國立臺灣師範大學
National Taiwan Normal University

電子郵件社交工程

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)

電子郵件社交工程攻擊之常見手法

From: Queens
Sent: Friday, February 17, 2012 1:15 AM
To: undisclosed-recipients:
Subject: Warning! Your mailbox is almost full.

You have exceeded your email limit quota of 450MB. You need to upgrade your email limit quota to 2GB within the next 48 hours. Use the below web link to upgrade your email account:

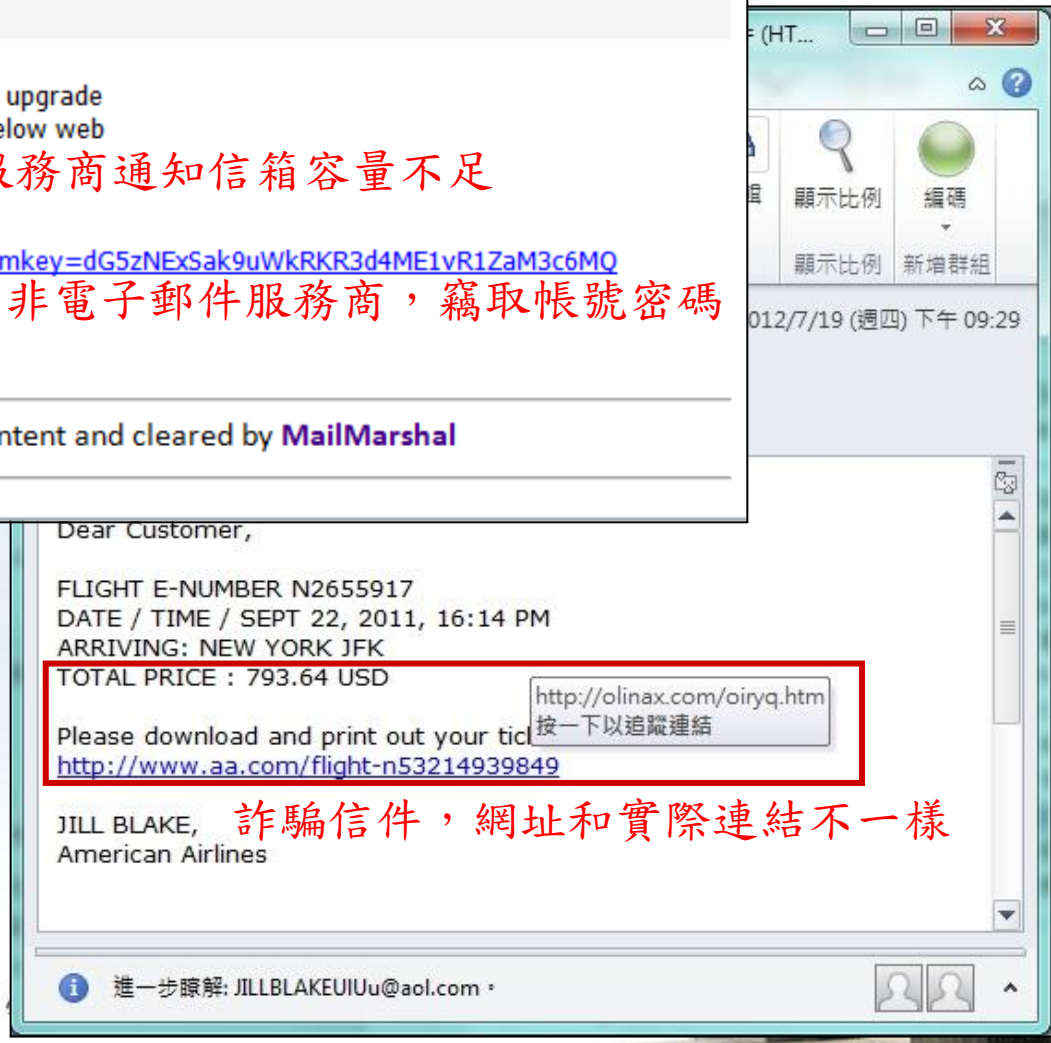
假冒電子郵件服務商通知信箱容量不足

click link below:
https://docs.google.com/a/blumail.org/spreadsheet/viewform?formkey=dG5zNExSak9uWkRKR3d4ME1vR1ZaM3c6MQ

連結使用google docs，非電子郵件服務商，竊取帳號密碼

Thank you for using our email.
Copyright ©2012 Email Helpdesk Centre.

This e-mail message has been scanned for Viruses and Content and cleared by **MailMarshal**



電子郵件社交工程攻擊之常見手法

亲爱的E-mail用户，
Prieto González, Ana (ana.prieto.gonzalez@xunta.es) 新增連絡人 2015/4/7 下午 12:38
收件者: undisclosed-recipients:

亲爱的E-mail用户，

假冒電子郵件服務商通知信箱異常，使用翻譯軟體，語意不明

此消息是从邮局互联网维护团队™，
目前，我们正在升级所有邮件数据库和电子邮件帐户中心IE主页视图，提升新的2015年反垃圾邮件和防病毒软件，超大邮箱空间安全设施。我们将删除它并没有更积极，以启用新帐户的用户创造更多的空间，所有的旧的和未使用的电子邮件帐户。

提交您的账户激活，您需要 点击这里 并通过正确填写您的详细信息，让你的电子邮件帐户将在24小时内被重新激活，没有任何延迟重新确认您的电子邮件帐户的详细信息。

點選連結竊取帳號密碼

感谢您的合作，
电子邮件系统管理员，
企业邮局互联网维护团队™，
警告代码：VX2G99AAJ，
中央的webmail队（BETA）

電子郵件社交工程攻擊之常見手法

虛構出一位美女利用社交工程，就能攻陷美國資訊安全部門

PW PingWest中文網 發表於 2013年11月05日 08:02 | 收藏此文 | g+1 173

美國政府資訊安全部門最近接受了一項滲透測試，結果證明信息安全部門的資訊也不安全——儘管該部門的主管並不使用社群網路，但他的電腦仍然被人以社交工程攻擊的方式攻破。

攻擊成功的關鍵在於一名被虛構出來的年輕女性員工Emily Williams。滲透測試的發起者World Wide Technology使用了一名美貌的年輕女性的真人照片偽造了個人資料。

身份資料偽造完畢後，這位被虛構出來的虛擬女性就開始在社群網路上與美國政府資訊安全部門的員工搭訕。她在24小時內就與60人成為Facebook好友。

快到耶誕節時，Emily就開始向這些員工發送帶有惡意連結的耶誕節卡片。存取這個連結的使用者會自動執行一個Java小程式，依次向團隊的其它成員發動攻擊以此來獲得管理員許可權。

最後，資訊安全部門的主管收到了一封帶有惡意連結的電子郵件，他打開了連結後，這台擁有管理員許可權的電腦就此被攻破。在這次滲透測試過程中，World Wide Technology成功地獲得密碼，安裝了惡意程式，並竊取到了國家機密文件。

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。

教育部規定開啟率、點閱率分為須低於10%、6%

教育部惡意郵件社交工程演練計畫(續)

- 測試信件標題

編號	信件類別	信件標題
Letter 1	時事類	鼎王認錯補償 打 8 折送鍋底
Letter 2	財經類	好文分享-兩岸服貿協議真的「利大於弊」？
Letter 3	旅遊類	跟著 KANO 電影四大場景，遊台灣棒球原鄉—嘉義
Letter 4	生活類	十二星座小孩該怎麼教？
Letter 5	知識類	煤炭的難題
Letter 6	科技類	「奈米」即將改變你的世界
Letter 7	美女類	F90--由 15 名性感妹子組成的遊戲代
Letter 8	美容類	打造千頌伊美鼻 醫師：微整注射不
Letter 9	健康類	8 種台灣版超級食物！你一定不能錯
Letter 10	新奇類	帶鹹味的繽紛，探索克里米亞腐海之

郵件主旨
【公告】人事異動通知
遠端教育訓練變更通知
Safari 漏洞或導致瀏覽歷史、Google 帳戶資訊外洩
如果您無法登入帳戶
【人事公告】員工加薪通知
【公告】人事異動通知
遠端教育訓練變更通知
Safari 漏洞或導致瀏覽歷史、Google 帳戶資訊外洩
如果您無法登入帳戶
【人事公告】員工加薪通知

收信軟體安全設定

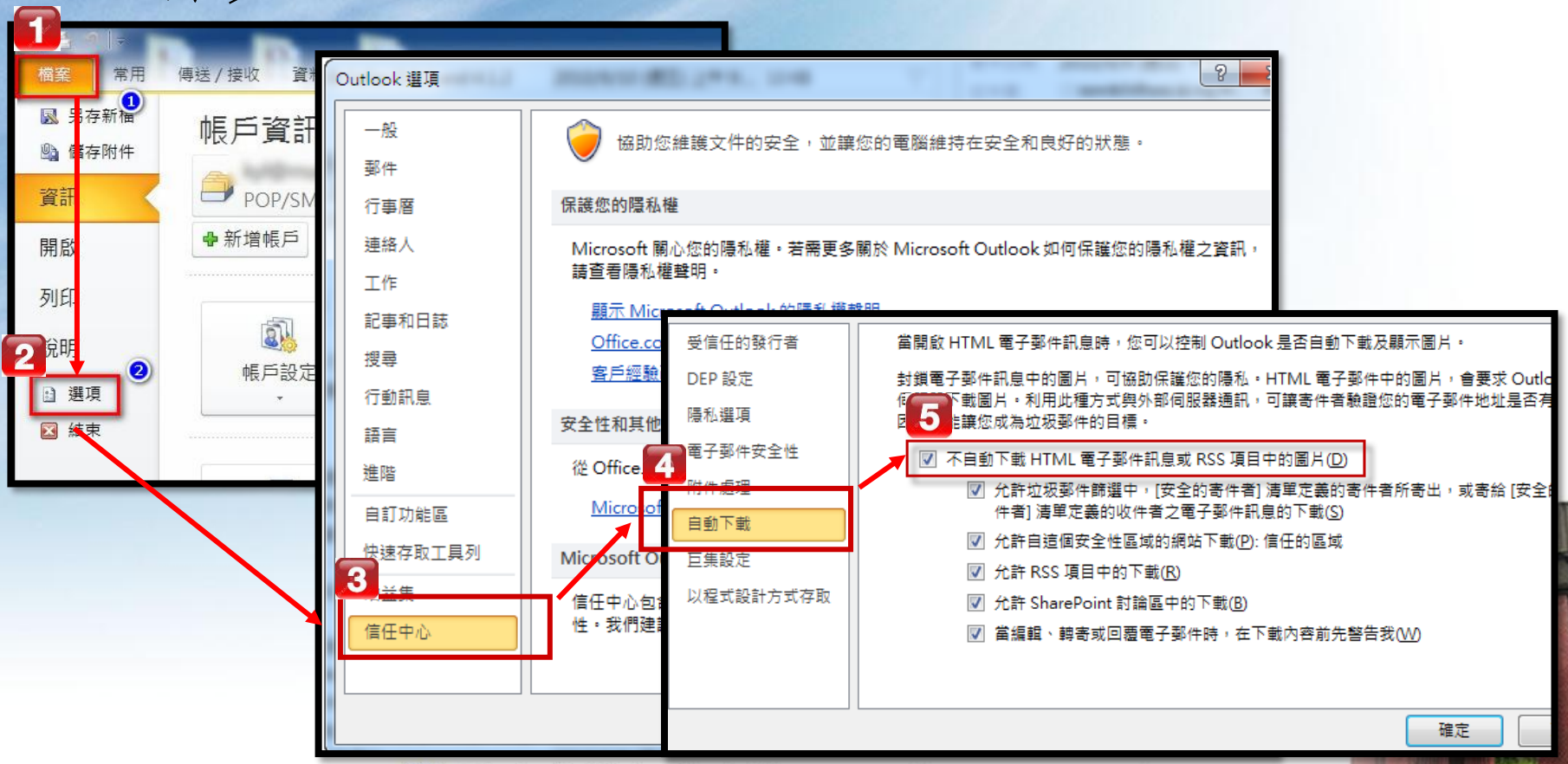
- **使用任何電子郵件軟體前，必須先確認**
  - 執行各種作業系統、應用軟體設定更新
    - Windows Update
    - Office Update
  - 必須安裝防毒軟體，並確實更新病毒碼
  - 收信軟體安全性設定
  - 啟用個人防火牆

Outlook 2007安全設定

- 「工具」->「信任中心」>「自動下載」->勾選〔不自動下載HTML電子郵件訊息或RSS項目中的圖片〕

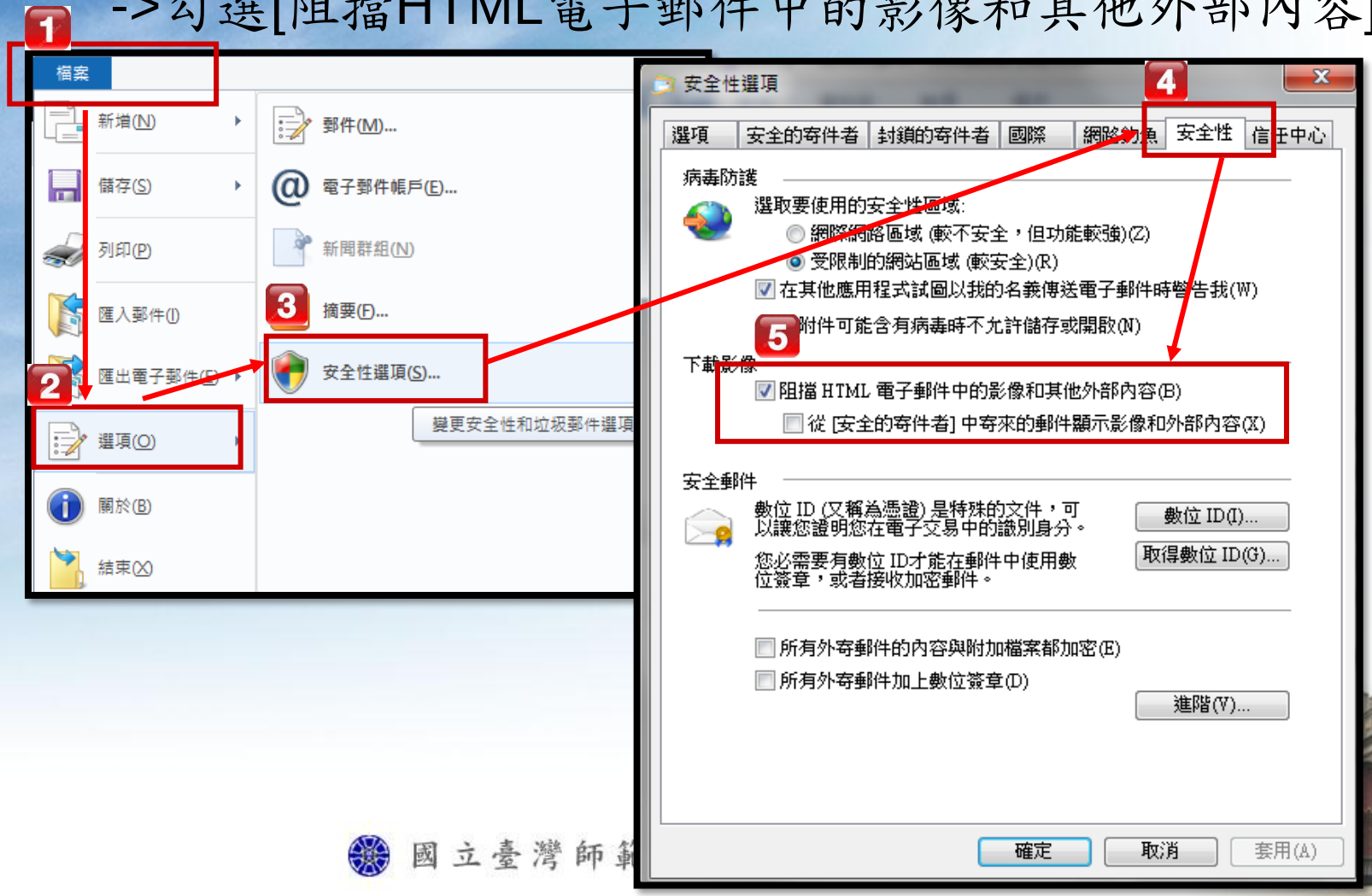
Outlook 2010安全設定

- 「檔案」 -> 「選項」->「信任中心」 >「自動下載」-> 勾選〔不自動下載HTML電子郵件訊息或RSS項目中的圖片〕



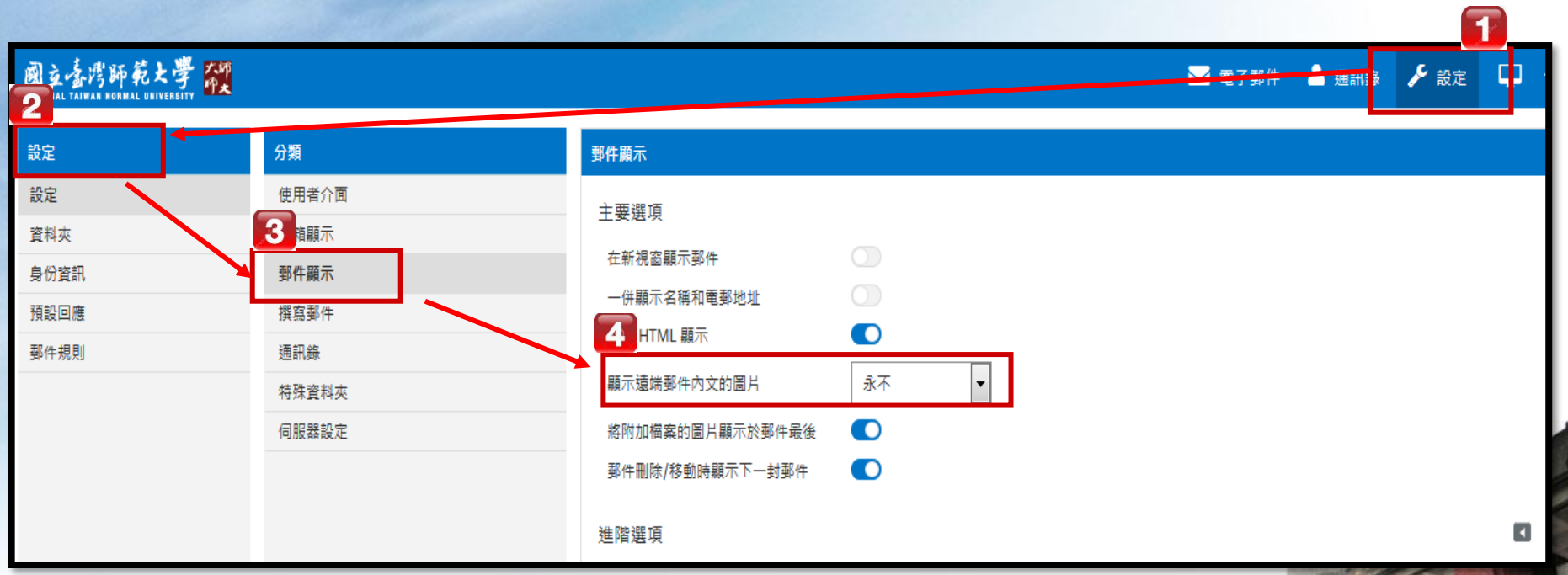
Windows Live Mail安全設定

- 「檔案」->「選項」->「安全性選項」->「安全性」->勾選[阻擋HTML電子郵件中的影像和其他外部內容]



師大Webmail信箱安全設定

- 「設定」 -> 「郵件顯示」 ->「顯示遠端郵件內文的圖片」選「永不」

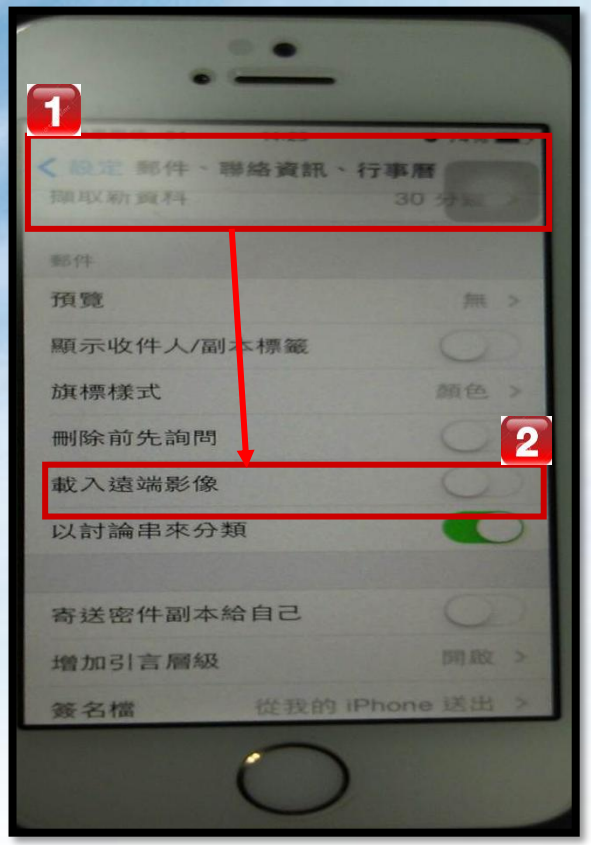


Gmail安全設定

- 選 ⚙ ->「設定」->「一般設定」的「圖片」->勾選「顯示不明外不圖片時，必須先詢問我」

iPhone安全設定

- 「設定」->「郵件、聯絡資訊、行事曆」->關閉「載入遠端影像」



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）

(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

- 在支援unicode的系統（windows 2000以上）可讓在它之後的字元變成從右到左顯示(right-to-left override; RLO)。所以例如本來“setup-txt.exe”這樣的檔名，在txt前面插入RLO控制字元之後就變成"setup-exe.txt"

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。