東方設計學院
TUNGFANG DESIGN INSTITUTE

資訊安全介紹

目錄

- 資訊安全基本概念介紹
- 社交工程
- 行動裝置使用安全

目錄

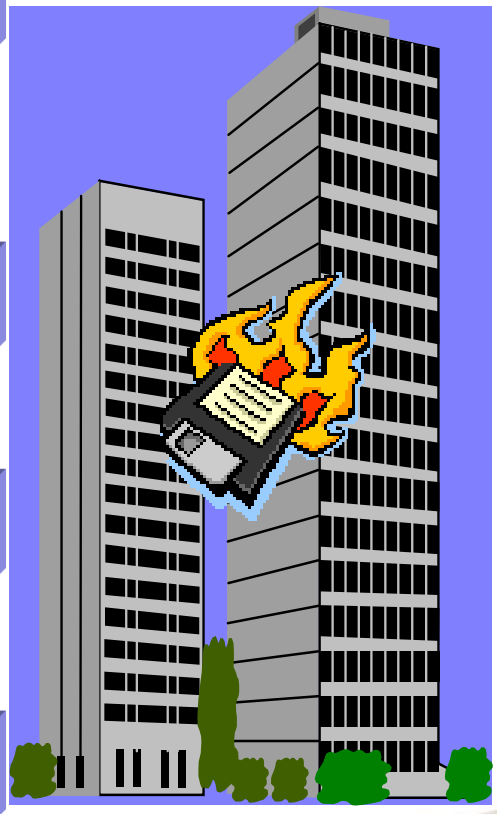
資訊安全基本概念介紹

資訊安全基本概念介紹

- 資安控管措施主要保護的東西是甚麼— 資訊資產（如： 客戶資料、 公司機密資訊...），也就是說在高度倚賴資訊及網路科技的今日，資訊資產已是組織或個人的一項非常重要的資產，就像其它重要的營運或個人資產一樣，具有相當之價值因此需要適當保護，尤其是高度依賴資訊化服務的組織及個人更形重要。
- 尤其在現今網際網路高度發展及應用，這些資訊資產也更有機會暴露於日益多樣的威脅與脆弱性中， 其對組織或個人所帶來的風

資訊安全問題可能造成的影響

組織資安問題



- 營收損失
- 客戶信心動搖
- 交易糾紛
- 資料處理內容不正確
- 組織聲譽受損
- 喪失組織或商業秘密
- 業務處理流程中斷
- 法律求償

目錄

社交工程

資安防護簡介(何謂社交工程)

社交工程定義

- 社交工程，英文為Social Engineering，是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為

攻擊目的

- 誘使被害人安裝破壞性的惡意程式，而造成系統破壞或網路癱瘓

資安防護簡介(何謂社交工程)

社交工程造成極大威脅的原因

- 利用使用者對於防範資訊詐騙沒有足夠的認知，騙取各項帳號密碼、個人資料、財務資料或組織重要資料等資訊
- 攻擊者不需具備頂尖的電腦專業技術，藉由人際關係互動進行犯罪行為

資安防護簡介(社交工程的類型)

- 將社交工程的攻擊進行分類，大致上可歸為以下兩種類型：
  - 非技術性

    利用欺騙/愚弄、模仿、暗中監視/偷聽、命令式口吻、假裝工作人員、假扮技術專家與**Dumpster Diving**
  - 技術性

    Phishing、**Vishing/Mishing**、跳出的視窗、有趣的軟體、垃圾郵件

資安防護簡介(非技術性的社交工程方式)

- **Pretexting/Impersonation 藉口/假扮(模仿)**
- **Spying and Eavesdropping 暗中觀察/偷聽**
- **Acting as a Technical Expert 假裝技術專家**
- **Support Staff 扮演工作人員**
- **Hoaxing 欺騙；愚弄**
- **Authoritative Voice 命令式的語氣**
- **Dumpster Diving 翻垃圾桶**

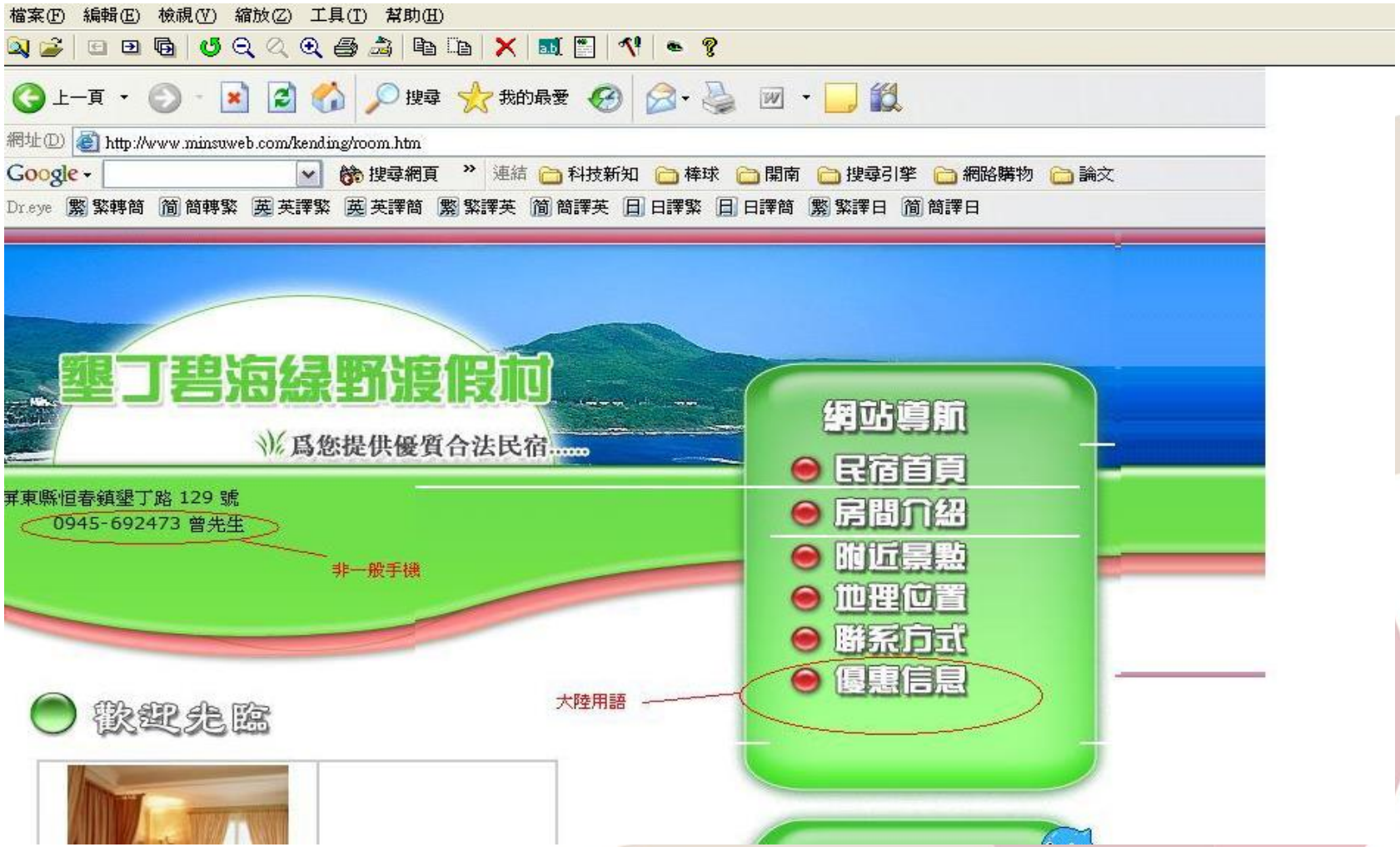
資安防護簡介(非技術性的社交工程方式)

- 翻垃圾車(Dumpster Diving)
  - **由目標的公司要搜尋敏感資料，可以由：**
    - 垃圾桶。
    - 印表後廢棄的紙張。
    - 使用者的桌面上的便條紙、便利貼…等。
  - **可以搜集到：**
    - 電話/手機號碼。
    - 聯絡的資訊。
    - 財務的資訊。
    - 有關操作的資訊(如密碼、重要的文件存放位置…等)。
  - **案例**
    - Oracle一直雇用私家偵探去翻微軟技術協會的垃圾桶，試圖找到這個組織行賄以便影響反托拉斯案的審理證據。

資安防護簡介(技術性的社交工程方式)

- 網頁或郵件的連結(Phishing)
- 瀏覽網頁時彈出的視窗(Popup Windows)
- 使用有趣的軟體(利用網頁/賭博遊戲的網站)
- 垃圾郵件
- 即時通訊的連結
- P2P軟體

案例一：利用假網頁騙取匯款



案例二：釣魚網頁

http://www.landbank.com.tw

http://www.1andbank.com.tw

例如：

遊戲X子

http://tw.gamania.com

vs. http://tw.gamannia.com

聯X銀行

http://www.ubot.com.tw

vs. http://www.obot.com.tw

案例三：利用P2P軟體獲取個資

目錄

電子郵件安全

電子郵件社交工程郵件類型

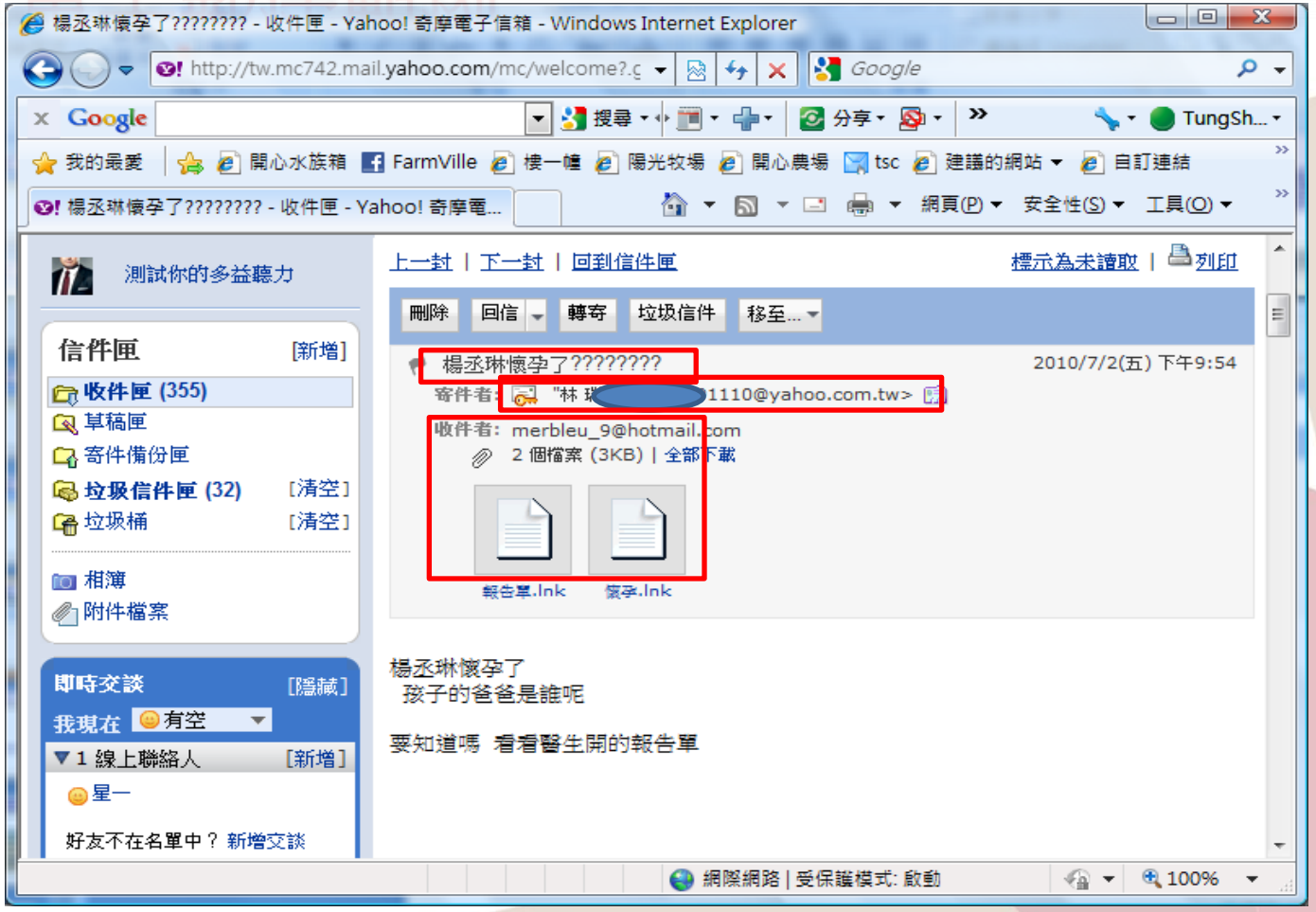
- 八卦影視
- 休閒娛樂
- 保健養生
- 財經資訊
- 情色內容
- 新奇資訊
- 郵件內容包含圖片、連結、*Word*附檔及*PowerPoint*附檔

惡意電子郵件之防範

惡意電子郵件範例一

惡意電子郵件之防範

惡意電子郵件範例二



惡意電子郵件之防範

惡意郵件防範停看聽(1)

- 惡意電子郵件防範宣導影片

- 停 – 使用任何電子郵件軟體前，必須先確認以下設定
  - 必須安裝防毒軟體，並確實更新病毒碼
  - 審慎開啟郵件及其附件或連結
  - 必須取消郵件預覽功能，避免無意開啟郵件
  - 設定過濾垃圾郵件機制
  - 建立電子郵件驗證機制(推動電子識別證)

惡意電子郵件之防範

惡意郵件防範停看聽(2)

- **看** – 收到郵件後，必須注意
  - 郵件主旨是否與本身業務相關
  - 其餘郵件不建議開啟，如需開啟應確認郵件來源
- 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
- 【寄件者】或【郵件主旨】與公務無關者，建議應立即刪除不要開啟郵件

惡意電子郵件之防範

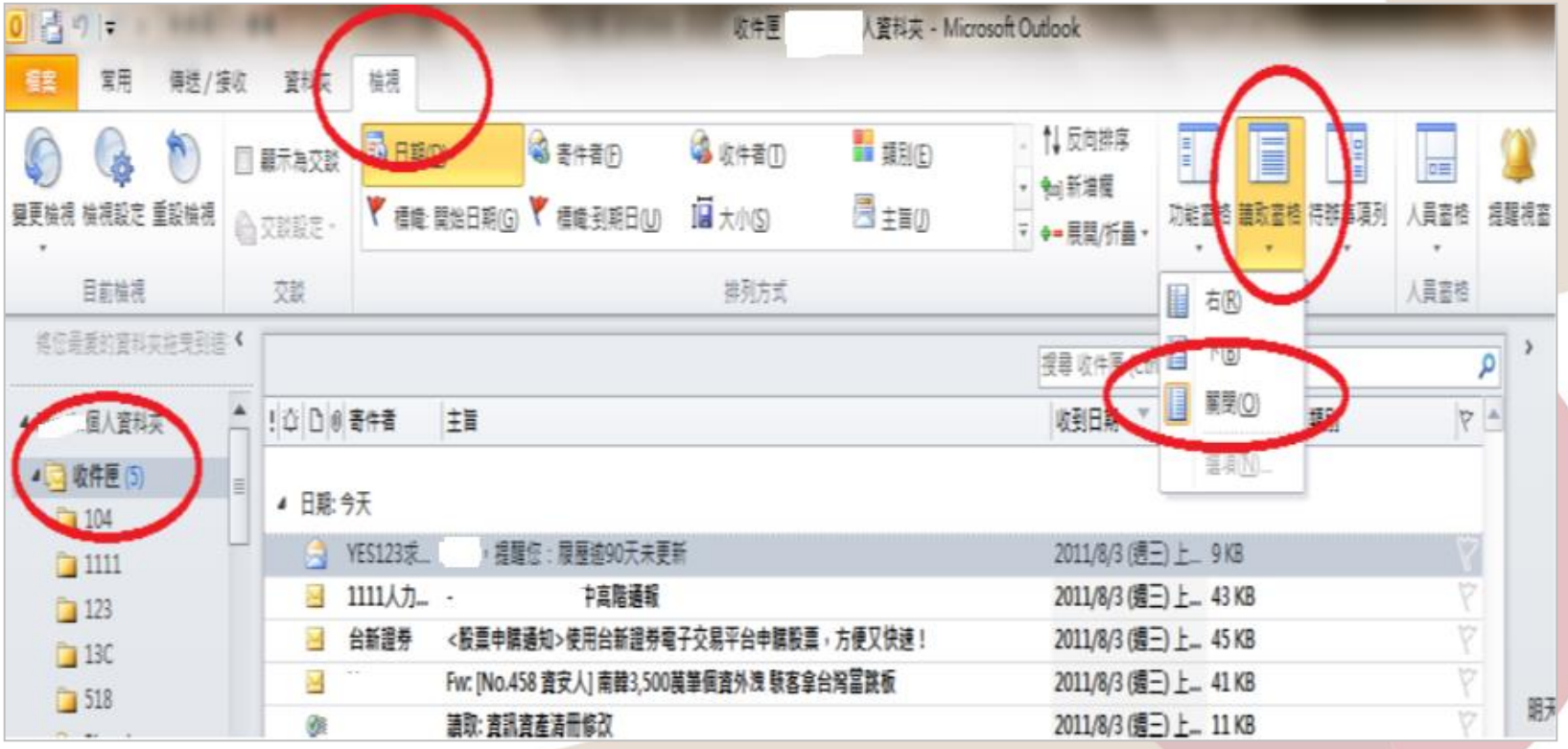
惡意郵件防範停看聽(3)

- 聽－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於開啟前確認郵件真偽

惡意電子郵件之防範

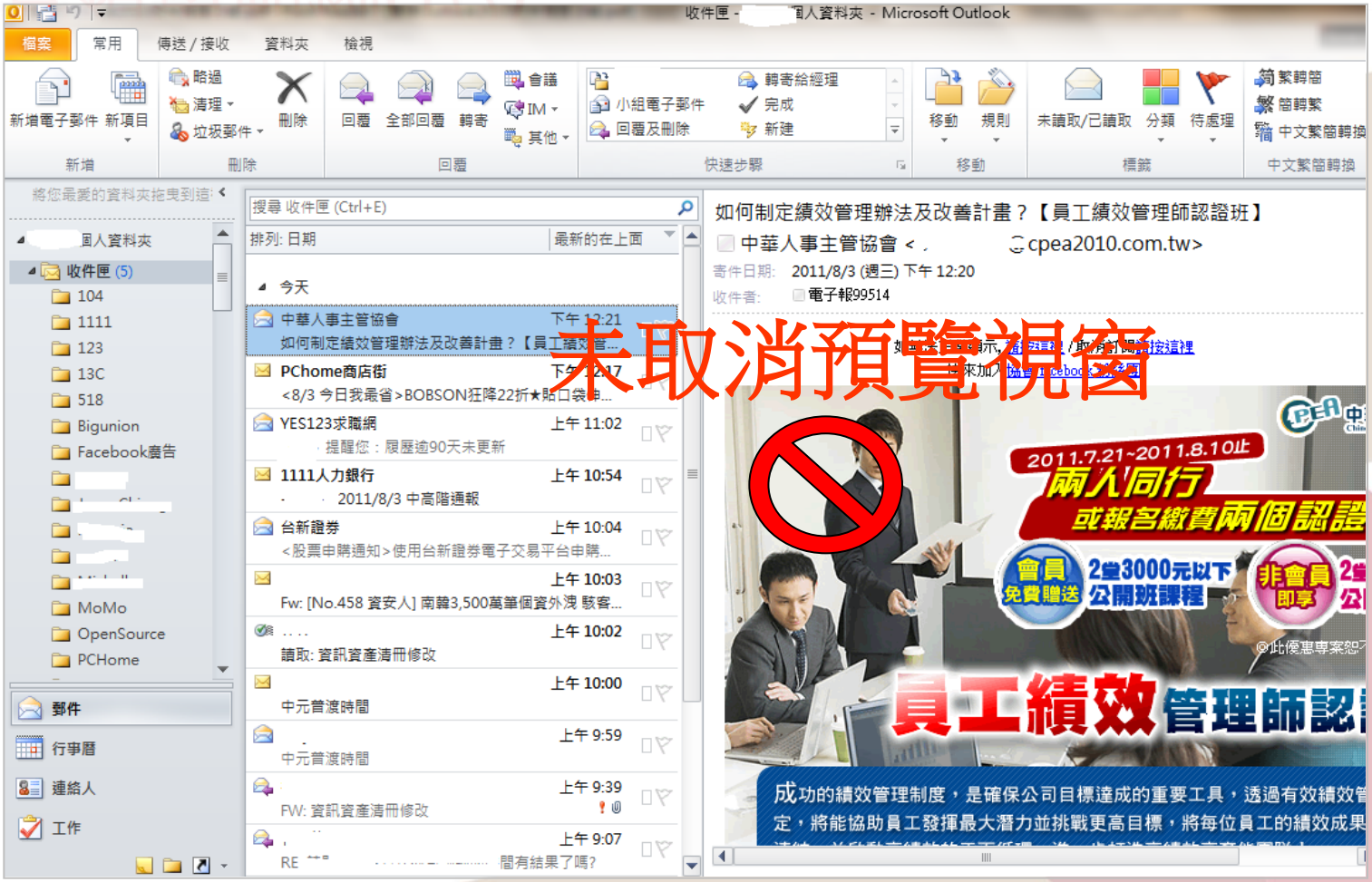
Outlook 2010取消讀取窗格功能

- 【檢視】>【收件夾】>【讀取窗格】>【關閉】
  (每個資料夾皆須各自設定成關閉)



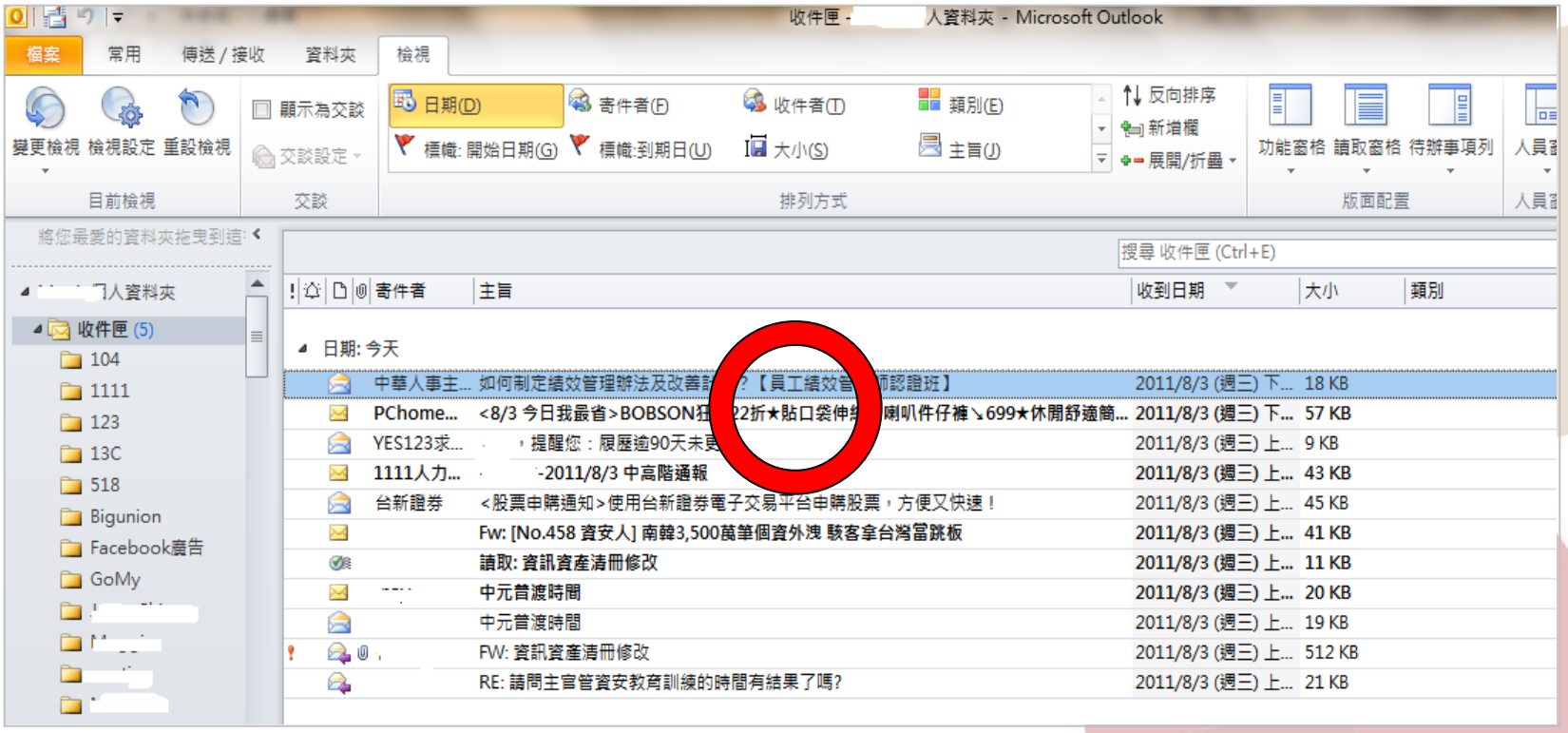
惡意電子郵件之防範

預覽視窗範例(1/2)



惡意電子郵件之防範

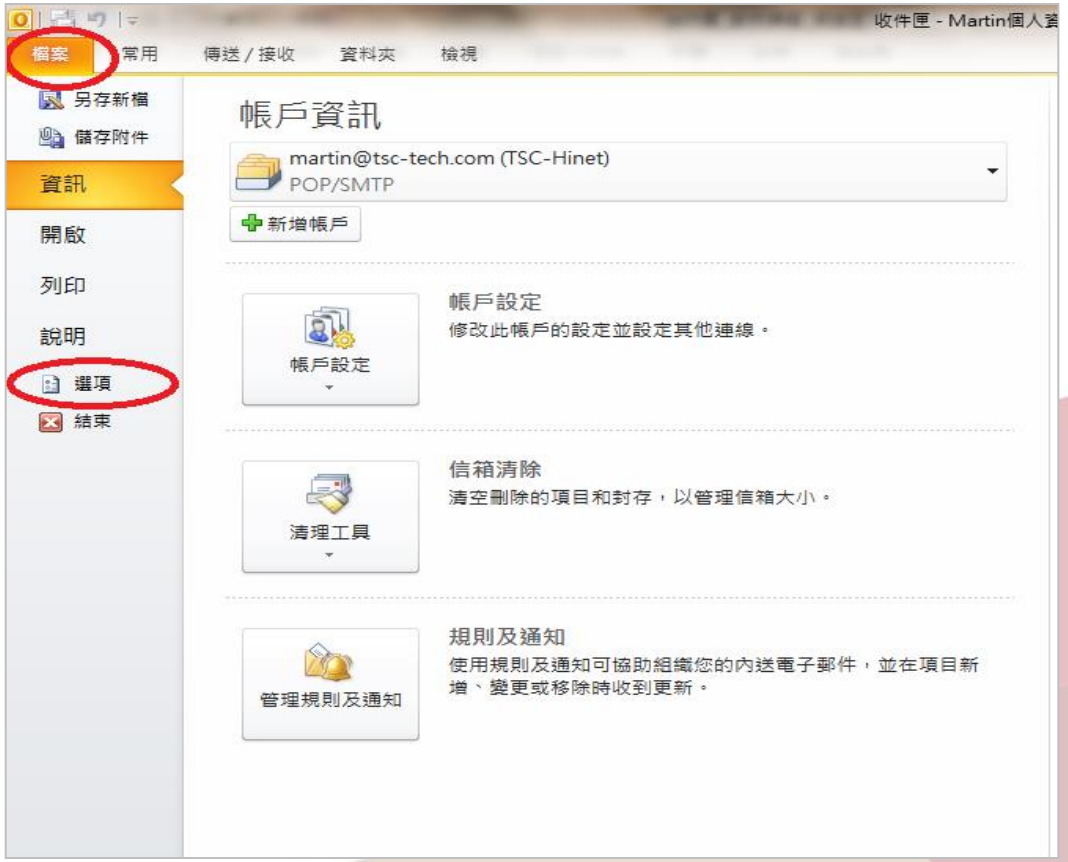
預覽視窗範例(2/2)



惡意電子郵件之防範

關閉Outlook 2010附件預覽功能(1/3)

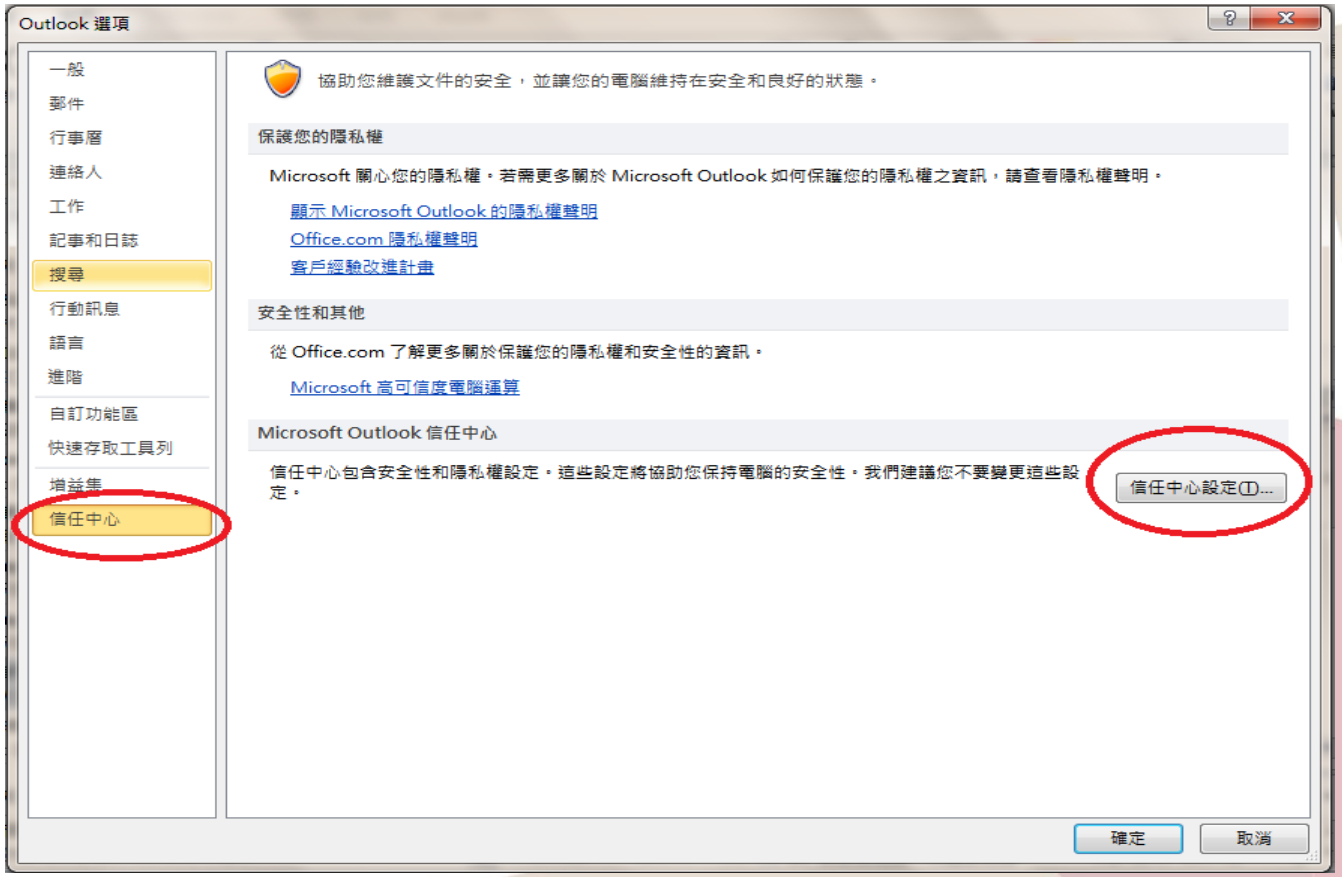
- 點選【檔案】>【選項】



惡意電子郵件之防範

關閉Outlook 2010附件預覽功能(2/3)

- 點取【信任中心】 > 右邊的【信任中心設定】

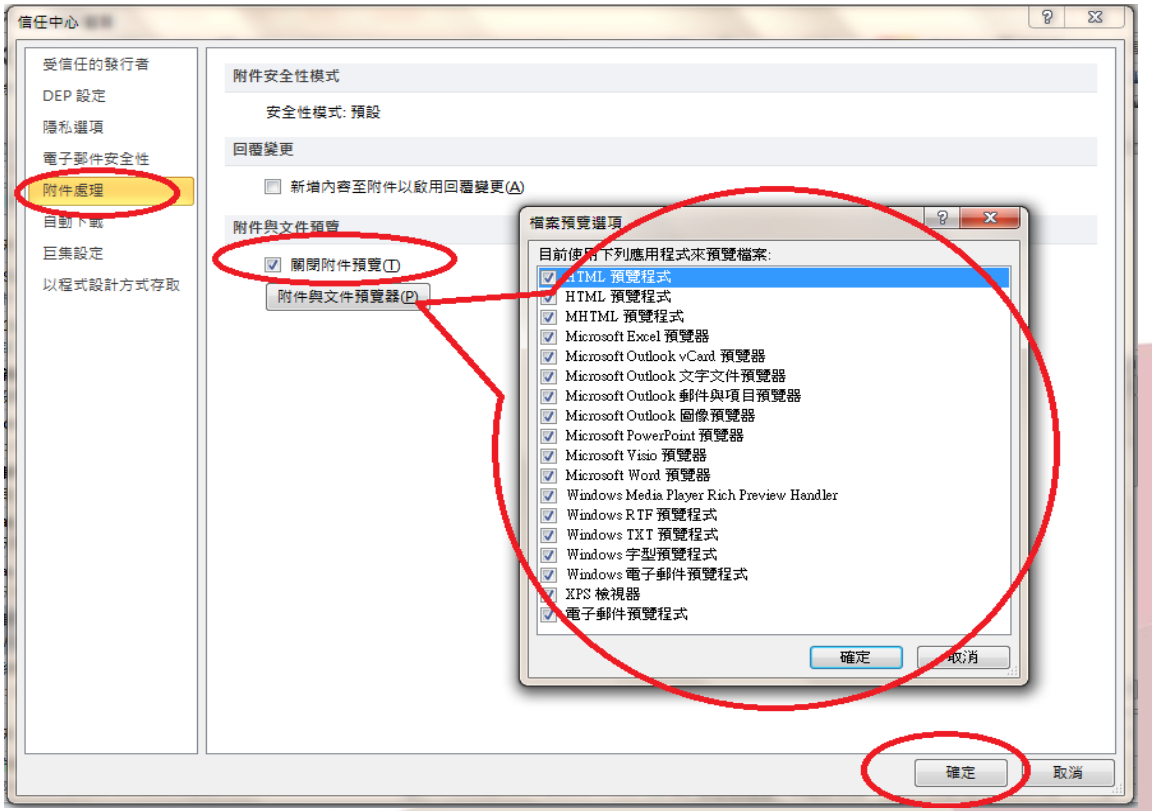


惡意電子郵件之防範

關閉Outlook 2010附件預覽功能(3/3)

- 【附件處理】 >勾選右邊的【關閉附件預覽】

(記得按【確定】後離開,並關閉Outlook後重新開啟outlook，設定才會生效)



惡意電子郵件之防範

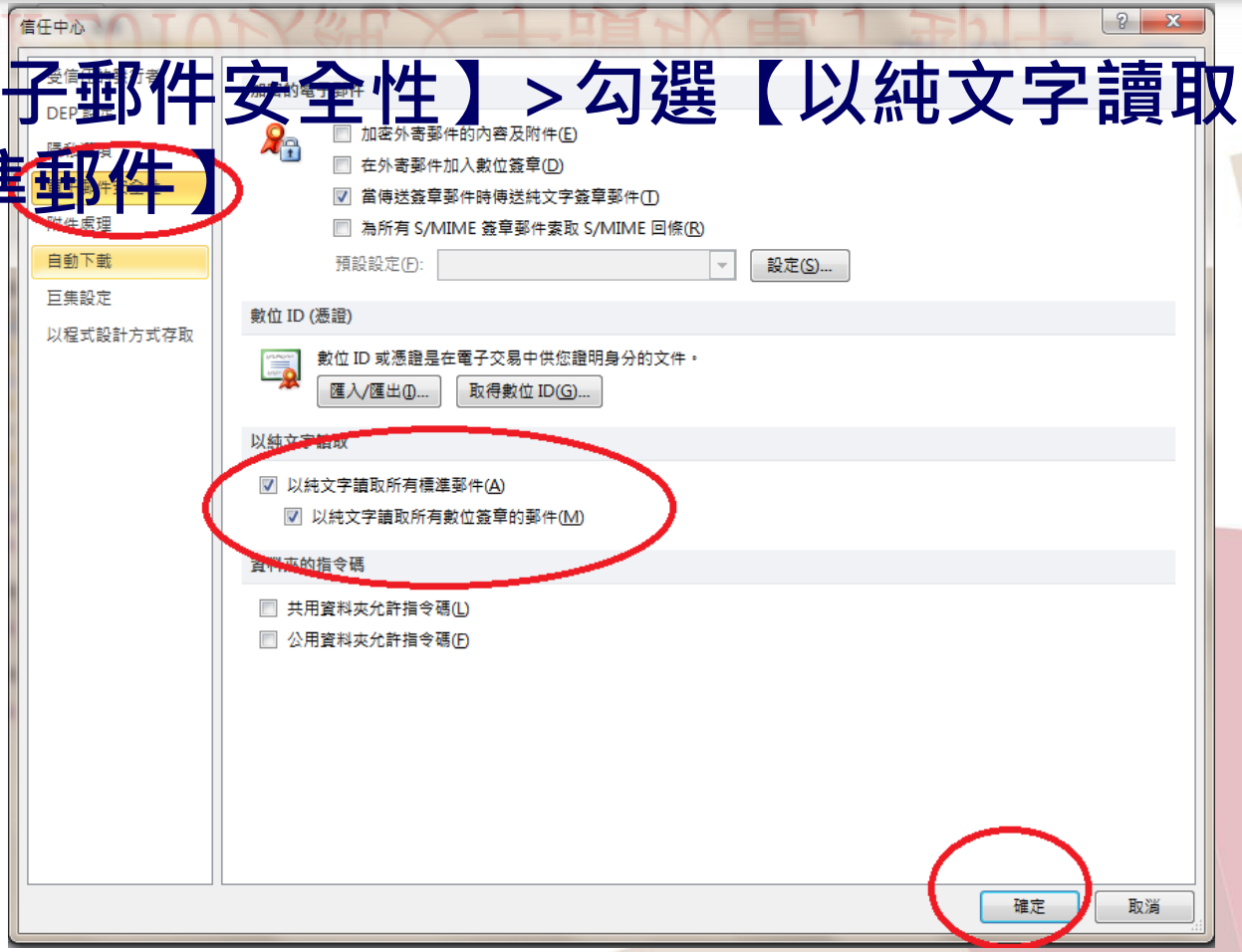
附件預覽範例

未關閉附件預覽功能

惡意電子郵件之防範

Outlook 2010以純文字讀取電子郵件

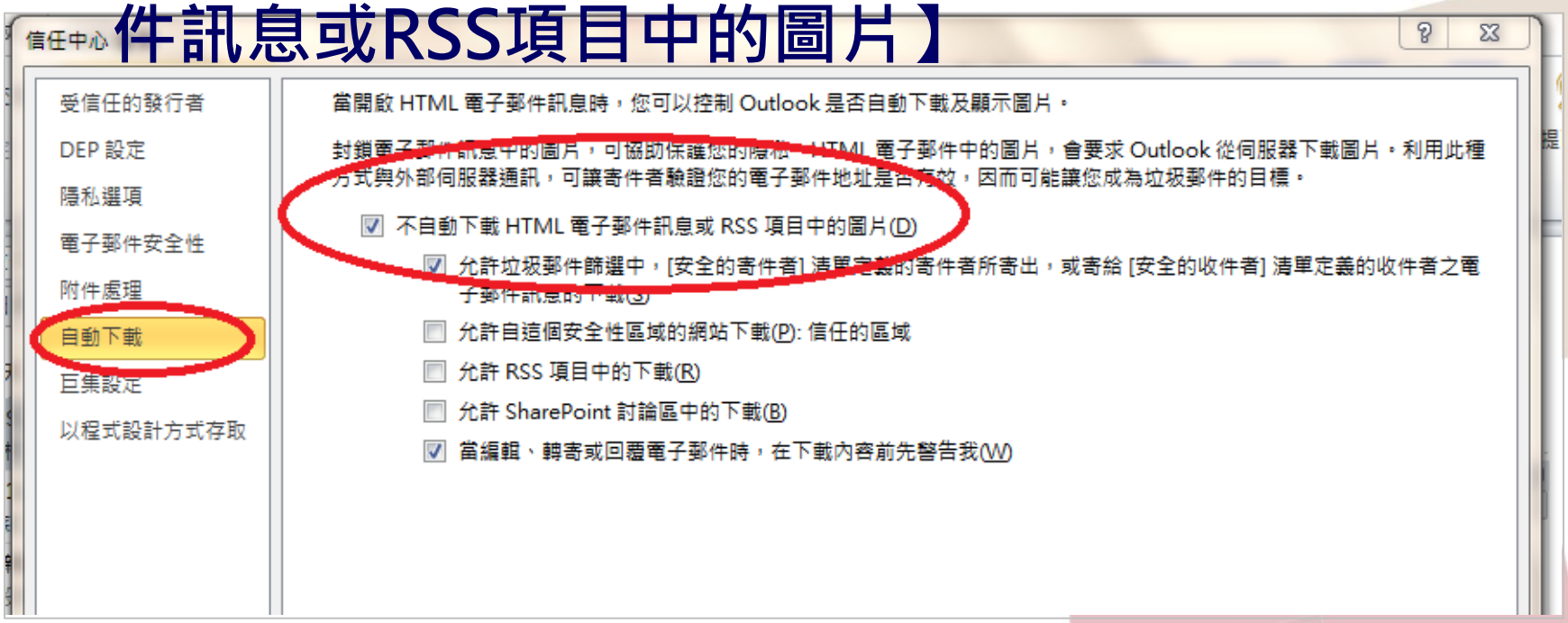
- 【電子郵件安全性】>勾選【以純文字讀取所有標準郵件】



惡意電子郵件之防範

Outlook 不自動下載HTML中的圖片

- 【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】



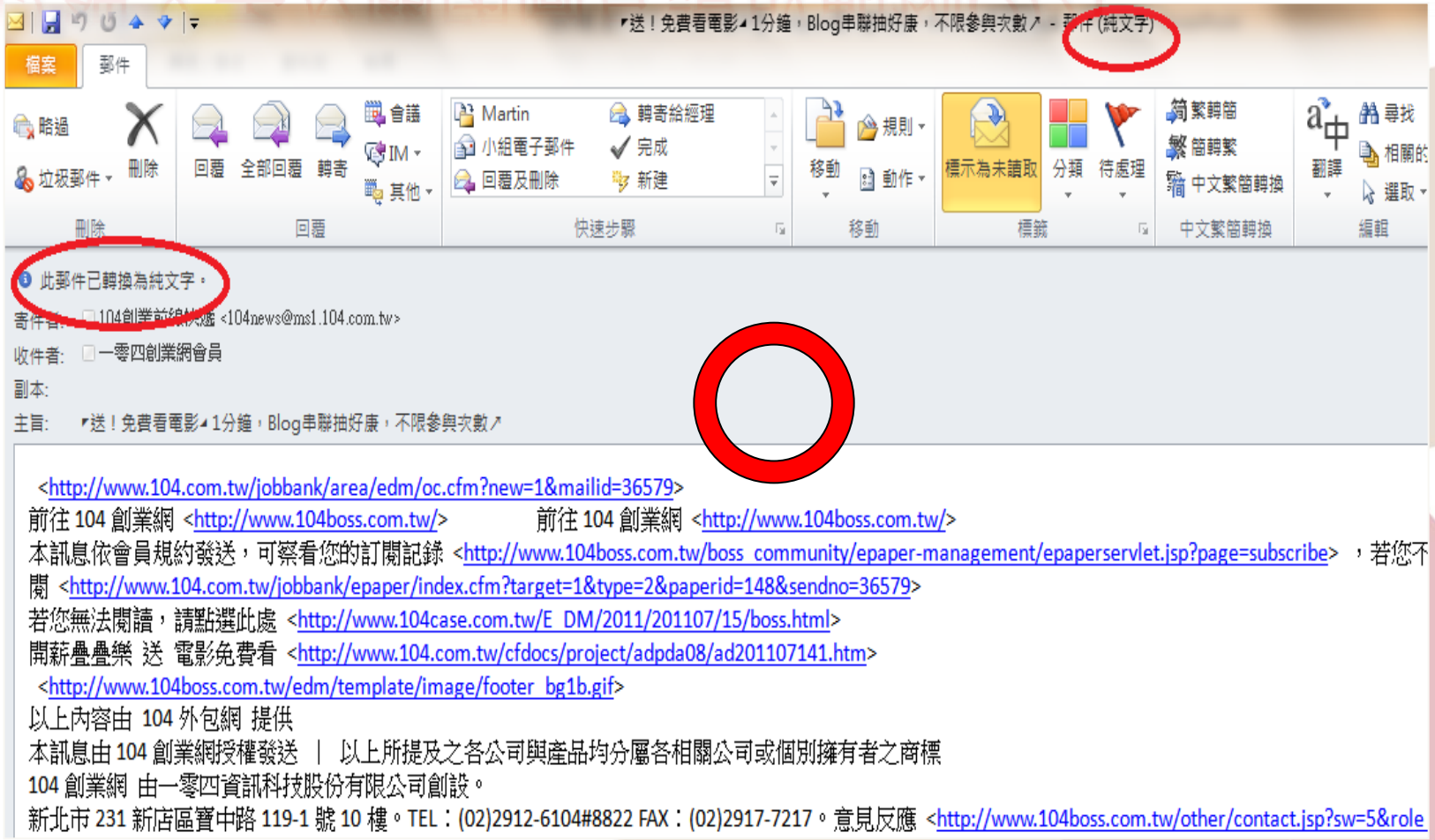
惡意電子郵件之防範

未以純文字及關閉圖片讀取範例(1/2)

未取消圖片預覽及以純文字讀取

惡意電子郵件之防範

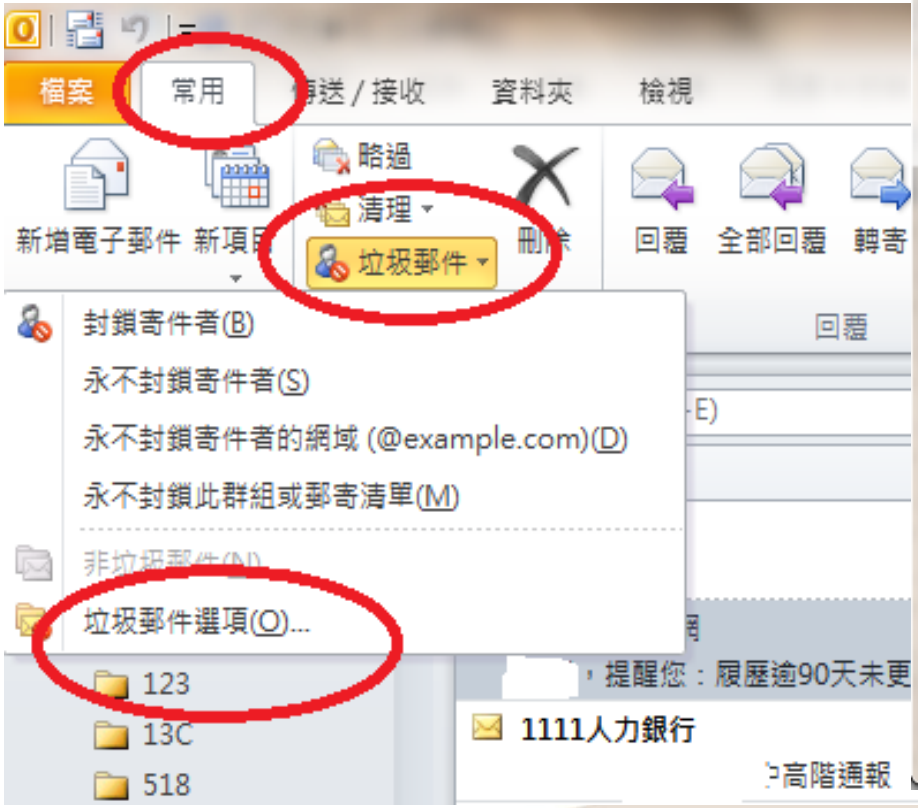
以純文字及關閉圖片讀取範例(2/2)

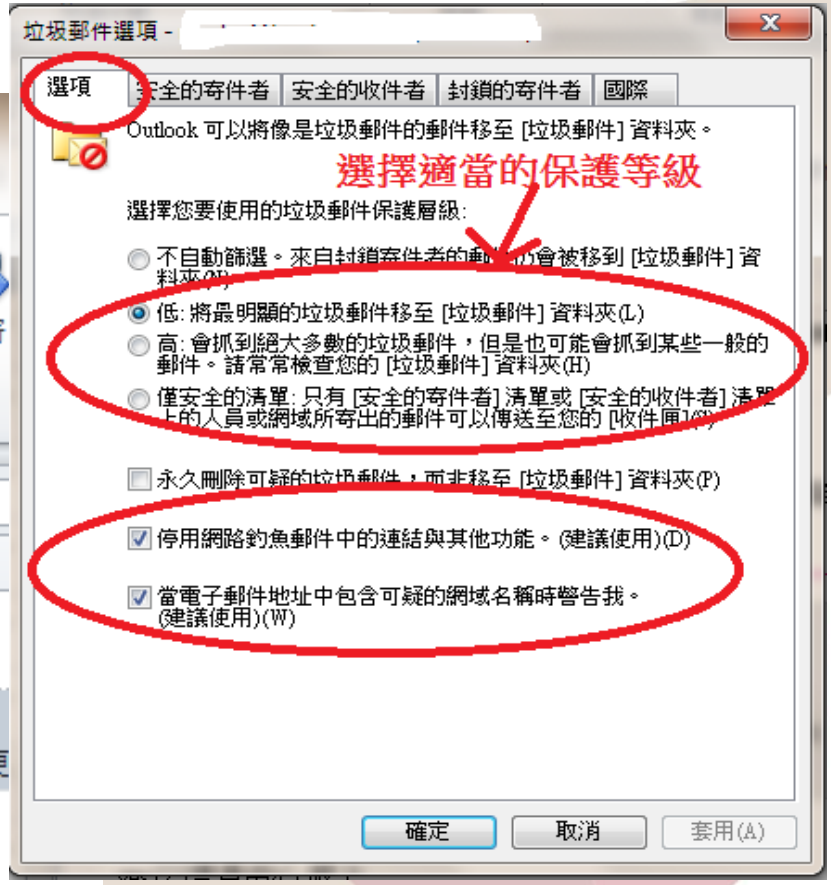


惡意電子郵件之防範

Outlook2010選用垃圾郵件功能

- 【常用】>【垃圾郵件】>【垃圾郵件選項】>【選項】>選擇適當的保護等級與保護





資安防護簡介(社交工程防範)

社交工程基本防護工作

- 執行各種作業系統、應用軟體更新及設定
- 要安裝防毒軟體、密碼設定要符合安全規定
- 不要輕易相信電話中任何非經正式授權的請求

電子郵件社交工程防範

- 絕不開啟跟自己無關的郵件及附件檔
- 不隨便開啟郵件中的超鏈結
- 不要任意的轉寄信件

惡意網站社交工程防範

- 不要任意的安裝軟體
- 不要輕易答應來自好友的點選請求
- 小心詐騙購物假社團的陷阱

教育部社交工程演練

- 演練對象：大專院校教職員工
- 演練時程
  - 上半年：5月1日~5月31日
  - 下半年：9月1日~9月30日
- 演練方式：

  教育部技術小組將會以偽冒公務、個人或公司行號等名義方式發送惡意之郵件給本校演練對象，當收件人開啟郵件或點閱郵件所附連結或檔案時，將會留下紀錄，此紀錄將成為後續統計惡意郵件開啟率及點閱率。
- 演練成效評量
  - 信件開啟率：不得高於10%
  - 附件或連結點閱率：不得高於6%
- 應辦理事項：

  社交工程宣導教育訓練課程

目錄

行動裝置使用安全

資安通報(續)

- **【愈智慧，愈危險！】手機也要防毒 防詐騙**

自由時報 – 2014年3月5日 上午6:14

智慧型手機盛行，詐騙戰場轉移至手機，社群軟體如LINE廣告訊息多，詐騙集團常以「XX裸照外流」等聳動標題，引誘民眾點擊連結不明網站，進而掉入小額詐款的陷阱，或竊取個資。使得手機防毒的議題益加被重視。

台灣民眾手機防毒認知不成熟，趨勢科技行銷經理朱芳薇表示：「民眾多有電腦必須安裝防毒軟體的認知，但對於手機，卻顯得輕忽。台灣手機使用者安裝防毒軟體，遠遠不到1成，少得驚人。而多數民眾喜愛下載免費程式，高達6成的病毒卻來自免費程式，手機若無防護機制，危險度高。」

Android自由度高，危險性高，希悅資訊總經理蕭伊婷也說：「Android平台因為給予軟體開發者高度自由，加上全球市占高，使得Android平台上的惡意程式暴增，遠多於相較封閉的iPhone系統，儘管Google已採取相關措施，成效有待加強。」此外，根據卡巴斯基調查，近98.05%惡意程式鎖定Android平台。

移動式個人裝置應用與安全(APP安裝授權審視原則1)

- Android系統APP安裝授權：第一步先從評分與評論、下載次數及開發軟體公司等開始，如無評論者可能要注意該APP如非新上架，那可能有問題。

移動式個人裝置應用與安全(APP安裝授權審視原則2)

- 詳細察看授權原則，另要注意是否全部查看如右圖紅框，尚有未查看部分，應全部瀏覽完畢。

移動式個人裝置應用與安全(APP安裝授權審視原則3)

- 同上頁說明，審視完授權原則，應考慮授權原則是否合宜，如無問題再點選紅框中的繼續按鈕

移動式個人裝置應用與安全(APP安裝授權審視原則4)

- 審視完原則後，即開始安裝，若此時覺得對該APP仍有疑慮，可按紅框中的X停止安裝，就會停止。

資安防護簡介(收、發電子郵件保護措施5)

- iPhone關閉郵件預覽功能
- 察看手機是否顯示預覽郵件內容。
- 如左圖紅框內為顯示郵件預覽內容

資安防護簡介(收、發電子郵件保護措施6)

- iPhone關閉郵件預覽功能
- 選擇紅框內之設定/郵件、聯絡資訊、行事曆選項

資安防護簡介(收、發電子郵件保護措施7)

- iPhone關閉郵件預覽功能
- 選擇點選紅框內之郵件預覽選項

資安防護簡介(收、發電子郵件保護措施8)

- iPhone關閉郵件預覽功能
- 由此可察看紅框內目前郵件預覽為2行

資安防護簡介(收、發電子郵件保護措施9)

- iPhone關閉郵件預覽功能
- 點選紅框內目前郵件預覽改為無之選項

資安防護簡介(收、發電子郵件保護措施10)

- iPhone關閉郵件預覽功能
- 再查看手機顯示預覽郵件均已消失不再顯示郵件預覽內容。

資安防護簡介(收、發電子郵件保護措施11)

- **Android by HTC關閉郵件預覽功能**
- **察看手機是否顯示預覽郵件內容。**
- **如左圖紅框內為顯示郵件預覽內容**

資安防護簡介(收、發電子郵件保護措施12)

- **Android by HTC關閉郵件預覽功能**
- **點選手機之menu鍵，會出現藍色框內等六項選項**
- **點選紅框內之更多**

資安防護簡介(收、發電子郵件保護措施13)

- **Android by HTC關閉郵件預覽功能**
- **處線新增帳號及設定兩個選項**
- **點選紅框內之設定選項設定**

資安防護簡介(收、發電子郵件保護措施14)

- **Android by HTC關閉郵件預覽功能**
- **選擇紅框內之一般設定選項**

資安防護簡介(收、發電子郵件保護措施15)

- **Android by HTC關閉郵件預覽功能**
- **選擇紅框內之直向內文預覽選項**

資安防護簡介(收、發電子郵件保護措施16)

- **Android by HTC關閉郵件預覽功能**
- **由此可察看紅框內目前郵件預覽為2行**

資安防護簡介(收、發電子郵件保護措施17)

- **Android by HTC關閉郵件預覽功能**
- **點選紅框內目前郵件預覽改為無之選項**

資安防護簡介(收、發電子郵件保護措施18)

- **Android by HTC關閉郵件預覽功能**
- **再查看手機顯示預覽郵件均已消失不再顯示郵件預覽內容**。

Thank you