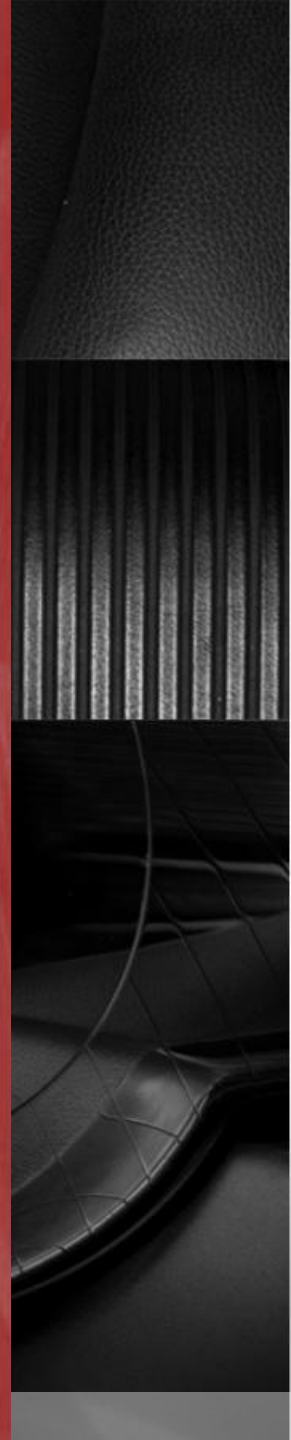
101年資訊安全暨惡意電子郵件社交工程演練教育訓練

報告單位：圖書館

報告日期：101年5月28日

報告時間：上午09:00~12:00

報告地點：J401國際會議廳



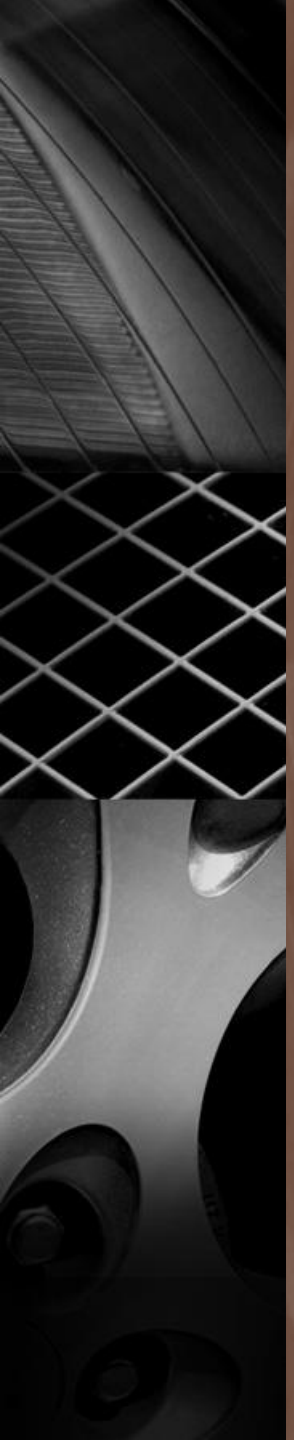
報告大綱

- 前言
- 100年資安動畫影片欣賞
- 社交工程演練相關說明
- 資訊安全作業注意事項
- 資訊安全相關法規
- 資安威脅發展趨勢
- 設定以文字方式開啟電子郵件

(政府機關（構）資訊安全責任等級分級)
教育部要求有關資訊安全教育訓練規定

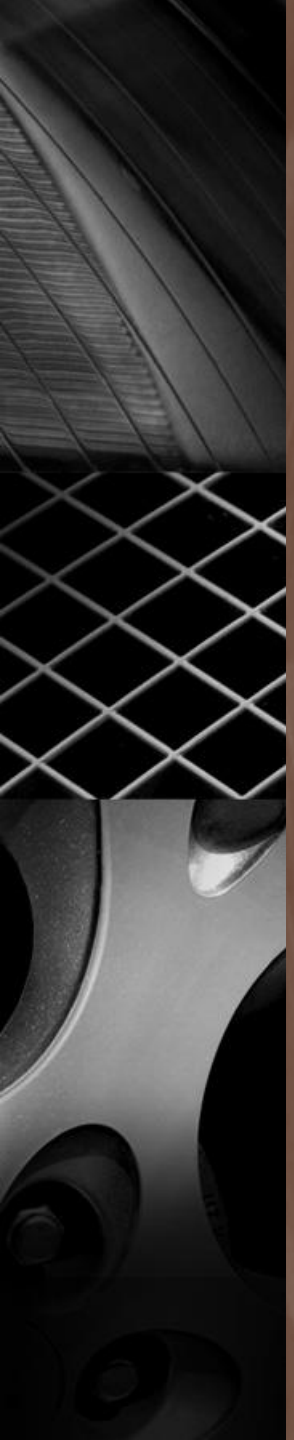
	防護縱深	ISMS推動作業	稽核方式	資安教育訓練(一般主管、資訊人員、資安人員、一般使用者)	專業證照	檢測機關網站安全弱點
A級	SOC、IDS、防火牆、防毒、郵件過濾裝置	通過第三者驗証	每年至少2次內稽	每年至少(3、6、18、3小時)資訊人員、資安人員需通過資安職能鑑定	維持至少2張資安專業證照	每年2次
B級	SOC(選項)、IDS、防火牆、防毒、郵件過濾	通過第三者驗証	每年至少1次內稽	每年至少(3、6、16、3小時）資訊人員、資安人員需通過資安職能鑑定	維持至少1張資安專業證照	每年1次

教育部98年06月16日台電字第0980104237號函
「政府機關(構)資訊安全責任等級分級作業施行計畫」



100年資安動畫影片

1. 資安週活動介紹 (http://www.youtube.com/watch?v=eIlZCS34G5c)
2. 100年資安動畫金像獎 第四名：資安了沒 (http://www.youtube.com/watch?v=1n6HWdAx_8E)
3. 100年資安動畫金像獎 第二名：個資英雄傳 (http://www.youtube.com/watch?v=jK437A5fnqI&context=C49ee8faVDvjVQa1PpcFMAdzod5NVOLk-g9rguWqLtFjxxOQ16Abs%3D)



社交工程演練相關說明

演練時程說明

1. 提報演練名單：5月(各機關學校提報)。
2. 各機關學校自行辦理宣導教育訓練：5月(全部行政人員)。
3. 教育訓練時數：1小時。
4. 教育部進行第1次演練：6月。
5. 各單位針對開啟惡意郵件或點閱惡意郵件附件內容人員，進行加強宣導：8 ~ 9月。
6. 教育部進行第2次演練：10月。

演練前宣導課程應分兩階段辦理：

- 第一階段（於演練作業辦理前）

  各機關學校應針對單位所有行政人員，全面性實施教育訓練。

- 第二階段（於演練作業完成後）

  針對開啟惡意郵件比例較高、點閱惡意郵件所附連結或檔案之人員再次進行教育訓練加強宣導，以強化其警覺性。

演練評量標準

- 各單位之惡意郵件開啟率及惡意連結(或檔案)點擊率計算方式如下：
  - 惡意郵件開啟率：開啟惡意郵件之人數 / 機關提報人數。
  - 惡意連結(或檔案)點擊率：點閱惡意郵件所附連結或檔案之人數 / 機關提報人數。
- 各單位之惡意郵件開啟率**應低於10%以下**；惡意連結(或檔案)點擊率**應低於6%以下**。

惡意電子郵件的特徵

- 透過電子郵件，可以讓收件者
  1. 誘騙進入假網站（網路釣魚）。
  2. 開啟惡意檔案（木馬後門）。
  3. 下載問題檔案（木馬後門）。
- 常見發燒話題：政治新聞、色情圖片、休閒養生。
- 網路郵件與網站詐騙技術演進，目前已到真假難辯。
- 駭客會假冒成使用者信任的人，進而讓使用者相信而去開啟郵件及含惡意程式之附件或超連結。
- 假冒寄件者方式，真假寄件者資料難以分辨。
- 附件檔案型態不一定是執行檔（.exe），可能是 .doc、.ppt、.mdb 等，甚至是 .rar。

當收到信件請先確認下列事項

1. 寄件人
   - 陌生人不要開
   - 寄件人是可以偽冒的(實作)
2. 主旨
   - 非公務郵件不要開
   - 主旨怪異不要開
   - 主旨吸引力與急迫性請注意
3. 寄件時間
   - 發信時間怪異不要開(台灣與國外差異)

若無法確認，先以電話與發信人確認後，再開啟郵件

當讀取信件時建議

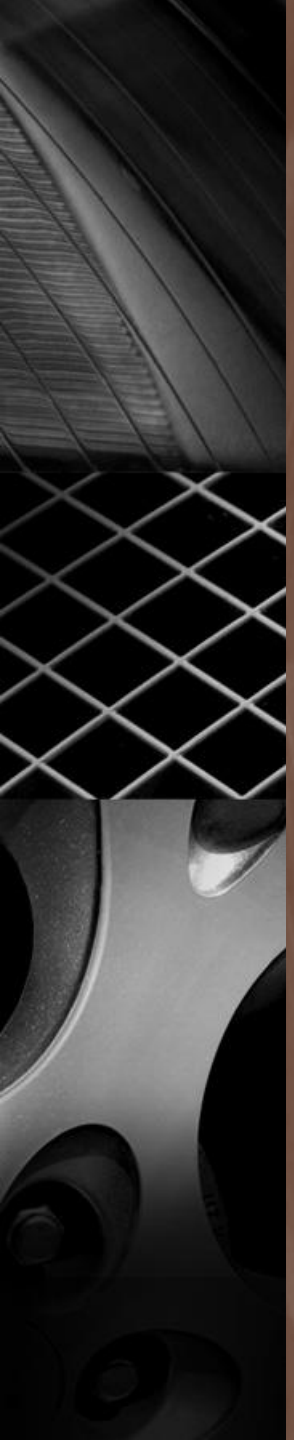
1. 內容
   - 要求輸入敏感與隱私資料不要輸入
   - 確認垃圾信件請刪除不要再轉寄他人
2. 附件
   - 請勿直接開啟
   - 下載掃毒確認安全再開啟
3. 連結 (避免上惡意連結的當)
   - 請勿直接連結
   - 建議開新網頁尋找網址或自己輸入網址
   - 連結網址為IP時請確認其安全性

寄信時應注意事項

1. 郵件信箱區分用途使用
   - 學校電子郵件帳號以學校公務用途為主
   - 私人信件可利用非學校電子郵件帳號寄送(可申請免費電子郵件帳號)
   - 學校用與其他用途請分開使用，不要都使用同一信箱
2. 寄信時
   - 寄給多人時，請使用密件副本寄信
   - 重要信件請勾選要求讀取回條後再寄信
   - 事後可用電話追蹤

為何不用系統攔截社交工程信件?

社交工程的目的在於取得人的關注力及信任，繼而進行資料的誘取，故在內容特徵上更會針對郵件過濾規則進行調整迴避，以期達到讓使用者能收到郵件點閱而完成騙取資料之目的



資訊安全作業注意事項

處理個資之電腦使用應注意事項(1/2)

- 處理個人資料的電腦需設置使用者帳號及密碼
- 密碼應包含文數字，至少8碼，每六個月更換一次
- 機密或敏感的資料檔案應以安全的方式保護，例如：加密、壓縮等
- 個人電腦內重要資料檔案，至少每月備份一次
- 個人電腦備應使用螢幕保護程式，設定螢幕保護密碼，並將螢幕保護啟動時間設定為15分鐘以內
- 交換個人資料檔案時，應對資料檔案加密，亦或是透過加密通道傳送。

處理個資之電腦使用應注意事項(2/2)

- 個人資料禁止存放於網路芳鄰分享目錄，並停用Guest帳號。
- 存放機密或敏感等級的資料檔案電腦應與外部網路隔絕（如：防火牆）。
- 存放個人資料之電腦應安裝防毒軟體，除至少每日更新病毒碼外，並應每週執形排程掃瞄。
- 存放個人資料之電腦應定期檢視、更新作業系統、應用程式漏洞（如：Windows作業系統、Windows Office、Adobe Acrobat等）。

使用合法授權軟體

- 圖書館每學期一次派員至各單位進行行政與教學用電腦使用授權軟體檢查，並將成效於辦理智慧財產權執行情形中回報教育部。
- 有關校園授權軟體清單，請參閱圖書館資訊技術組網頁，網頁清單內容不包含各系科或各型計畫採購教學用研究用之軟體。

自由軟體(或共享軟體)

- 根據自由軟體基金會的定義，自由軟體(Freeware)是一種可以不受限制地自由使用、複製、研究、修改和分發的軟體。
- 所謂「免費軟體(Freeware)」或「共享軟體(Shareware)」都是著作權法上受保護之電腦程式著作，並不因為其名為「共享」或「免費」，或在網路上允許任何人自由下載，便表示該電腦程式著作不受著作權法保護。
- 教育部校園自由軟體數位資源推廣服務中心 http://ossacc.moe.edu.tw/

可能感染病毒木馬的途徑列舉如下

1. 電子郵件：附件檔案包含病毒碼檔案、郵件網頁要求下載安裝檔案。
2. 即時通與網頁瀏覽：點選網頁超連結要求下載安裝檔案、用戶檔案傳送（已經不多見）。
3. 下載軟體：免費工具，盜版軟體、好玩遊戲、可愛圖案、螢幕保護程式。
4. USB隨身碟與拇指碟（傳播媒介）

電腦使用者常見危險行為

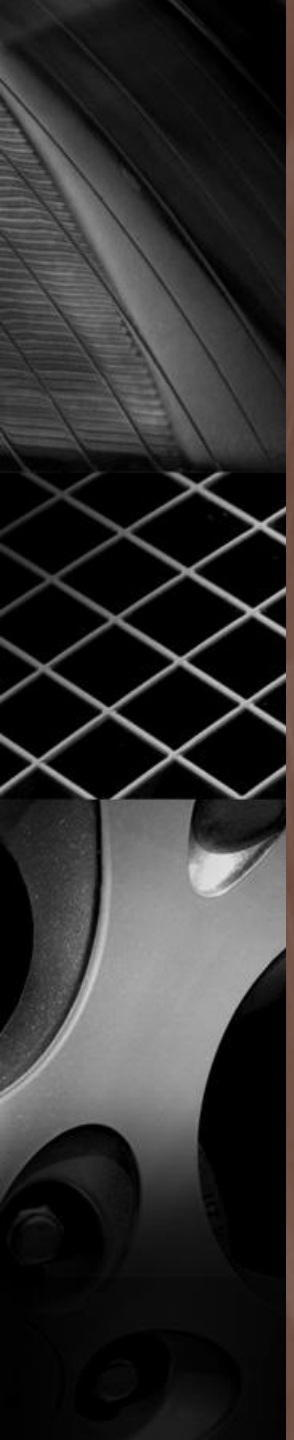
1. 冒然使用P2P軟體確未預先（事後）處理安全問題。
2. 自行安裝即時通（IM）軟體容易造成蠕蟲感染與傳送木馬捷徑。
3. 長時間離開座位或下班未將電腦關機，容易造成駭客入侵的最佳時機。
4. 錯誤觀念：我的電腦沒有重要資料，駭客不會找上我啦！

自我防護的交戰守則(1/2)

1. 電子郵件防護
   - 寄件者不詳或不認識，異常，不要開啟。
   - 主旨標題過於吸引我們，異常，不要開啟。
   - 可疑附件檔案(exe、dll、scr、bat、pif、com、vbs、pps、...)，異常郵件，不要開啟。
   - 不要直接按下郵件連結，觀察超聯結網址是否相符。
   - 檢舉可疑信件與網站。

自我防護的交戰守則(2/2)

2. 密碼帳號防護
   - 不要使用懶人密碼（1234、qazplm、qwert，...）。
   - 不要使用豬頭密碼（密碼＝帳號）。
   - 安全密碼的字數長短（6-8，英數字+符號）。
3. 資料檔案防護（常備份資料檔案）
   - USB隨身碟的備份，注意備份檢查程序。
   - 將『我的文件』，壓縮後，燒至唯讀光碟片。



資訊安全相關法規

資訊安全相關法規

- 刑法(防駭條款)
- 個人資料保護法
- 個人資料保護法施行細則
- 著作權法

➢ 第358條至第360條之罪，須告訴乃論。

刑法第36章 妨害電腦使用罪

- 網路犯罪行為大約可歸類下列三種
  - 以網路作為犯罪工具–網路詐欺、網路恐嚇等
  - 以網路作為攻擊標的–竄改檔案、阻斷式服務攻擊、駭客入侵、電腦病毒等
  - 以網路作為犯罪場所–如色情、誹謗、賭博等
- **第358條 無故入侵電腦罪**
  - 無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。(為遏止駭客入侵行為)

➢ 第358條至第360條之罪，須告訴乃論。

妨害電腦使用罪主要內容

- **第359條 無故取得、刪除或變更他人電磁紀錄罪**
  - 無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。(為確保電腦內部電磁紀錄安全)
- **第360條 無故干擾電腦系統罪**
  - 無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。(為維護電腦及網路運作正常)

妨害電腦使用罪主要內容

- **第361條 對公務機關犯罪之加重**
  - 對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一。(為確保國家安全)
- **第362條 製作供犯罪程式罪**
  - 製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。(為防止犯罪工具之利用與擴散)

個人資料保護法(1/2)

- 為規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用，特制定本法。
- 個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

個人資料保護法(2/2)

盡告知義務與獲得書面同意

- 機關對個人資料之蒐集或利用的原則
  應尊重當事人之權益，依誠實及信用方法為之
  不得逾越特定目的之必要範圍，以確保當事人權益，避免人格權受到侵害
- 是否揭露個人資料，應由當事人本身審慎決定
- 第51條 有下列情形之一者，不適用本法規定：
  自然人為單純個人或家庭活動之目的，而蒐集、處理或利用個人資料。
  於公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料。

著作權法修正案

- 行政院於98年5月13日公佈著作權法部分條文修正，第六章之一**「網路服務提供者民事免責事由」**或稱**「ISP責任避風港條款」**
- 網路服務提供者包含：
  - 連線服務提供者(Hinet、Seednet、TANet等)
  - 快速存取服務提供者
  - 資訊儲存服務提供者(提供部落格、網路拍賣服務等)
  - 搜尋服務提供者(Google等搜尋引擎)

侵犯著作權行為

經著作權人舉證

- 使用者構成著作財產權之侵害，**ISP構成共同侵權行為**

ISP與使用者依法負民事連帶賠償責任

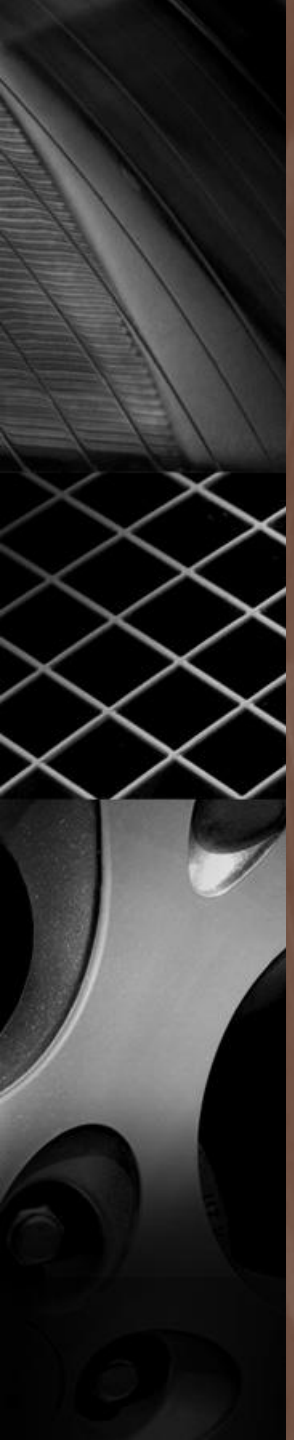
- 使用者　→依法負刑事責任：3年以下有期徒刑
- ISP行為人→依法負刑事責任：3年以下徒刑
- ISP(法人) →依法負刑事責任：罰金

避風港條款 & 三振條款

- 避風港條款
  - ISP業者接獲侵權通知，立即移除或關閉涉有侵權的內容。依法不負民事與刑事責任。
  - 移除或關閉後，立即告知「使用者」。使用者有回覆通知，立即轉送著作權人。著作權人必須在十天內提起訴訟證明，若著作權人沒有在十天內提出訴訟證明，必須在十四天內恢復使用者內容。
- 三振條款
  - 網路使用者如有三次涉及侵權情事，將可能被終止全部或部分的網路服務

業務項目服務說明

- 垃圾郵件處理機制說明
- 防毒軟體安裝網頁
- TV公播與LED跑馬燈播放系統



資安威脅發展趨勢

2009年六大資安事件

- 安全軟體商賽門鐵克回顧2009年六大資安事件，分別是：1.網路黑市批發個資、2.社群網站遭劫、3.網購平台個資外洩、4.駭客入侵電子郵件、5.垃圾郵件以及6.惡意病毒感染。
- 隨開心農場遊戲暴紅，facebook網站出現惡意連結，Twitter也一度遭受垃圾郵件入侵，資安問題成為這些社群網站重大挑戰。
- 此外，網路購物市場也爆發幾次網購平台個資外洩事件，佔詐騙事件35%，也讓網購安全性亮起紅燈。其他包括垃圾郵件暴增以及電子信箱帳號密碼外洩等事件。

資料來源：賽門鐵克防毒公司

2010年重大資安事件回顧

- 2010年間最受安全產業討論的議題Stuxnet(編按：2010 年11月Stuxnet蠕蟲攻擊伊朗核電廠，鎖定水庫、油井、電廠等重要基礎設施。大多數Stuxnet的攻擊目標出現在伊朗，引發意圖破壞核子設施的陰謀論說。)。毫無疑問的是，Stuxnet是一款高度精良的惡意軟體。但就衝擊度而言，多數的使用者並未受顯明的影響。它不偷盜資料，不促銷假防毒軟體，也不會大量傳送垃圾訊息。
- 過度強調Stuxnet預告了惡意軟體威脅影響「真實世界」機構的新世代來臨，也不完全正確。早在2003年，Slammer蠕蟲就打擊了俄亥俄州一個核能機構，並關閉了一個監視系統。而DOWNAD\Conficker蠕蟲攻擊了多個高知名度機 構如醫院（甚至影響了MRI磁核共振造影），執法單位，甚至不同的軍事機構。

資料來源：趨勢科技網站

最近更新文章

2012/5/28
把握技術革新 IT向前行

2012/5/28
徒手打造pfSense負載平衡器

2012/5/25
透過網頁隨時隨地開發專案 Cloud9 IDE提供雲端開發環境

2012/5/25
六大路徑引領職涯發展

2012/5/24
在Cisco路由器設定ISDN

2012/5/23
從IT資料找出商業價值 精誠助企業創造營運智慧

2012/5/23

首頁 ▷ 深度專訪 ▷

2012/1/30

2011資安回顧

吳傳輝

在跨年煙火的亢奮過後，大家還是會緬懷過去一年民國百年的精采。當然，整體資安市場在過去一年也發生了很多鬧哄哄的事件，因此在邁入新年之際，各大企業在經營策略與資安管理上也需重新檢視。

過去一年資安市場發生許多鬧哄哄的事件，所謂知己知彼，百戰百勝，藉由回顧2011年資安四大威脅，希望讓企業對整個大環境的安全走向掌握得宜。這些資安問題仍然是威脅發展的基調，攻擊特性可能會更為精密與針對性，企業應做好資安防護計畫，嚴正以待。

2011資安回顧

- 進階持續性威脅（APT）
- 行動惡意程式肆虐、資料遺失風險大增
- 地下經濟浮上檯面
- SSL憑證機構遭入侵

內部員工不慎將資料洩露外，更要嚴防將行動裝置當成竊取企業機密資料工具的惡意行為。

遭受攻擊的企業多數為化學相關的研究、開發及製造業者，其目的在於竊取智慧財產，例如設計文件、配方與製程等企業機密資料。

駭客透過竊取SSL憑證攔截網路用戶傳送機密資料

資料來源：網管人

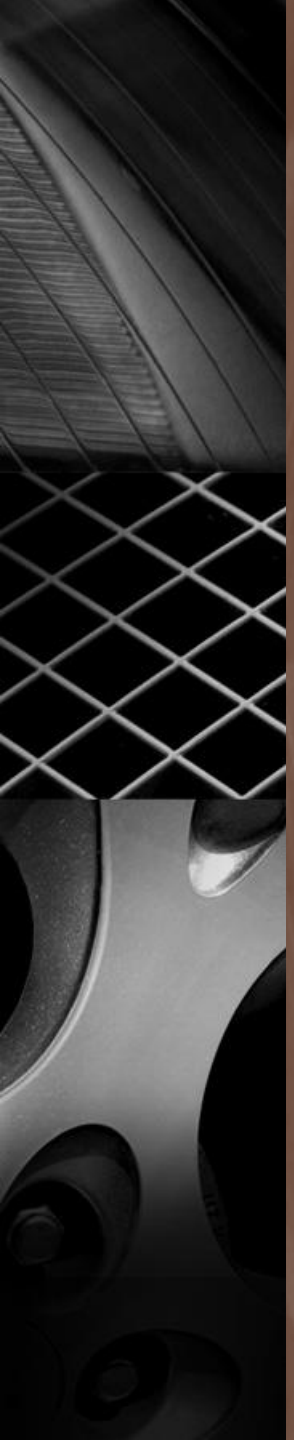
進階持續性威脅（APT）

1. 鎖定目標
2. 收集資訊
3. 發動攻擊

受攻擊往例分享

1. 攻擊者無法取得目標單位的E-mail等帳號資訊，於是透過社交網站蒐集到在目標單位工作的人員，再伺機慢慢靠近接觸，取得對方信任後再透過寄送惡意郵件等手法，逐步滲透。（有玩過facebook這類社交網站的應該知道要找到彼此陌生的兩個人間的共通朋友，並不是太困難的事吧）
2. 某知名網站，由於該網站資安防護體系還算完整，駭客久久無法攻破，於是轉個彎改採間接方式，研究與其介接的周邊服務，成功突破了周邊服務後再沿路慢慢打回去，最終還是成功竊取了該網站所儲存的大量機敏資訊。

原文網址: MIS的逆襲－企業怎麼面對APT攻擊？,Information Security 資安人科技網 http://www.informationsecurity.com.tw/article/article_detail.aspx?aid=6321#ixzz1w6bLYJaN

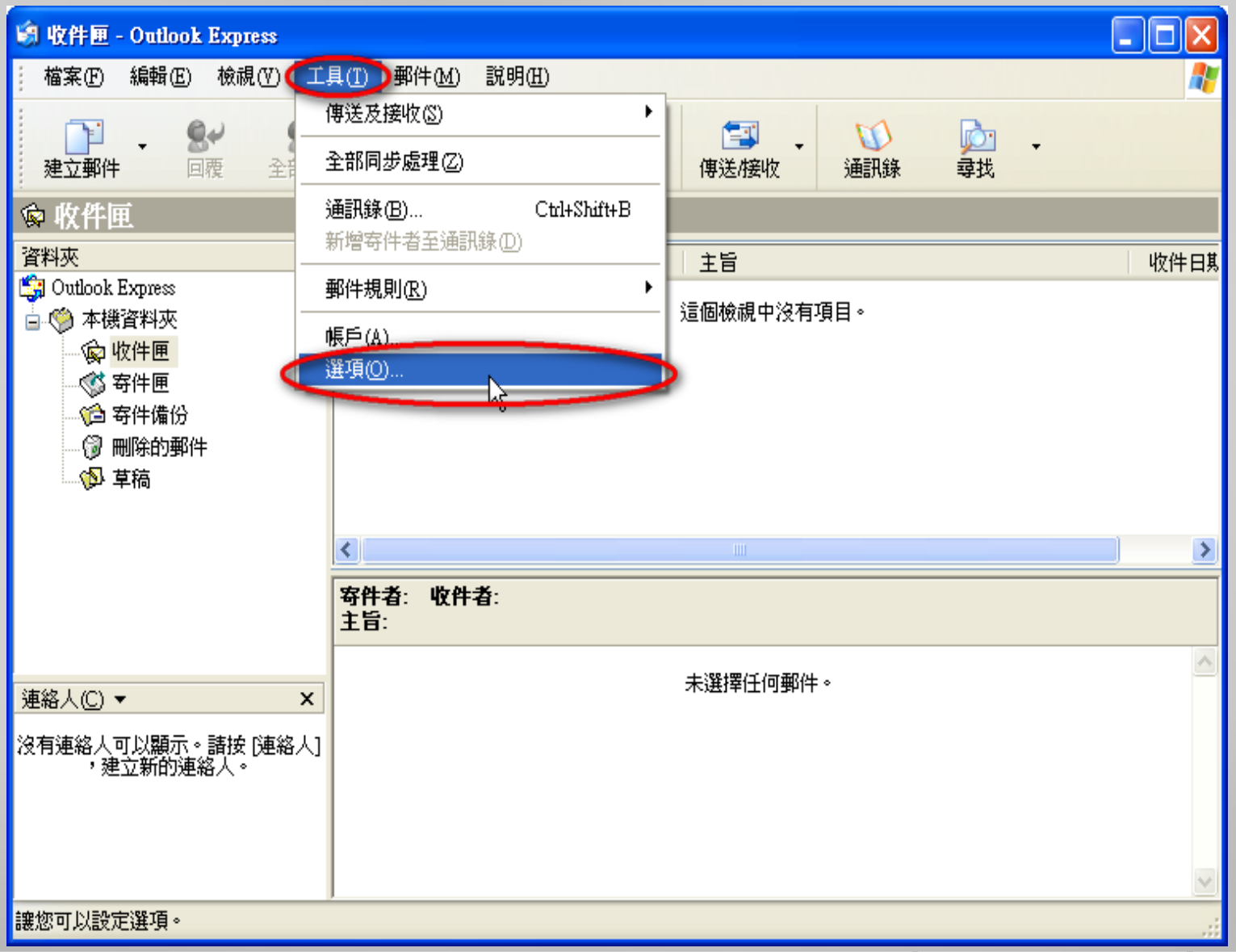


設定以文字方式開啟電子郵件

1.開啟 Outlook express，點選【工具】>【選項】

Outlook express

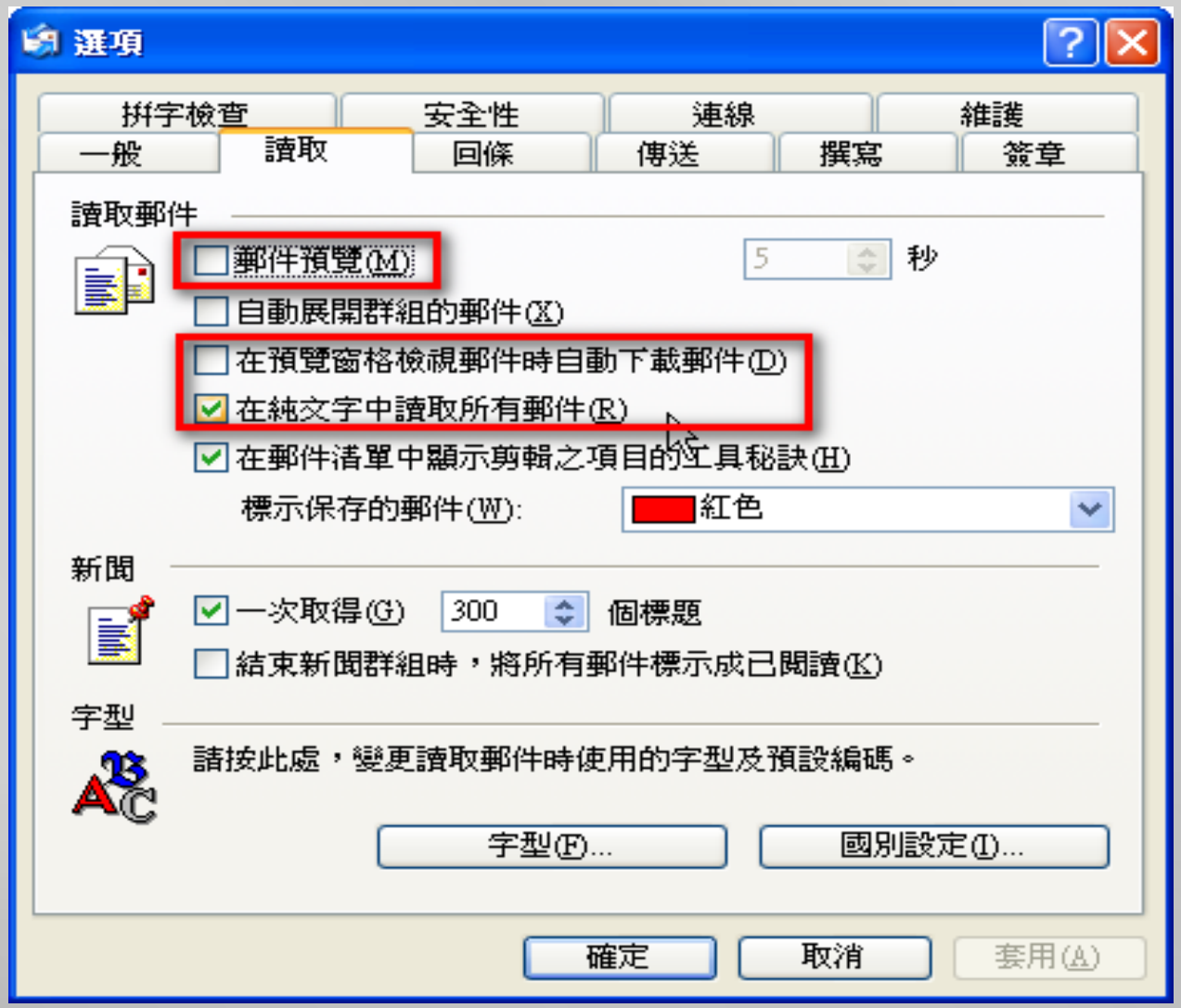
關閉自動下載郵件、在純文字中讀取所有郵件



2.再點選【讀取】，關閉【郵件預覽】與【在預覽窗格檢視郵件時自動下載郵件】，開啟【在純文字中讀取所有郵件】

Outlook express

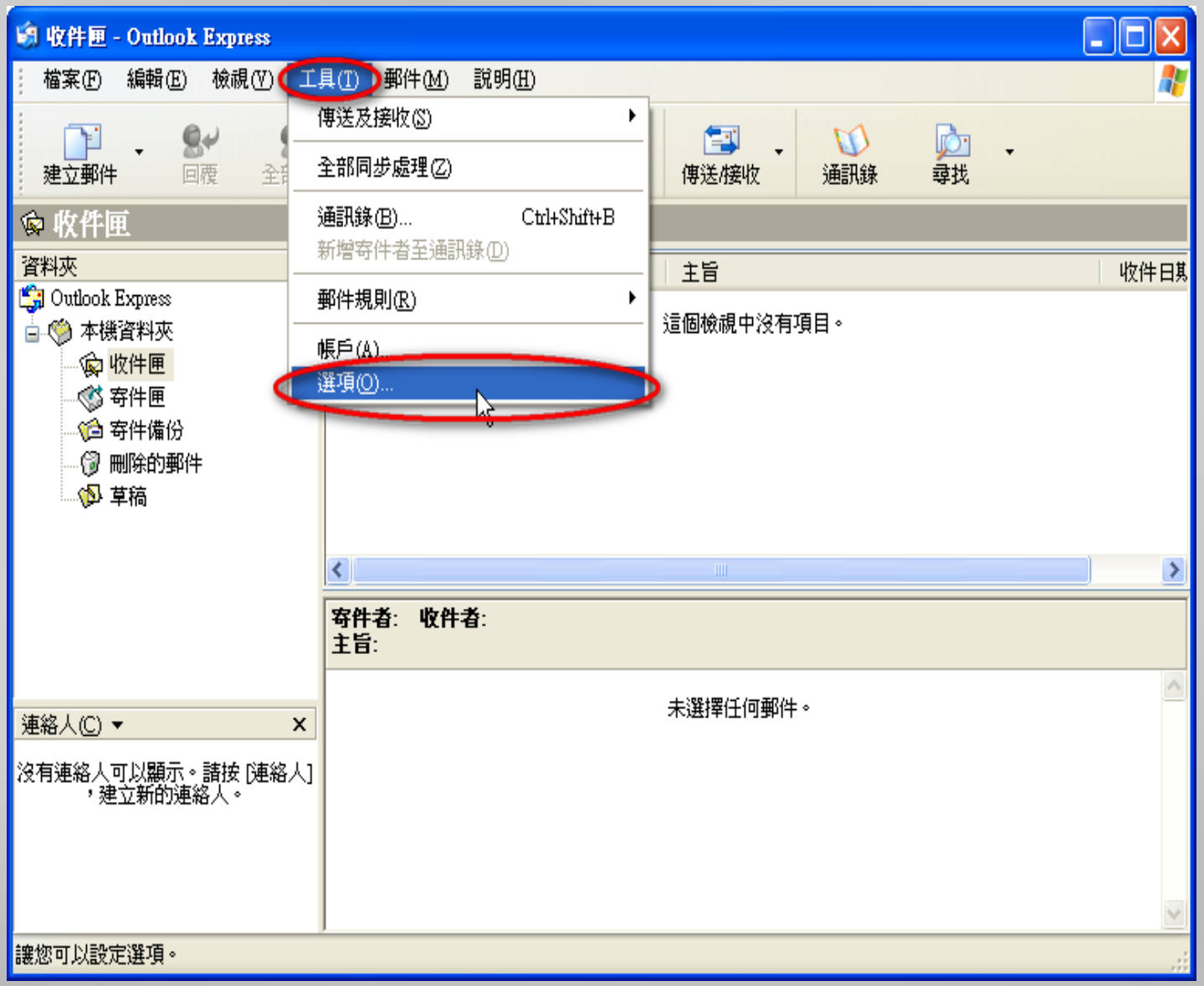
關閉自動下載郵件、在純文字中讀取所有郵件



1. 點選【讀取】> 【版面配置】

Outlook express

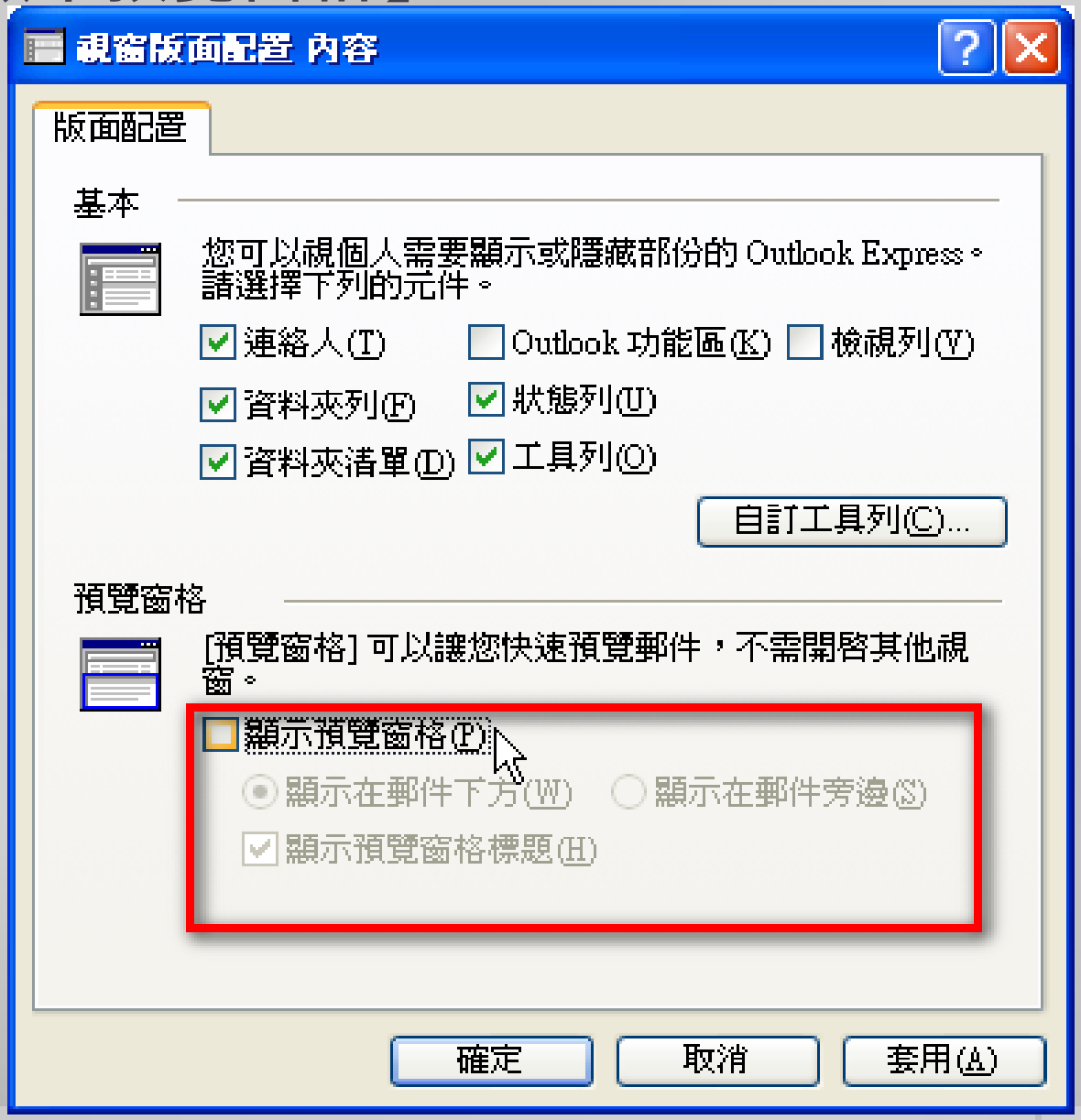
關閉預覽窗格



2. 關閉【顯示預覽窗格】

Outlook express

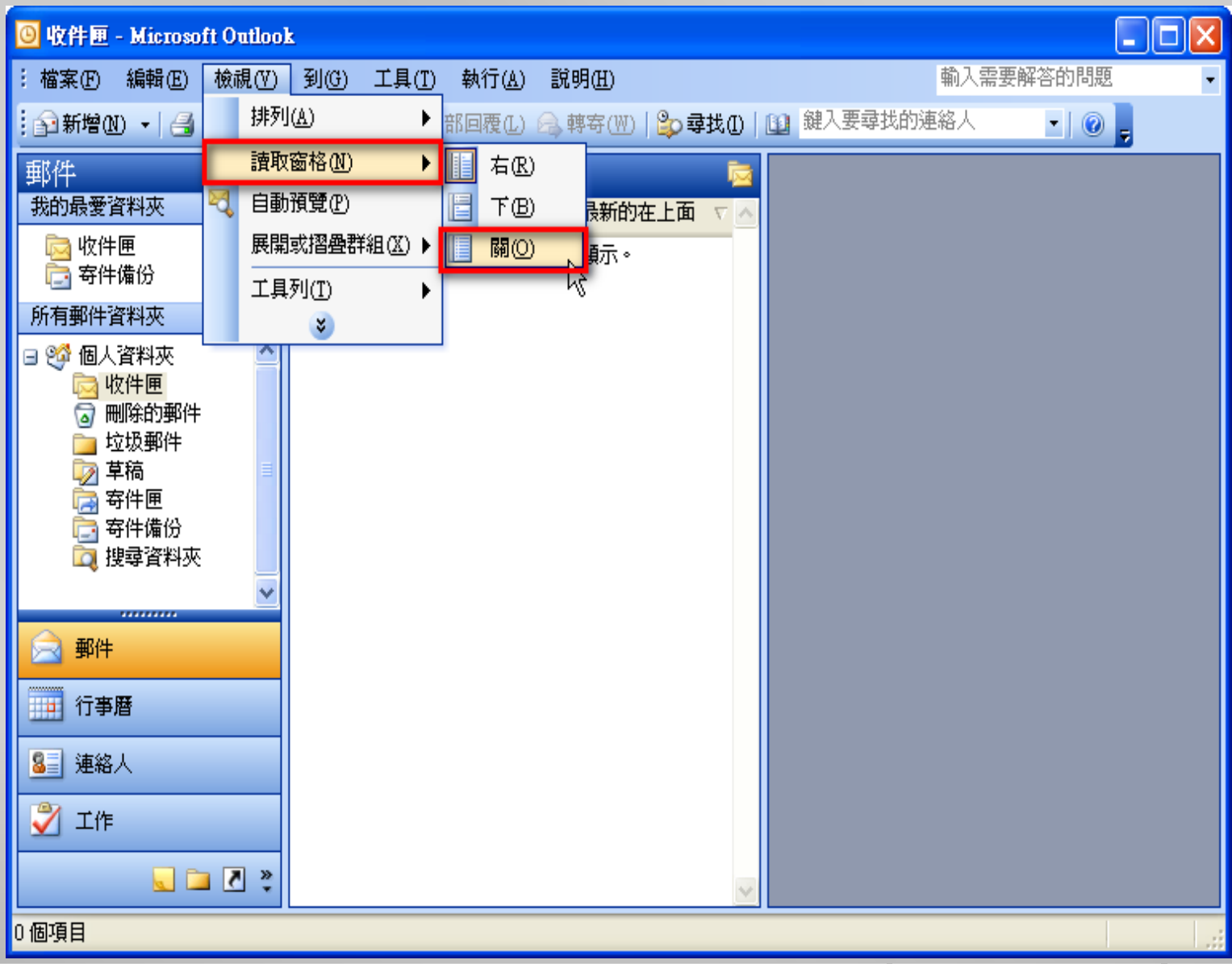
關閉預覽窗格



1. 關閉讀取窗格

Ootlook

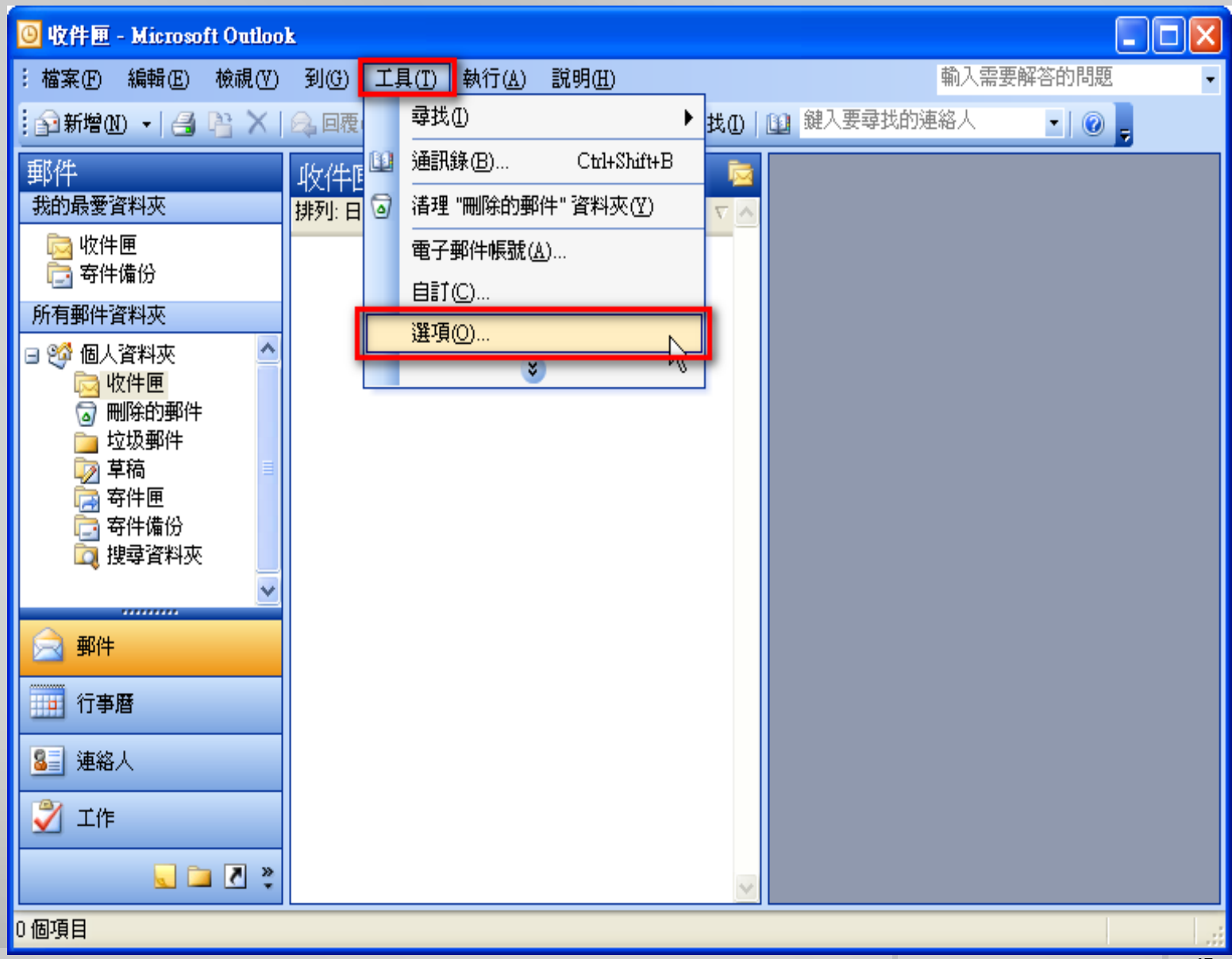
關閉讀取窗格、在純文字中讀取所有郵件



2. 以【純文字讀取所有標準郵件】

Ootlook

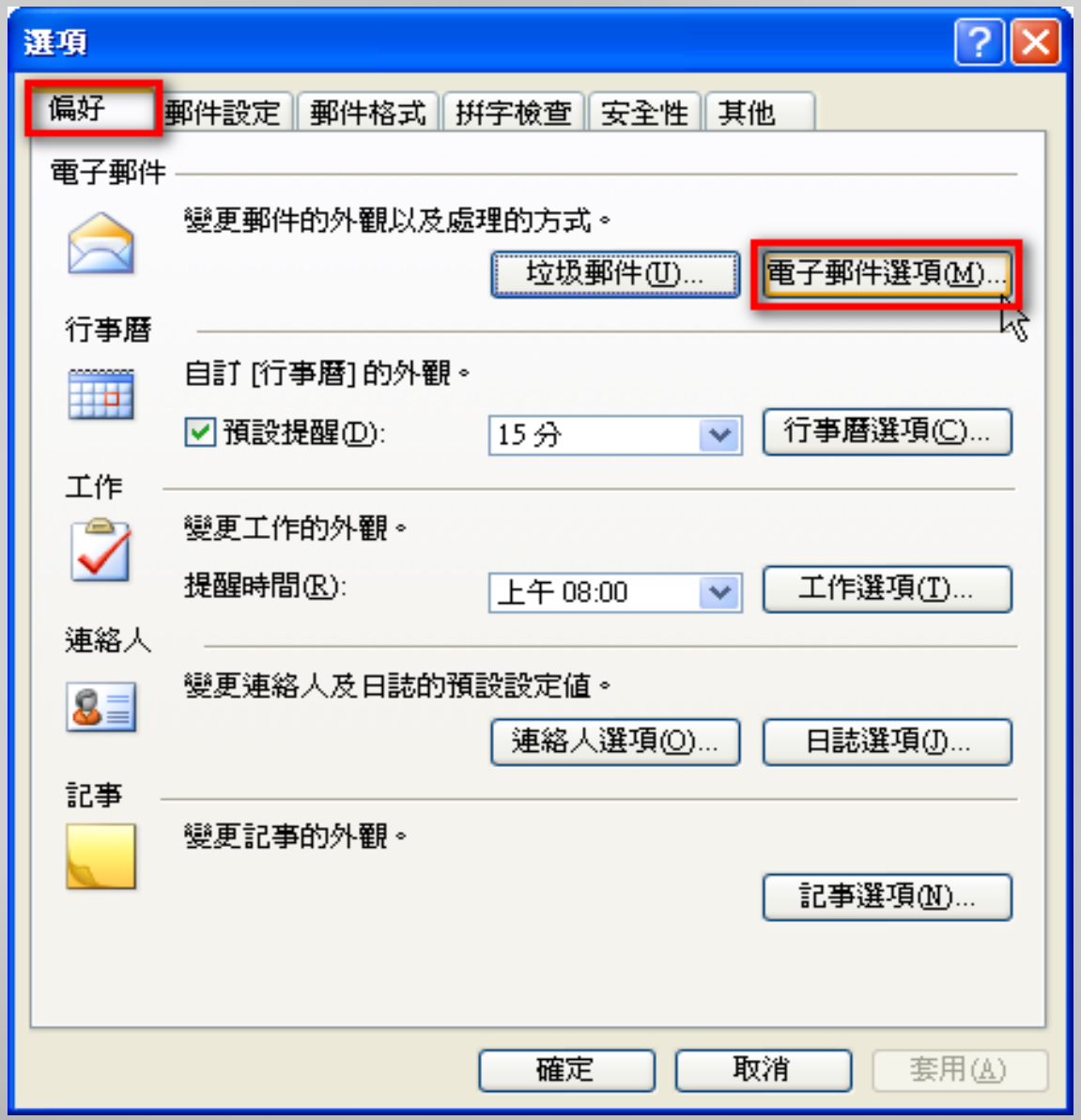
關閉讀取窗格、在純文字中讀取所有郵件



2. 以【純文字讀取所有標準郵件】(續)

Ootlook

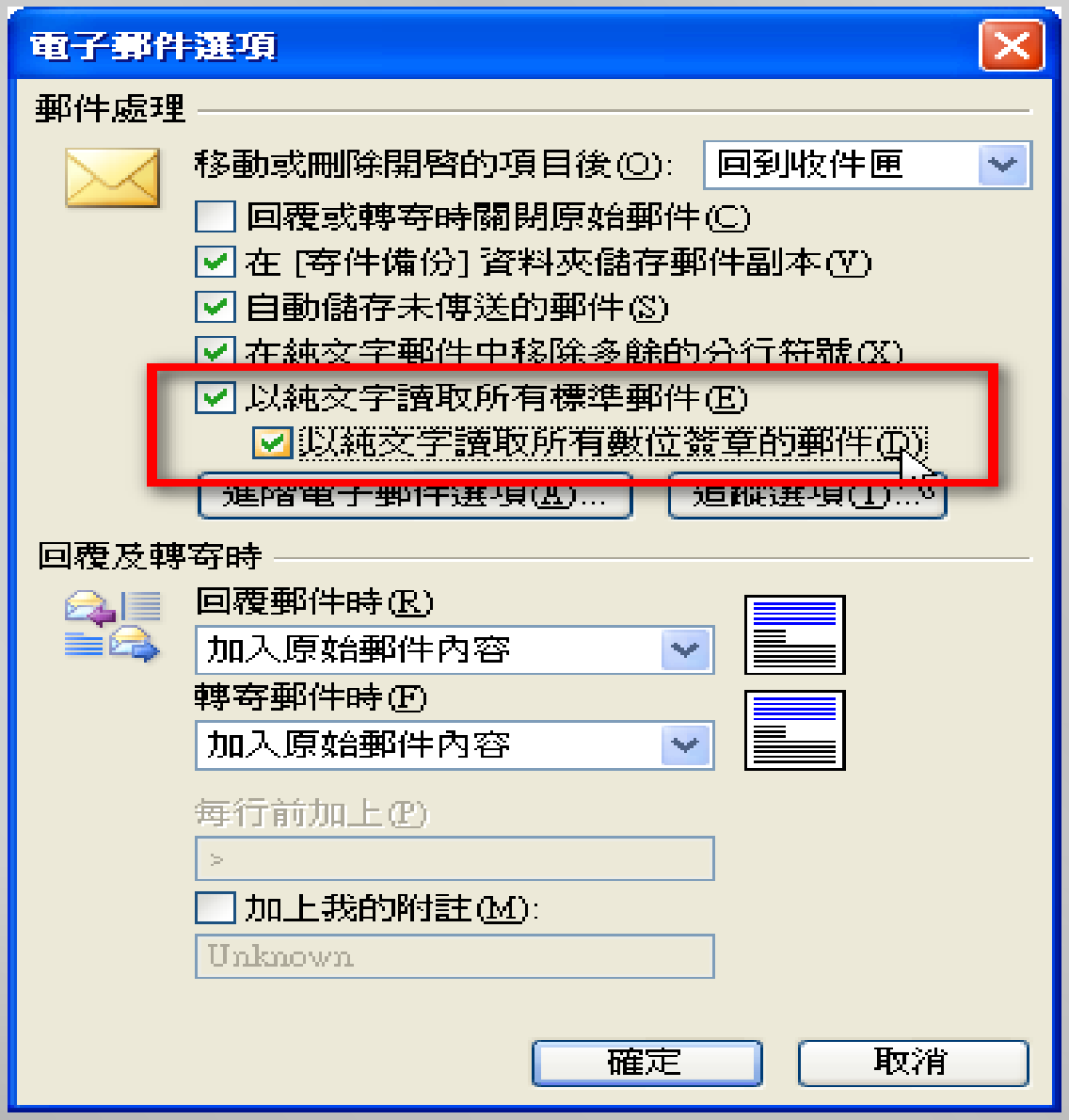
關閉讀取窗格、在純文字中讀取所有郵件



2. 以【純文字讀取所有標準郵件】(續)

Ootlook

關閉讀取窗格、在純文字中讀取所有郵件

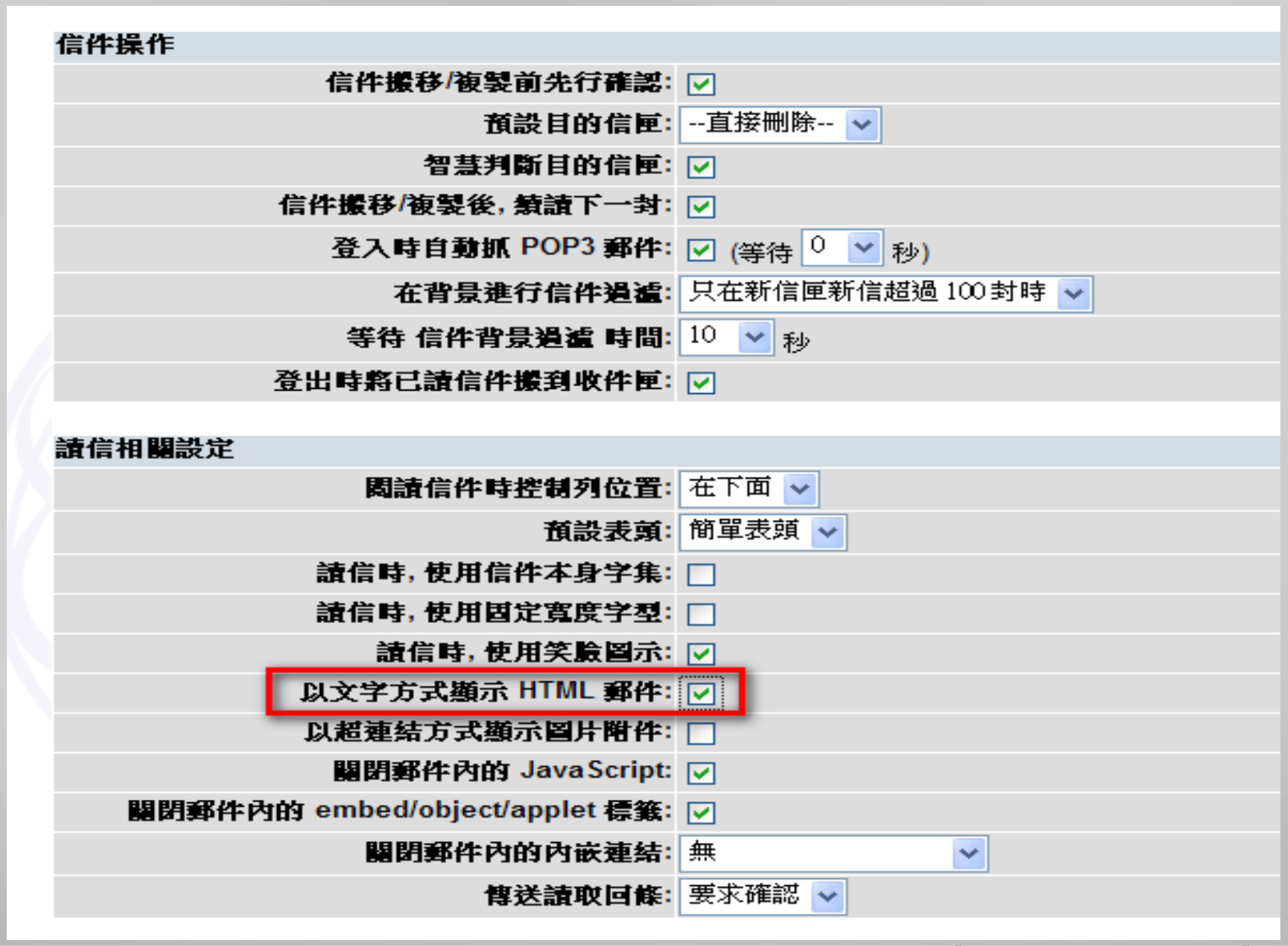


1. 點選【設定】

WebMail以文字方式顯示HTML郵件

2. 往下捲至【讀信相關設定】，勾選【以文字方式顯示HTML郵件】

WebMail 以文字方式顯示 HTML 郵件



簡報完畢，敬請指教

請幫忙繳回測驗問卷

感謝大家！