
輔仁大學

電子郵件社交工程攻擊宣導

2012.06.01

同仁對於可疑電子郵件應有警覺性

□ 為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

□ 我是否應該開啟這封郵件？

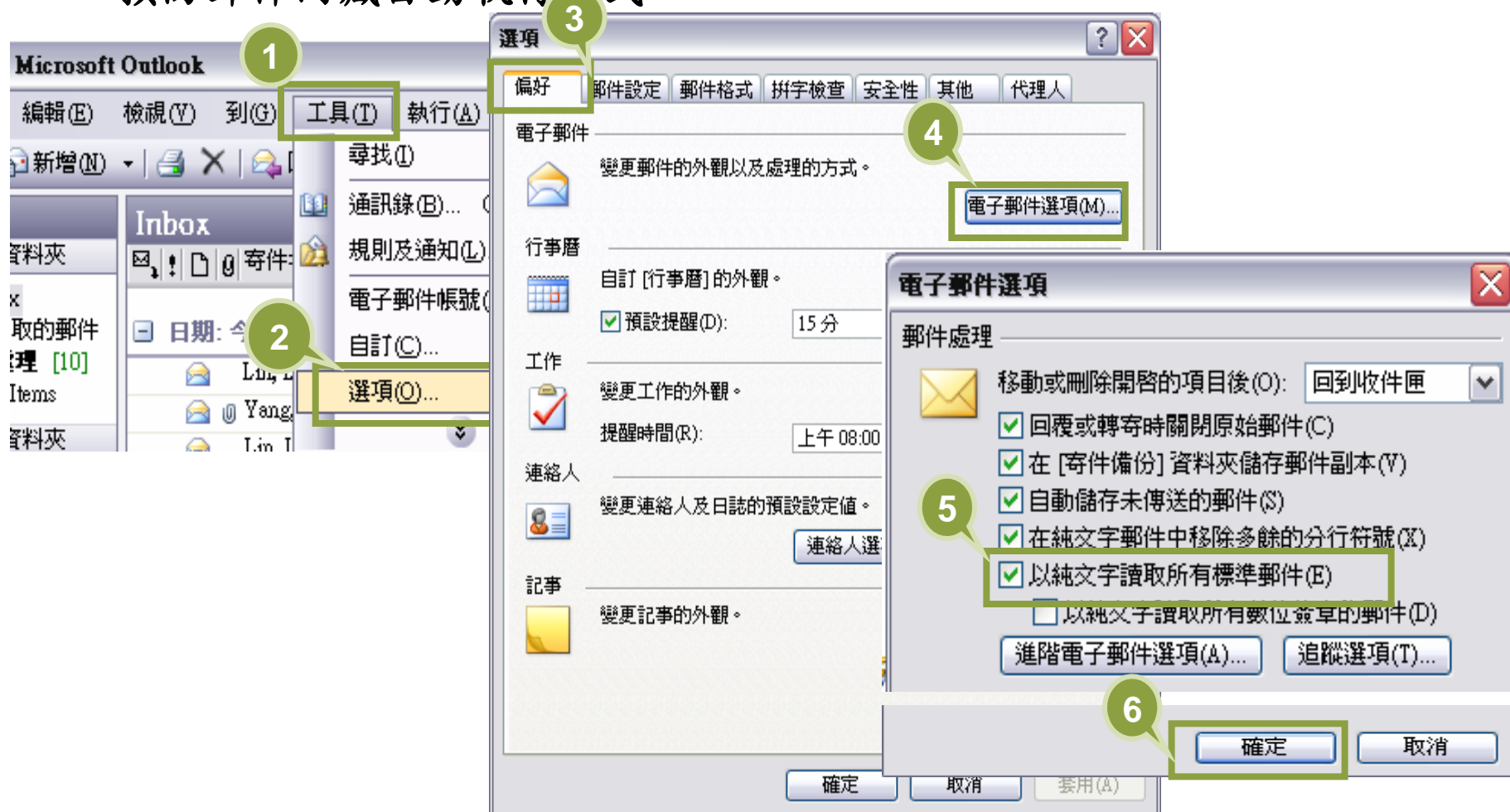
- 是否與業務工作相關
- 不開啟(點選)連結是否有影響
- 審慎查證(寄件者或資訊科)

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為「以純文字模式」開啟郵件。
- 不隨意開啟及轉寄與業務無關之電子郵件及網站。
- 如發現為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偽或通報資訊科查證。
- 不隨意開啟郵件(確認寄件人)
- 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

以純文字開啟郵件

- 預防郵件內藏自動執行程式



判斷郵件真偽



電子郵件社交工程手法



詐騙者



惡意網站



跳板主機



使用者

機密資料

帳號/密碼



惡意郵件攻擊

■ 好康報、養生保健、休閒娛樂、公務相關、美食、八卦新聞…

發信者: 陳慶長<michael@ecommer.gov.tw>
主旨: 新聞局與網站合作 推出消費券好康平台
內容: 新聞局與網站合作 推出消費券好康平台

新聞局與 Yahoo! 奇摩合作, 推出「好康平台」, 讓商家可以免費登錄搭配消費券的優惠專案, 而消費者只要動動手, 就能快速比較出對自己最有利的消費券使用方式。

消費券好康平台上的分類方式, 有 2 種, 一種是 19 個商家分類, 例如: 百貨用品、餐廳小吃、服飾美容等等, 另外一種是 25 個縣市分類, 網友點選縣市分類網頁, 就能鎖定自己打算光顧的縣市商店, 搜尋有哪些優惠, 相當適合要參加地方政府消費券抽獎的民眾查詢。[立即查詢消費券好康](#)



發信者: 吳惠<janeflin@yahoo.com.tw>
主旨: Fwd: 乳醣菌讓古人命長 幫今人減肥
內容: Fwd: 乳醣菌讓古人命長 幫今人減肥

【元氣周報/記者劉敏敏/報導】衛生署疾管局副局長施文儀/資料提供】

問台灣的成年人「今天喝鮮奶了嗎?」不少人搖頭, 其中有人會回答「我喝鮮奶會拉肚子」; 若問「今天喝優酪乳了沒?」搖頭的人更多, 但極少人會回答「我喝優酪乳會拉肚子」。為什麼?

亞洲人常患乳糖不耐症, 無法消化牛奶中乳糖, 喝鮮奶時容易腹脹、腹瀉; 而優酪乳中的乳醣菌可產生乳糖分解酶, 因此可透過飲用乳醣菌產品如優酪乳, 獲取奶品中的鈣質而不會腹瀉。

此外, 發酸乳還具有免疫調節作用, 能增強人體免疫力、抵抗力、及降低膽固醇, 預防泌尿生殖系統細菌感染等。

但多少人知道什麼是乳醣菌? 常聽到的, 不外乎是「乳醣菌幫助體內環保」、「乳醣菌是腸道守護神」。[進一步了解乳醣菌的好處](#)



(記者陳立凱/攝影)

發信者: 包大人<judge08@food.cfm.tw>
主旨: Fwd: Slow and steady wins the race
內容: 基隆「開封包子」多汁 八塊錢香

【聯合報/記者游明煌/報導、攝影】

基隆市八堵路一家賣「開封包」的包子店, 皮薄餡多又多汁, 內餡除有高粱菜、瘦肉外, 還添加 6 種不同配料, 是老闆張侯莉麗的家傳秘方, 讓包子吃起來特別美味可口。

開封包是啥? 一般人聽起來可能霧煞煞, 其實是老闆張侯莉麗巧思取的名字, 因為她祖父、祖母在大陸河南開封賣過包子, 她是第三代傳人, 從小就看著母親做包子, 看著、看著也就學會了。後來嫁到台灣, 在基隆開起包子店, 取名開封當紀念。[開封包子的好吃秘訣](#)



開封包皮薄餡多, 吃起來很可口。

http://mag.udn.com/mag/happylife/storypage.jsp?f_MAIN_ID=279&f_SUB_ID=3828&f_ART_ID=169571

發信者: 趙醫師<doctorC@dcqanda.com.tw>
主旨: Re: 感冒多喝水? 醫師: 不正確
內容: Re: 感冒多喝水? 醫師: 不正確

【記者饒震宇/台北報導】

感冒多喝水會好? 前台北市仁愛醫院主治醫師趙致成提出反駁。他說, 在他 17 年看診經驗, 近世感冒或感冒病患中, 有超過百分之五十的病患因少喝水而痊癒, 他提醒久咳不癒、氣喘及支氣管癌患者少喝水。[看醫師詳細解說](#)



前仁愛醫院主治醫師趙致成倡議, 咳嗽、氣喘等感冒患者應少喝水, 病情會更快痊癒。


記者饒震宇/攝影

發信者: STARS<supermodel@starpics.collect.com>
主旨: 娜姐陳年裸照 待價而沽
內容: 娜姐陳年裸照 待價而沽

【聯合報/記者賈怡雯/綜合報導】

歌壇天后瑪丹娜 30 年前的兩張裸體舊照, 將於 2 月 12 日透過美國佳士得拍賣公司拍賣, 儘管當年擔任模特的瑪丹娜只收到 25 美元的報酬, 但現在拍賣每張照片的價格可能超過 1 萬美元 (約台幣 33 萬元)。

50 歲的瑪丹娜已是歌壇大姊姊, 但 20 歲的她卻為了生活在紐約當舞者, 不惜裸體拍裸照。此次拍賣的裸照有一張正面全裸的照片是由攝影師率佛瑞蘭德所拍系列照片, 後來賣給「花花公子」, 並刊登在 1985 年的該雜誌上。[新聞照片搶先看](#)



瑪丹娜的裸體舊照拍賣價可能超過 33 萬新台幣。

(美聯社)

發信者: 阿墨<AndersonHWI@gmail.com>
主旨: 「愛卡拉」成長 7 成 中華電千元好康
內容: 「愛卡拉」成長 7 成 中華電千元好康

【聯合報/記者郭安國/台北報導】

宅經濟發燒不僅線上遊戲玩家大幅成長, 就連線上卡拉 OK 也熱了起來, 中華電信 MOD 的卡拉 OK、線上卡拉 OK 網站愛卡拉最近業績都出現大幅成長。

愛卡拉執行長張澤銘表示, 去年九月開始愛卡拉會員數就已大幅成長, 當時也是金融風暴期間, 10、11 月會員數和業績更出現 70% 以上的成長, 不景氣, 愈來愈多的網友選擇利用線上卡拉 OK 解壓。[省錢 KTV 的詳細資訊](#)



宅經濟當紅線上卡拉 OK 也是人氣旺、會員成長快速。圖/iKala 提供

測試郵件清單

郵件	郵件種類	郵件標題	寄件者
1	趣味遊戲	Fw:台灣Facebook農田滿種第一人，share農民幣密技	婷婷<tintin336@yahoo.com.tw>
2	政治	李家同：免試入學，窮人孩子出頭不易	教改聯誼會 <callcenter@tw.standardchartered.com>
3	衛生保健	Re:多吃B群吧，新聞說國人維生素B群最缺	菁菁<annie0908@mail2000.com.tw>
4	趣味遊戲	fw:豬認「狗」當媽！瘋狂吸奶 狗媽媽爆瘦10公斤	蕙玲<linlin@npm.gov.tw>
5	情色	林嘉綺代言電玩演出，聽奧女神：最後一次裸露	電玩週報<game@ms66.url.com.tw>
6	新聞時事	像世界末日般，雪梨沙塵染紅歌劇院圖集	weather<weather@yam.com>
7	旅遊休閒	日月潭纜車啟用，旅遊Passport搶手	雄貓旅行社<travel_cat@pie.com.tw>
8	新聞時事	汽車貨物稅減徵3萬最後倒數，腳步加快	汽車雜誌<car@ferrari.com>
9	網路新知	青年安心成家方案，逾5成買前不知道	永慶房仲網<customer@sinyi.com.tw>
10	八卦	連父親都瞞？林志玲爸爸要當阿公卻不知?!	阿霞<info@log.1-apple.com.tw>

網頁型測試郵件範例

寄件者: City Caf
日期: 2009年5月4日 上午 11:11
收件者: [redacted]
主旨: 週年慶送咖啡活動起跑囉

封鎖了某些圖片以協助防止寄件者辨識您的電腦，請按這裡來下載圖片。

美式咖啡通常在速食店、咖啡店，甚至是一般的餐廳都可以喝到。通常它的名稱為「熱咖啡」、「美式咖啡」、「本日咖啡」或是「綜合咖啡」。

而在價錢上美式都是最便宜的喔！口感上會比較清淡，通常都會附上糖包和奶精球。

日式咖啡


早期一般西餐廳與比較傳統的簡餐咖啡大多都是使用日式咖啡。而日式咖啡分成「單品咖啡」與「綜合咖啡」，常見的品項如「藍山」、「曼特寧」、「摩卡」、「巴西」，而綜合咖啡則有「曼巴」、「摩爪」或就稱為「綜合咖啡」。通常日式亦是會附糖包與奶球讓您自己調味！想深入學習咖啡的人，可以由喝日式單品咖啡來入門。而有些日式咖啡也會做花式的變化，如加入一些其他的素材，像是「鮮奶油、巧克力、酒」，至於如何變化，主要是看吧台咖啡師傅個人的創意。

[參加週年慶活動~](#)

<http://211.79.204.64/Email/default.aspx?d1=2009Q2test&d2=101&d3=www.citycafe.com.tw&d4=click&d5=http://www.citycafe.com.tw/>

釣魚郵件記錄方式

郵件頭部資訊：

寄件者: 美惠
日期: 2009年4月9日 下午 04:19
收件者: [redacted]
主旨: Fw: 乳酸菌讓古人命長 幫今人護腸
附加檔案:  乳酸菌的健康密碼.doc (41.6 KB)

封鎖了某些圖片以協助防止寄件者辨識您的電腦，請按這裡來下載圖片。

乳酸菌讓古人命長 幫今人護腸
【元氣周報／記者劉惠敏／報導；衛生署疾管局副局長施文騰／資料提供】

問台灣的成年人「今天喝鮮奶了嗎？」不少人搖頭，其中有人會回答「我喝鮮奶會拉肚子」；若問「今天喝優酪乳了沒？」搖頭的人更多，但極少人會回答「我喝優酪乳會拉肚子」。為什麼？

亞洲人常患乳糖不耐症，無法消化牛奶中乳糖，喝鮮奶時容易腹脹、腹瀉；而優酪乳中的乳酸菌可產生乳糖分解酶，因此可透過飲用乳酸菌產品如優酪乳，獲取奶品中的鈣質而不會腹瀉。

此外，發酵乳還具有免疫調節作用及降低膽固醇、預防泌尿生殖系統細菌感染等。

但多少人知道什麼是乳酸菌？常聽到的，不外乎是「乳酸菌幫助體內環保」、「乳酸菌是腸道守護神」。[進一步了解乳酸菌的好處](#)

圖片未下載時不會被紀錄

未下載圖片時仍可點選連結

（記者陳立凱／攝影）

http://211.79.204.64/Email/default.aspx?d1=gg&d2=153&d3=...&d4=click&d5=http://mag.udn.com/mag/life/storypa

防範惡意電子郵件使用者防護

□ 停 — 使用任何電子郵件軟體前，須先確認以下設定

- 是否已安裝防毒軟體並確實更新病毒碼
- 取消郵件預覽功能(outlook express/檢視/版面配置/預覽窗格，不要勾選顯示預覽窗格的設定)
- 儘量使用純文字模式開啟信件(outlook express/工具/選項/讀取/讀取郵件，☒在純文字中讀取所有郵件)

□ 看 — 收到信件後必須注意

- 信件主旨是否與本身業務相關
- 開啟信件前須先確認信件來源，否則建議刪除

□ 聽 — 若懷疑信件來源必須進行確認

- 透過電話或電子郵件向寄件人確認信件真偽

資安案例分享e-mail社交工程及防護

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


» 電子郵件社交工程之防護

▶ 學習完本單元，您將能夠：

- ▶ 分辨電子郵件的真偽
- ▶ 操作保護機密資料的步驟
- ▶ 列出基本的資安防護工作項目

請點選左列課程章節，進行學習。

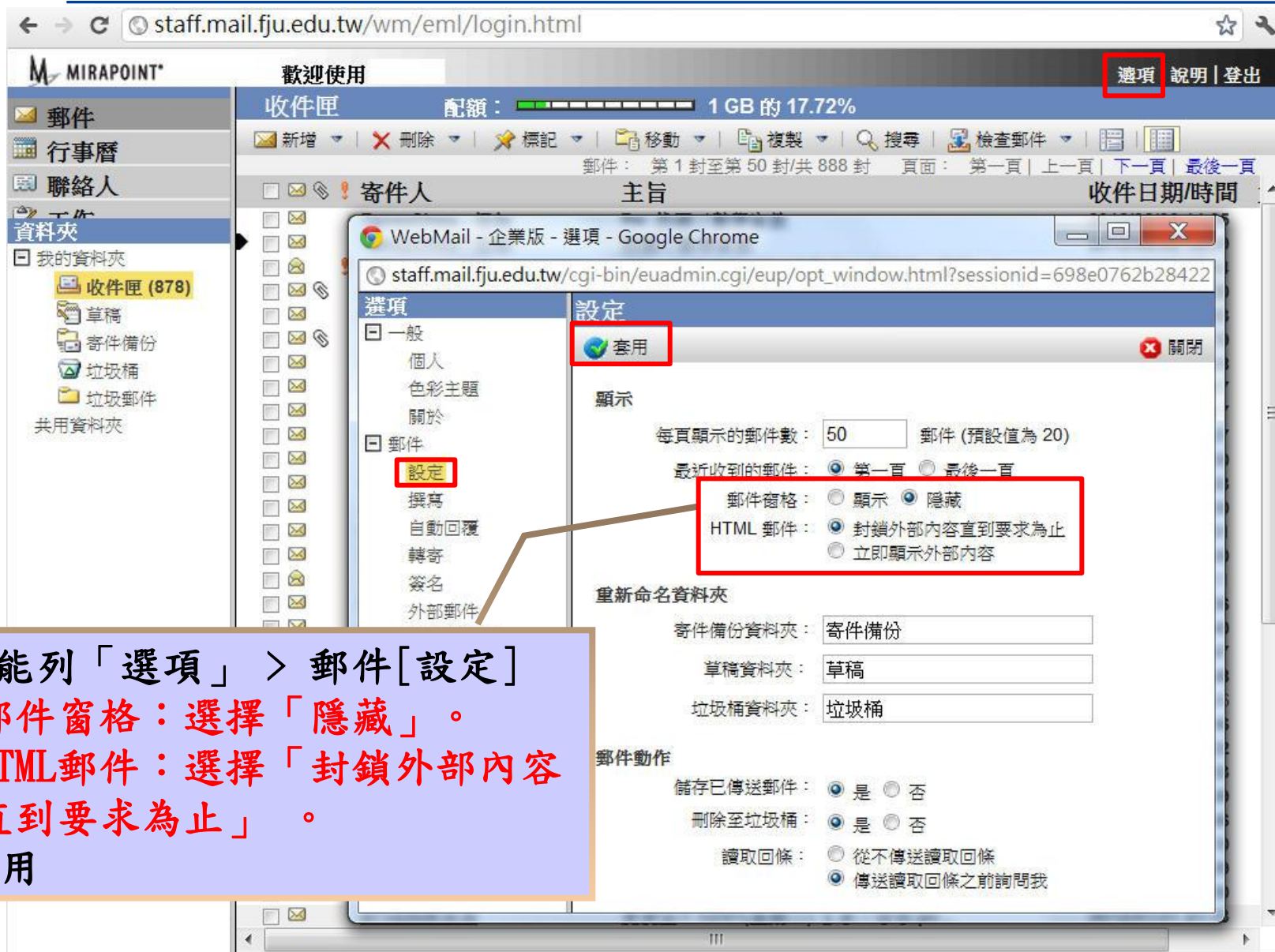
行政院研究發展考核委員會



資安網站→資安攻防演練→資安案例分享-e-mail社交工程及防護

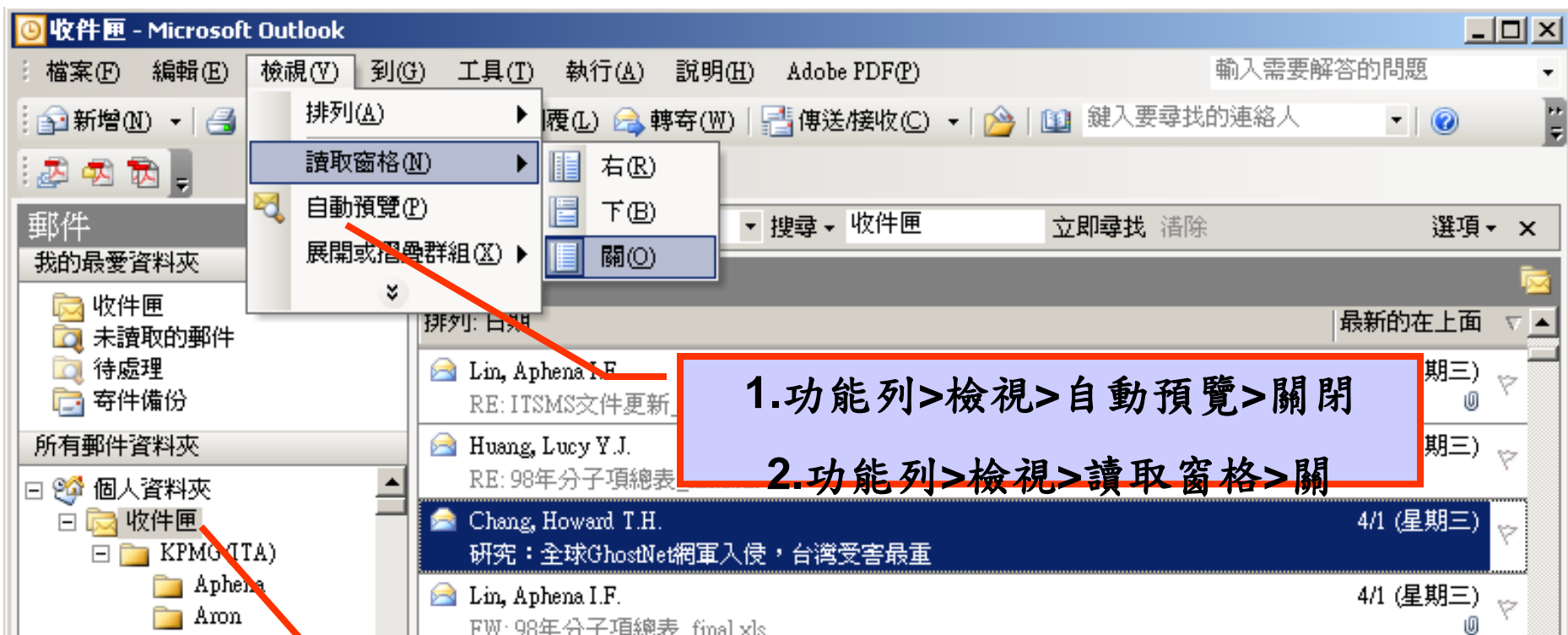
本校WebMail設定

WebMail設定-郵件窗格、HTML郵件



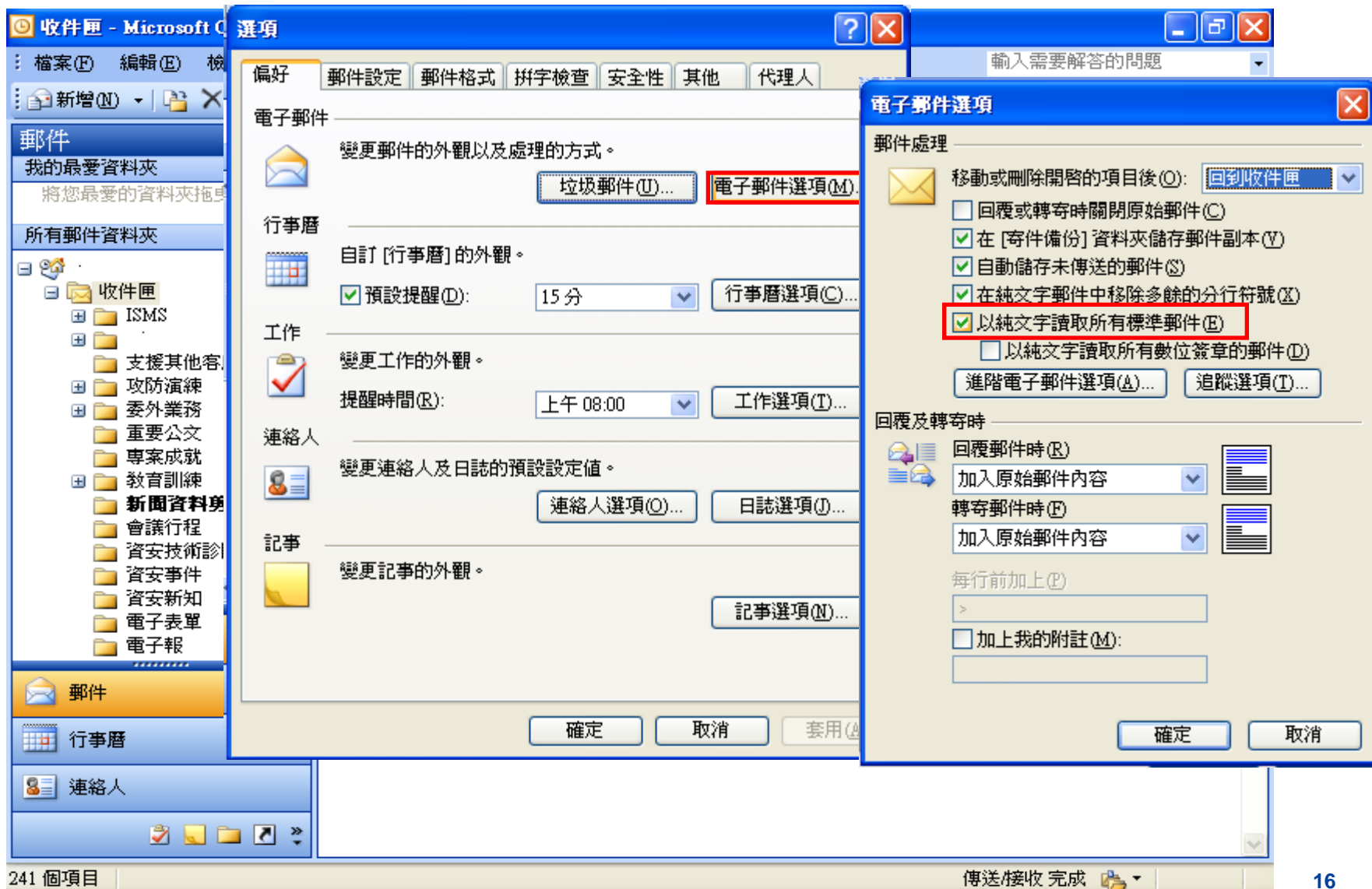
Microsoft Outlook 設定

一、Outlook取消郵件預覽

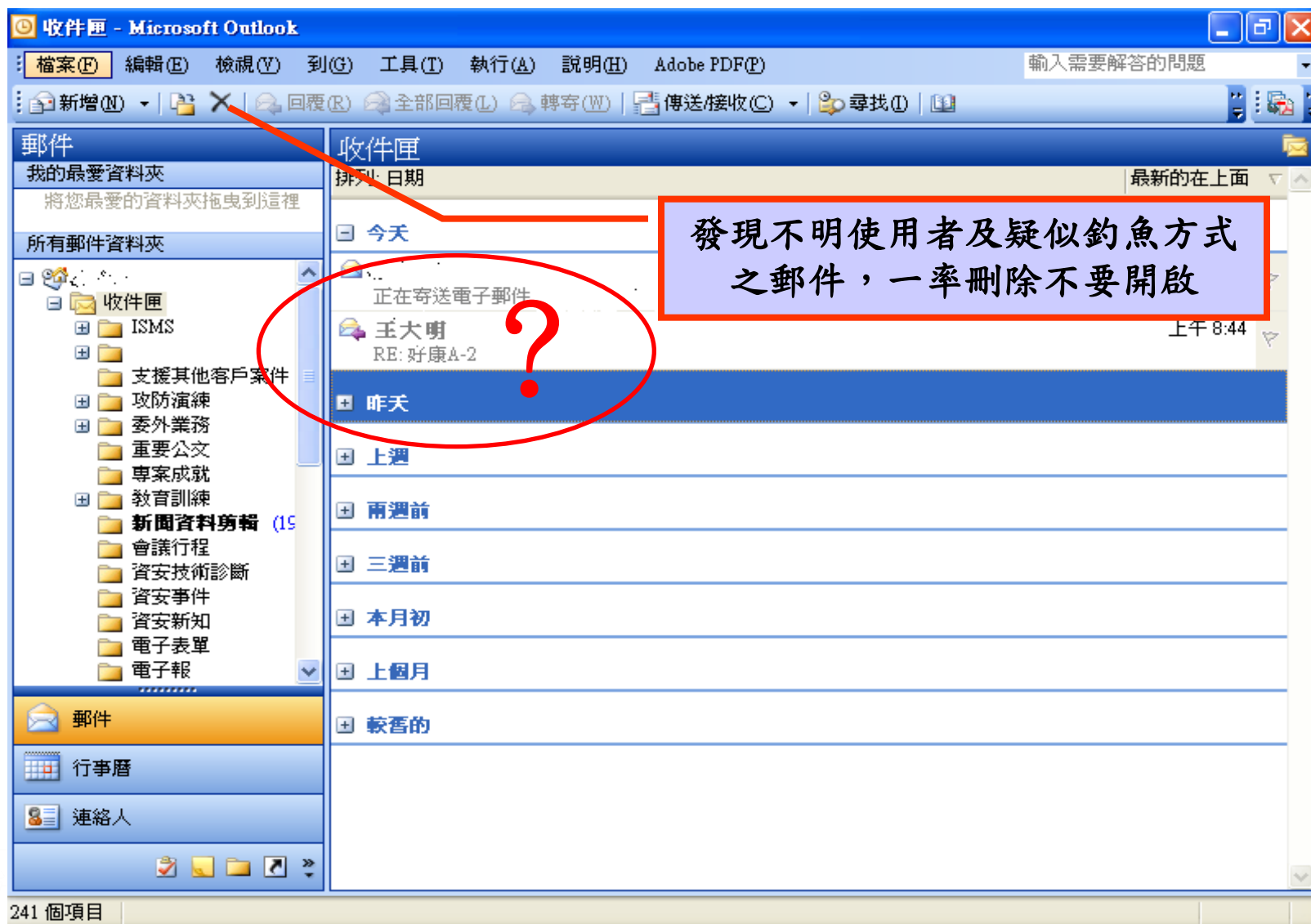


每個資料夾均須完成以上設定才算完成

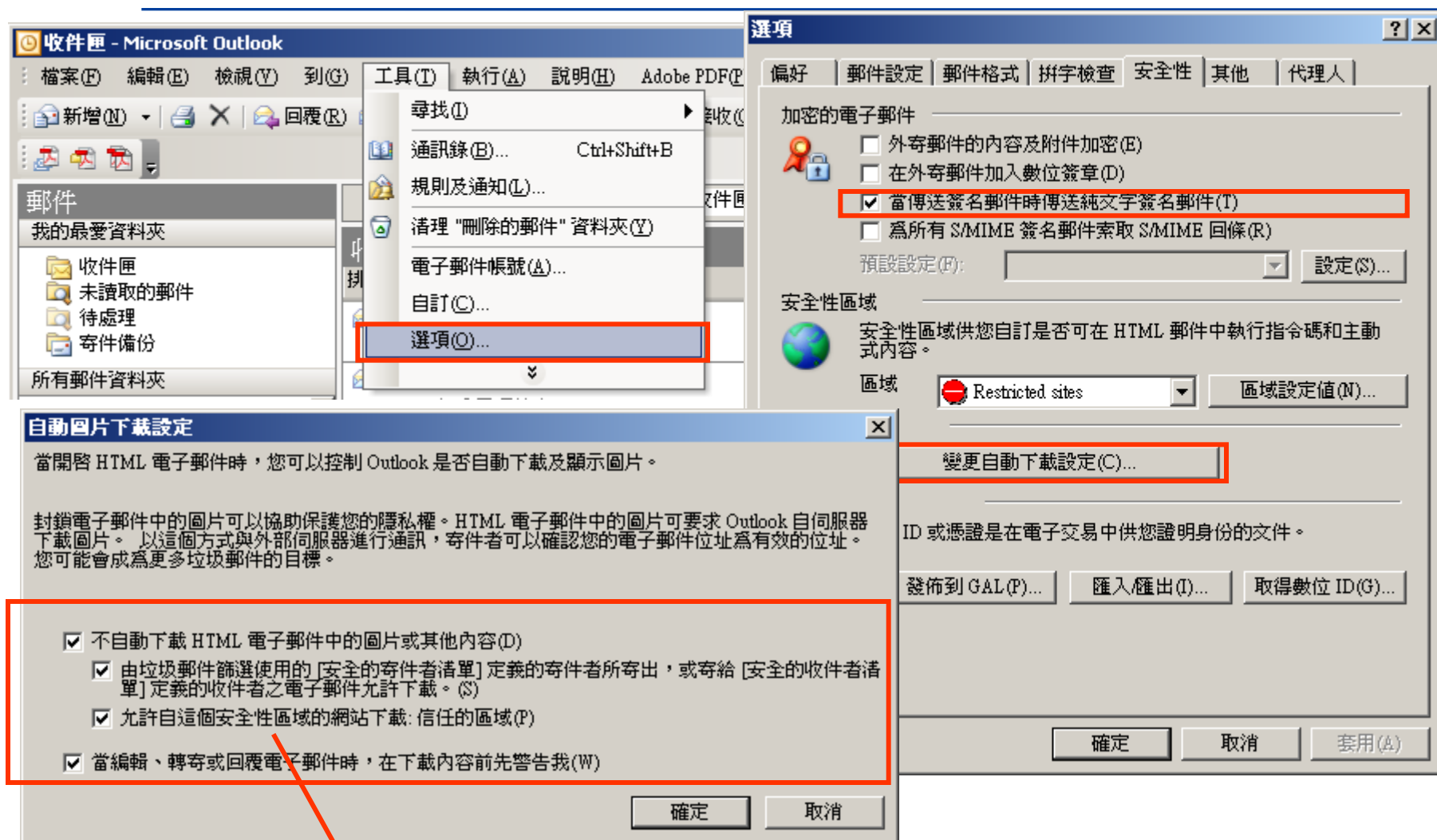
二、Outlook設定純文字模式開啟郵件



三、Outlook刪除不明來源郵件

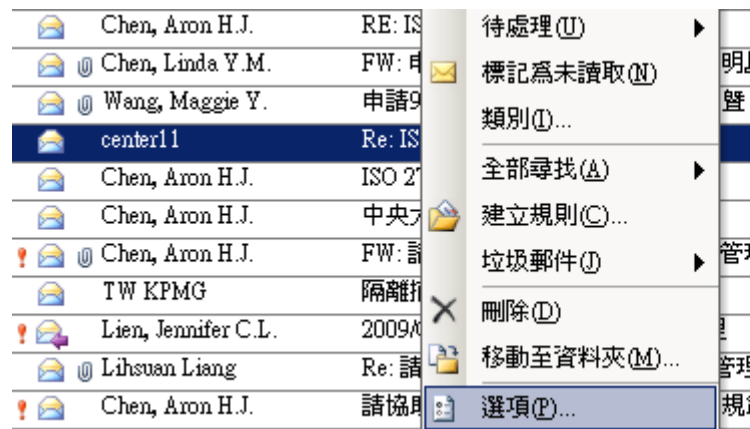


四、設定阻擋HTML電子郵件中的圖片



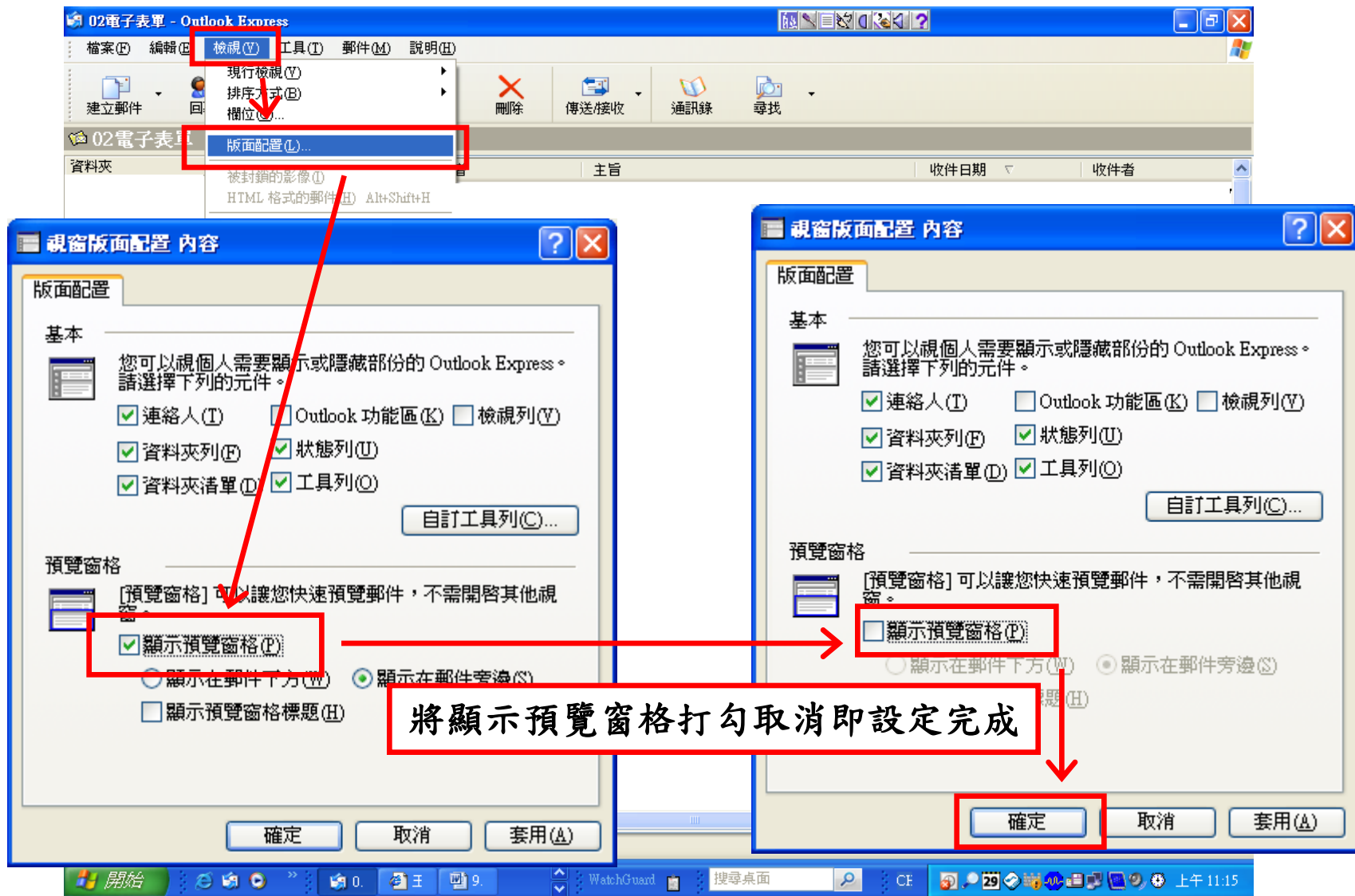
“自動圖片下載設定”內選項均須打勾

五、Outlook確定發信者電子郵件帳號

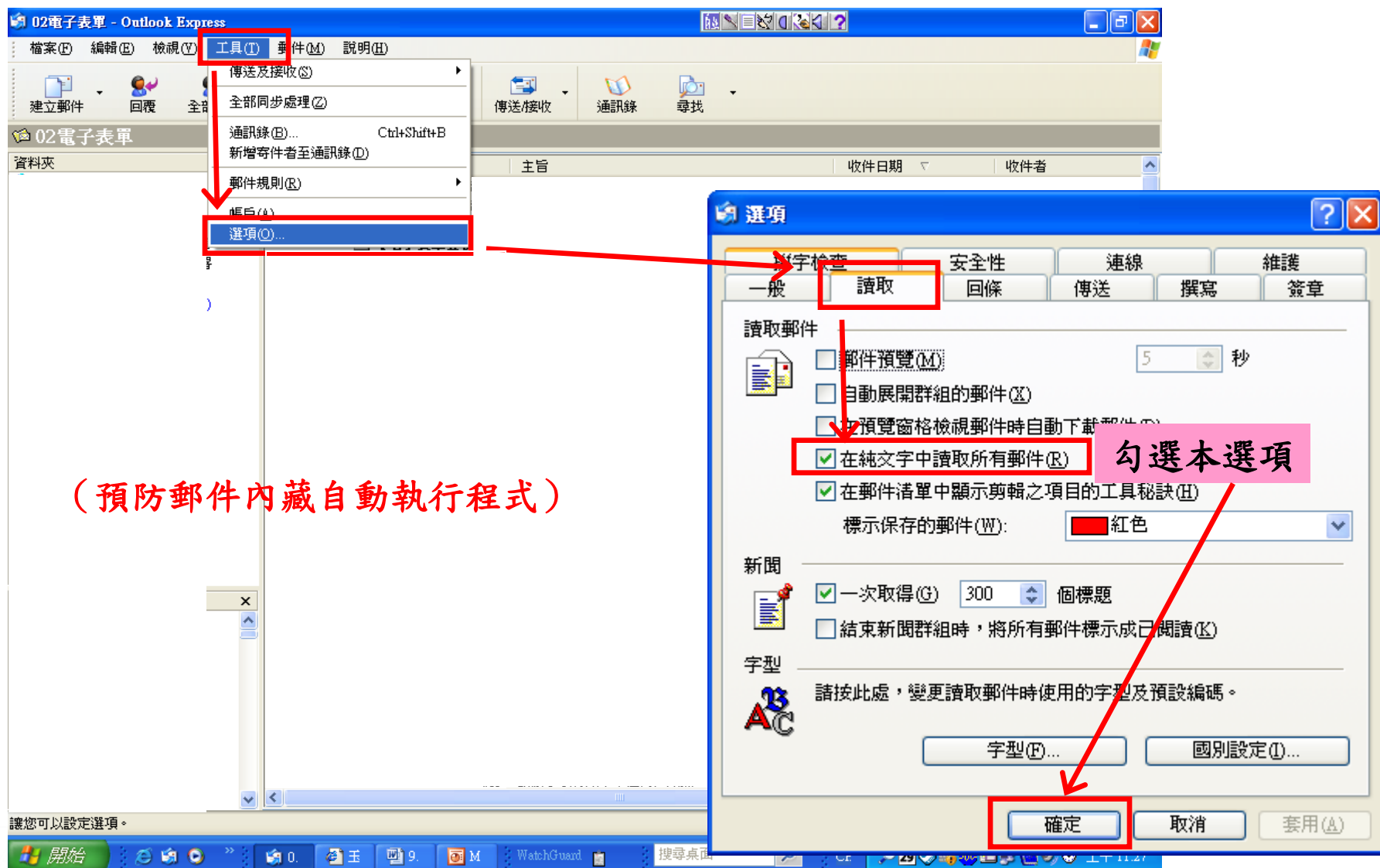


Outlook Express設定

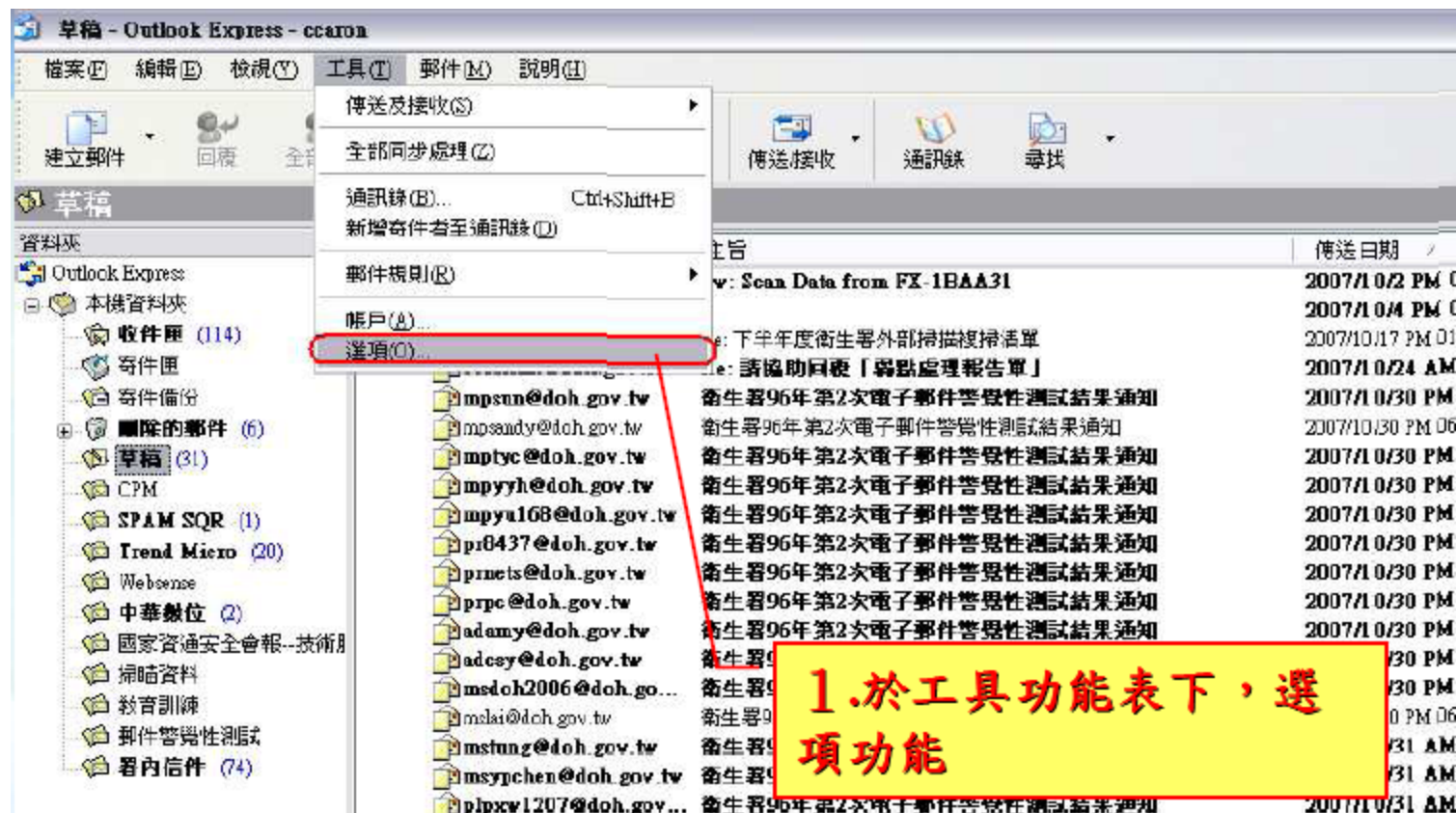
一、Outlook Express關閉預覽視窗設定



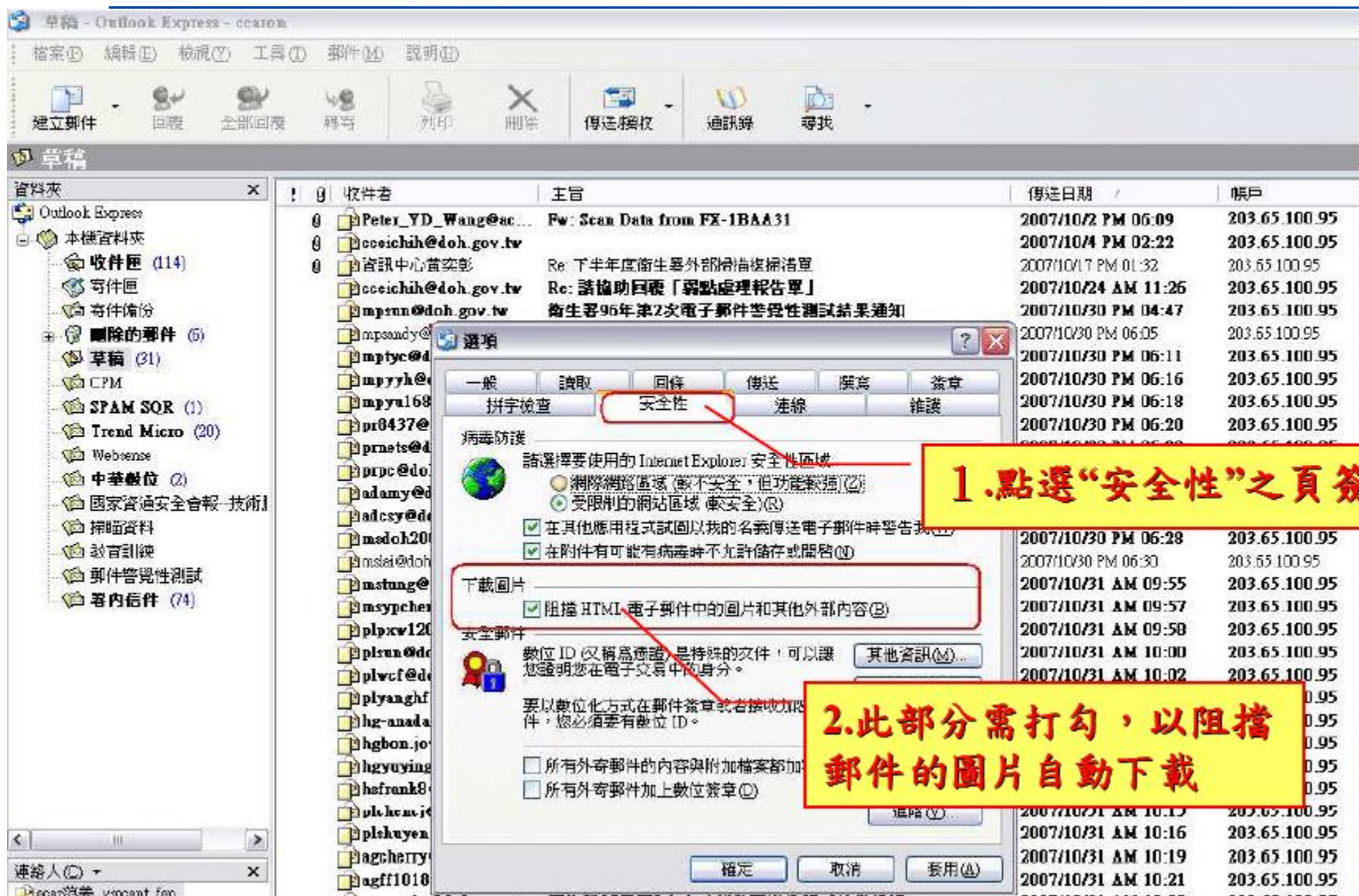
二、Outlook Express以純文字模式開啟郵件



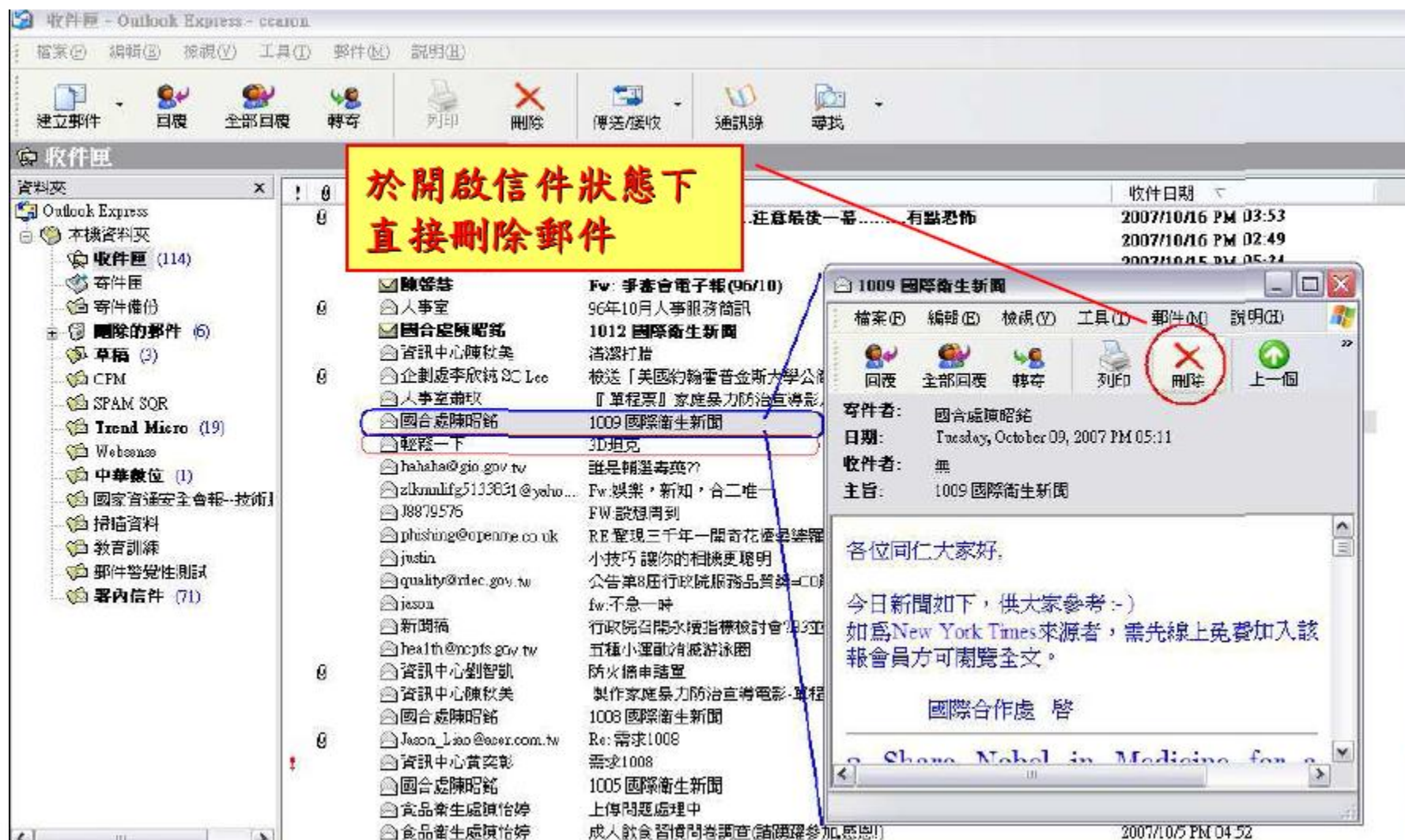
三、設定Outlook Express阻擋電子郵件中的圖片



三、設定Outlook Express阻擋電子郵件中的圖片(續)

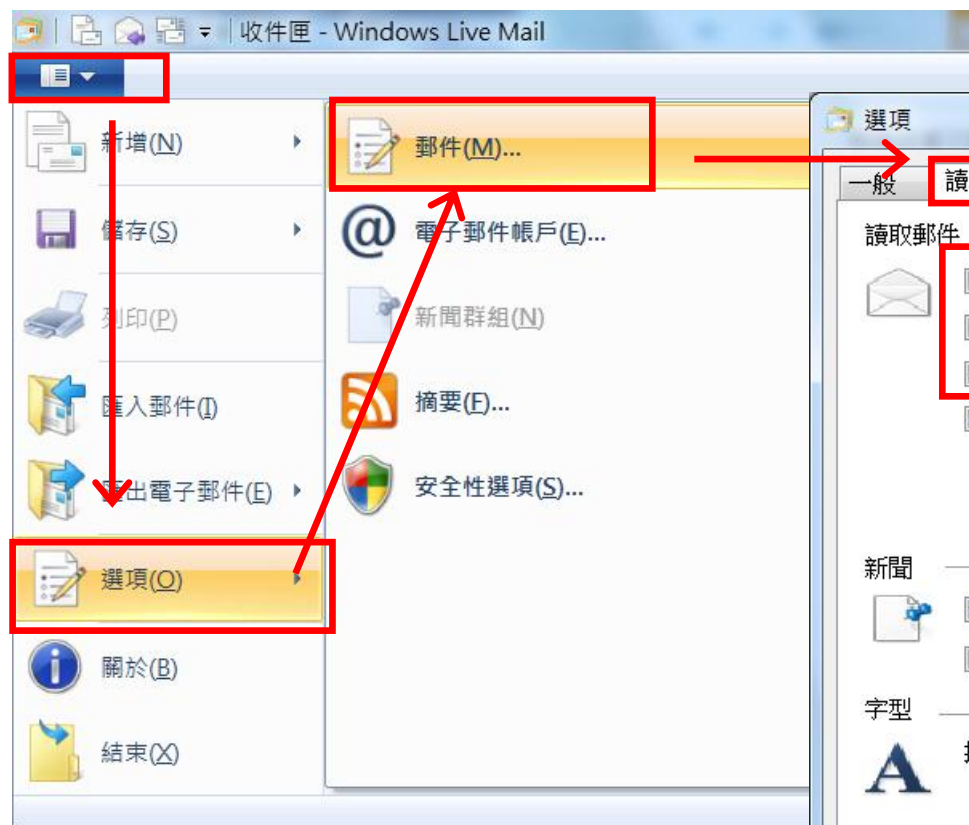


Outlook及Outlook Express操作注意

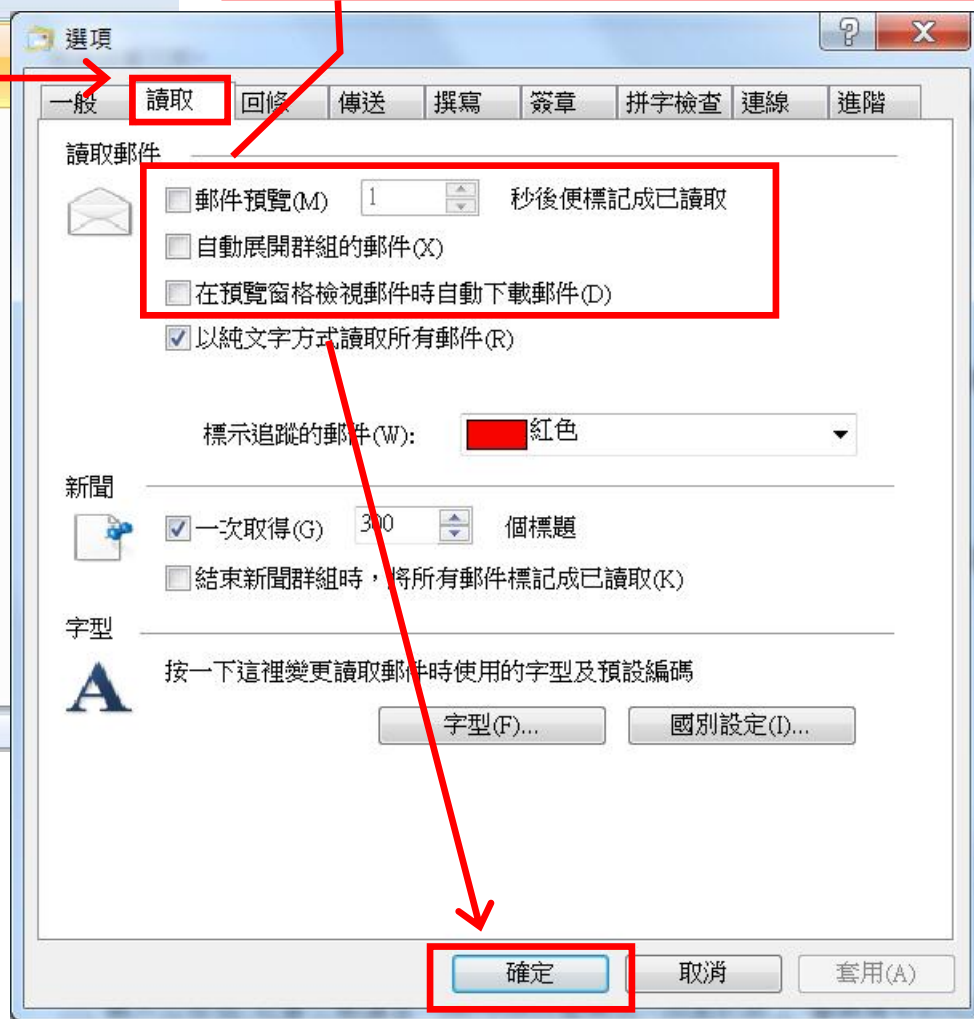


Windows Live Mail設定

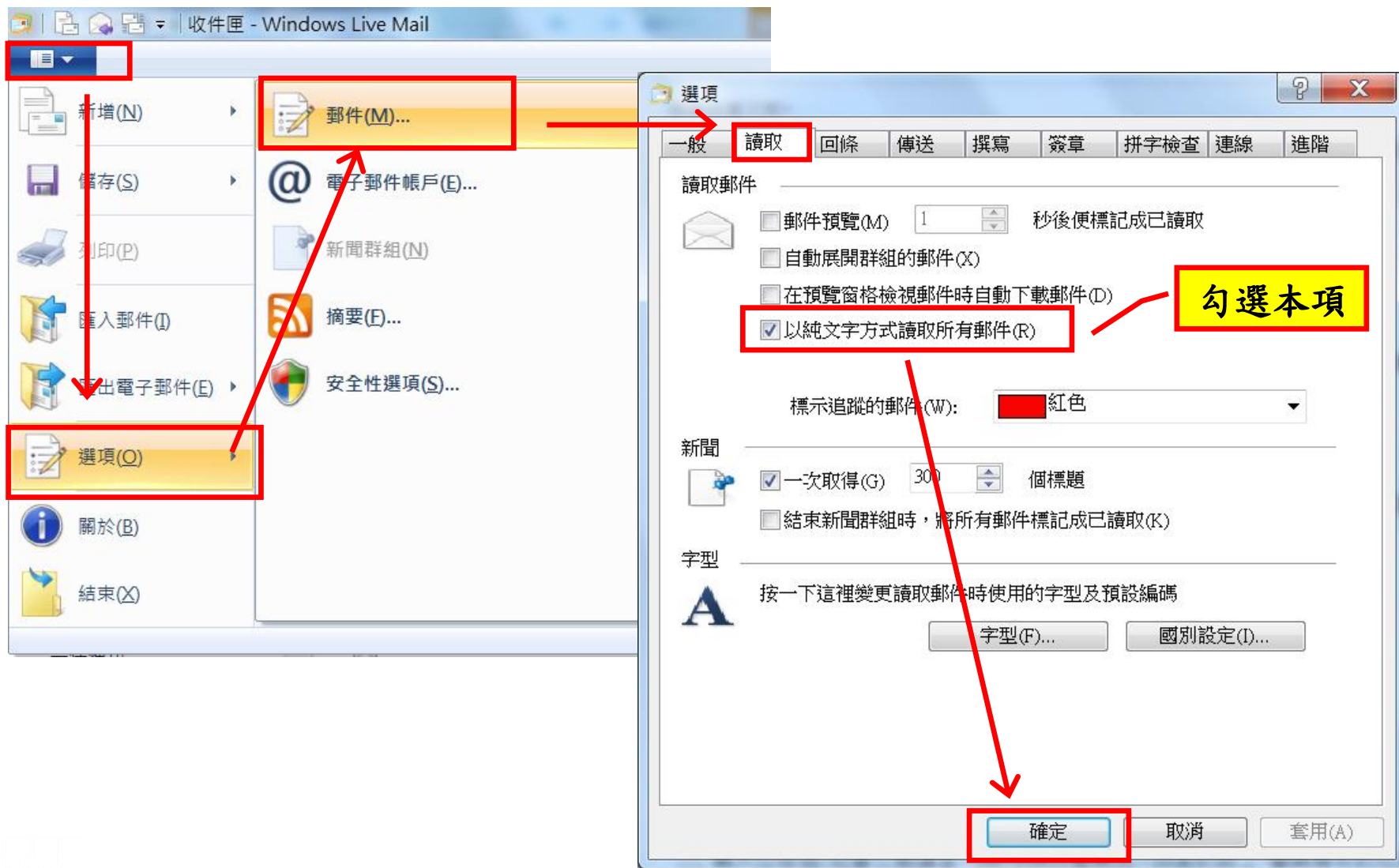
一、Windows Live Mail關閉預覽視窗設定



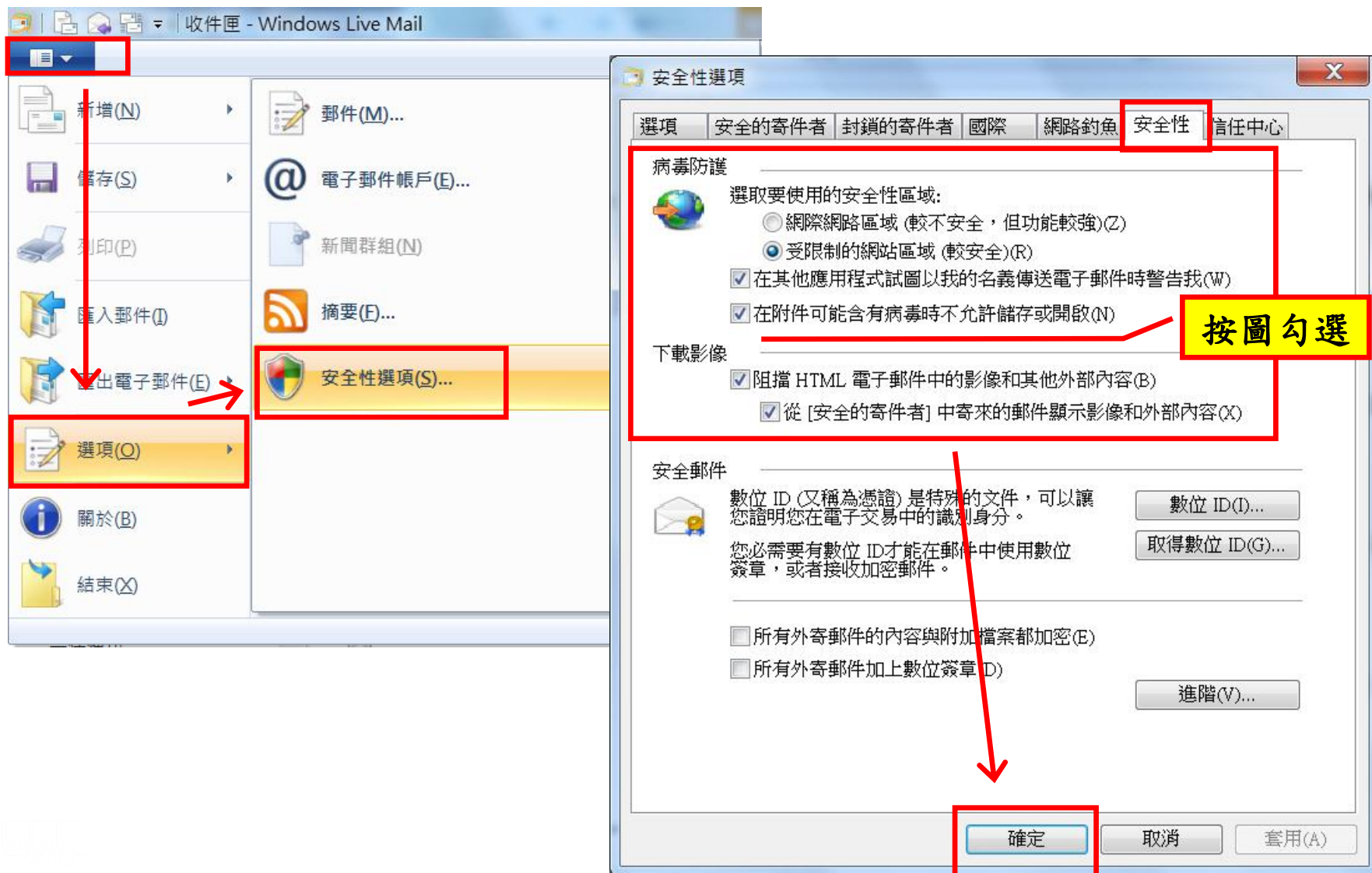
將顯示預覽窗格取消勾選即設定完成



二、Windows Live Mail以純文字模式開啟郵件



三、設定 Windows Live Mail 阻擋電子郵件中的圖片



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
- 不要開啟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(續)

- 不將Email留在任何公開的網頁上
- 不開啟來歷不明之信件
- 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

結論

- 預防重於治療
- 隨時注意更新
- 正確的觀念



問題與討論

