國立臺灣師範大學
National Taiwan Normal University

電子郵件安全設定

資訊中心 網路系統組
柯文傑 網路電話:3733

為什麼e-mail不能亂開？

假冒學校名義，騙取e-mail帳號密碼。利用騙取的帳號密碼寄送垃圾信件。

This is a WebNews Email Account Update
See the below mailing information

Update Your NTNU Email Now.

Dear NTNU Email Owner,This message is from NTNU messaging center to all NTNU Email owners. We are currently upgrading our data base and e-mail center. We are deleting all unused NTNU email to create more space for new one.To prevent your account from closing you will have to update it below so that we will know that it's a present used account.

However NTNU has been receiving complaints from our customers for unauthorised use of the NTNU Email. As a result we are making an extra security check on all of our Customers mailbox in order to protect their information from theft and fraud.

Warning!!! Email owner that refuses to update his or her Email,within two days of receiving this warning will lose his or her Email permanently. You are require to send us the below information via : info.emailteams@gmail.com

Requested Information

Email Username : ....
Email Password : .....
Date of Birth : .....
Country or Territory : .....

Thanks for your co-operation.

非本校e-mail

校內信件不會用英文

為什麼e-mail不能亂開？(續)

駭客使用立委辦公室名義，寄發軍事新聞題材之惡意電郵給記者。由於內容與寄件者的專業屬性吻合，造成多位記者受騙開啟信件而遭植入後門程式

www.appledaily.com.tw ▪頭條要聞 ▪兩岸國際 ▪財經 ▪娛樂 ▪體育 ▪副刊

日蘋報果

聰明玩家情報站

記者收毒郵 疑中駭客搞鬼

列印本頁

2006年04月10日

【黃敬平／台北報導】中國駭客再度傳出利用網路植入有病毒的木馬程式對台灣進行攻擊，但這回受害的不是軍方，而是立委與媒體記者。國民黨立委林郁方國會辦公室信箱上月底以「中共對台用兵，國防部之最新評估」發出一封電郵，不少接獲電郵的記者因此中毒，引起國安單位高度關切，國安局官員說，這次中毒者的檔案資料遭慢速分批送出，不易察覺，是新的駭客攻擊嘗試。

林郁方否認發電郵

這封電郵發自三月三十一日晚上十時，寄件人顯示爲 ly10717b@ly.gov.tw，而非林郁方辦公室平常顯示的「林郁方國會辦公室」，但因電郵主旨是國防軍事的中共動態，不少採訪立法院、軍事或總統府等路線的記者以爲是新聞稿，一時不察，打開附檔後紛紛中毒。林郁方辦公室助理揭仲否認當晚曾發出此封電郵，他說，當時辦公室沒有人，他也沒用這個地址在其他電腦發出任何電郵。揭仲將將此事報告林郁方，並把電腦送到立院資訊中心檢查，工程師說電腦無異狀，也無發出該信的跡象。但可能代表立院的資訊保護系統遭破解，若有該電郵原始檔案，即能循線追溯來源。

國安局官員分析，這次發自立委信箱的有毒電郵「針對性」發給各媒體記者，且中毒者資料遭慢速分批送出，不易察覺，算是一種新的嘗試，頗類似去年攻擊國軍衡山指揮所的手法。

信件中的附檔夾帶病毒。

為什麼e-mail不能亂開？（續）

網友注意：騙徒藉麥可傑克森死訊發惡意郵件

(法新社)2009年6月27日 星期六 21:50

（法新社華盛頓 26日電） 美國 國土安全部（Department of Homeland Security）網路安全部門今天警告，網路騙徒正企圖利用巨星麥可傑克森（Michael Jackson）和法拉佛西（Farah Fawcett）過世的消息來行騙。

美國電腦安全緊急應變小組（U.S. Computer Emergency Readiness Team，US-CERT）表示，該機構「已得知有關報告，即利用麥可傑克森和法拉佛西死訊發出的垃圾郵件、釣魚攻擊（phishing attacks）和惡意程式已增加」。

國土安全部國家網路安全處（National CyberSecurity Division）的操作部門電腦安全緊急應變小組說：「這些電子郵件可能會企圖以釣魚攻擊方式騙取網友的個人資料，或在網友回覆時，記錄電郵地址。」

該小組說：「此外，這些電郵也可能含有惡意程式，或連線到看似合法但含有惡意程式的網站。」

緊急應變小組籲請網友在打開垃圾郵件時務必謹慎，並建議網友，務須確定防毒軟體已更新。（譯者：中央社張佑之）

開啟信件，信件中圖片夾帶木馬、後門程式等。

信件中的圖片若有顯示出來就有可能中毒。

信件中的連結為惡意網站，附件有可能夾帶病毒。

為什麼e-mail不能亂開？（續）

e-mail攻擊方式

- 附件檔利用系統漏洞進行攻擊，如.doc, .pdf ,.jpg (請定時更新windows update及office update)
- 附件檔為執行檔(.exe)，執行後立即中毒。
- 假冒知名單位騙取個人資料。
- 提供假連結騙取資料。

什麼是社交工程？

- 社交工程為利用人性弱點或利用人際之信任關係，獲取不當資訊。
- 指不用程式即可獲取帳號、密碼、信用卡密碼、身分證號碼、姓名、地址或其他可確認身分或機密資料的方法。這些方法多半是使用與人互動的技巧。
- 早期社交工程是使用電話或其他非網路方式來詢問個人資料，而目前社交工程大都是利用電子郵件或網頁來進行攻擊。

電子郵件社交工程攻擊之常見手法

利用寄發電子郵件，假冒親友或公司等相關寄件者，誘騙收件者信任，開啟郵件進行非法攻擊行為。

- 利用吸引人的主旨誘騙開啟郵件
- 偽冒寄件者
- 誘騙登入帳號、密碼(騙取資料)
- 通知重新認證(騙取資料)
- 開啟惡意連結(釣魚網站)
- 下載惡意附件檔(木馬病毒)

可疑電子郵件之特徵

- 陌生人或極少來往對象的來信
- 非正常的寄信時間
- 過於聳動或緊急的主旨
- 主旨與發信人的習性不同
- 需要輸入敏感資料的信件

可疑電子郵件之自我保護措施：

- 非公務業務相關、不明來源與可疑之電子郵件請直接刪除，勿開啟、勿轉寄。

  學校電子郵件帳號以處理學校公務用途為主，其他用途可申請外界免費電子郵件帳號，以確保郵件帳號使用之單純性。

- 不輕易點選、下載或回傳電子郵件內的連結、附件檔案與資料。

- 設定收信軟體安全設定

教育部惡意郵件社交工程演練計畫

- 透過電子郵件社交工程測試信件，針對教育部所屬機關學校進行使用電子郵件警覺性測試。
- 由本校提供所有職員(含工友、約用人員、專案助理)email名單，再由教育部自行挑選抽測人員。

- 測試成功定義

  信件開啟：打開信件本文內所含圖片且完成圖片下載之動作，認定為測試成功。若無圖片下載，不會有安全漏洞。

  連結點選：偵測受測者於收到測試信件後，開啟信件並點擊信件中之URL連結或附檔。

預計99年開啟率、點閱率分為低於10%、6%

98年合格率為16%、9%

教育部惡意郵件社交工程演練計畫(續)

- 第一次測試為5月份，本次共寄發五封測試信，

政治、體育	軍方賣官內幕、洋基球團虧待王建民
休閑娛樂	自行車旅遊私房路線、聯合報邀請您賞桐花
科技新知、保健養生	USB成病毒溫床！台灣電腦今年Q1中毒率列入全球第四大 蛀牙不是病，痛起來要人命
投資理財、保健養生	景氣復甦了嗎？新流感H1N1大流行期間，個人保健注意事項
情色、影視新聞	瑤瑤與舒舒，你喜歡誰

本校第一次測試合格

教育部惡意郵件社交工程演練計畫(續)

- 第二次測試為9月份，本次共寄發10封測試信

編號	信件類別	信件標題
1	生活類	讓你感動的動人廣告
2	投機類	如何提高中獎機率!!
3	旅遊類	【HiNet 旅遊網首發團】 獨家限量獨享好康超低價!!
4	旅遊類	【HiNet 旅遊網首發團】 暑假獨家好康 數量有限 請速報名
5	健康類	健康新搬步!!?你如何活的更健康
6	電腦科技類	七夕前後交友網站爆高量 慎防網路桃色陷阱
7	影視類	文英阿姨病逝 留給觀眾無限懷念
8	影視類	昔日玉女紅星 酒井法子自首 坦承吸毒
9	趣味類	親愛的同事!放鬆一下
10	購物類	iPhone 最新推出 3Gs 便宜到不敢相信！！

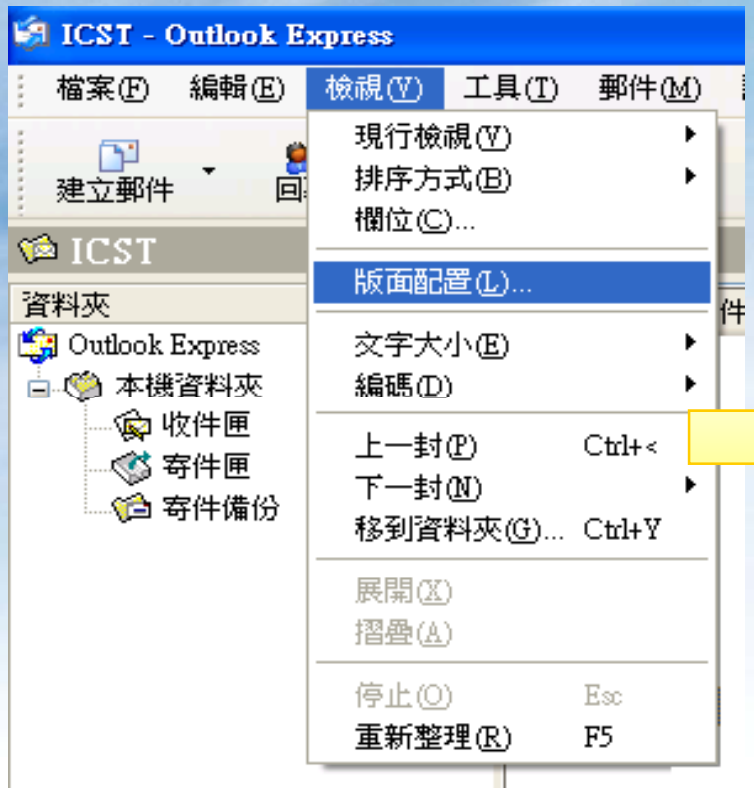
本校第二次測試不合格

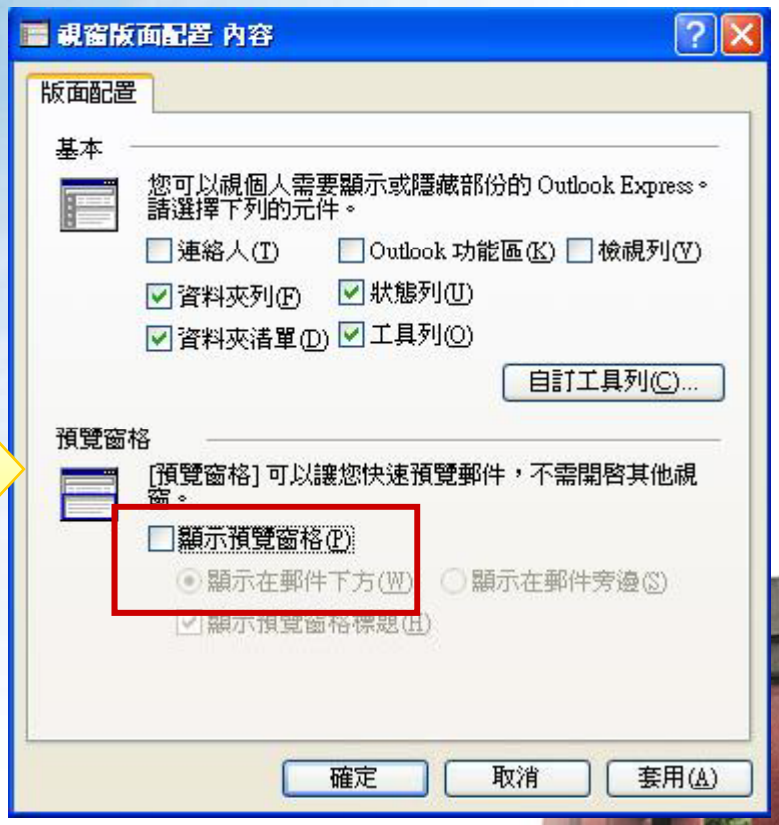
收信軟體安全設定

- 使用任何電子郵件軟體前，必須先確認
  - 執行各種作業系統、應用軟體設定更新
    - Windows Update
    - Office Update
  - 必須安裝防毒軟體，並確實更新病毒碼
  - 收信軟體安全性設定
  - 啟用個人防火牆

Outlook Express安全設定

- 取消「顯示預覽窗格」

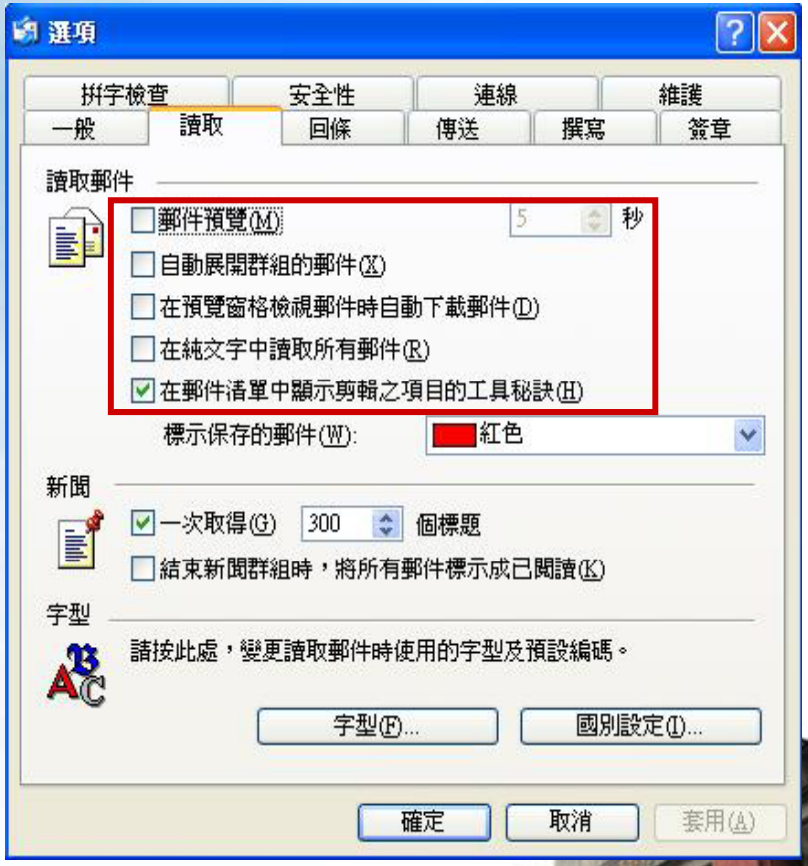




Outlook Express安全設定

工具－＞選項－＞讀取

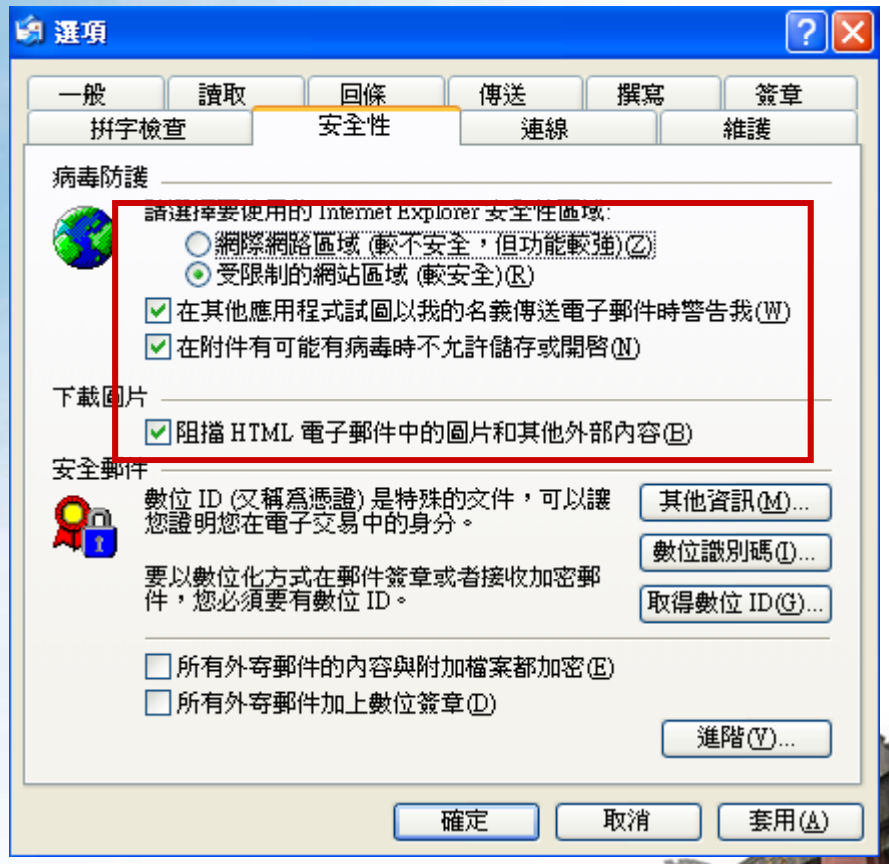
- 取消「郵件預覽」
- 取消「自動展開群組的郵件」
- 取消「在預覽窗格檢視郵件時自動下載郵件」
- 勾選「在純文字閱讀所有郵件」(最好要勾選，若閱讀有困難，可不勾選)



Outlook Express安全設定

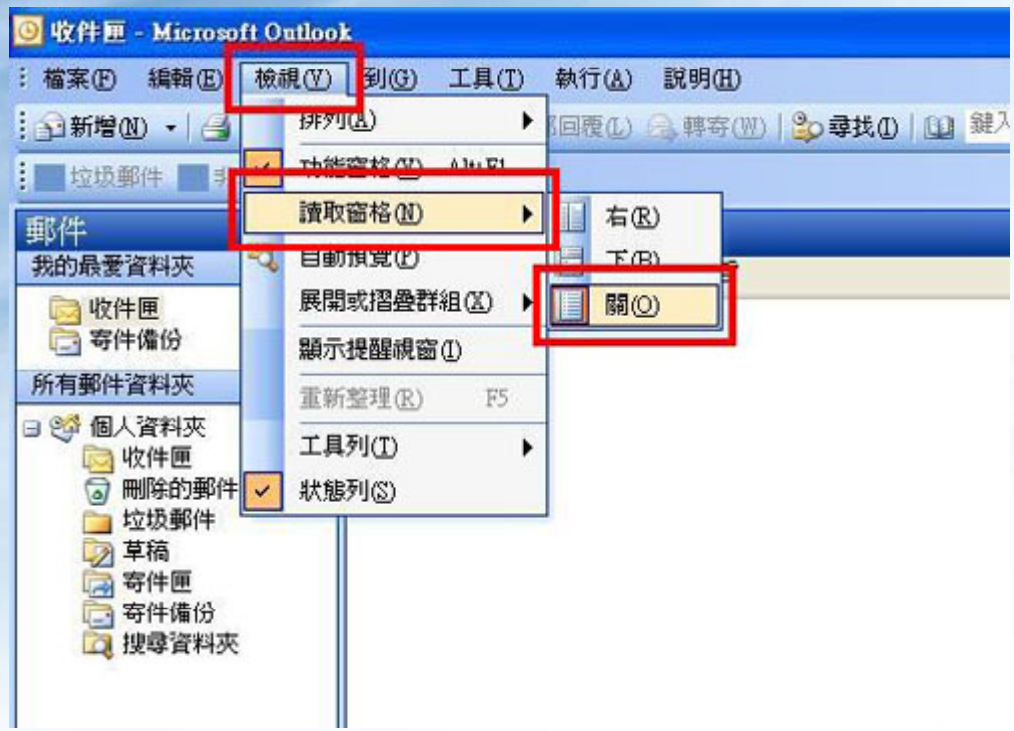
工具－＞選項－＞安全性

- 設定安全性區域為「受限制的網站區域」
- 勾選「在其他應用程式試圖以我的名義傳送電子郵件時警告我」
- 勾選「在附件有可能有病毒時不允許儲存或開啟」
- 勾選「阻擋HTML電子郵件中的圖片和其他外部內容」



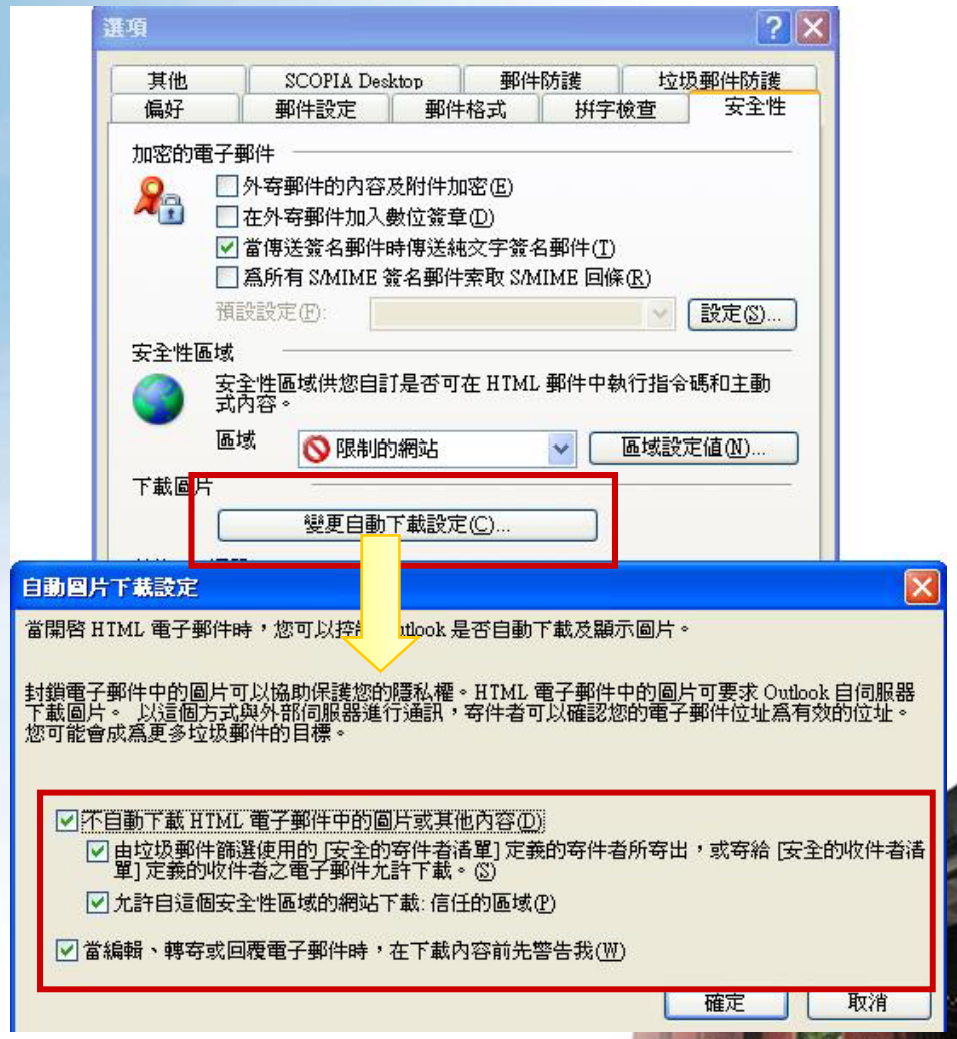
Outlook 2003安全設定

- 取消「讀取窗格」－＞選「關」



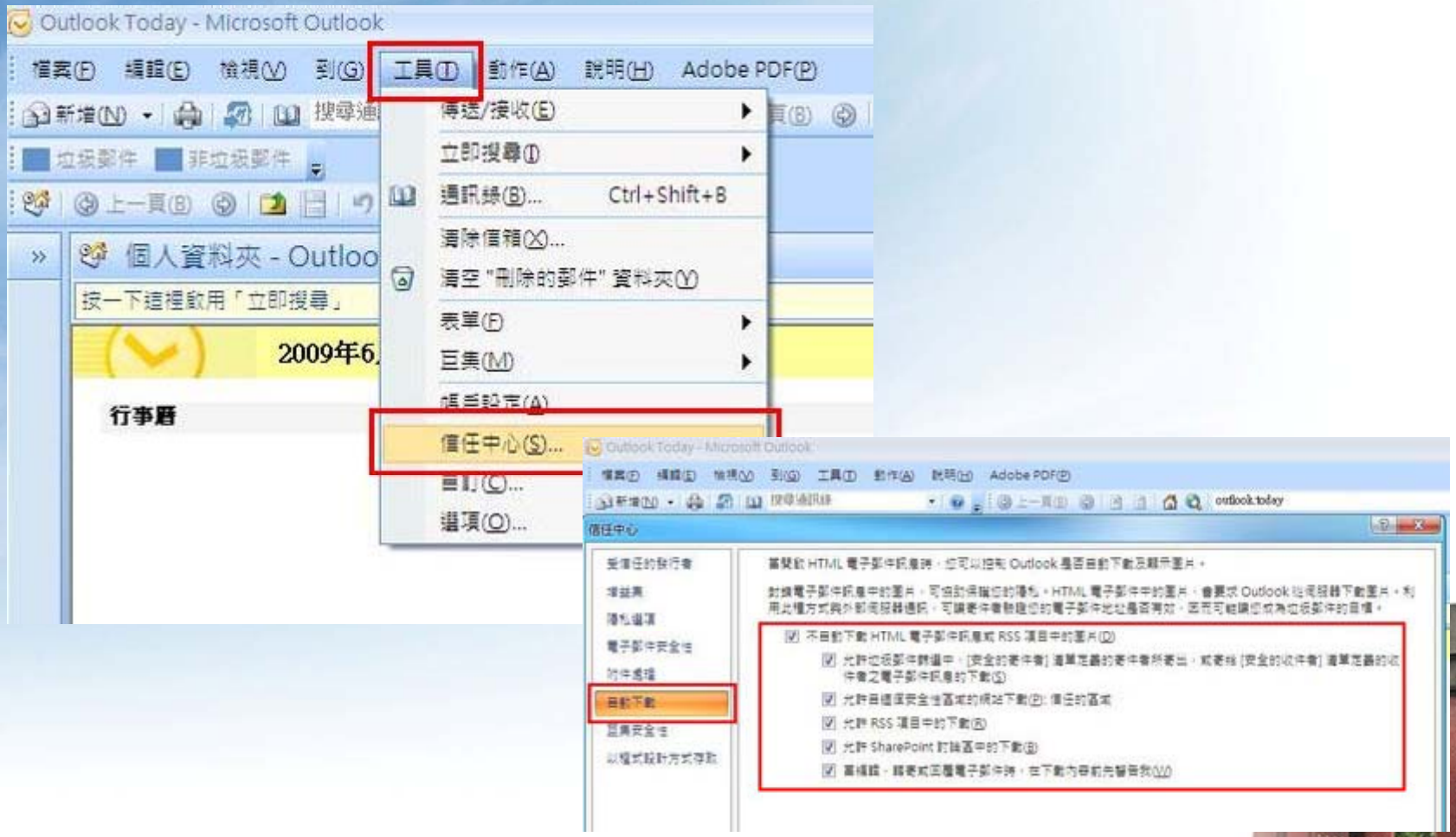
Outlook 2003安全設定

- 工具－＞選項－＞安全性
- 「變更自動下載設定」所有選項都勾選



Outlook 2007安全設定

- 工具－＞信任中心－＞自動下載〔全部都勾選〕

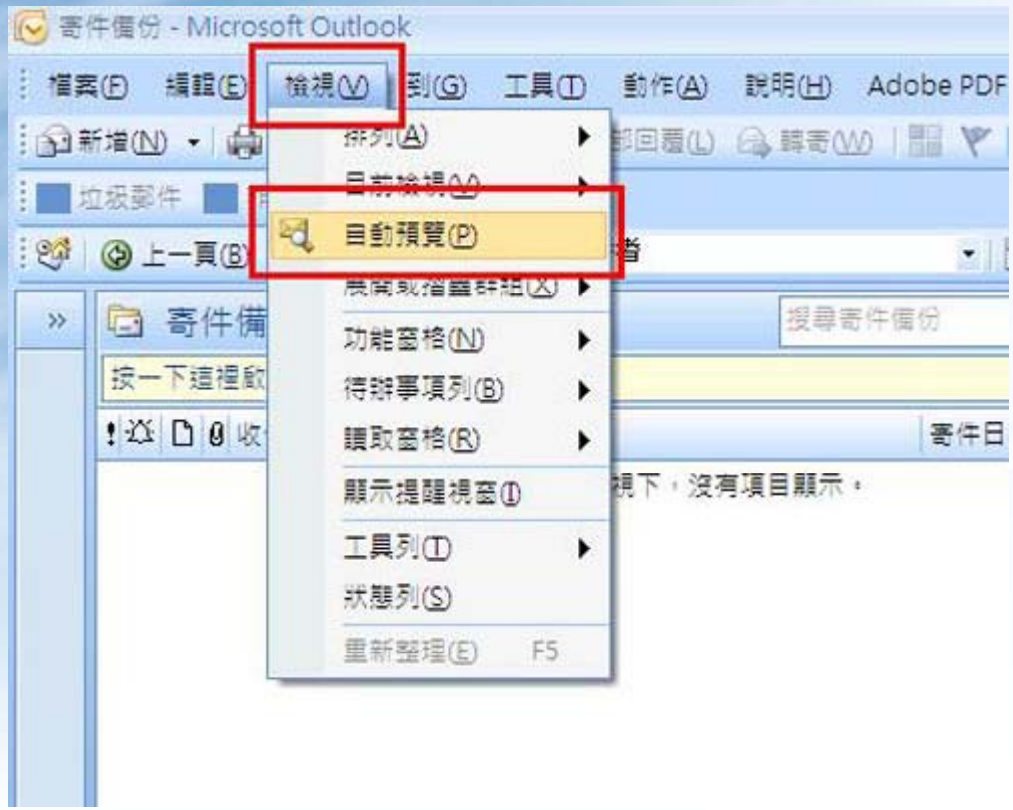


Outlook 2007安全設定

- 「檢視」－＞「讀取窗格」－＞選「關」

Outlook 2007安全設定

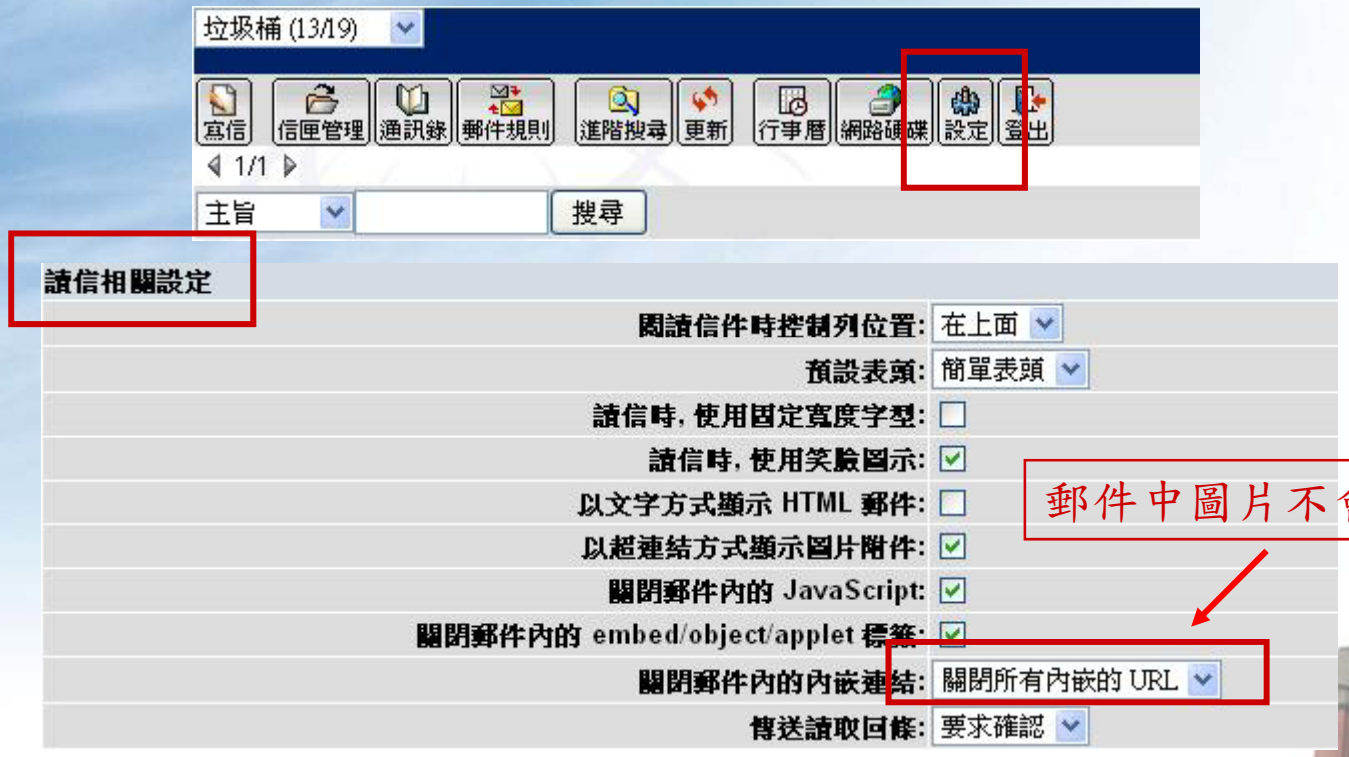
- 「檢視」－＞關閉「自動預覽」



Webmail安全設定

- 「設定」－＞「讀信相關設定」（依下圖方式設定）

（若要增加安全性，可勾選「以文字方式顯示HTML郵件」）

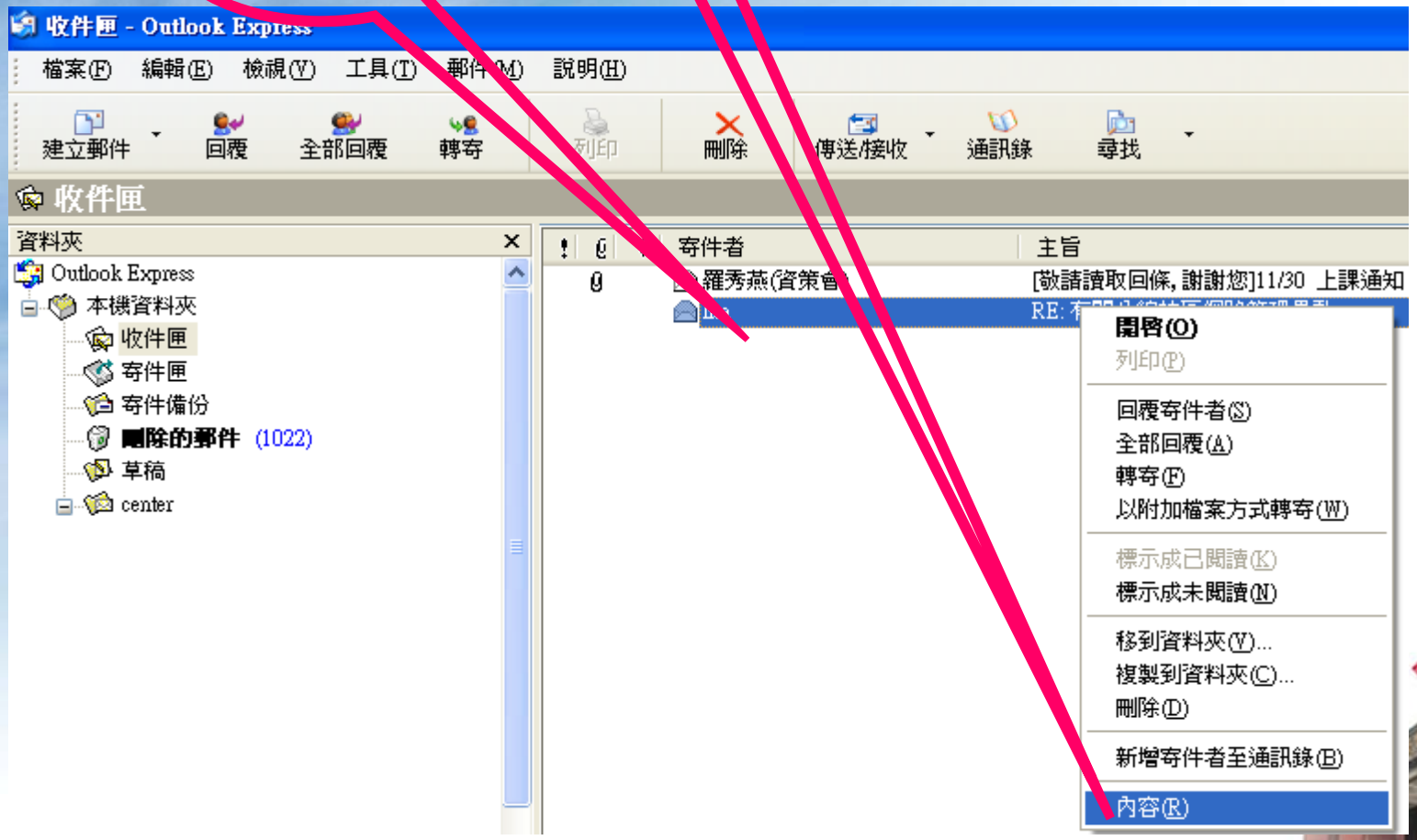


收信注意事項

- 開啟電子郵件前應先依序檢視：
  (1)、【寄件者】
  (2)、【郵件主旨】
  (3)、【附加檔案】等郵件訊息

收信注意事項（續）

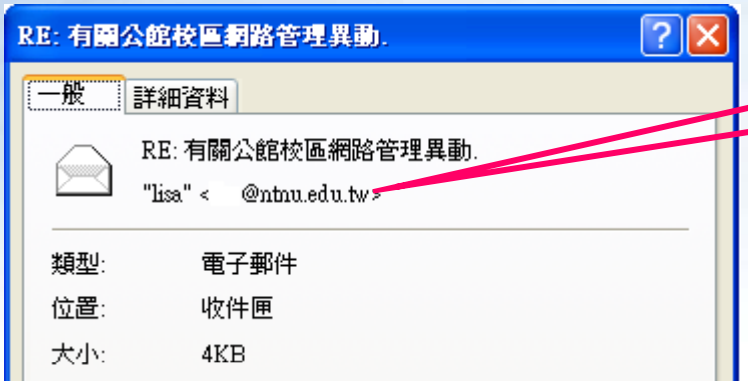
在信件上按「滑鼠右鍵」再點選「內容」以檢視郵件相關訊息



收信注意事項（續）

(1)、檢視【寄件者】

1. 若【寄件者】與您業務相關且認識，並確認電子郵件信箱位址無誤，如有冒用偽裝情形，則建議直接刪除該郵件。
2. 若【寄件者】來自政府機關，其信箱位址應屬於gov.tw，若【寄件者】來自非政府機關，則應特別謹慎確認。
3. 師大內部信件一定來自ntnu.edu.tw



檢視寄件者信箱位址是否正確？

收信注意事項（續）

(2)、檢視【郵件主旨】

- 若【郵件主旨】與您業務無關或主旨怪異，則建議直接刪除該郵件。

收信注意事項（續）

(3)、檢視【附加檔案】

- 若【附加檔案】名稱顯示與您業務無關或檔名怪異、錯誤，請勿開啟【附加檔案】或建議直接刪除該郵件。
- 若電子郵件中帶有副檔名為 .doc或 .ppt等之附件，應特別小心勿任意開啟附加檔案。
- 副檔名為雙副檔名者應立即刪除。如. jpg. exe。
- 高危險檔案類型. exe, . com, . scr, . bat, .cmd, . lnk

收信注意事項（續）

- 若懷疑郵件來源，必須進行確認
  - 透過電話或電子郵件向寄件人確認郵件真偽

不要在開啟郵件狀況下，直接按刪除鈕，應回到郵件清單(index)下刪除郵件，以免無意間直接開啟下一封郵件。

收信注意事項（續）

注意事項：

- 收信
  - 檢查寄件者的真偽
  - 確認信件內容的真實度
  - 不輕易開啟郵件中的超連結以及附件
  - 開啟超連結或檔案前，確認對應軟體（如IE、Office、壓縮軟體）都保持在最新的修補狀態
- 轉信或寄信
  - 未經查證之訊息，不要轉寄
  - 轉寄郵件前先將他人郵件地址刪除，避免別人郵件地址傳出
  - 寄送信件給群體收件者時，應將收件者列在密件副件，以免收件人資訊外洩。