99年度資安教育暨防範惡意郵件社交工程演練教育訓練

報告時間：99年4月29日

報告單位：圖書館資訊技術組

	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

前言

最近資安新聞與案例

- 網路安全方面：
  - 網拍帳密被盜？ → 可能是亂點連結惹得禍
- 電子郵件安全方面：
  - 高盛案例為鑑 → 使用公司信箱宜慎
- 即時通安全方面：
  - MSN假網友 → 詐借門號認證

網安／網拍帳密被盜？可能是亂點連結惹得禍

NOWnews 今日新聞 更新日期：2010/04/27 10:06 記者蘇湘雲／台北報導

網路拍賣愈來愈夯，不過，根據資安業者觀察發現，最近一年以來所流竄的郵件病毒手法已然翻新，從單純的exe檔案換為含有後門的文件檔案，藉此躲避防火牆阻擋與防毒軟體偵測，而網友如果曾在網拍「問與答」中點選別人的連結網頁，也可能使個資遭受盜取。

許多人以為郵件病毒是靠exe檔案來散播，只需留意附件並靠防毒軟體偵測，即可安枕無憂。但事實上，HiNet SOC資安監控中心研究人員發現，郵件病毒正逐漸改成利用.lnk或含有後門的文件檔案來進行感染，駭客透過預設的檔案類型，在檔案內夾藏惡意指令，發動毒害攻擊。

此外，有網拍習慣的網友應留意，最近是否收過「我拍到裸模在大街上拍照」這類標題聳動的電子郵件，或是曾經在拍賣網站的收信夾中或者在網站上的「問與答」專區，點選了詢問者的商品連結？資安業者指出，上述

資料來源：http://tw.news.yahoo.com/article/url/d/a/100427/17/24m9l.html

高盛案例為鑑 使用公司信箱宜慎

更新日期：2010/04/27 12:05

高盛集團被美國金管單位指控詐欺，關鍵人物高盛交易員（圖雷）發送給女朋友、自我吹噓的電子郵件，恐怕會成為他犯罪的證據，因為電子郵件露餡，而麻煩上身的例子，屢見不鮮，不過多數人似乎永遠學不到教訓。（夏明珠報導）

職員使用公司的電子信箱，從事私人通信，這種事情，大概每個人都做過。像圖雷這樣，給自己惹上大麻煩的雖不多見，但是不同程度、性質類似的案例也不勝枚舉。

圖雷和高盛執行長（布蘭克范恩）今天要到參議院調查小組，針對美國證管會指控高盛賣空自己出售的商品，形同詐欺的坑殺投資人一案答詢。圖雷曾經對自己竟然想得出這種吃乾抹淨的行銷手法，洋洋得意，幹了虧心事，他要是閉嘴也就罷了，壞就壞在他還忍不住拿出來自我吹噓，向女朋友炫耀。

資料來源： http://tw.news.yahoo.com/article/url/d/a/100427/1/24met.html

MSN假網友 詐借門號認證

自由時報 更新日期：2010/04/27 04:11

謊稱手機螢幕故障

〔記者王昶閔、黃敦硯／台北報導〕❶「我的手機螢幕壞了，可否請您幫我收個簡訊？」如果好友突然在MSN上這樣向你求救，可得提高警覺，因為這個友人可能是詐騙集團化身，目標是你的手機門號，好心幫忙，下場不是荷包失血，就是成了人頭戶！

網路上傳出有詐騙集團盜用民眾MSN帳號，❷利用拍賣網站帳號申請機制，或以電信業者小額付費，騙取手機門號與認證碼，藉以從事不法。小陳就有類似經驗，一位久未見面的好友突然上線，透過MSN跟他寒暄幾句後，以手機螢幕壞掉為由，希望小陳協助代收簡訊，並轉述內容。

❸小陳爽快地將手機號碼以MSN傳給對方，不久手機就傳來一封簡訊，內容是一組數字與英文認證碼，他將這組密碼透過MSN轉述給好友，事成後對方就匆匆下線。

小陳越想越不對，直接打電話向友人求證，才發現友人的MSN帳號早遭到駭客盜用，自己很可能是遇上了詐騙集團，擔心自己成了人頭戶。

資料來源： http://tw.news.yahoo.com/article/url/d/a/100427/78/24m3s.html

清查電子看板系統(BBS)

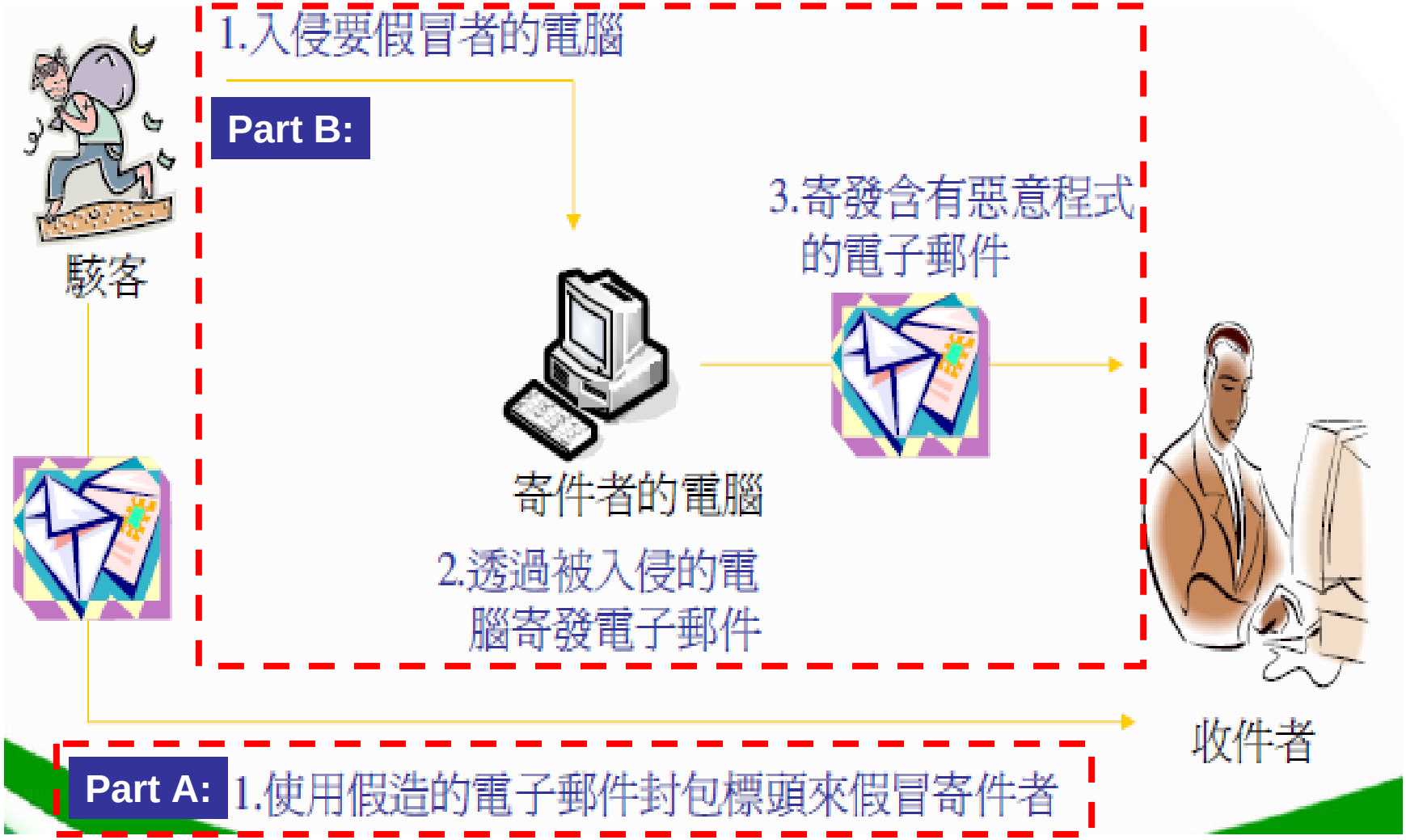
- 教育部係依據行政院秘書長99年4月21日院臺教字第0990023121號函辦理
- 行政院秘書長函轉立法院黃委員偉哲等22人提案
- 請各大專院校全面清查電子看板系統(BBS)是否有不法份子入侵從事不法業務，並要求各院校提出相關審查報告。

壹、什麼是社交工程

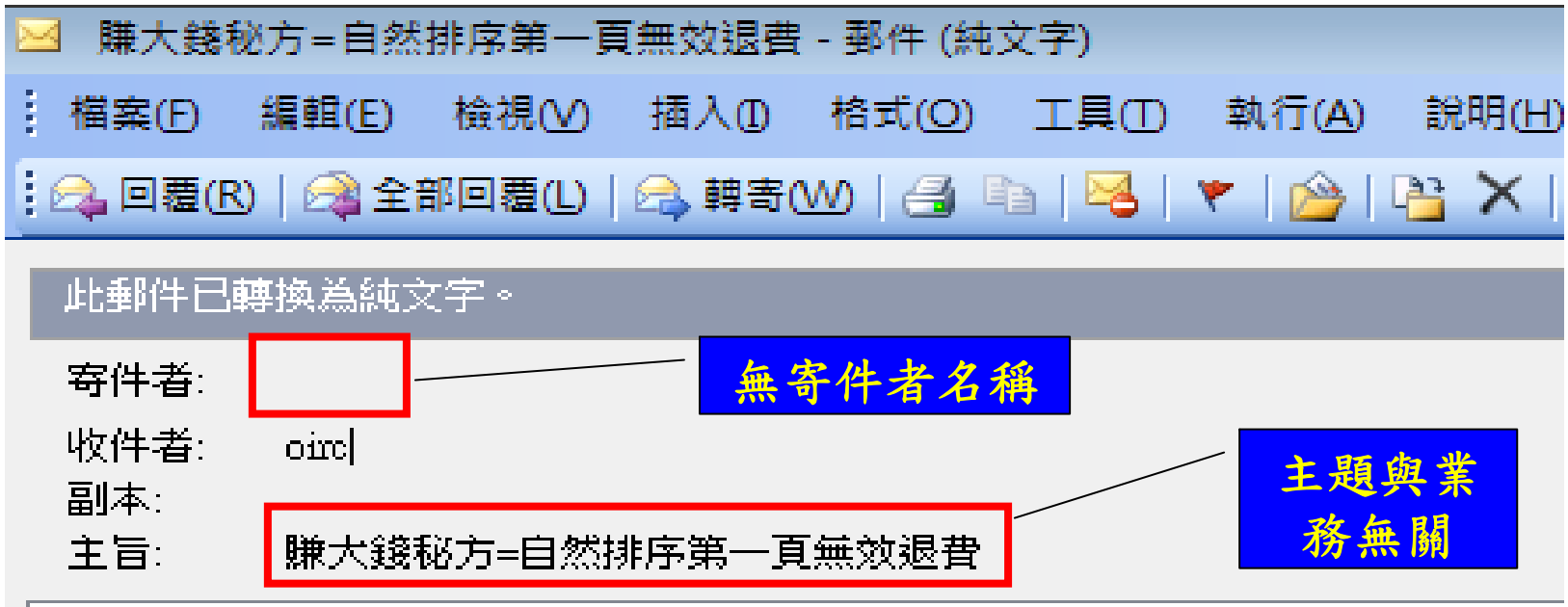
什麼是社交工程

- 超級騙騙騙 阿嬤篇
  - 詐騙事件層出不窮，犯罪手法也不斷翻新，民眾除了要明辨詐騙手法之外，也要了解當詐騙事件發生後，應該如何反應與解決。影片類別：內政及國土影片
  - 長度：0:4:0
  - 上架日期：2008-10-20
  - 來源提供：內政部警政署 (網址：http://media.www.gov.tw/media.do?id=324)

如何發送惡意郵件



範例：騙取郵件帳號密碼



【保證您的網站再雅虎 Google第一頁】 <http://ideagroup.com.tw/bossco/front/bin/ptd

親愛的 廠商、網站負責人 您好~ <http://ideagroup.com.tw/bossco/front/bin/ptdetail.j

1.關鍵字自然排序保證讓您客戶大增，保證讓客戶自動上門，? <http://ideagroup.cor

2.請由此進入影片說明如何讓客戶自動上門， <http://ideagroup.com.tw/bossco/front/b

3.我們不做第二頁 只做第一頁 且用公司合約保證 "履約保證，無效退費" <http:/

4.現在推出"客戶自動上門超值專案" <http://ideagroup.com.tw/bossco/front/bin/ptdetail.

貳、99年度電子郵件社交工程演練說明

1. 教育訓練要求

- 資安教育訓練應納入社交工程防制有關之認知宣導。
- 各機關學校人員**每年至少需接受1小時**社交工程防制宣導講習。
- 辦理**兩階段**宣導課程：
  - **第一階段（於演練作業辦理前）**：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比例較高**之「**應重點宣導人員**」再次進行宣導，以強化其警覺性。

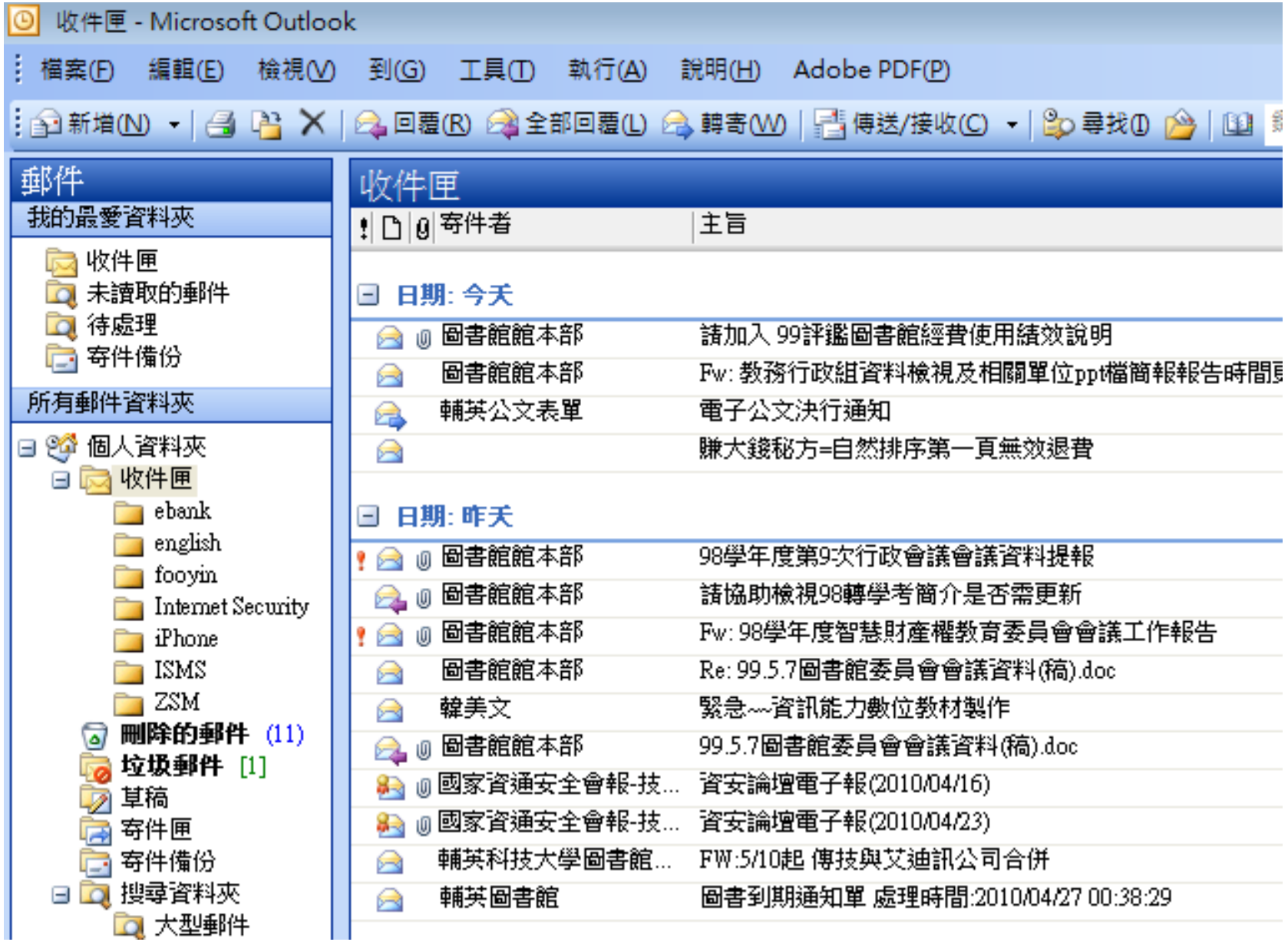
2. 演練時程

1. 提報演練名單：**4月** (學校1/2行政人員)
2. 辦理教育訓練：**4月** (全部行政人員)
3. 教育部進行**第1次演練**：**5月**
4. 各機關學校辦理再教育訓練：**6~8月** (開啟、點閱惡意郵件比率較高人員)
5. 本部進行**第2次演練**：**9月**
6. 各機關學校辦理再教育訓練：**10月** (開啟、點閱惡意郵件比率較高人員)

3. 要求標準

適用單位	98年度目標	99年度目標
大學、區域網路中心、縣(市)教育網路中心	點閱率< 9% 開啟率< 16%	點閱率< 6% 開啟率< 10%

- **開啟率**：信件透過**預覽**或**點開方式開啟**，且信件本文內所含圖片亦完成圖片下載之動作。
- **點閱率**：受測人員**點選信件內文中之連結網址**，若信件包含多個連結，不論點選幾個，都將只記錄一次。


收件匣 - Microsoft Outlook
檔案(F) 編輯(E) 檢視(V) 到(G) 工具(T) 執行(A) 說明(H) Adobe PDF(P)
新增(N) 回覆(R) 全部回覆(L) 轉寄(W) 傳送/接收(C) 尋找(I)
郵件
我的最愛資料夾
收件匣
未讀取的郵件
待處理
寄件備份
所有郵件資料夾
個人資料夾
收件匣
ebank
english
fooyin
Internet Security
iPhone
ISMS
ZSM
刪除的郵件 (11)
垃圾郵件 [1]
草稿
寄件匣
寄件備份
搜尋資料夾
大型郵件
收件匣
寄件者
主旨
日期: 今天
圖書館館本部 請加入 99評鑑圖書館經費使用績效說明
圖書館館本部 Fw: 教務行政組資料檢視及相關單位ppt檔簡報報告時間更
輔英公文表單 電子公文決行通知
賺大錢秘方=自然排序第一頁無效退費
日期: 昨天
圖書館館本部 98學年度第9次行政會議會議資料提報
圖書館館本部 請協助檢視98轉學考簡介是否需更新
圖書館館本部 Fw: 98學年度智慧財產權教育委員會會議工作報告
圖書館館本部 Re: 99.5.7圖書館委員會會議資料(稿).doc
韓美文 緊急~~資訊能力數位教材製作
圖書館館本部 99.5.7圖書館委員會會議資料(稿).doc
國家資通安全會報-技... 資安論壇電子報(2010/04/16)
國家資通安全會報-技... 資安論壇電子報(2010/04/23)
輔英科技大學圖書館... FW:5/10起 傳技與艾迪訊公司合併
輔英圖書館 圖書到期通知單 處理時間:2010/04/27 00:38:29


收件匣 - Microsoft Outlook
檔案(F) 編輯(E) 檢視(V) 到(G) 工具(T)
新增(N) 回覆(R)
錯誤示範!!!
郵件
我的最愛資料夾
收件匣
未讀取的郵件
待處理
寄件備份
所有郵件資料夾
個人資料夾
收件匣
ebank
english
fooyin
Internet
iPhone
ISMS
ZSM
刪除的郵件
垃圾郵件
收件匣
排列: 日期 最新的在上面
今天
圖書館館本部 下午 ...
請加入 99評鑑圖...
圖書館館本部 上午 ...
Fw: 教務行政組資料...
輔英公文表單 上午 ...
電子公文決行通知
上午 6:07
賺大錢秘方=自然排...
昨天
圖書館館本部 (週二...
98學年度第9次...
請加入 99評鑑圖書館經費使用績效說
圖書館館本部 [lb@mail.fy.edu.tw]
此郵件已轉換為純文字。
收件者: 啟中
附件: 99評鑑圖書館經費使用績效說明
啟中:
請於最後一段分項有關"資安"、網路及Elearning的
阿姐

4. 演練執行方式

- 以偽冒公務、個人或公司行號等名義發送惡意郵件給演練對象
- 寄發電子郵件類型
  - 郵件類型分為*休閒娛樂*、*保健養生*、*科技新知*、*八卦影視*、*情色內容*、*財經資訊*等
  - 信件內容包含*連結網址*或*word附檔*
- 當收件人執行下列動作後，即留下紀錄
  - **開啟郵件**
  - 開啟郵件中**網頁連結**或**附件檔案**

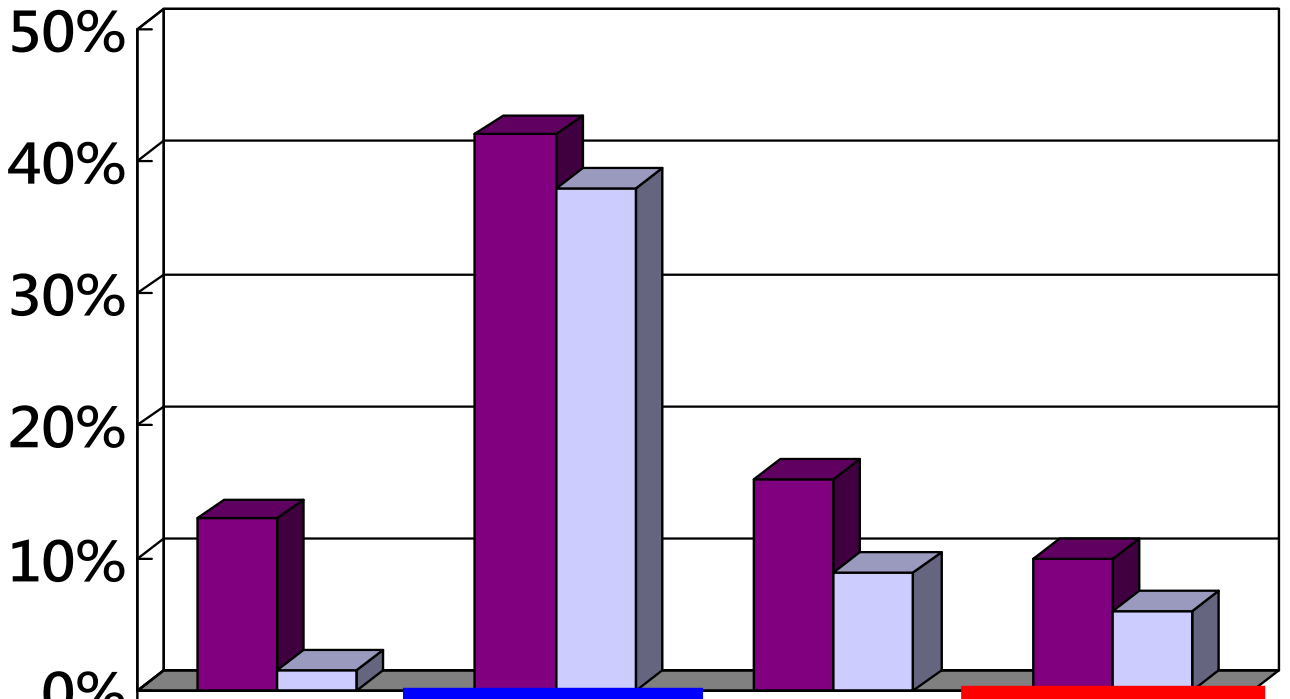
5. 上次演練使用郵件主旨 (1/2)

組別	信件類別	信件標題
Letter 1	政治類	軍方賣官內幕
Letter 2	體育類	洋基球團虧待王建民
Letter 3	休閒娛樂類	自行車旅遊私房路線
Letter 4	休閒娛樂類	聯合報邀您賞桐花
Letter 5	科技新知類	USB 成病毒温床！台灣電腦今年Q1中毒率列入全球第四大
Letter 6	保健養生類	蛀牙不是病，痛起來要人命
Letter 7	投資理財類	景氣復甦了嗎？
Letter 8	保健養生類	新流感 H1N1 大流行期間，個人保健注意事項
Letter 9	休閒娛樂類	蔡依林愛無赦+練舞功超神奇混音版

5. 上次演練使用郵件主旨 (2/2)

組別	信件類別	信件標題
Letter 1	生活類	讓你感動的動人廣告
Letter 2	投機類	如何提高中獎機率!!
Letter 3	旅遊類	【HiNet旅遊網首發團】 獨家限量獨享好康 超低價!!
Letter 4	旅遊類2	【HiNet旅遊網首發團】 獨家限量獨享好康 超低價!!
Letter 5	健康類	健康新撇步!!?你如何活的更健康
Letter 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
Letter 7	影視類	文英阿姨病逝 留給觀眾無限懷念
Letter 8	影視類2	昔日玉女紅星 酒井法子自首 坦承吸毒
Letter 9	趣味類	親愛的同事!放鬆一下
Letter 10	購物類	iPhone 最新推出3Gs 便宜到不敢相信！！

6. 上(98)年度成績



	98年5月	98年9月	98年標準	99年標準
點閱率	13%	42%	16%	10%
開啟率	2%	38%	9%	6%

參、相關防護措施

1.可疑的電子郵件特徵

- 過於聳動的主旨與緊急要求。
- 不正常的發信時間。
- 陌生人或少往來對象來信。
- 認識的人來信但主旨或內容與其習性不符。
- 要求輸入私密資料送出。

2.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 (寄件者或資訊中心)

3.寄送電子郵件應注意事項

- 郵件信箱功能分配
  - 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
- 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

4.收到電子郵件時應注意事項

- 寄件人
  - 陌生人不要開
  - 寄件人是可以偽冒的(實作)
- 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
- 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

5.讀取電子郵件時應注意事項

- 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
- 附件
  - 請勿直接開啟
  - 下載掃毒確認安全再開啟
- 連結
  - 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

6.注意連結與附檔

- Com
- Exe
- Scr
- Lnk
- Bat

木馬程式

小心木馬就在你身邊

垃圾郵件

雖然您現在已經有收不完的垃圾郵件，但您還是要曉得不要製造機會給垃圾郵件業者...

題外話

轉寄網路郵件，可能沒注意到要保護他人個資而外洩了他人的郵件信箱、個人資料...

你粉熱心..但是

不加思索地轉寄網路郵件，根本是在協助散播謠言，甚至可能吃上毀謗官司...

電腦處理個人資料保護法

- 第33條-**意圖營利**違反第七條、第八條、第十八條、第十九條第一項、第二項、第 二十三條之規定或依第二十四條所發布之限制命令，致生損害於他人者，**處二年以下有期徒刑、拘役或科或併科新臺幣四萬元以下罰金**。
- 第34條-**意圖為自己或第三人不法之利益或損害他人之利益**，而對於個人資料檔案 為非法輸出、干擾、變更、刪除或以其他非法方法妨害個人資料檔案之正確，致生損害於他人者，**處三年以下有期徒刑、拘役或科新臺幣五萬元以下罰金**。

電腦處理個人資料保護法—罰則

- 第49條 非公務機關之代表人、管理人或其他有代表權人，因該非公務機關依前三條(第46-48條)規定受罰鍰處罰時，除能證明已盡防止義務者外，應並受同一額度罰鍰之處罰。

- **非公務機關要證明「無故意或過失責任」才能免責，公務機關則須負「無過失責任」。**

7.自我防護

- 技術層面
  - 修補系統漏洞 .....XP sp3
  - 安裝防毒軟體
  - 安裝間諜程式檢查軟體，開啟防火牆。
  - 關閉信件預覽及html功能
- 行為層面
  - 開啟信件前，請...三思啊！
  - 開啟連結時，請...三思啊！
  - 開啟附件檔案時，請...三思啊！

8.你可以做得到

- 個人資料不放於網路
- 避免使用非法軟體或破解軟體
- 別讓好奇心害了你
- 養成資料備份習慣
- 有狀況即時通報資訊單位
- 校內禁止避免使用點對點傳輸軟體
  例如：edonkey,foxy,kuro等
- 不是所屬業務信件一律不開(Pchome,Yahoo…..)
- 陌生郵件一律不開!!!
- **不要太八卦, 萬一開了怪怪的郵件就*不要再轉寄*!!!**

9.保護機密資料

- 不論使用者使用哪一種防衛機制，駭客總是能找到一條路徑來入侵，為了保護我們的資料，應該進行：
  - 實體隔離
  - 資料加密

9A.實體隔離

- 實體隔離定義
  - 將組織敏感、重要的資料存放在無法對外連線到網際網路的特殊機器或區段上。
  - 例如：各國軍方均會各自發展不連接網際網路的軍事網路系統
  - 簡單來說就是：「斷絕網際網路連線」

9B.資料加密

- 資料加密的保護
  - 資料在儲存、傳送、處理的過程中都應該進行加密，讓駭客就算取得資料也看不懂。
  - 加密的方式若是使用密碼的方式，則應該注意密碼的強度（長度、複雜度）。
  - 例如：在資料儲存時**壓縮加密**，**密碼**與被傳送的資料，一定要**分由不同信件**或**其他方式**傳遞。

結論

- 使用者在收取電子郵件時應有的習慣
  - **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。
- 使用者在平時應有的行為
  - 啟用防火牆
  - **對重要資料進行加密、備份（先加密再備份）**
  - 保持在最低的使用權限
  - 提高警覺，加強危機意識。

- 網路與現實世界一樣，處處是危機，保持高度的警覺性是必要的。
- 注意瀏覽網頁、電子郵件等網路應用，可能帶來的危害。
- 應謹防社交工程的詐騙行為。
- 使用必要的防護工具，並勤做更新。
- 沒有正確的資安觀念，就沒有安全的電腦環境。

報告完畢

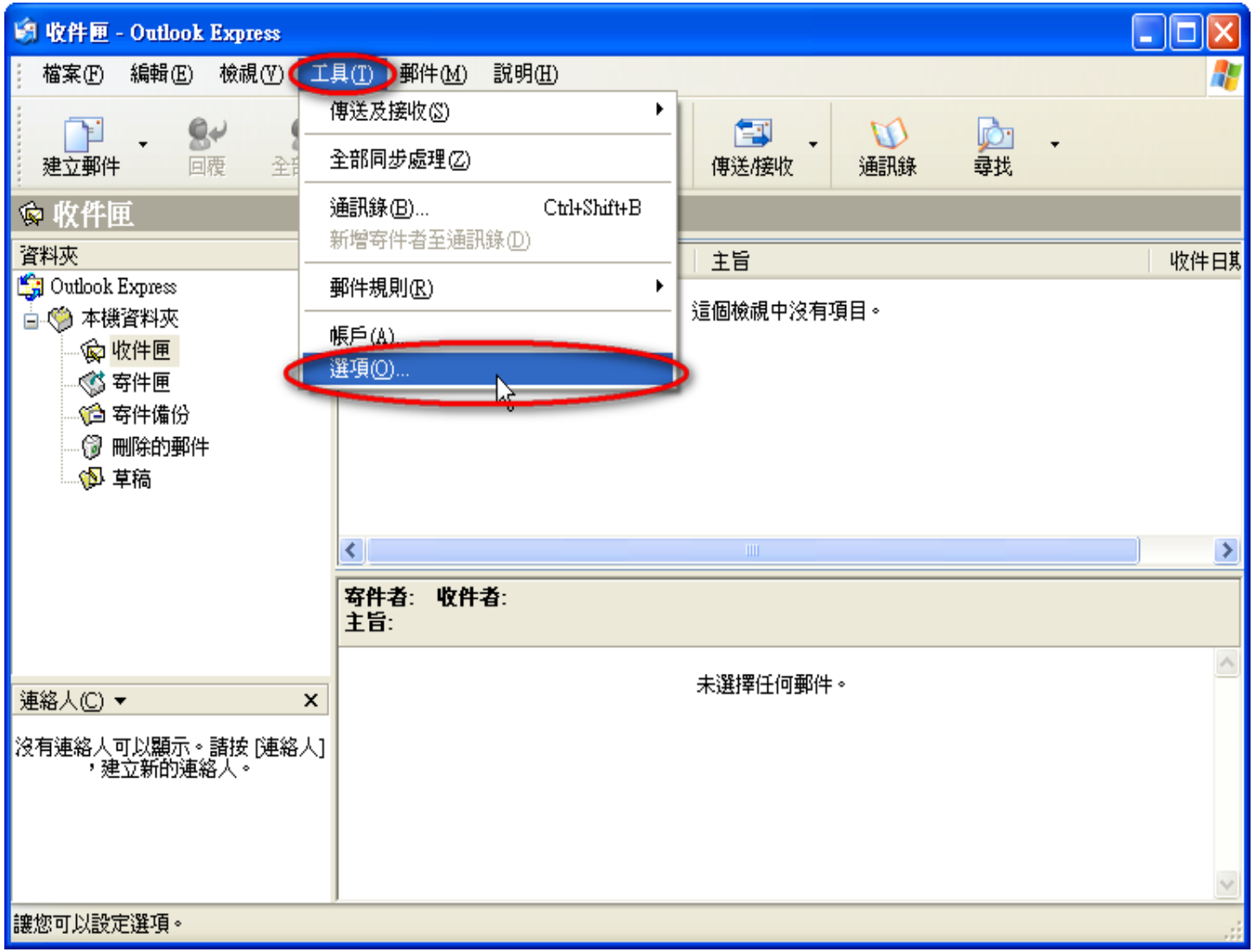
Q&A

補充：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

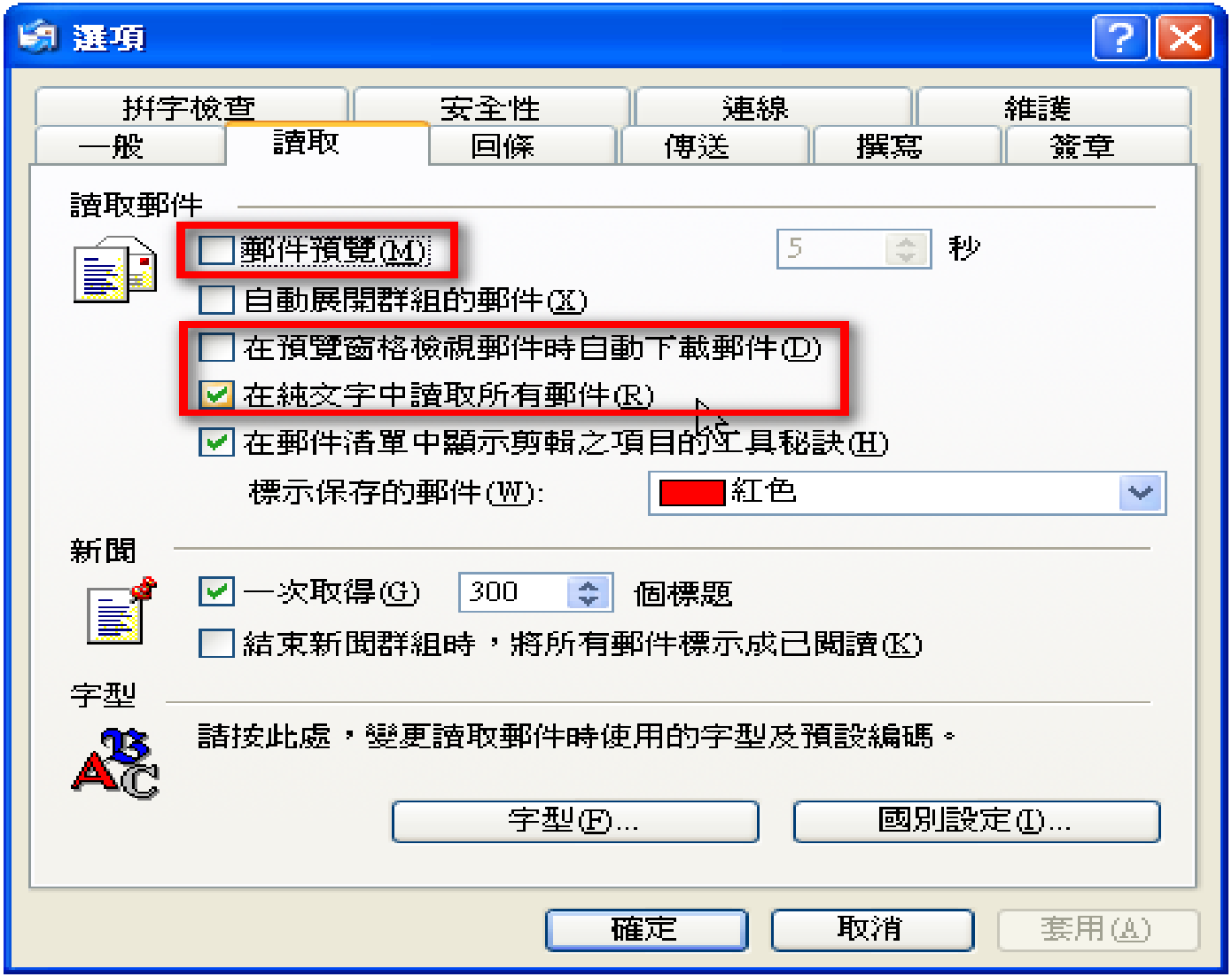
關閉自動下載郵件、在純文字中讀取所有郵件



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

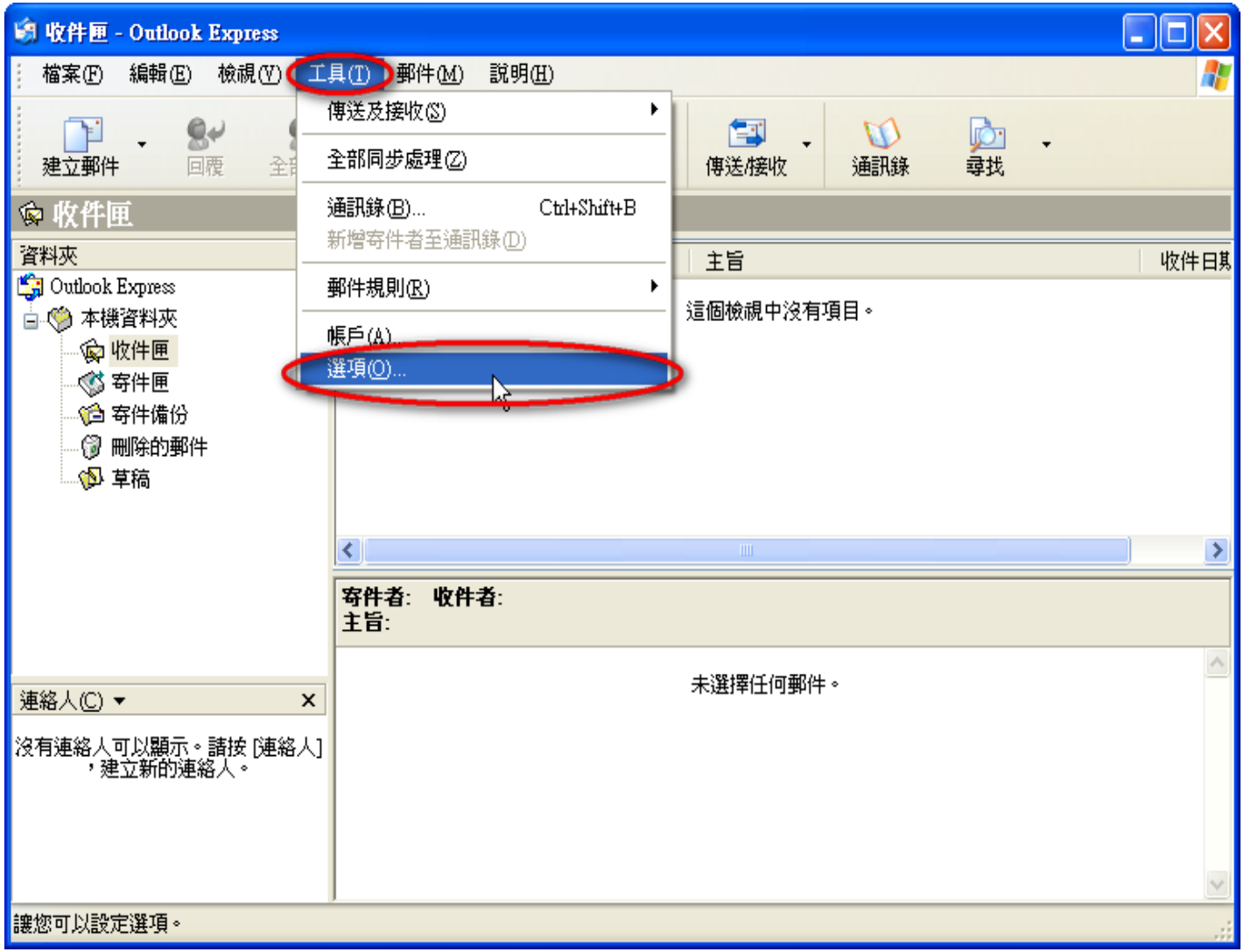
關閉自動下載郵件、在純文字中讀取所有郵件



1. 點選【讀取】>【版面配置】

Outlook express

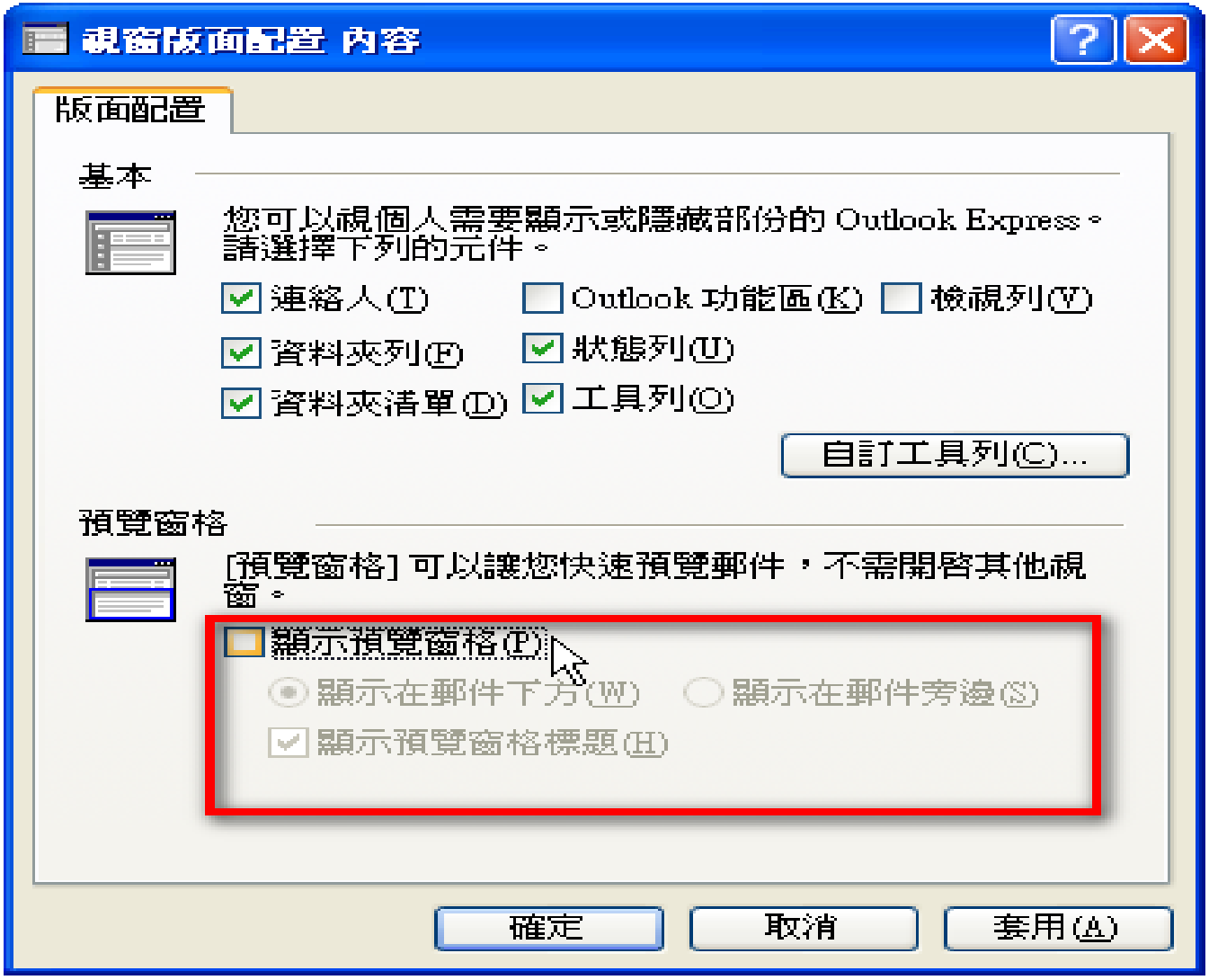
關閉預覽窗格



2. 關閉 【顯示預覽窗格】

Outlook express

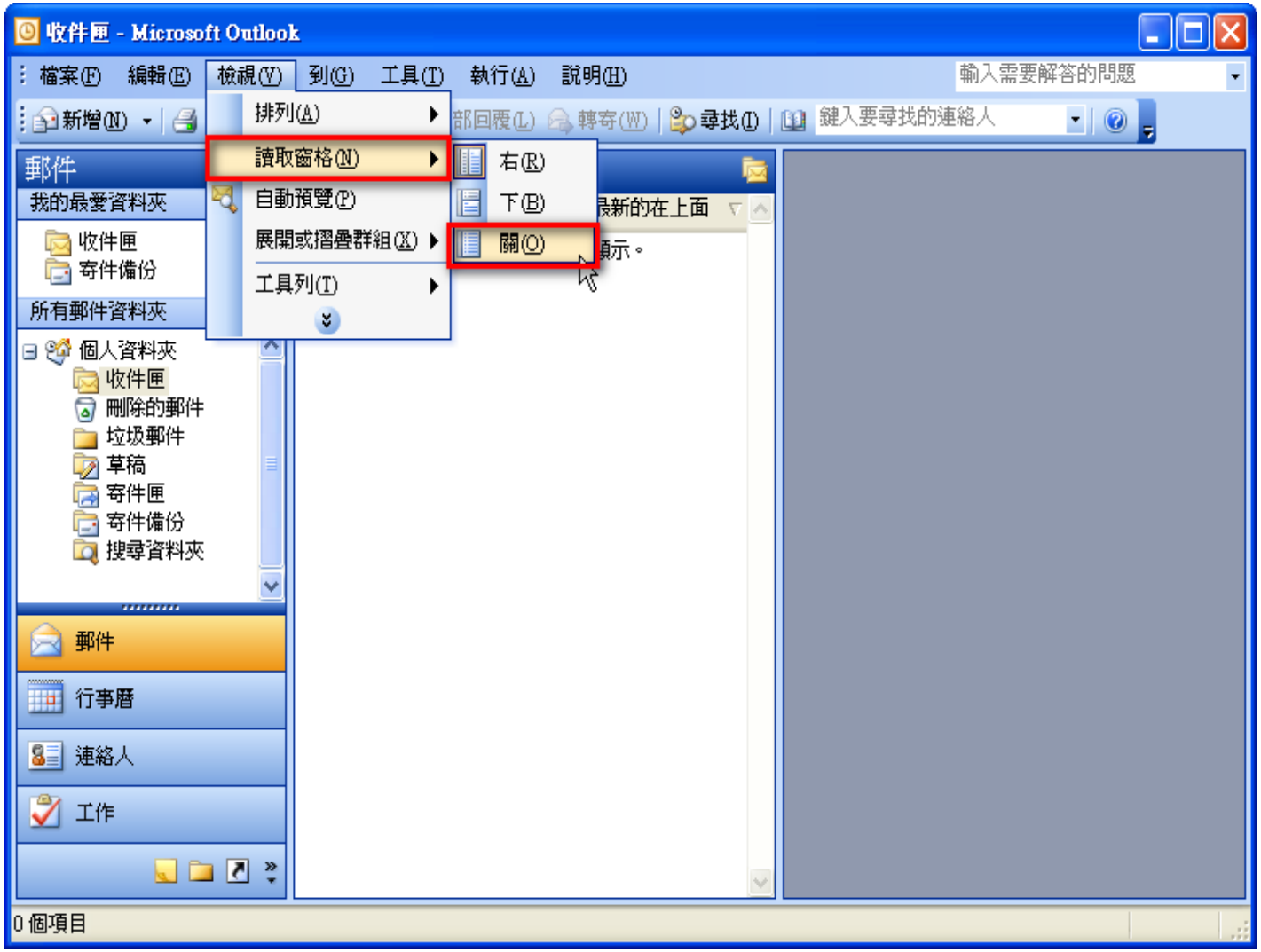
關閉預覽窗格



1. 關閉讀取窗格

Ootlook

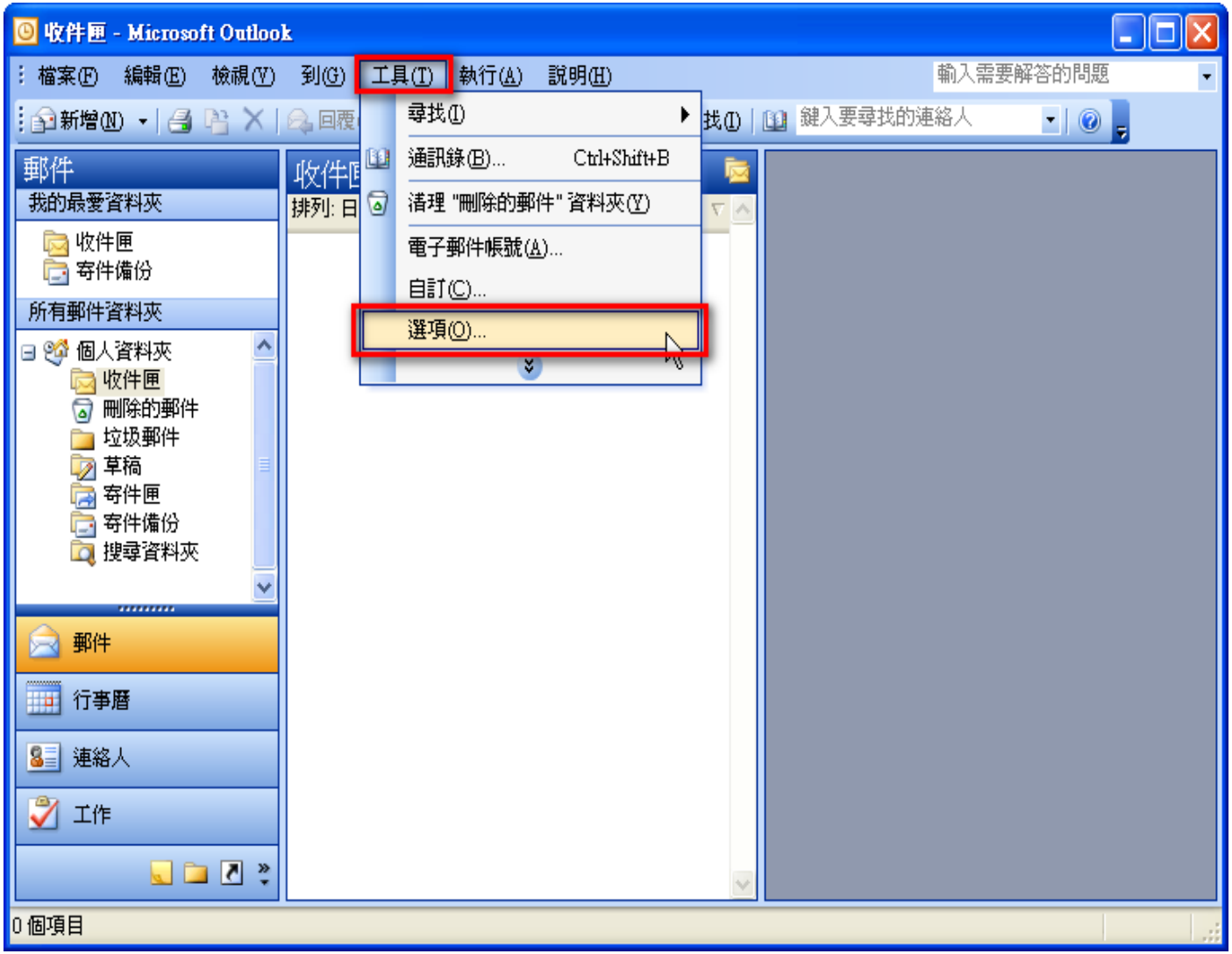
關閉讀取窗格、在純文字中讀取所有郵件



2. 以 【純文字讀取所有標準郵件】

Ootlook

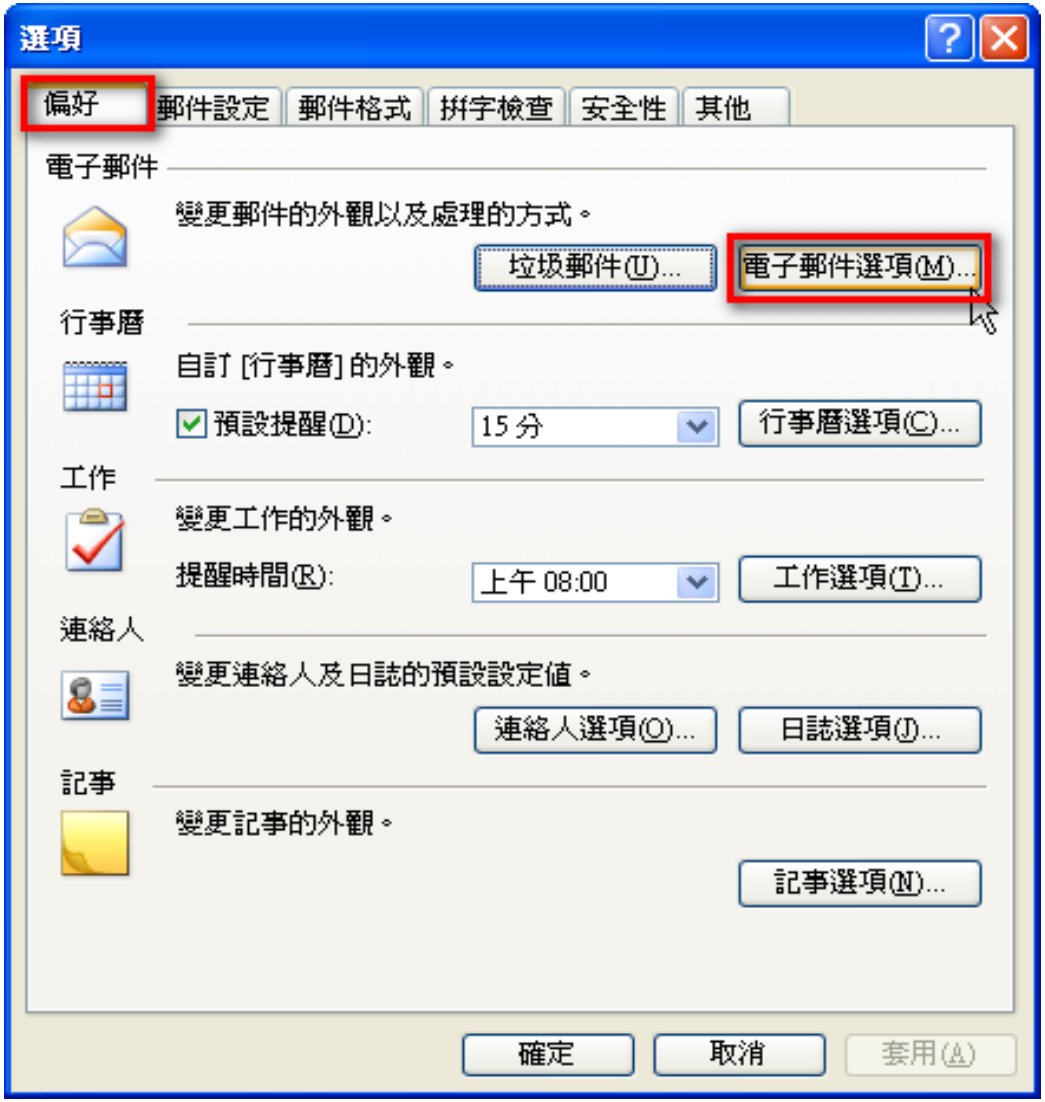
關閉讀取窗格、在純文字中讀取所有郵件



2. 以【純文字讀取所有標準郵件】(續)

Ootlook

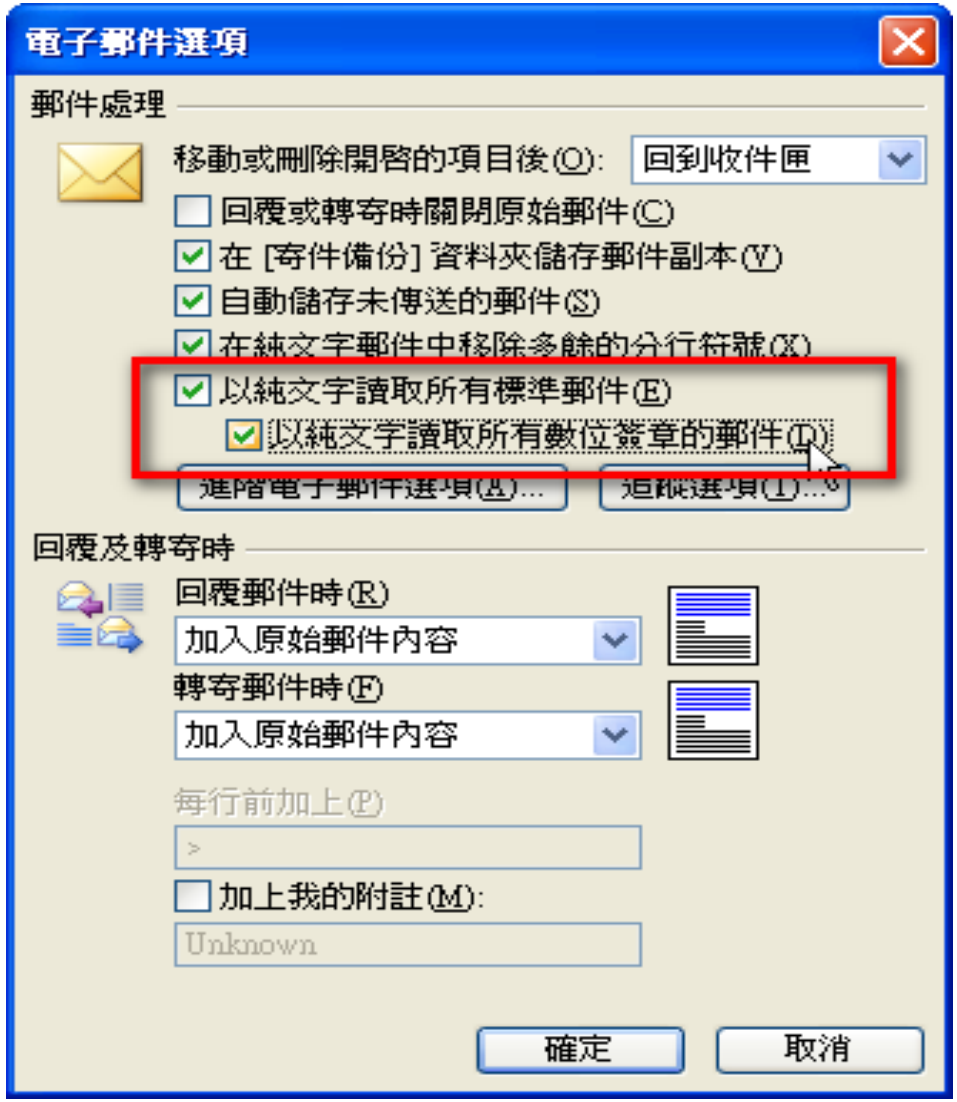
關閉讀取窗格、在純文字中讀取所有郵件



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