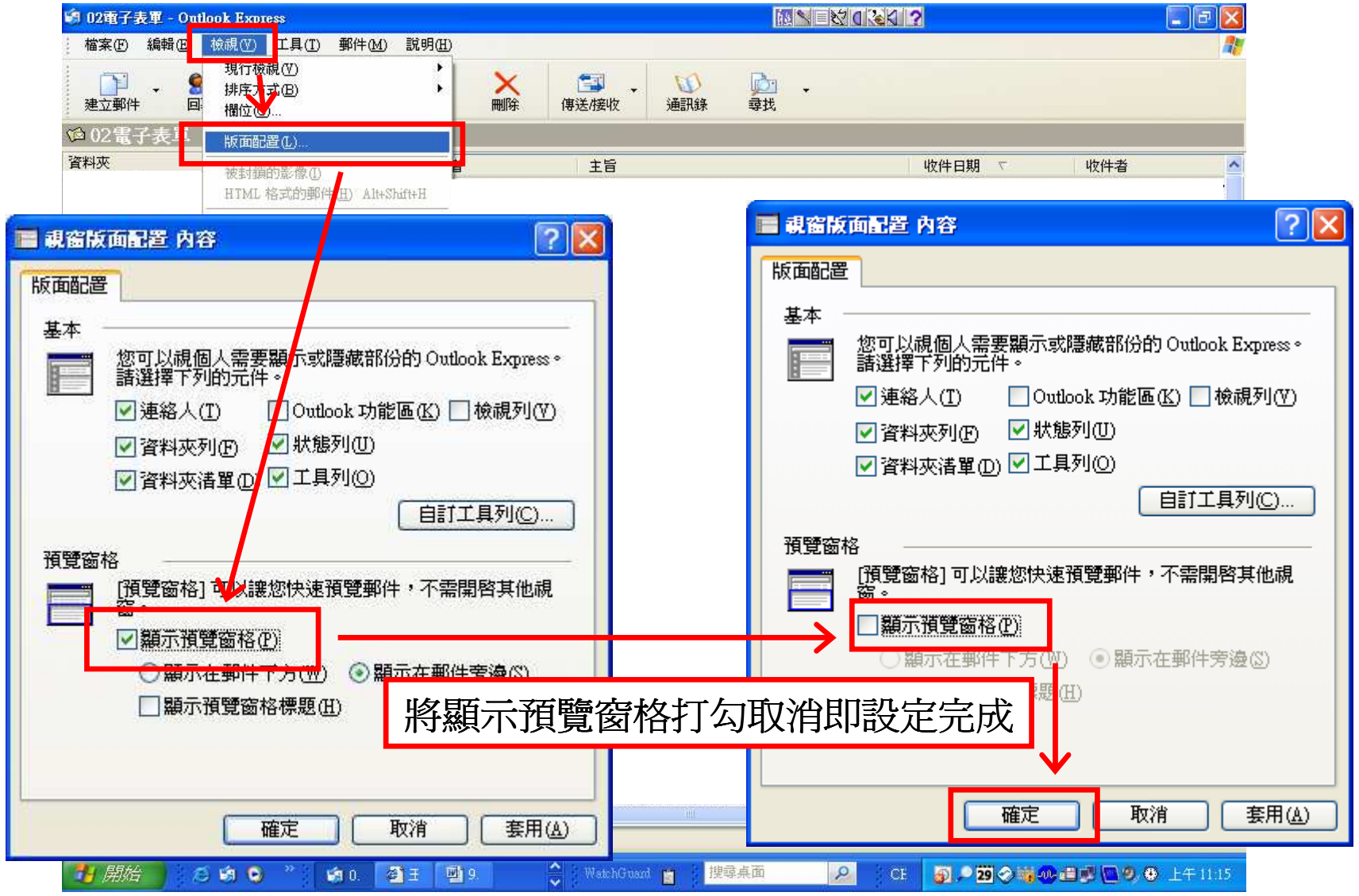
四、設定阻擋HTML電子郵件中的圖片



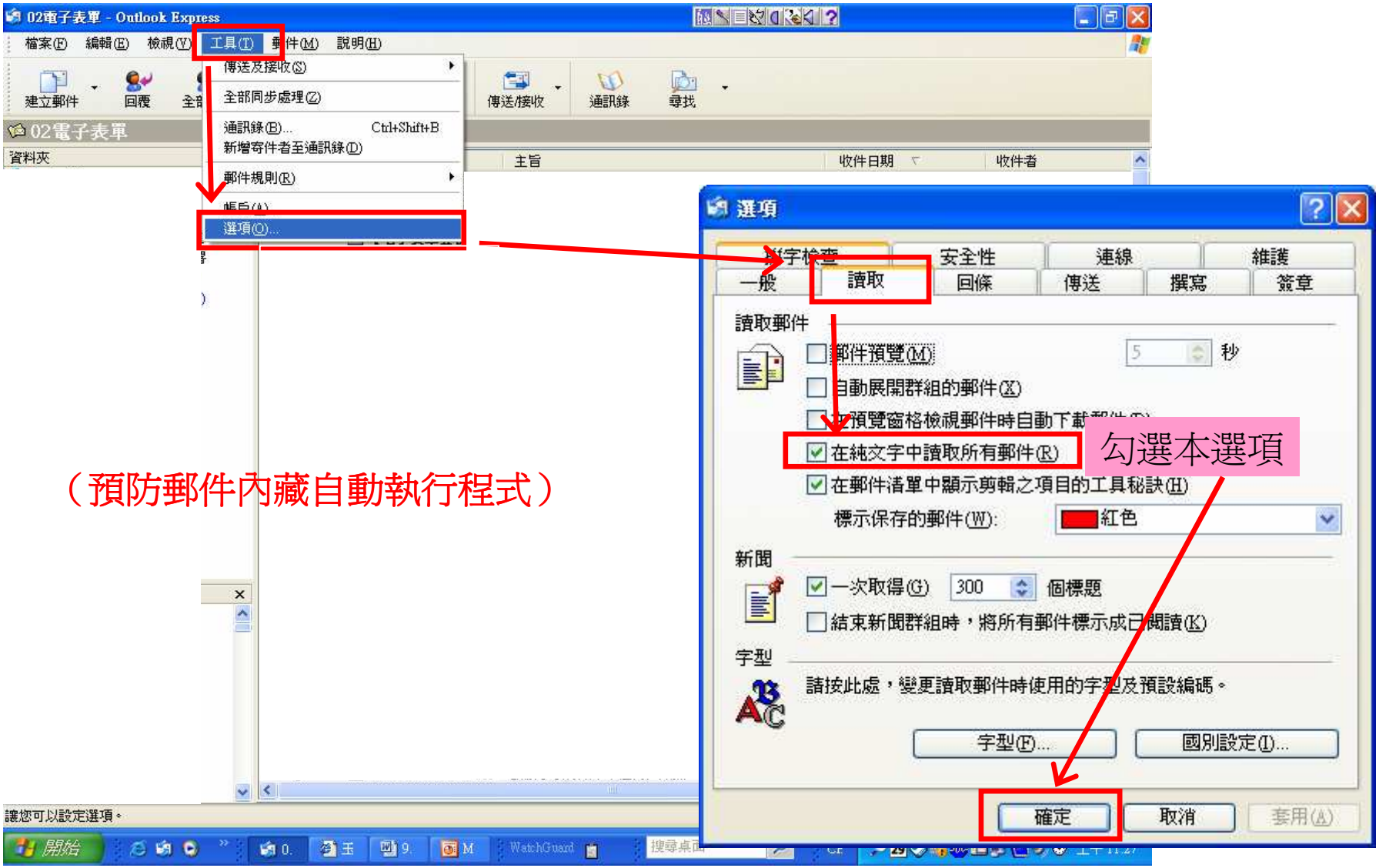
“自動圖片下載設定”內選項均須打勾

五、Outlook確定發信者電子郵件帳號

一、Outlook Express關閉預覽視窗設定



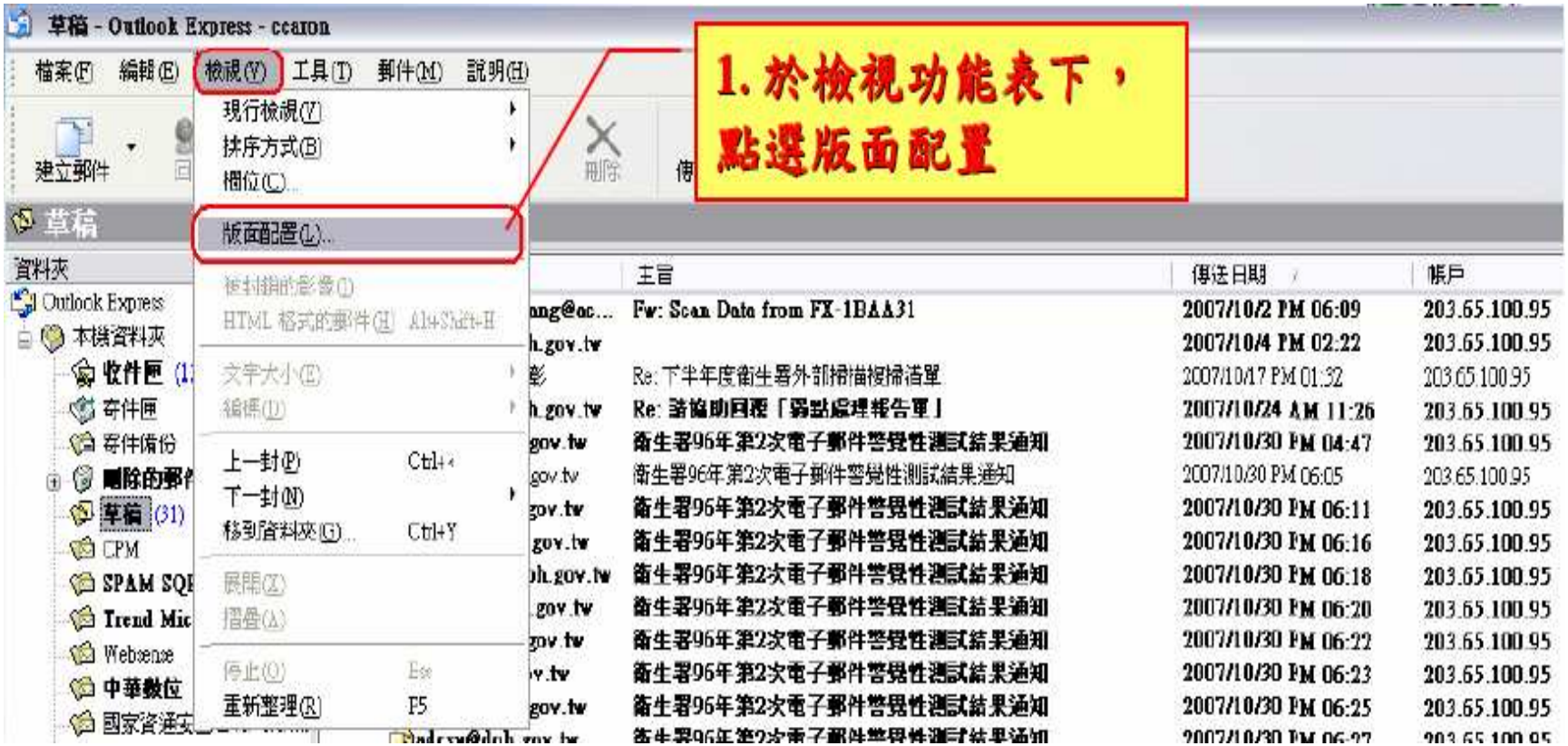
二、Outlook Express以純文字模式開啓郵件



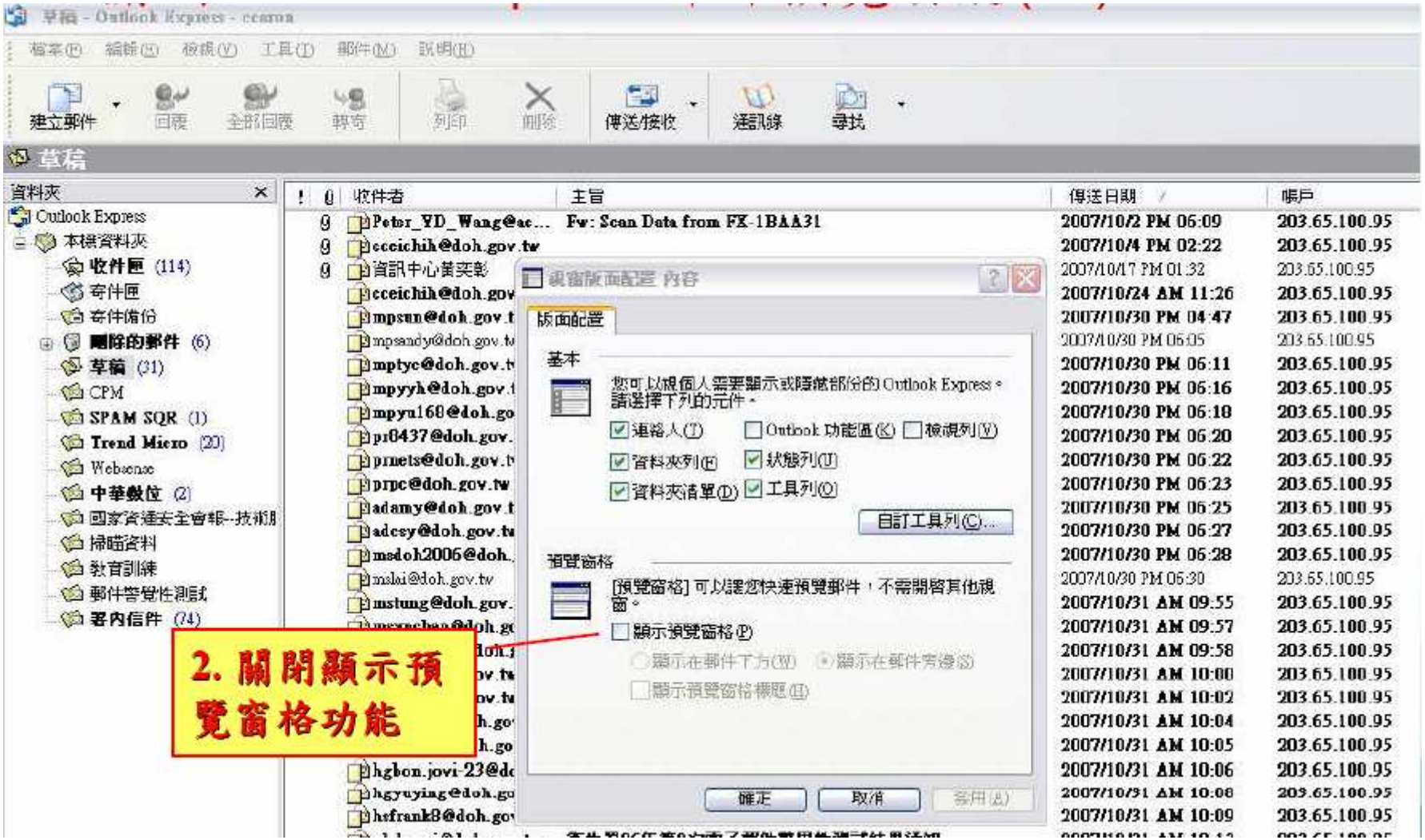
（預防郵件內藏自動執行程式）

勾選本選項

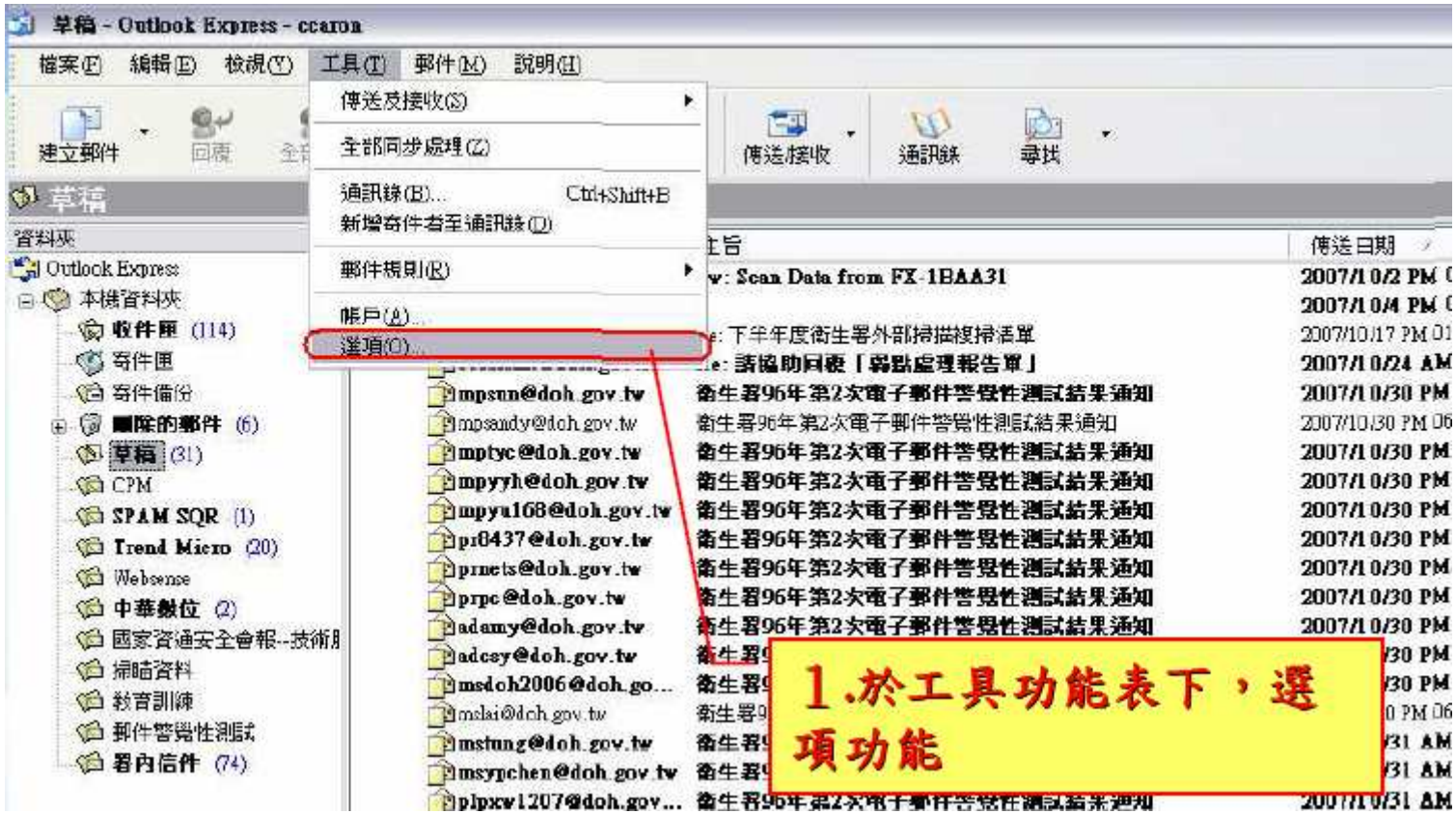
三、關閉Outlook Express郵件預覽功能



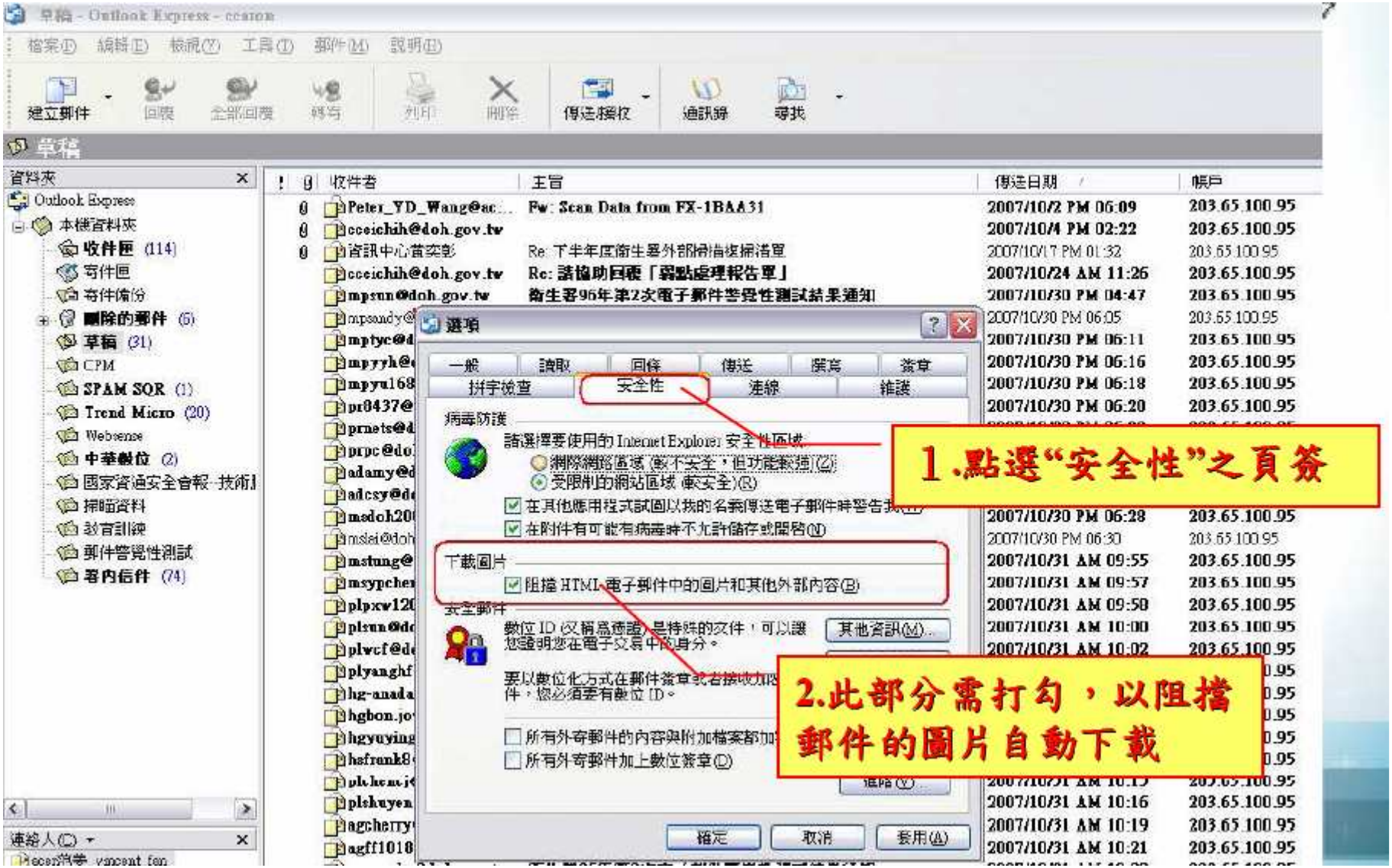
三、關閉Outlook Express郵件預覽功能



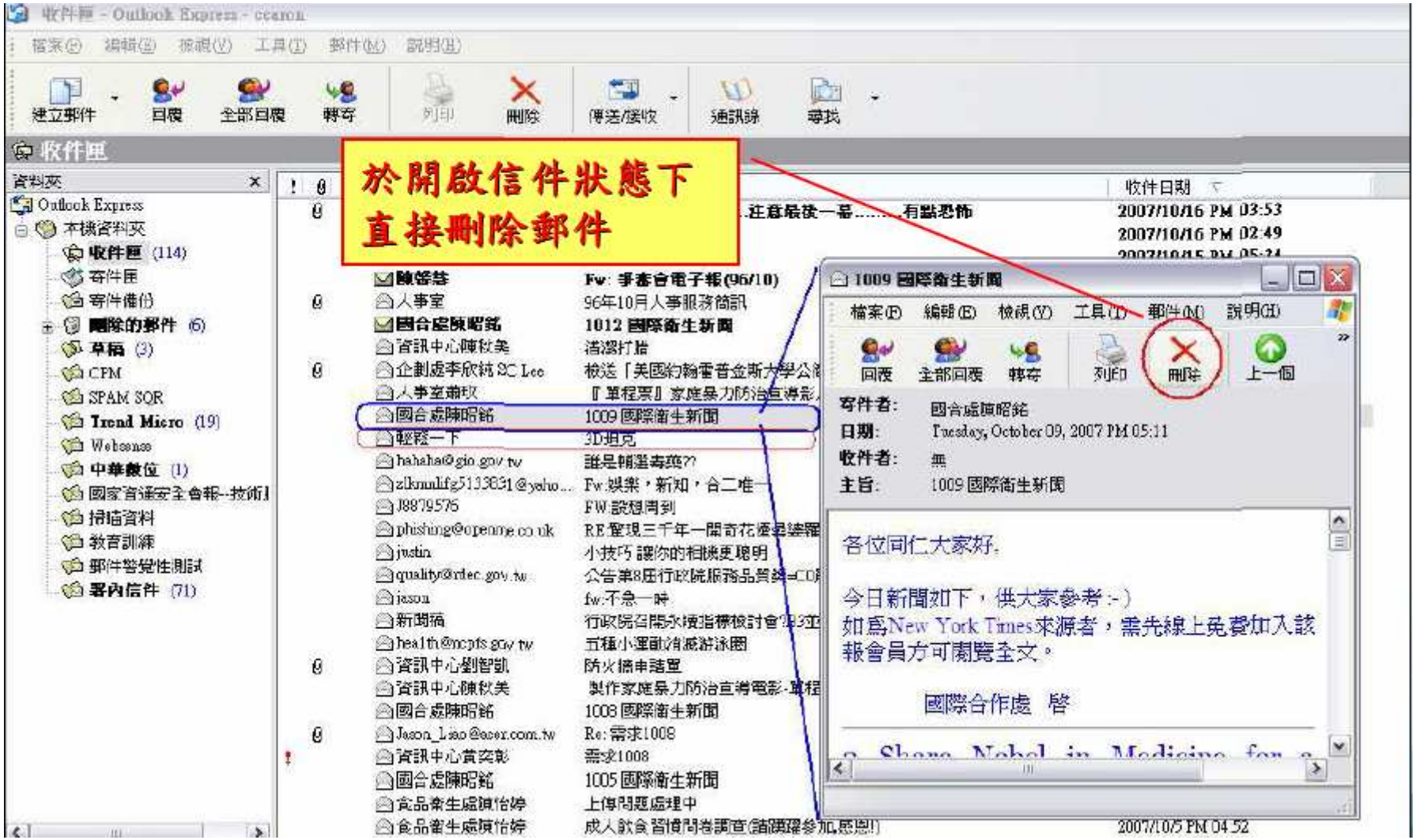
四、設定Outlook Express阻擋電子郵件中的圖片



四、設定Outlook Express阻擋電子郵件中的圖片



Outlook及Outlook Express操作注意



改善個人習慣

- 不要瀏覽非工作相關或不信任的網站
- 不要下載安裝未經認可的軟體或程式
- 隨時更新作業系統與應用程式
- 安裝必要的防護軟體
- 不要開啓可疑或非工作相關的信件附檔
- 對任何提到"緊急"或"個人金融"保持懷疑態度
- 對信件有任何一點疑慮千萬不要點選Email裡的超連結
- 不要填寫Email裡有關個人金融資料的表格
- 在網站上輸入信用卡號或個人資料時先確認該網站安全性

改善個人習慣

- 不將Email留在任何公開的網頁上
- 不開啓來歷不明之信件
- 不轉寄非必要之信件
- 不回應任何未知的信件
- 安裝防止網路釣魚詐騙的工具軟體
- 經常或定期登入你的網路帳號
- 定期確認你的銀行帳戶、信用卡的交易狀態都正確無異常
- 確認你的瀏覽器、收信軟體、文書軟體及其他程式是最新版本，而且都已更新修補程式
- 自助互助，告知相關單位你發現的網路釣魚事件


Thank You !