

防範惡意電子郵件社交工程

以下內容截取自政治大學防範惡意電子郵件社交工程教材



內容提要

教育部電子郵件社交工程演練說明

- 社交工程之攻擊目的
- 電子郵件社交工程手法介紹

Outlook Express 安全性設定

Outlook 安全性設定(2003,2007,2010)

電子郵件與社交工程 演練說明





為什麼要推動防範社交工程

政府推動服務資訊化公教人員接觸機密資訊設備機率高。

教育單位人員對於資訊安全的防護心態普遍較弱。

教育單位普遍課餘上網機率高於其他單位。

教育人員比較有愛心與正義感。

各校執行社交工程



教育部惡意電子郵件社交工程演練計畫

演練時程：

教育部第1次演練：4月下旬

教育部第2次演練：9月

教育部惡意電子郵件社交工程 演練計畫



各校提供全校行政同仁及約聘顧同仁e-mail 帳號給教育部加入演練。

教育部將本校提供名單參與4、9月份的實際演練。

教育預定於12月底前公告演練情形，選取績優單位、持續改善單位、加強改善單位及未依本執行方案辦理單位。



演練執行方式

以電子郵件寄送為主。

郵件主題分為政治、公務、健康養生、旅遊等類型，郵件內容包含連結網址或word附檔。

由技術小組以偽冒公務、個人或公司行號等名義發送惡意郵件給演練對象。

以前演練郵件列表舉例參考

編號	信件類別	信件標題
Letter 1	生活類	您的報稅內容正確嗎?申報綜所稅 7 大錯誤必罰!
Letter 2	美女類	!!台灣最美獸醫 連桃太郎都驚豔!!
Letter 3	健康類	炎炎夏日 防曬不能少!
Letter 4	知識類	地震時如何有效的保護自己
Letter 5	旅遊類	上海世博會 台灣館 天燈造型 驚艷全場
Letter 6	趣味類	我家有小車神~七歲展現停車特技的小女孩!
Letter 7	社會類	美《時代》百大人物 愛心婦陳樹菊入列
Letter 8	時事類	201 順向坡位置大分析
Letter 9	科技類	陽明團隊揭秘 基因 Cisd2 讓人長壽!
Letter 10	財經類	史上最難搶「鐵」飯碗 錄取率僅 1.25%



防範社交工程郵件重點

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!!!



何謂社交工程？

社交工程，英文為Social Engineering，是以影響力或說服力來欺騙他人以獲得有用的資訊，這是近年來造成企業或個人極大威脅和損失的駭客攻擊手法。

簡單來說「社交工程」，就是詐騙！透過電話、電子郵件等方式偽裝身份誘騙您上勾受騙...



社交工程目的?

詐財勒索。

取得個人或機關機密資料。

收集可用E-MAIL帳號當成進行郵件攻擊

收集YAHOO 或露天拍賣帳號進行網拍
詐騙。

植入病毒。



社交工程的威脅？

惡意人士不需要具備頂尖的電腦專業技術，只要企業員工對於防範詐騙沒有足夠的認知，就可以輕易地避過了企業的軟硬體安全防護，而騙取到各項帳號密碼、個人資料、財務資料或公司重要資料等資訊，對企業所造成的損害與威脅，完全不下於網路上的各種駭客攻擊。



社交工程的各種攻擊方法

電話詐騙。

電子郵件詐騙。

網路釣魚。

圖片內含惡意程式。

偽裝修補程式。

即時通 (MSN, Yahoo, Skype...)。



電子郵件詐騙

有下列症狀的同仁請注意了:

吃飽太閒

太有正義感

太有愛心

好奇寶寶

太容易被唬

很多人會開啟觀看和熱心地轉寄...

安!幫忙 幫忙找人!!!

檔案(F) 編輯(E) 檢視(V) 工具(T) 郵件(M) 說明(H)

回覆 全部回覆 轉寄 列印 刪除 上一個 下一個 通訊錄

寄件者: 我是...豆(=^ω^=)/
日期: 2008年9月22日 下午 11:22
收件者: [REDACTED]
主旨: 安!幫忙 幫忙找人!!!
附加檔案: Pic00325.zip (272 KB)

安 安!
請幫忙轉寄: 不會花您太多時間, 拜託囉!!
我的愛女小彤五歲被強行抱走!!!
警方查了幾天都沒線索 只好透過網路管道請大家幫忙了
夾帶的是相片是被抱走的前幾天照的 那天剛好是穿這身衣服
有線索的請 聯絡 0921811 [REDACTED] 田為

Pic00325.zip - WinRAR (evaluation copy)

File Commands Tools Favorites Options Help

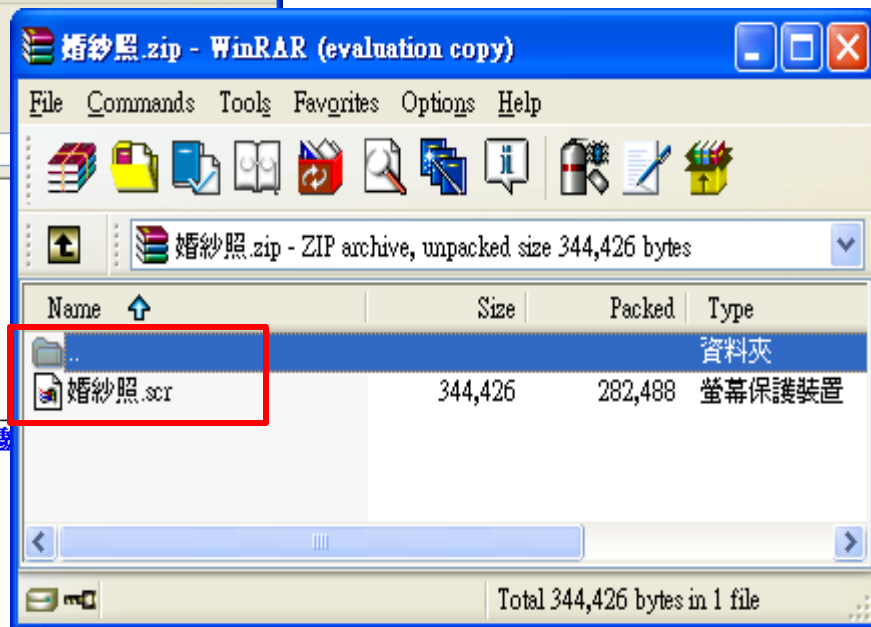
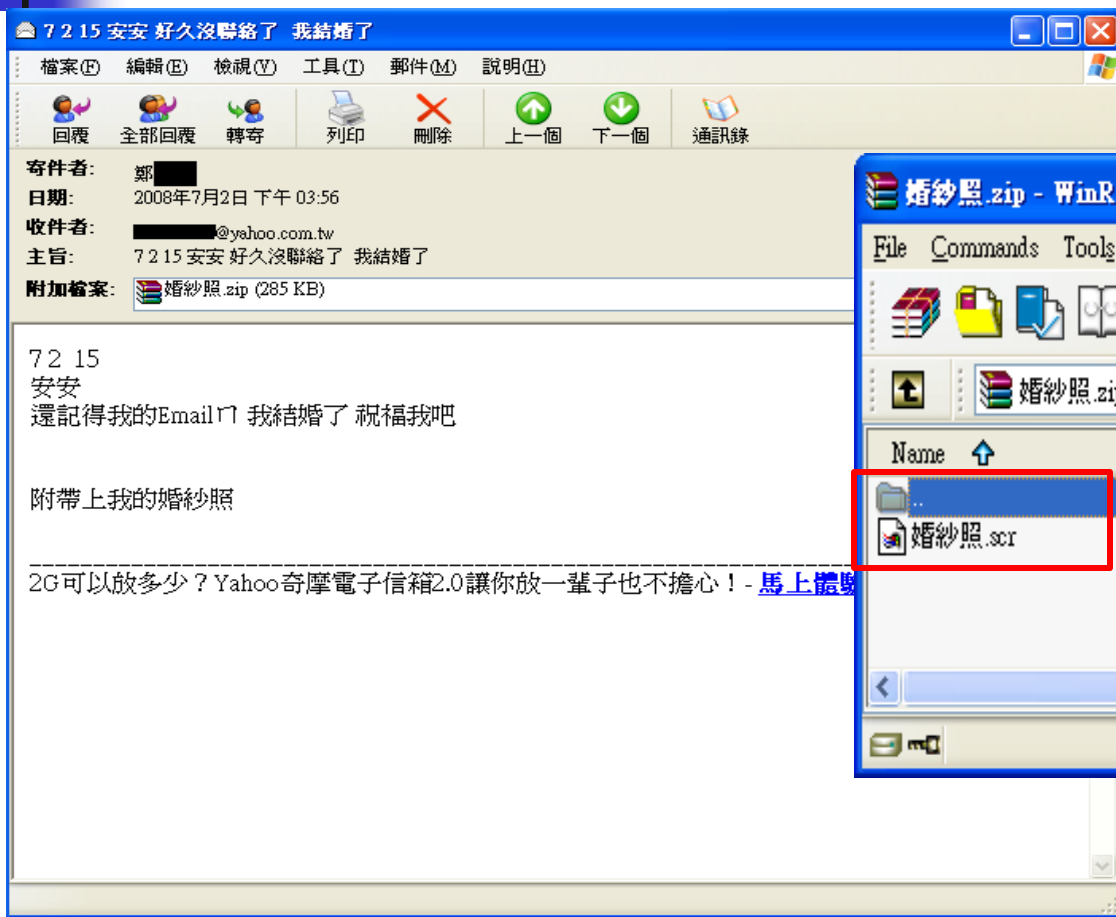
Add Extract To Test View Delete Find Wizard Info

Pic00325.zip - ZIP archive, unpacked size 332,949 bytes

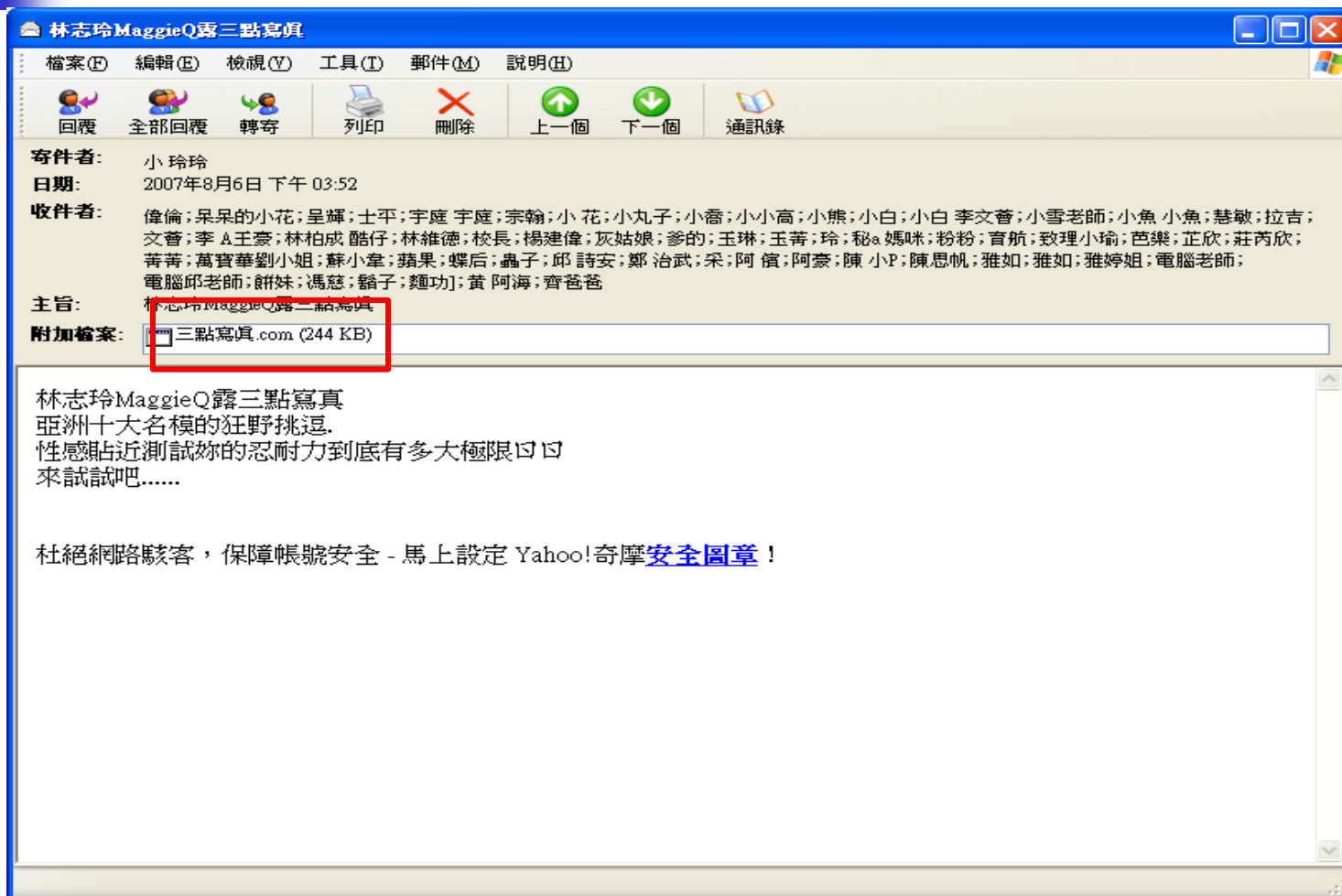
Name	Size	Packed	Type
..			資料夾
彤彤.scr	332,949	270,217	螢幕保護裝置

Total 332,949 bytes in 1 file

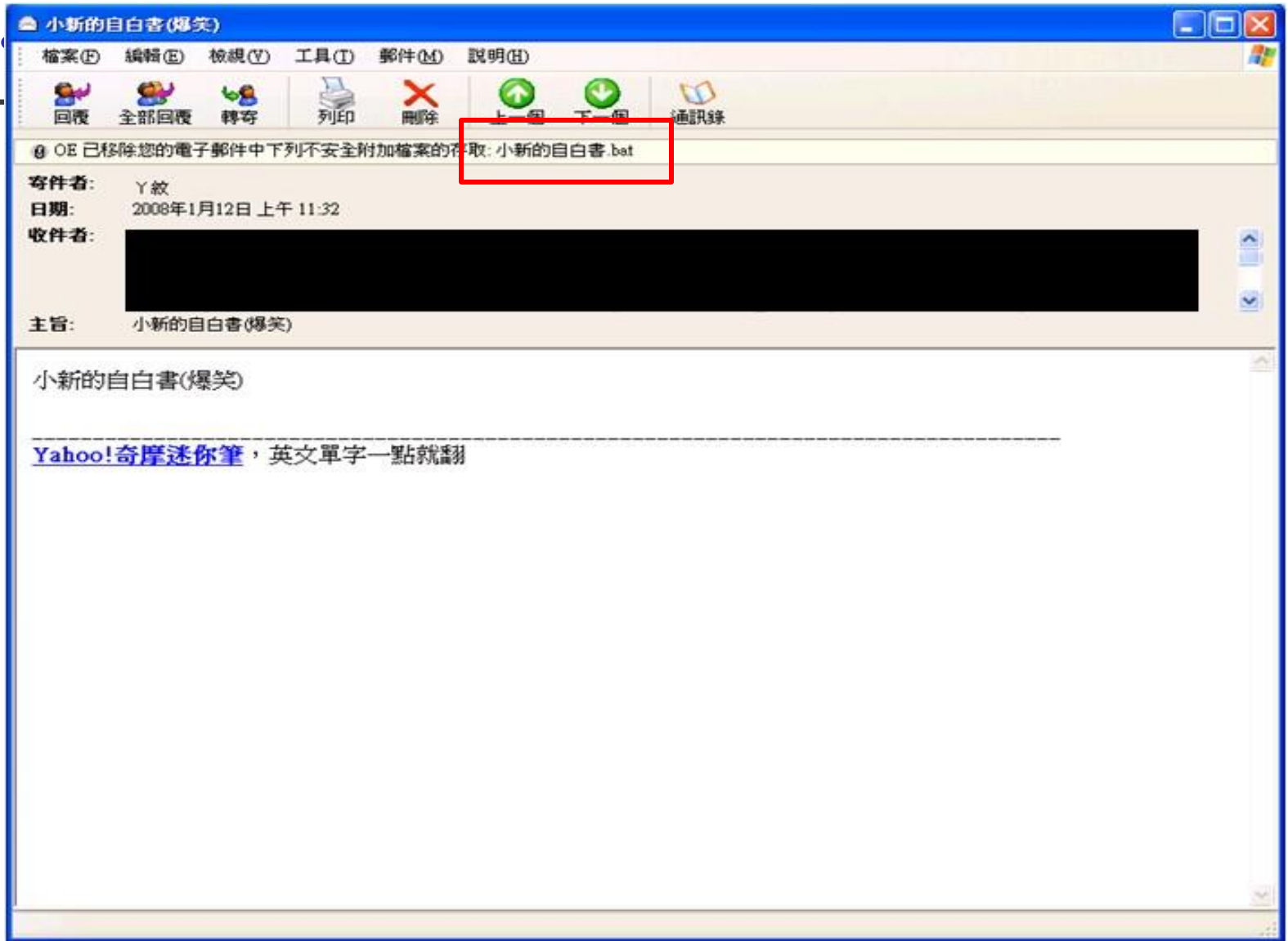
朋友說他結婚了..(but 他結過婚了啊)



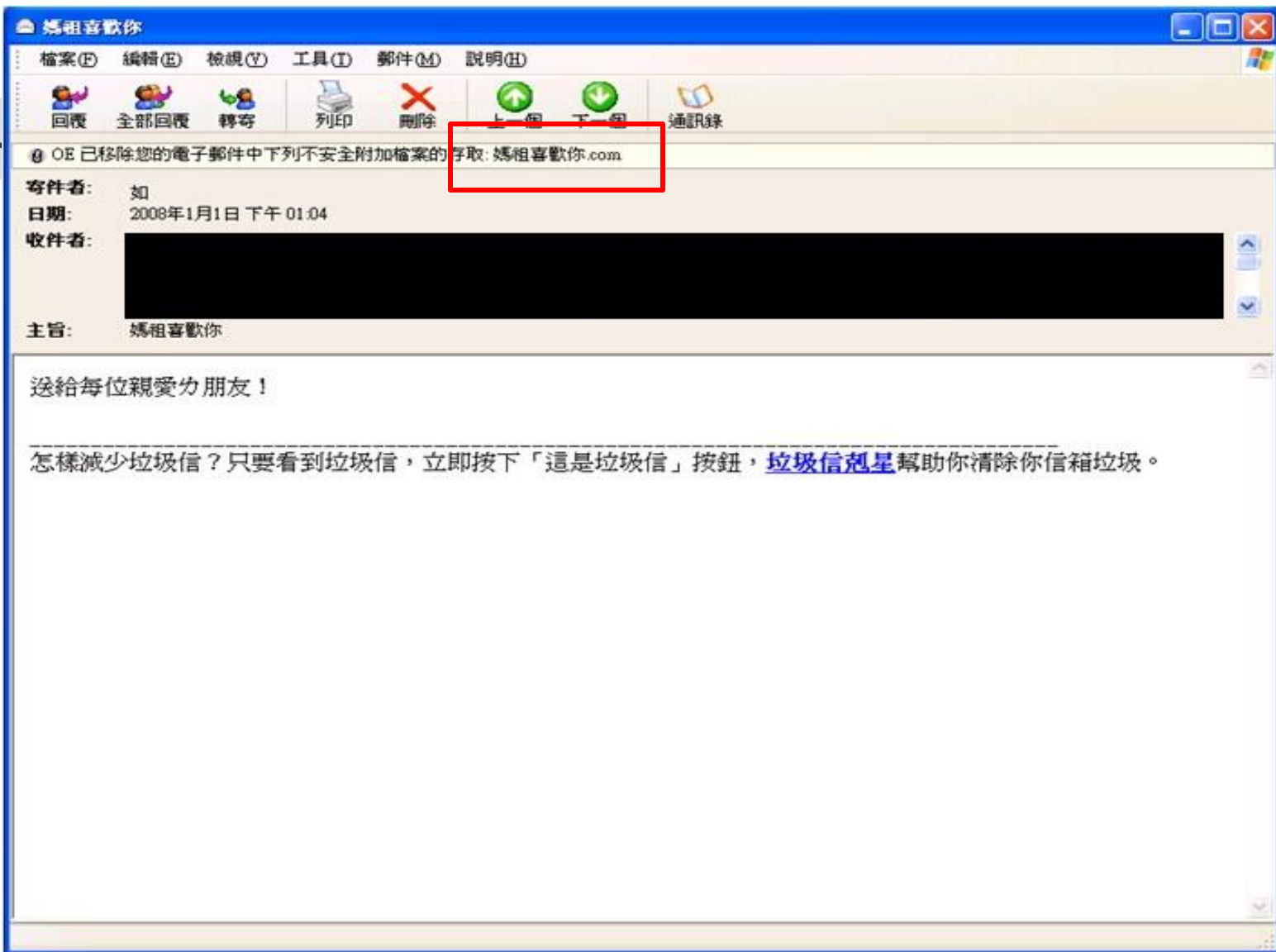
色情郵件標題



附檔名bat也是惡意程式執行檔



內容看似一般網路轉寄郵件...



惡意程式郵件也會將檔案隱藏在.zip檔...



安安眼看新年馬上就要到來了.祝你在新的一年里快快樂樂.心想事成.萬事如意先通過E-mail給你送上新年賀卡再拜個早年~~

免費下載迷





各種惡意程式郵件範例

潘金蓮與西門慶
春節禮物 同學
會相片 **yahoo!**
回復郵件
茱麗亞娜視窗第十三版
2008年十二生肖運程
小時候ㄉ照片 生日照
片
視窗化工具 投資
明細 極品空姐 我
換信箱了囉 新號
碼 媽祖喜歡你 破
解女王版 **ATM**領
錢時要注意 超口
愛
謎底

這運動會否太累
破解女王版 陳冠希和
鍾欣桐床上照 從前的
照片 星語專用視窗化
昨晚夢到你ㄉ
張柏芝 我女
兒相片 煎餃
算命 籃球寶
貝 美女裸照
聚會照片 魔
獸開圖程式
看看你和我誰智商高
網路姊妹花 私人相
片 請問都是甚麼人
太妙ㄉ一定要看

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



網路釣魚

偽裝知名企業或機關單位寄發的電子郵件，通知收件人必須重新驗證密碼或登入某網址輸入個人資料等，這種詐騙稱為網路釣魚。

網路釣魚就是一種典型的社交工程攻擊。


偽「我的拍賣賣場」陷阱...

新莊新泰路套房/雅房分租,近棒球場,板橋,泰山,五股工業區,輔大,ikea般的生活環境Yahoo!奇摩拍賣 - Microsoft Internet Explorer

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

← 上一頁 → 搜尋 ★ 我的最愛


網址(D) <http://tw.f5.page.bid.yahoo.com/tw/auction/e21822597> 移至 連結 >>



用途	一般住宅	行政區域	板橋
使用坪數	10坪以下	房型	套房
屋齡	新成屋	格局	一房

近捷運	無	近學校	無	近公園	無	近百貨公司	無
電梯	無	電視	無	陽台	無	附家具	無
洗衣機	無	冰箱	無	冷氣空調	無	車位	無

請用滑鼠點擊下邊(前往我的拍賣賣場)

 點擊這黃色長長的圖標就可以直接到我另一個賣場~還有很多一元起標商品全面結束營業大出清喔~保證買到賺到~

雅虎國際資訊 © 版權所有 2007 Yahoo! Taiwan Inc. All Rights Reserved. [服務條款](#) [隱私權政策](#) [政策與規則](#) [交易安全](#)

<http://yahoooo.c65.163ns.com/data/bak/> 網際網路

開始 新莊新泰路套房/雅... 4 bmp - 小畫家 下午 10:12

你確定你真的是在Yahoo購物?

登入 - Yahoo!奇摩 - Microsoft Internet Explorer

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

← 上一頁 → 搜索 我的最愛

網址(D) <http://yahooo.c65.163ns.com/data/bak/> 連結 >>

YAHOO!
奇摩

歡迎使用Yahoo奇摩
享受 Yahoo!奇摩 的超讚功能

- 使用免費的電子信箱及即時通訊。
- 使用反間諜軟體及網頁跳窗阻擋，保護您的電腦安全。
- 了解您所在地區的天氣及目前溫度。
- 隨時更新！最新的音樂、娛樂、體育消息。

登入
Yahoo!奇摩

啟用安全章 ▶ 啟用

帳號:

密碼:

記住我的帳號密碼(說明)

登入

[忘記密碼](#) | [登入說明](#)

還沒有Yahoo!奇摩帳號?
註冊帳號免費又容易

[立即註冊](#)

雅虎國際資訊 版權所有 © Yahoo! Taiwan Inc. All Rights Reserved. | [服務條款](#)
請注意：我們會收集您在Yahoo!奇摩網站的個人資訊
想知道我們怎麼使用您的相關資料，請參考 [隱私權政策](#)。
a26150606

完成

開始 新莊新泰路套房/雅... 2.bmp - 小畫家 登入 - Yahoo!奇摩 - ... 網際網路 下午 10:13

用APNIC網頁的查詢結果...

Query the APNIC Whois Database - Microsoft Internet Explorer

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

← 上一頁 → 搜尋 ☆ 我的最愛

網址(D) http://wq.apnic.net/apnic-bin/whois.pl 移至 連結 >>

APNIC Asia Pacific Network Information Centre

Info & FAQ | Resource services | Training | Meetings | Membership | Documents | Whois & Search | Internet community

You're here: Home » Database Quick Links

Query the APNIC Whois Database

Need help?

- General search help
- Help tracking spam and hacking
- To assist you with debugging problems, this whois query was received from IP Address []. Your web client may be behind a web proxy.

```
% [whois.apnic.net node-1]
% Whois data copyright terms http://www.apnic.net/db/dbcopyright.html

inetnum:      221.224.0.0 - 221.231.255.255
netname:      CHINANET-JS
descr:        CHINANET jiangsu province network
descr:        China Telecom
descr:        A12, Xin-Jie-Kou-Wai Street
descr:        Beijing 100088
country:      CN
admin-c:      CH93-AP
tech-c:       CJ186-AP
mnt-by:       APNIC-HM
mnt-lower:    MAINT-CHINANET-JS
mnt-routes:   MAINT-CHINANET-JS
remarks:      This object can only modify by APNIC hostmaster
```

中國電信集團

開始 新莊社區電... 14.bmp - 小畫... TWNIC-財團... CAWINDOWS... Untitled Docu... Query the APN... 下午 11:03

網路釣魚Phishing



利用偽造的網頁作為誘餌，詐騙使用者洩漏如帳戶密碼等個人機密資料。

釣魚網頁畫面與官方網站相同，但其實這個網址並非官方網站。

以相似的字元來偽裝網址，例如：
以數字的0來替換英文的O
以數字的1來替換英文的l。



網頁中的惡意程式執行檔連結

Yahoo! 奇摩家族 - Microsoft Internet Explorer

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

← 上一頁 → 刷新 主页 搜尋 我的最愛

網址 http://tw.club.yahoo.com/clubs/Spice_Girls/ 移至 連結

YAHOO!
奇摩
CLUB 家族


Yahoo! 奇摩家族

我的家族
[家族首頁](#)
[公佈欄](#)
[討論區](#)
[投票所](#)
[寫真集](#)
[酷連結](#)
[檔案庫](#)
[精華區](#)
[簽名簿](#)
[資訊區](#)
[管理區](#)
[登入](#)

Yahoo! 奇摩

COOL	大學生為學費賣身 大學生為學費賣身	★ " 孤單 a 皮蛋 " ? (s29717161) 留言給我!	2006/03/24 17:06:30
COOL	皮耶羅蜜月新婚愛妻裸	就是愛睡覺~夕~ (e0960151267) 留言給我!	2006/03/16 18:22:55
COOL	〈玉女心經〉圖文 (玉女心經>圖文並茂版)	★ " 孤單 a 皮蛋 " ? (s29717161) 留言給我!	2006/02/18 14:59:25
COOL	天啊!曾s上月收入70萬 她就是,找對行業,用對方法...短短兩年內,收入暴增..	gtjf07231153 (gtjf07231153) 留言給我!	2006/02/10 15:02:55
COOL	性愛手記 性愛手記: 將做愛進	振男 (k20702g) 傳訊給我!	2006/01/31 06:48:18
COOL	好淫蕩的叫聲 好淫蕩的叫聲	振男 (k20702g) 傳訊給我!	2006/01/27 21:49:28
COOL	2005全年最佳化妝舞會 好多好Q的造型哦,下次有化妝舞會我就要模仿一個	小黑龍 (a29212689) 留言給我!	2006/01/19 11:16:44
COOL	擺脫上班族的宿命1654 失業轉業創業加盟第一首業在家工作網路上班族165424	fgh12171606 (fgh12171606) 留言給我!	2006/01/15 16:52:11
COOL	*窮人知道保位子;富?/a> ..*窮人知道保位子;富人知道換位置.過去是經營餐廳	kkk131003645 (kkk131003645) 留言給我!	2006/01/13 17:34:13
COOL	林書融自拍性感照,難	" 誰來愛 " (s29717161) 留言給我!	2006/01/04 17:34:13

Microsoft Internet Explorer

 您將前往的網頁: <http://www.cn-call.com/seelove.exe> 可能含有病毒, 請按「確定」取消連結。

[確定](#)

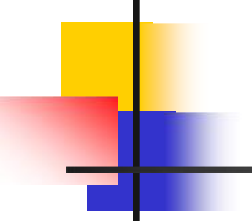
倉 半



瀏覽網頁中獎率**10%**

2007年5月的Google的研究報告指出，在全球450萬個網頁進行深入分析後，發現十分之一的網頁都具發佈「自動下載程式」。

即網際網路上平均有十分之一的網頁含有惡意程式或疑似惡意程式！



這些惡意程式，可以在使用者不知情的情況下自動安裝木馬程式、間諜軟體和其他病毒程式。

惡意程式散播方式通常利用情色、聳動、趣味等標題文字吸引使用者點選，點選後會直接下載安裝惡意程式。

防範網站惡意程式的正確認知

- 1、惡意程式陷阱皆是利用使用者好奇心誘騙開啟，因此千萬不要因為好奇心肆意開啟連結。
- 2、當點選連結後出現「您將前往的網頁可能含有惡意程式」等類似訊息文字，代表該連結為網站外連結，並可_實能為一惡意程式執行檔，應立即取消連結的執行。
- 3、留意圖示連結、文字連結等實際的網址URL，實際連結的網址可能和畫面上顯示的網址不同。可將滑鼠游標停留在圖示連結、文字連結上，由畫面左下方顯示的實際連結網址，確認畫面顯示的是否為偽連結網址。

畫面網址與實際網址URL不同

親愛的電子郵件使用者 - 郵件 (純文字)

刪除 回覆 全部回覆 轉寄 會議 IM 其他

收件匣 - svater... 規則 OneNote 標示為未讀取 簡繁轉簡 繁簡轉繁 中文字體轉換

轉寄給經理 小組電子郵件 移動 動作 待處理 分類 中文繁簡轉換

a中 尋找 相關的 顯示比例 新增至 Evernote

翻譯 顯示比例

此郵件中多餘的分行符號已經移除。

寄件者: 台灣電子郵件管理員中心 <tw@chgsh.chc.edu.tw> 寄件日期: 2015/11/9 (週一) 下午 03:38

收件者: undisclosed-recipients:

副本:

主旨: 親愛的電子郵件使用者

**顯示為: 彰化的教育部 mail 信箱
收件者卻沒有註名是誰
主旨也只有寫: 親愛的電子郵件使用者**

親愛的電子郵件使用者

您的郵箱已超過其存儲限制由電子郵件管理員設置, 您將無法接收新郵件, 直到你重新驗證 它。

點擊這裡: <https://formcrafts.com/a/15618?preview=true> 信箱容量超過, 需點下列網址驗證, 但該網址卻是國外網站

在其他的重新驗證您的電子郵件帳戶作為目前使用的帳戶。

2015 Copyright By 台灣電子郵件管理員中心

--

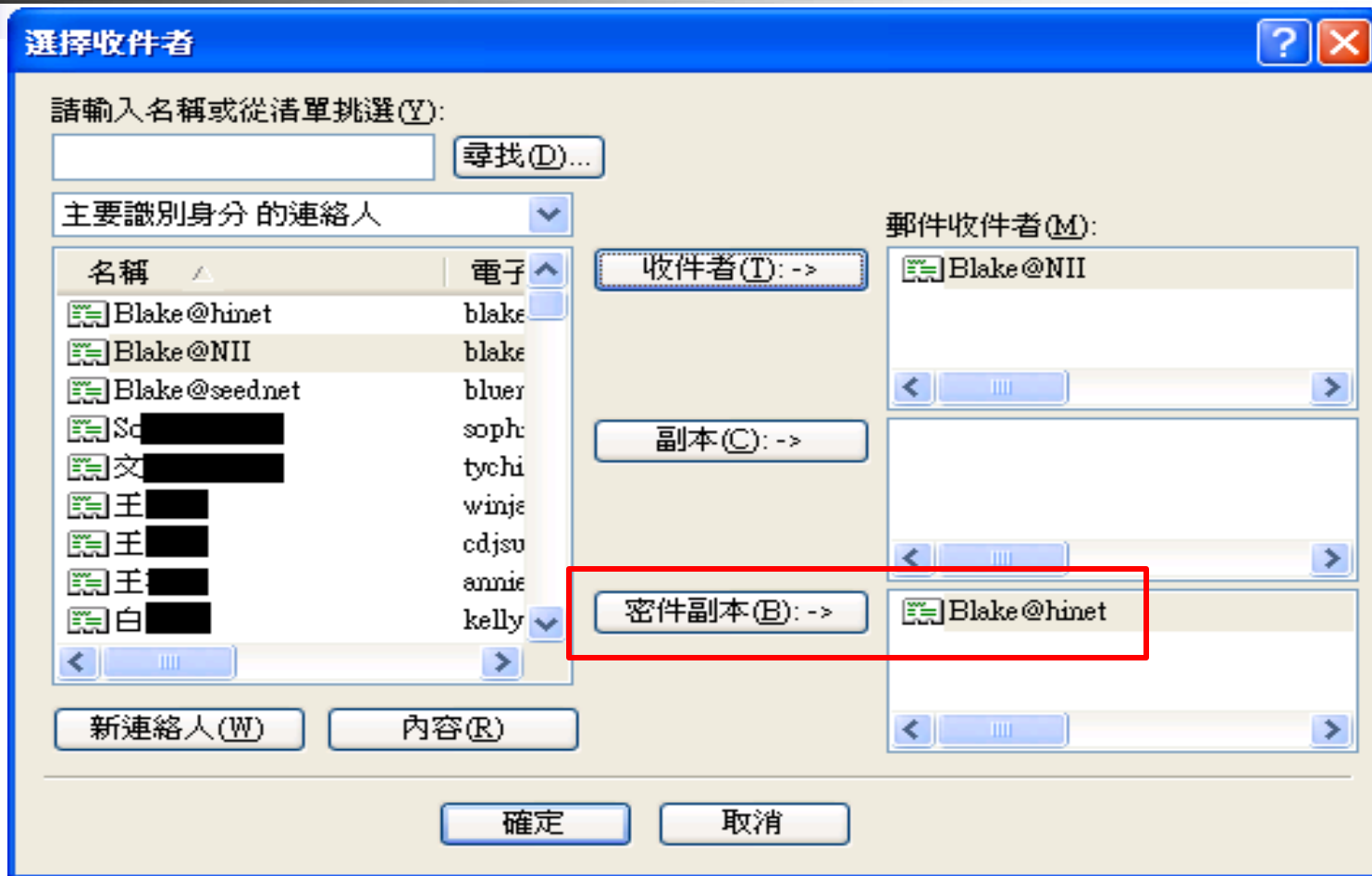
This message has been scanned for viruses and dangerous content by MailScanner, and is believed to be clean.

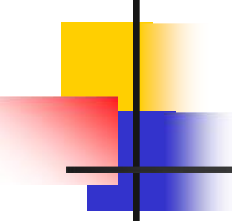
此信為釣魚信件, 是為了騙取帳號密碼, 竊取入侵電腦。

請勿點選。

台灣電子郵件管理員中心

使用密件副本功能保護收件人 郵件信箱資料





面對詐騙攻擊與 電子郵件使用安全 應有的防範認知

社交工程電子郵件的陷阱

緊急的問題!!希望高手可以幫幫忙~

檔案(F) 編輯(E) 檢視(V) 工具(T) 郵件(M)

回覆 全部回覆 轉寄 列印 刪除

寄件者: Lee Ian
日期: 2008年3月10日 下午 04:44
收件者:

主旨: 緊急的問題!!希望高手可以幫幫忙~

鎖了某些圖片以協助防止寄件者辨識您的電腦,請按這裡來下載圖片。

幫幫忙啦! 我想買隻索尼愛立信行動電話, W810和W610這兩款都不錯!
可是買w610它的記憶卡是m2刀.
w810的記憶卡是ms pro duo.m2插上轉接卡就是ms pro duo所以實用性較高.
而w610的記憶卡塞是硬塑膠不像w810是象皮的<=<容易變形.不知道買什麼好了!
<http://www.horvm.com/index.asp?w810-w610i.jpg>
幫我看看拿個主意可以嗎? 一定要跟我說啦!

林志玲MaggieQ露三點寫真

檔案(F) 編輯(E) 檢視(V) 工具(T) 郵件(M) 說明(S)

回覆 全部回覆 轉寄 列印 刪除

寄件者: 小玲玲
日期: 2007年8月6日 下午 03:52
收件者: 偉倫; 呆呆的小花; 呈輝; 士平; 宇庭 宇庭; 宗翰 文睿; 李 A王豪; 林柏成 酷仔; 林維德; 校長; 楊 菁菁; 萬寶華劉小姐; 蘇小章; 蘋果; 蝶后; 蟲子; 電腦邱老師; 餅妹; 馮慈; 騷子; 麵功; 黃 阿海; 林志玲MaggieQ露三點寫真

主旨: 林志玲MaggieQ露三點寫真

附加檔案: 三點寫真.com (244 KB)

林志玲MaggieQ露三點寫真
亞洲十大名模的狂野挑逗.
性感貼近測試妳的忍耐力到底有多大極限! 口
來談話吧.....

[魔兽]&血洗部落@#

檔案(F) 編輯(E) 檢視(V) 工具(T) 郵件(M) 說明(S)

回覆 全部回覆 轉寄 列印 刪除 上一個 下一個 通訊錄

寄件者: 小瑛
日期: 2007年12月31日 下午 03:02
收件者:

主旨: [魔兽]&血洗部落@#

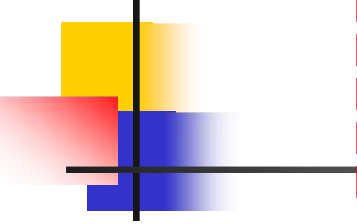
美版滿屏都是法師超強<http://tw.club.yahoo.com/clubs/zmmf/61212m.jpg>

怎樣減少垃圾信? 只要看到垃圾信, 立即按下「這是垃圾信」按鈕, [垃圾信剋星](#)幫助你清除你信箱垃圾。

惡意網頁連結

惡意程式附檔

遠端圖片下載



開啟郵件... 點
擊郵件中的連結...
開啟郵件中的附檔...

您可能已經明白了 不要點擊連結與隨意
開啟這些附檔， 但您可能還是疑惑 為什
麼開啟郵件也算違規？



為什麼要求不能「開啟郵件」？

您可能覺得只要不開郵件附件和不點擊連結，就不會中招...

- 但其實有些惡意程式是利用ActiveX功能來執行的。
- 由於您的電子郵件可能是HTML格式，而HTML可以撰寫ActiveX，所以您只要瀏覽電子郵件，就觸發ActiveX執行！



啟用預覽視窗等同「開啟郵件」

利用IE漏洞，不開啟附檔也會中毒

2004年3月，Beagle.O電腦病毒使用IE漏洞攻擊，使用者在Outlook / Outlook Express環境下啟用信件預覽功能，信件中的script就會啟動，連結到惡意程式網站下載病毒程式

Gmail 中的 收件匣 - Microsoft Outlook

檔案(F) 編輯(E) 檢視(V) 到(G) 工具(T) 動作(A) 說明(H) 鍵入需要解答的問題

新增(N) X 回覆(R) 全部回覆(L) 轉寄(W) 傳送/接收(C) 搜尋通訊錄

郵件 << 收件匣 搜尋收件匣

我的最愛資料夾 >>

- 收件匣
- 未讀取的郵件
- 寄件備份

郵件資料夾 >>

- 所有郵件項目
- 收件匣
- 垃圾郵件
- 保留郵件
- 待辦事項

郵件

行事曆

連絡人

工作

1826 個項目

收件匣

按一下這裡啟用「立即搜尋」

寄件者	主旨	收到日期	大小
陳維民	RE: 種子學校4月份到點訪輔與教育訓練...	2009/4/10 (星期...	140...
許雅雯(...)	種子學校4月份到點訪輔與教育訓練時間...	2009/4/10 (星期...	58 KB
許雅雯(...)	【中興大學】展開之空白「威脅及弱點...	2009/4/10 (星期...	2 MB
Sharon ...	[提醒] 每雙週交付Time Sheet	2009/4/10 (星期...	169...

[提醒] 每雙週交付Time Sheet

Sharon [REDACTED]@nii.org.tw

寄件日期: 2009/4/10 (星期五) 下午 06:10

收件者: [REDACTED]@nii.org.tw

預覽視窗(讀取窗格)

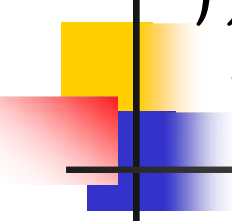
訊息 | timesheet(Mar)_0330.xls (121 KB)

Dear all,

又雙週囉！請大家交付新版 IRM Time Sheet (請詳附件工作表一：每週工作排程表)。

待辦事項列 (星...)

今天: 6 個工作



所以除了不要點擊連結與隨意開啟附檔外，您應該曉得的安全防護還包括：

關閉自動下載圖片
關閉預覽視窗

不要自動回覆讀信回條

考慮設定以純文字格式讀取郵件

社交工程的定義

利用**人性弱點**、**人際交往**或**互動特性**所發展出來的一種攻擊方法。

早期社交工程是使用「電話」或其他「非網路」方式來達到目的。

目前社交工程大都是利用「**電子郵件**」或「**網頁瀏覽**」來進行攻擊。

運用「**廣告心理學**」，透過文案、圖案或照片等諸多媒體，藉由電子郵件寄達消費者（受害者），誘使受害者「**衝動反射**」開啟郵件，達到入侵之目的地。



假冒『寄件者』的身分

✓ 業務相關

- ▶ 上級單位
- ▶ 主官管
- ▶ 平行單位

✓ 親朋好友

✓ 資安相關

- ▶ 資訊中心
- ▶ 技服中心

這封郵件以高重要性傳送。

寄件者: 國家資通安全會報技術服務中心 [ncert@icst.org.tw]
收件者: ncert@icst.org.tw
副本:
主旨: [緊急事件警訊] 國家資通安全會報技術服務中心 (事件編號: ICST-ALT-2009-0001)
簽名者: ncert@icst.org.tw

寄件日期: 2009/5/4 (星期一) 下午 06:18

國家資通安全會報 技術服務中心
緊急事件警訊

發布編號	ICST-ALT-2009-0001	發布時間	2009/05/04 18:18:10
事件主旨	請加強防範駭客假冒國家資通安全會報技術服務中心發送之惡意電子郵件		
事件描述	國家資通安全會報技術服務中心近日發現有駭客假冒技術服務中心名義，發送夾帶惡意程式附檔之信件，當使用者開啓郵件附檔後，即會被植入後門程式。 目前已發現的信件特徵如下，若有收到類似不明信件，請勿開啓： 寄件者：ncert@icst.org.tw(無數位簽章) 主旨：[資安訊息警訊] 國家資通安全會報技術服務中心 (事件編號：ICS T-ANA-2009-0003) 附件名稱：98eventlist.pdf		
	建議所有相關單位： 1. 請阻擋並監控以下中繼站： 203.123.217.240:TCP:80		

資安「社交工程」手法 (1/2)

- ✓ 取得信任，衝動點選！
- ▶ 假冒「親戚、朋友、長官」
- 魚叉式目標
- ▶ 假冒「利害關係人」
- 銀行、交易網站、社群網站、嗜好網站
- ▶ 假冒「微軟 OS、病毒軟體」更新
- ▶ 使用與業務相關「郵件主題」與「附件」
- ▶ 令人「感興趣」，容易「感性衝動」的郵件主題與內容。

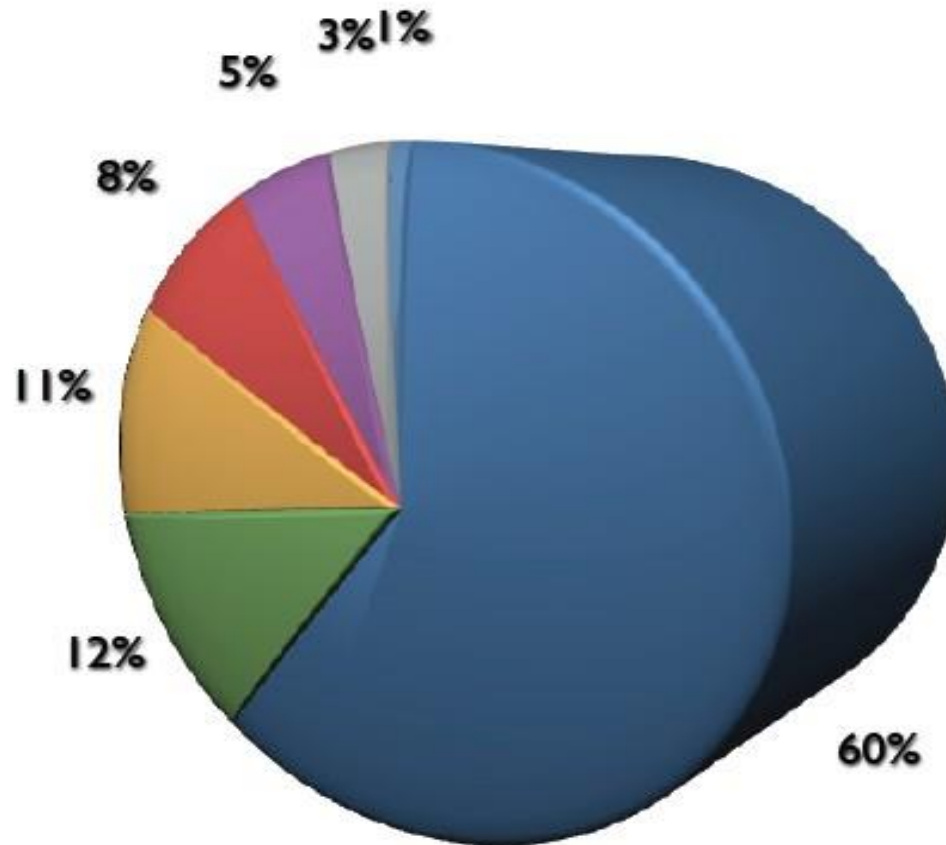
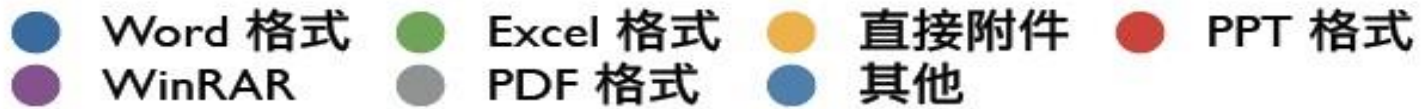


資安「社交工程」手法 (2/2)

- ✓ 含有「惡意程式（木馬、後門）」的附件或連結
 - 副檔名清單
 - Java Script/ i-Frame 等網頁自動執行語法
- ✓ 利用「應用程式」之弱點
 - MS 作業系統
 - Adobe (PDF)
 - Flash Player
- (包括「零時差」攻擊)
 - IE 瀏覽器
 - MS Office

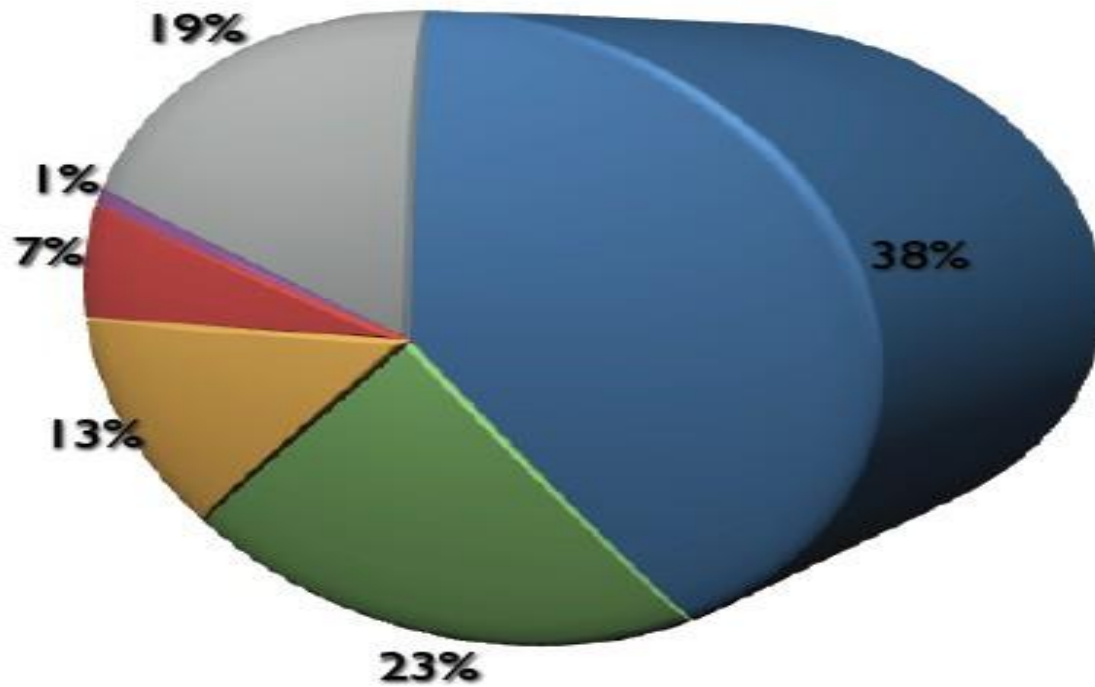


惡意郵件「軟體弱點」運用比例



惡意郵件「主旨內容」分析比例

- 政治新聞
- 生活議題
- 假冒公務與個人名義
- 情色八卦
- 公務通告
- 其他類別





社交工程的受害衝擊

✓ 個人權益

- ▶ 個資外洩
- 詐騙恐嚇
- ▶ 帳密被盜
- 財產損失
- 人頭帳號
- ▶ 幫凶刑責
- ▶ 考績罰則

✓ 單位權益

- ▶ 機敏外洩
- ▶ 聲譽受損
- 社交工程演練排名
- ▶ 訴訟罰款
- 個人資料保護法
- 國家賠償
- 舉證責任在「被告」

發送信件樣本01



發送信件樣本02

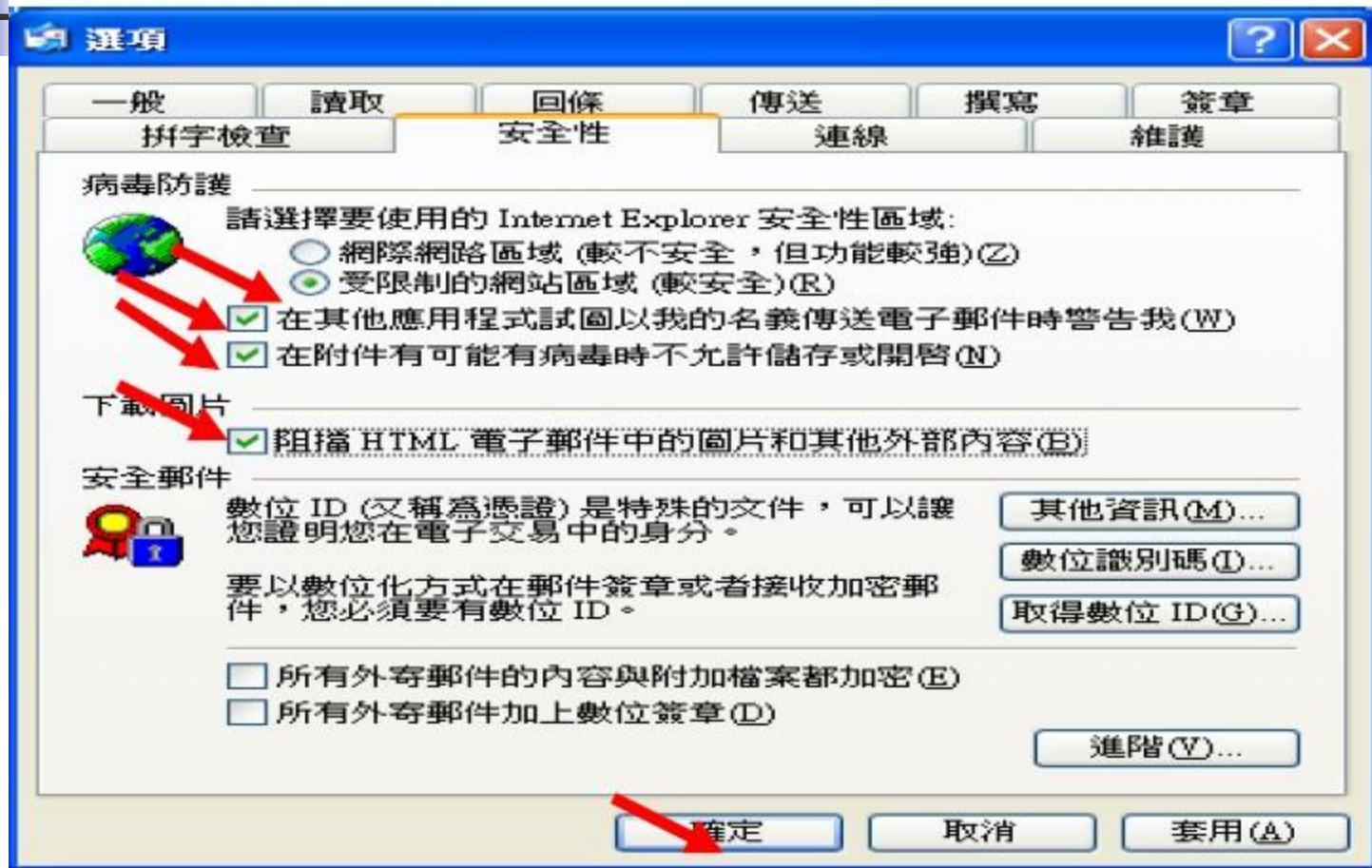
The collage features several browser windows:

- 八卦 (Gossip):** A window showing a news article with a yellow callout box containing the characters "八卦".
- 醫藥 (Medicine):** A window displaying a medical article about UVB and skin protection, with a yellow callout box containing the characters "醫藥".
- 娛樂 (Entertainment):** A window showing a news article about the 2009 Taipei International Flower and Garden Show, with a yellow callout box containing the characters "娛樂".
- 情色 (Erotic):** A window displaying a magazine-style page with photos of women and the characters "情色" in a yellow callout box.

Other visible text includes "風光收入", "無法抗拒的誘惑天使美艷", "2009台北國際花卉展開始囉!", "蛋糕房 金姦俏女郎", and "溫泉".

一、Outlook Express 安全性設定(XP 版)：

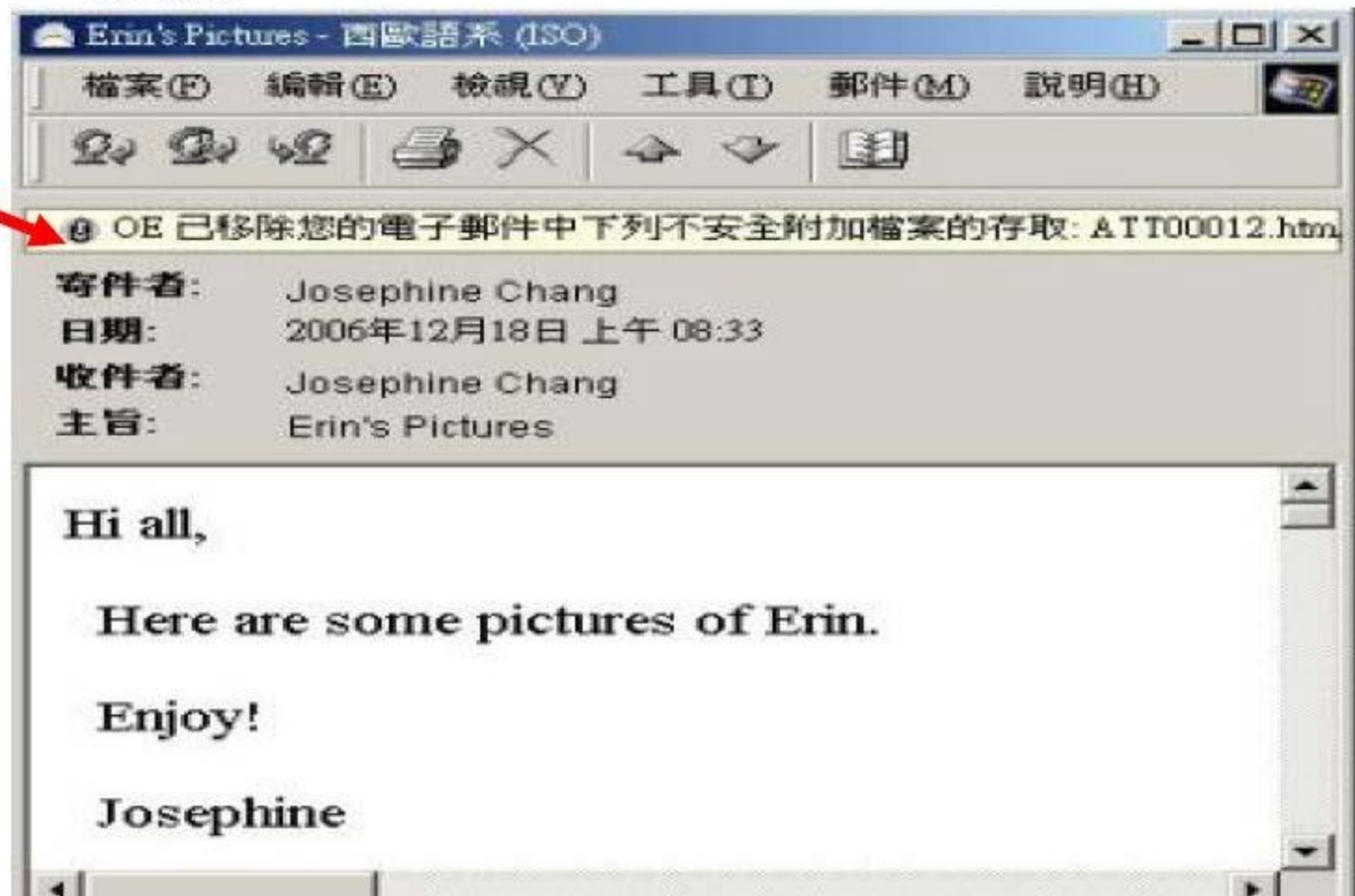
步驟1. Outlook Express 點選 工具 -- 選項 - 安全性 出現下面畫面並依下列箭頭指示之勾選設定，並按確定鈕。



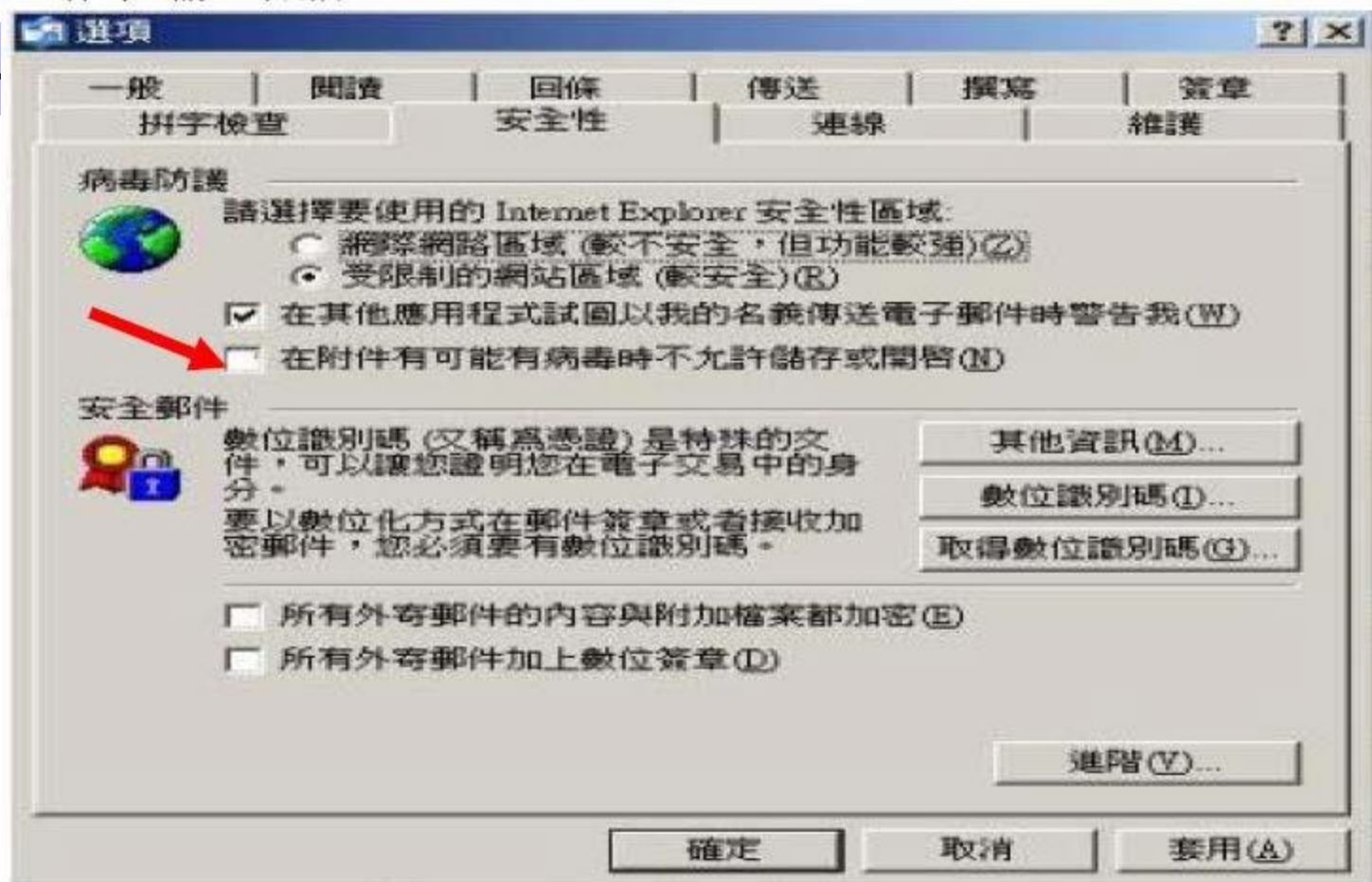
步驟2. 未來開信會阻擋對外連線下載圖片(如下畫面), 若為正常信件, 只要按下箭頭之地方, 即可恢復正常之畫面, 若為可疑信件時, 請立即刪除。



步驟3. 如上圖點選在附件有可能有病毒時不允許儲存或開啓即可封鎖不安全的附加檔案

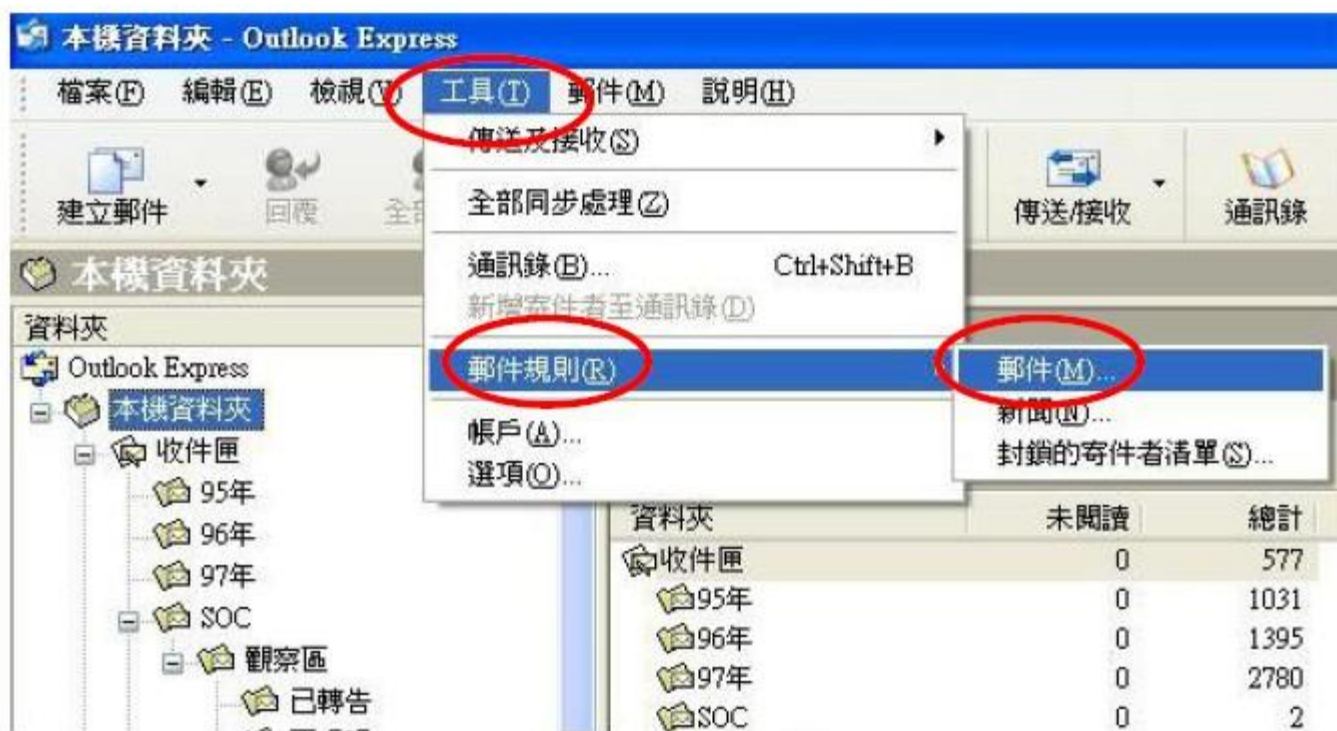


步驟4. 若為正常信件，只要按下箭頭之地方，即可正常存取附檔，若為可疑信件時，請立即刪除。



二、設定郵件規則，將常往來、熟悉的人員設定分類，較容易防範來路不明或詐騙郵件

步驟1. 點選「工具」→「郵件規則」→「郵件」



步驟2. 於「郵件規則」頁籤中，點選「新增」



步驟3. 選擇相關條件並指定寄件者之信件移至指定資料夾，點選「確

定」完成新增

新郵件規則

請先選擇 [條件] 和 [動作]，然後在 [描述] 中指定值。

1. 選擇規則的條件 (C):

- 寄件者包含人員
- 主旨包含特定的文字
- 郵件本文包含特定的文字
- 收件者包含人員

2. 選擇規則的動作 (A):

- 移至指定的資料夾
- 複製到指定的資料夾
- 刪除
- 轉寄郵件給人員

3. 規則描述 (按加底線的值即可進行編輯) (D):

在郵件寄到之後套用此規則

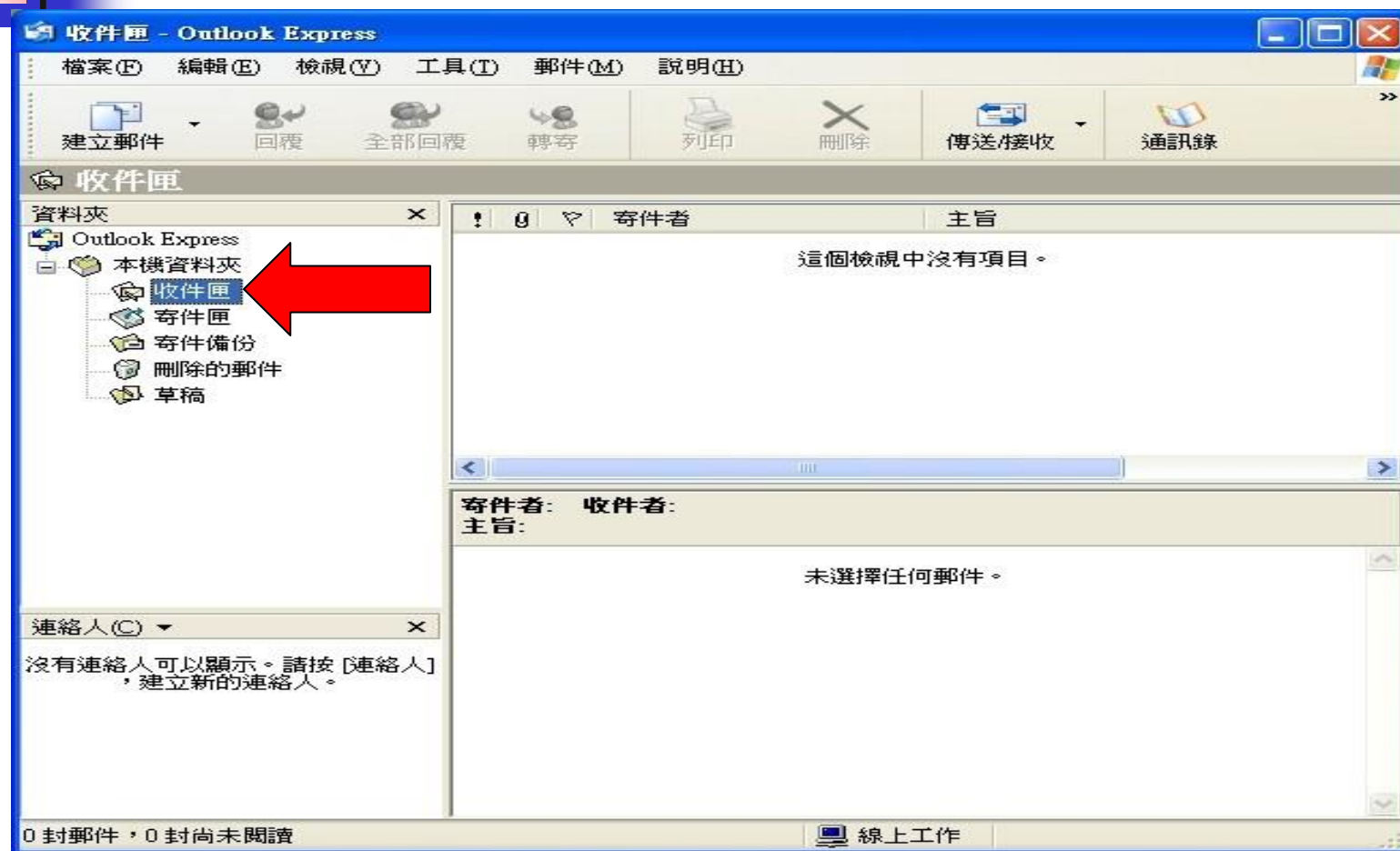
4. 規則的名稱 (N):

新的郵件規則 #5

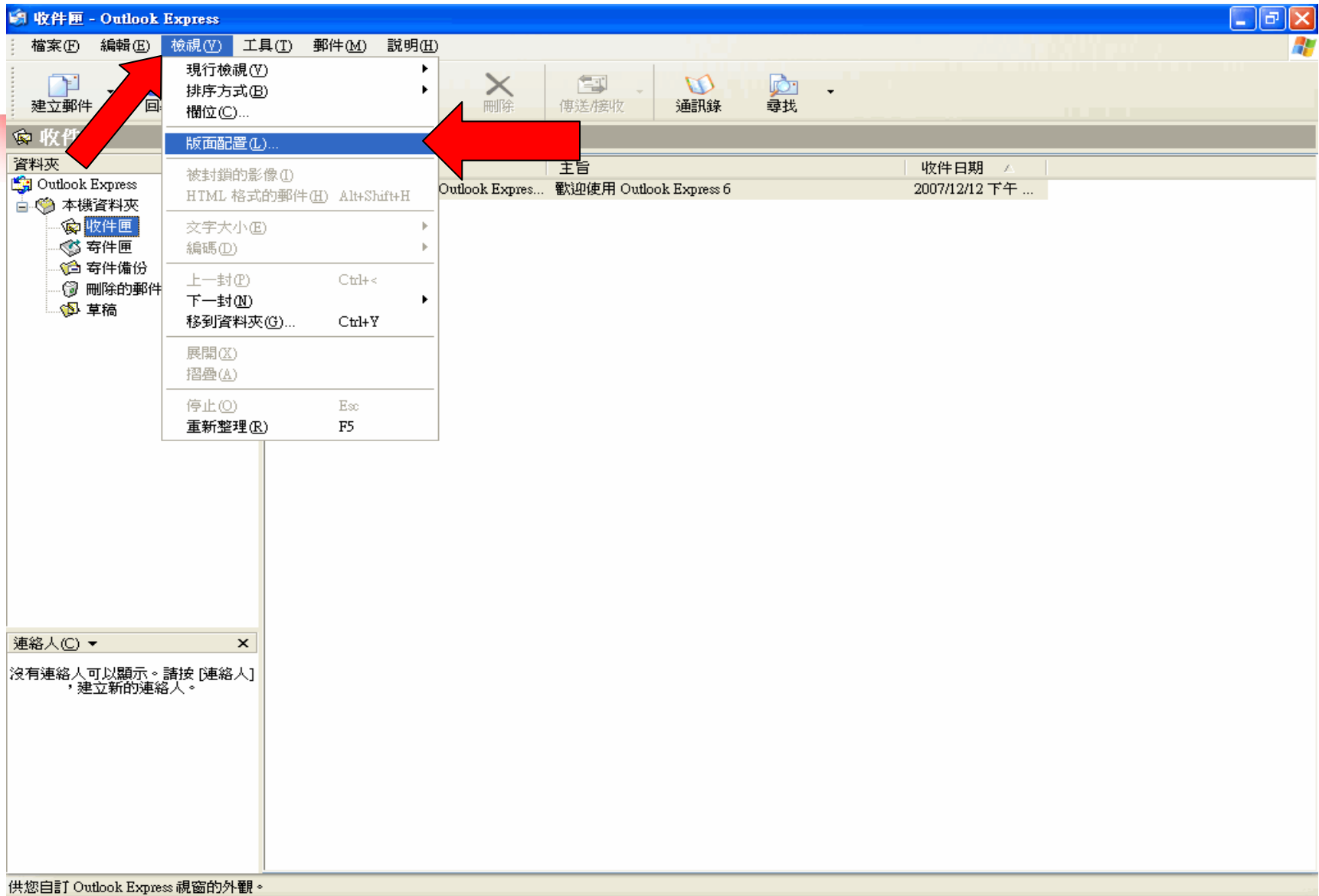
確定 取消

關閉郵件預覽功能

Outlook Express 操作方式



步驟 2 點選『檢視』功能裡的『版面配置』。



步驟3將『顯示預覽窗格』勾勾取消，按下『確定』





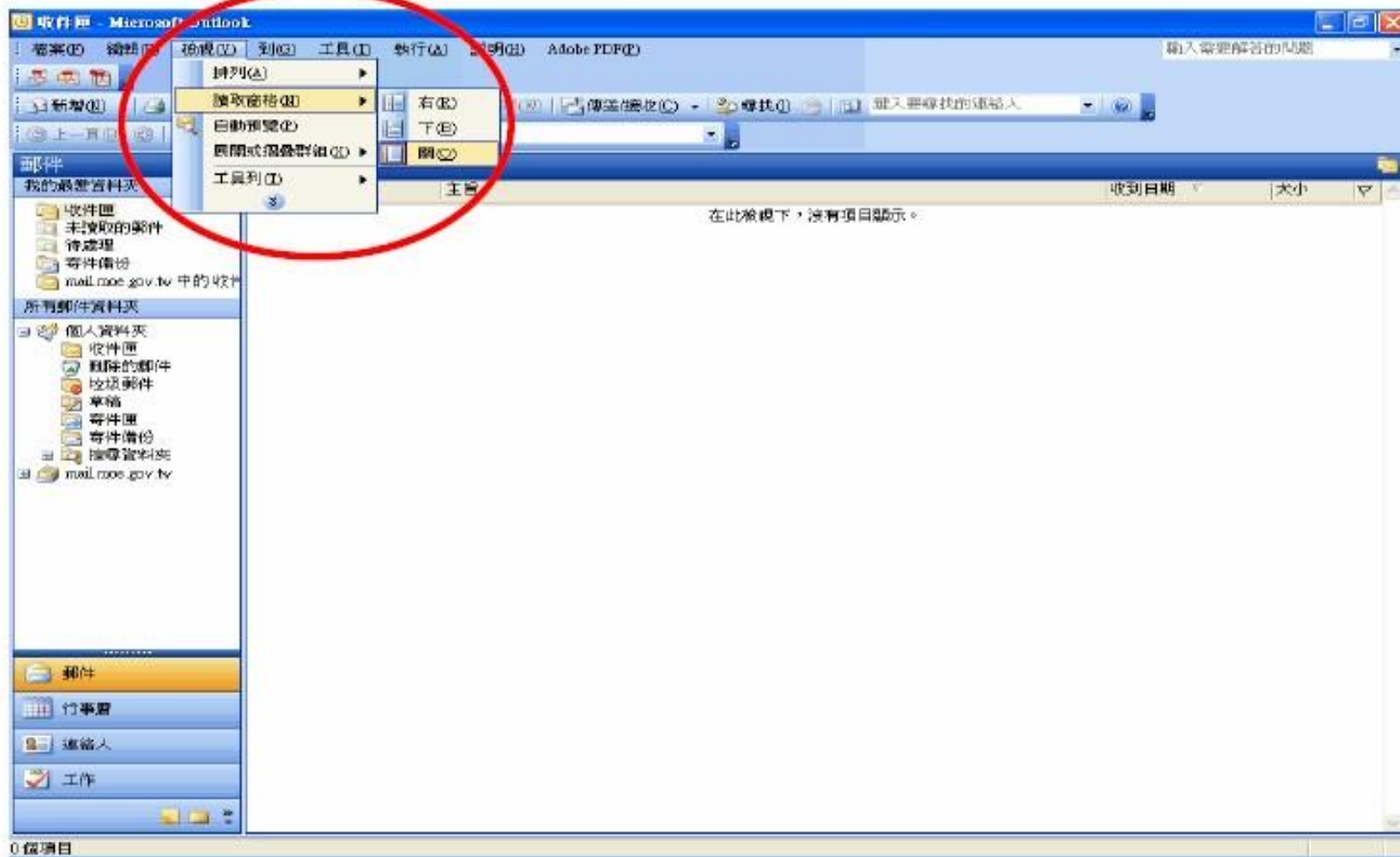
outlook 安全性設定

1. 使用電子郵件時提高警覺及培養良好使用習慣才不易受騙。
2. 讀取信件時，應注意寄件者、主旨是否有不尋常。
3. 不隨意讀取非業務相關及來路不明的電子信件內容，以免被植入後門程式竊取資料。
4. 不轉發非業務相關之電子信件。
5. 不隨意開啟附件及點選超連結，點選超連結時需注意與文字內容是否一致。
6. 設定郵件規則，將常往來、熟悉的人員設定分類，較容易防範來路不明或詐騙郵件。
7. 郵件帳號及瀏覽器應取消記憶密碼功能，以避免帳號密碼記錄被駭客利用木馬程式竊取。
8. 除非您瞭解附件的來源且您知道會收到該附件，否則請勿開啟任何附件，並請立即刪除該郵件。
9. 如果您必須寄送電子郵件附件給別人，請告知收件人，以免您的信件被誤認為病毒。
10. 為確保不被釣魚信件所駭或攻防演練所記錄，若您使用Outlook 依照下列方式設定安全性（調整郵件內的安全性設定，禁止下載圖片和超連結等），其他收信軟體亦請參考其相對處設定。

Outlook 2003

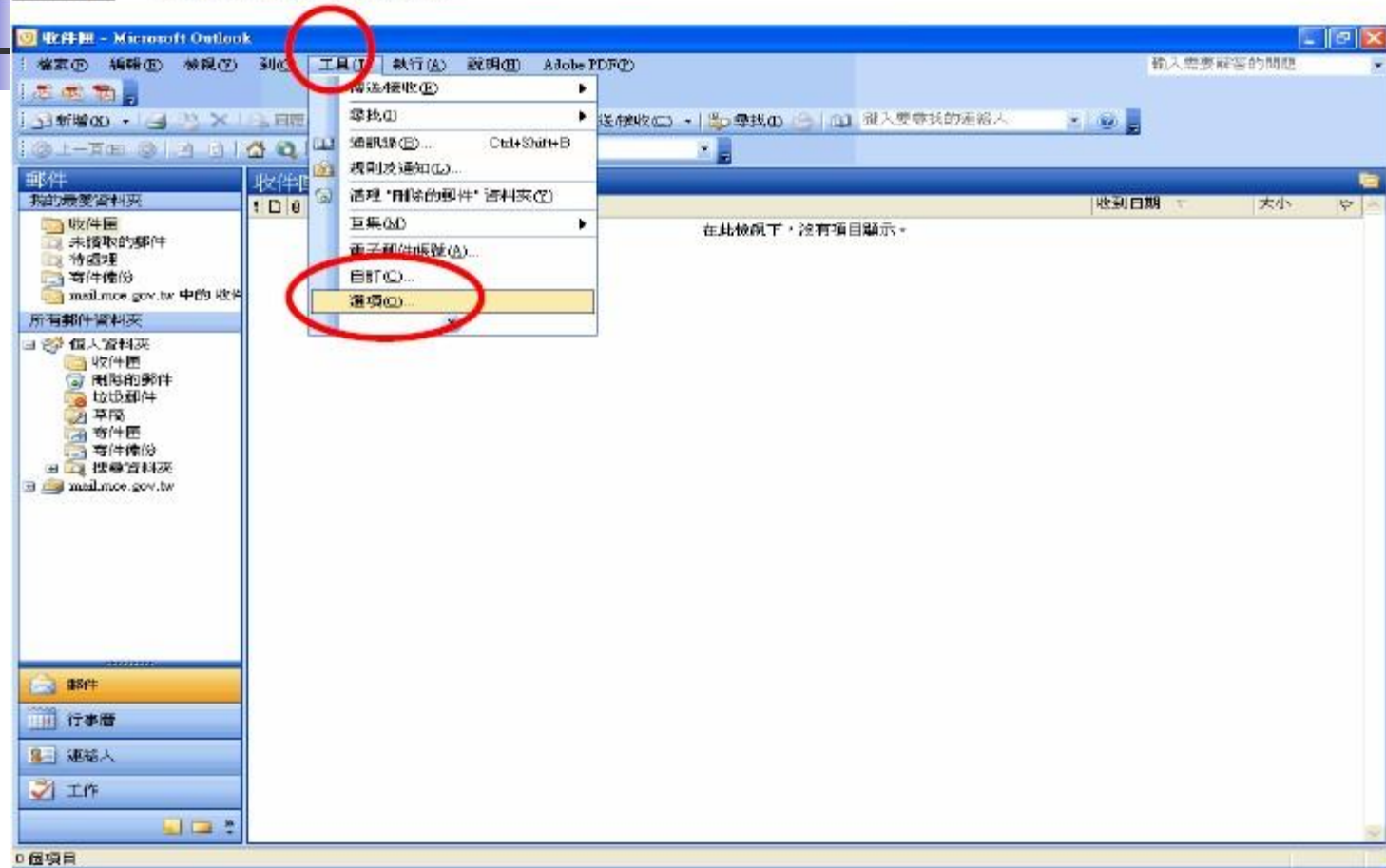
一、郵件設定取消預覽窗格,不預覽郵件內容

打開 outlook 選取檢視內的讀取窗格，設定為關閉

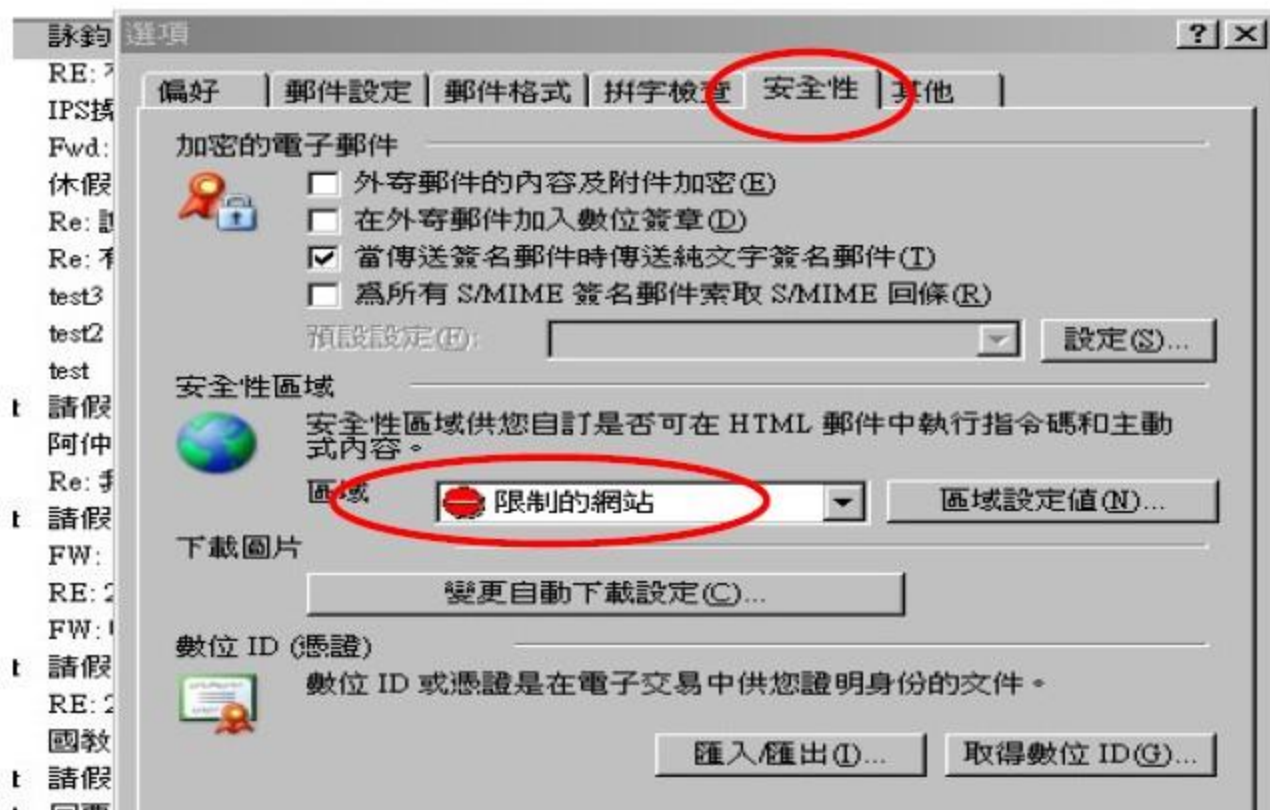


二、調整郵件內的安全性設定，禁止下載圖片和超連結

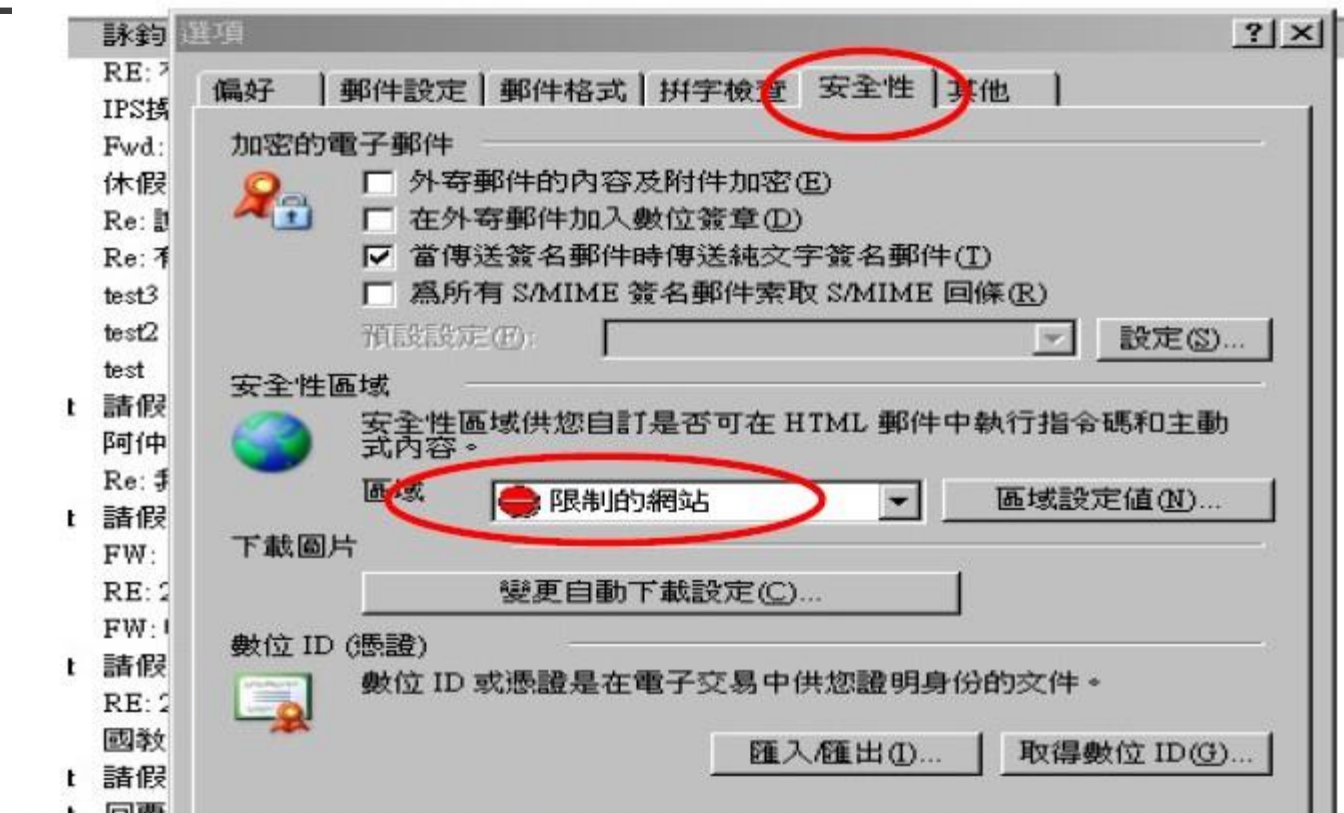
步驟1. 選取工具內的選項



步驟2. 選取頁籤安全性設定調整區域為「限制的網站」，點選「變更自動下載設定」

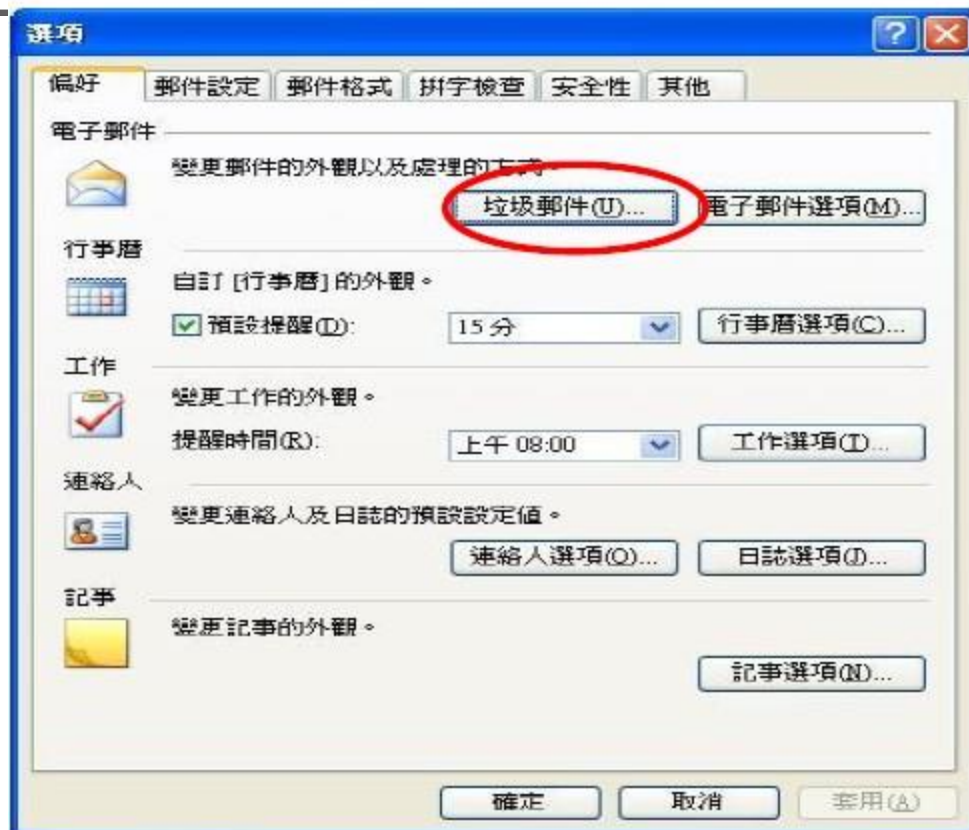


步驟2. 選取頁籤安全性設定調整區域為「限制的網站」，點選「變更自動下載設定」

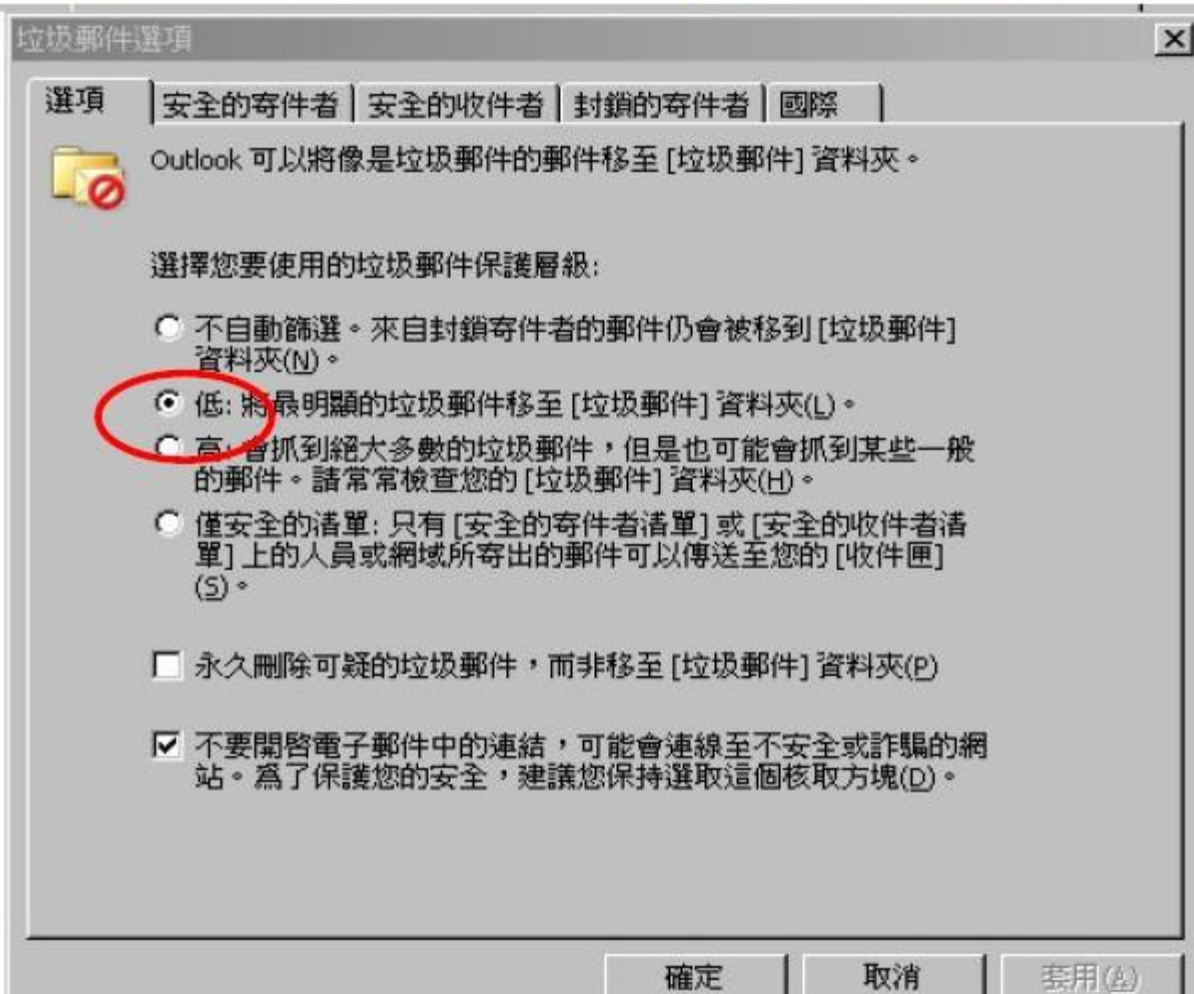


三、調整垃圾郵件選項和封鎖寄件者

步驟1. 點選「偏好」頁籤中「垃圾郵件」選項




步驟2. 選擇「低：將最明顯的垃圾郵件移至「垃圾郵件」資料夾」



垃圾郵件選項

選項 | 安全的寄件者 | 安全的收件者 | 封鎖的寄件者 | 國際

 Outlook 可以將像是垃圾郵件的郵件移至 [垃圾郵件] 資料夾。

選擇您要使用的垃圾郵件保護層級：

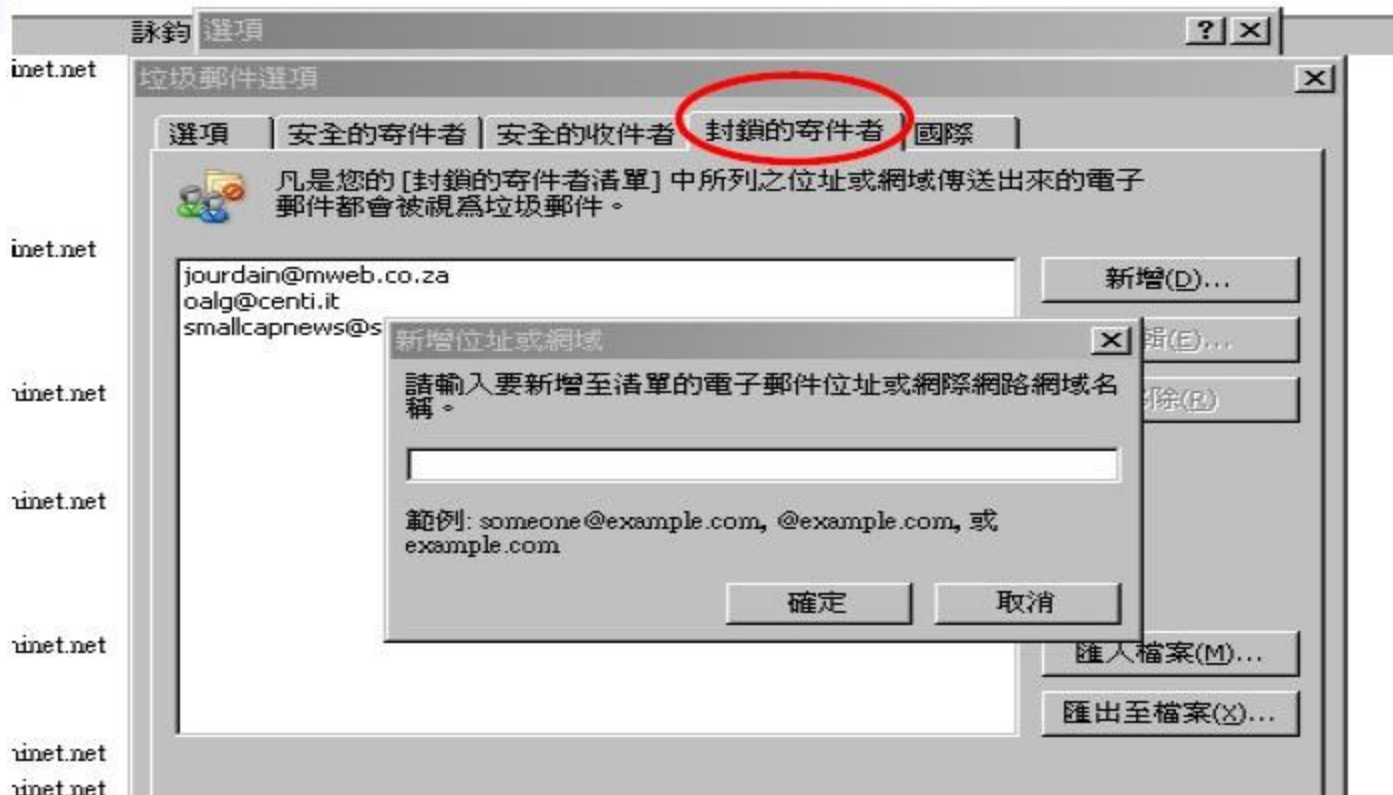
- 不自動篩選。來自封鎖寄件者的郵件仍會被移到 [垃圾郵件] 資料夾(N)。
- 低：將最明顯的垃圾郵件移至 [垃圾郵件] 資料夾(L)。
- 高：會抓到絕大多數的垃圾郵件，但是也可能會抓到某些一般的郵件。請常常檢查您的 [垃圾郵件] 資料夾(H)。
- 僅安全的清單：只有 [安全的寄件者清單] 或 [安全的收件者清單] 上的人員或網域所寄出的郵件可以傳送至您的 [收件匣] (S)。

永久刪除可疑的垃圾郵件，而非移至 [垃圾郵件] 資料夾(P)

不要開啓電子郵件中的連結，可能會連線至不安全或詐騙的網站。為了保護您的安全，建議您保持選取這個核取方塊(D)。

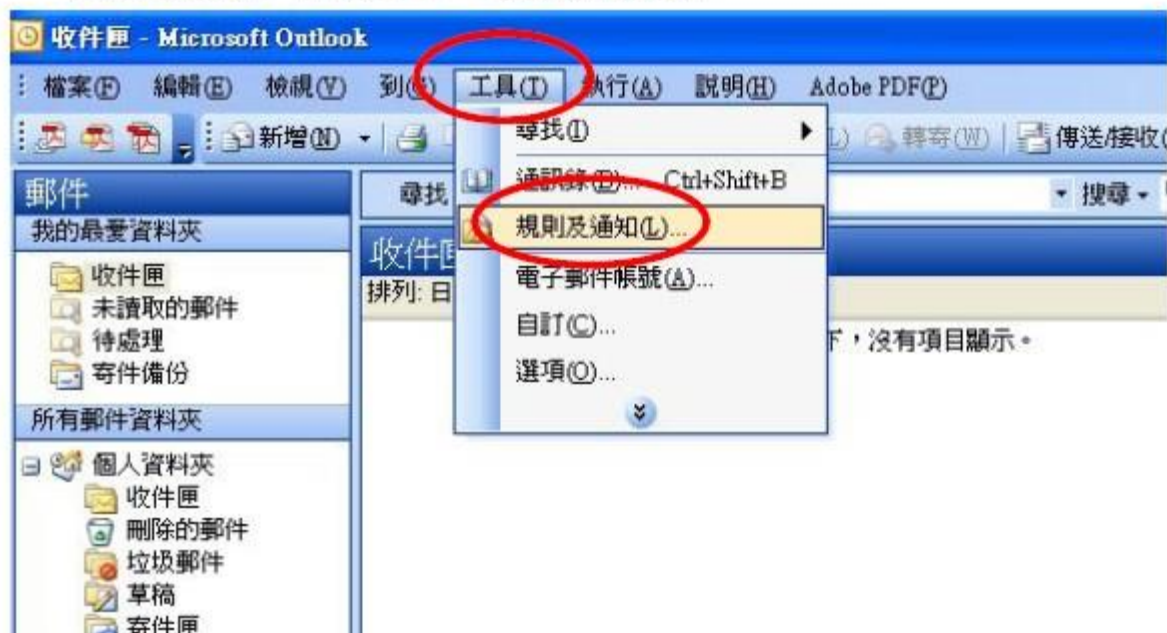
確定 取消 套用(A)

步驟3. 點選「封鎖的寄件者」頁籤，並選擇「新增」後輸入欲封所之名單，完成「確定」。

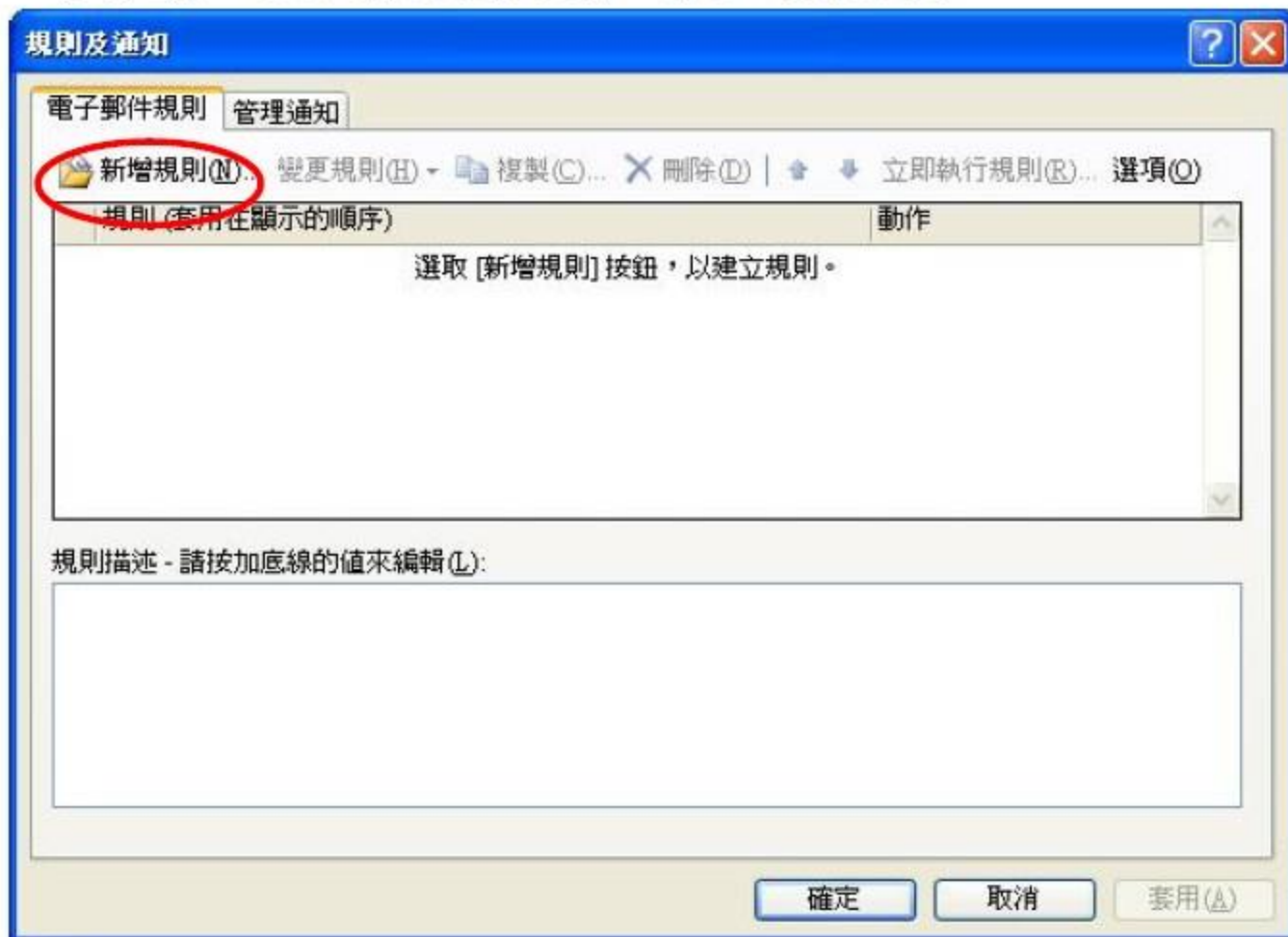


四、設定郵件規則，將常往來、熟悉的人員設定分類，較容易防範來路不明或詐騙郵件

步驟1. 點選「工具」中「規則及通知」



步驟2. 於「電子郵件規則」頁籤中，點選「新增規則」



步驟3. 選擇「從某人移動郵件至資料夾」後，點選「下一步」。



步驟4. 勾選「寄件者個人或通訊群組」後，並選擇指定的寄件者及特
夾，後完成

規則精靈

您要檢查的條件是？
步驟 1: 選取條件(C)

- 寄件者 個人或通訊群組清單
- 主旨中有 特定單字
- 經 已指定 帳號
- 僅傳送給我
- 當我的名字出現在收件者方塊時
- 標示為 重要性
- 標示為 敏感度
- 對 動作 附加標幟
- 我的名字在 [副本] 方塊中
- 我的名字在 [收件者] 或 [副本] 方塊中
- 我的名字不在 [收件者] 方塊中
- 收件者 個人或通訊群組清單
- 內文中含有 特定單字

步驟 2: 編輯規則描述 (在加上底線的值上按一下)(D)

郵件送達後
寄件者 個人或通訊群組清單
將其移動到 特定 資料夾

取消 < 上一步(B) 下一步(N) > 完成

Outlook2007關閉預覽

The screenshot shows the Microsoft Outlook 2007 interface. The 'View' menu is open, and the 'Preview' option is disabled (greyed out). The 'Preview' option is highlighted with a red box. The 'Preview' option is located in the 'View' menu, under the 'Preview' sub-menu. The 'Preview' option is located in the 'View' menu, under the 'Preview' sub-menu. The 'Preview' option is located in the 'View' menu, under the 'Preview' sub-menu.

The main pane displays a list of emails. The selected email is from '系統管理者' (System Administrator) with the subject '政大電算中心 MailGates Notification' and a date of '2010/8/21 (週六) 上午 ... 29 KB'. The list includes several other similar notifications from '系統管理者' and 'ewavs701@nccu....'.

From	Subject	Received	Size
系統管理者	政大電算中心 MailGates Notification	2010/9/3 (週五) 下午 3...	7 KB
系統管理者	政大電算中心 MailGates Notification	2010/9/3 (週五) 上午 1...	17 KB
系統管理者	政大電算中心 MailGates Notification	2010/9/2 (週四) 下午 3...	9 KB
系統管理者	政大電算中心 MailGates Notification	2010/8/31 (週二) 上午 ...	17 KB
系統管理者	政大電算中心 MailGates Notification	2010/8/30 (週一) 上午 ...	17 KB
系統管理者	政大電算中心 MailGates Notification	2010/8/26 (週四) 上午 ...	29 KB
系統管理者	政大電算中心 MailGates Notification	2010/8/25 (週三) 上午 ...	18 KB
系統管理者	政大電算中心 MailGates Notification	2010/8/24 (週二) 上午 ...	17 KB
系統管理者	政大電算中心 MailGates Notification	2010/8/23 (週一) 上午 ...	24 KB
系統管理者	政大電算中心 MailGates Notification	2010/8/22 (週日) 上午 ...	36 KB
系統管理者	政大電算中心 MailGates Notification	2010/8/21 (週六) 上午 ...	29 KB
系統管理者	政大電算中心 MailGates Notification	2010/8/20 (週五) 上午 ...	22 KB
系統管理者	政大電算中心 MailGates Notification	2010/8/19 (週四) 上午 ...	21 KB
系統管理者	政大電算中心 MailGates Notification	2010/8/18 (週三) 上午 ...	21 KB
系統管理者	政大電算中心 MailGates Notification	2010/8/17 (週二) 上午 ...	17 KB
系統管理者	政大電算中心 MailGates Notification	2010/8/16 (週一) 上午 ...	16 KB
系統管理者	政大電算中心 MailGates Notification	2010/8/15 (週日) 上午 ...	17 KB
系統管理者	政大電算中心 MailGates Notification	2010/8/14 (週六) 上午 ...	25 KB
系統管理者	政大電算中心 MailGates Notification	2010/8/12 (週四) 上午 ...	17 KB
ewavs701@nccu....	教育部網站應用程式弱點監測平台-政治大學電子計算機中心營運點-新增檢測網站通知	2010/8/6 (週五) 下午 1...	7 KB
ewavs701@nccu....	教育部網站應用程式弱點監測平台-政治大學電子計算機中心營運點-新增檢測網站通知	2010/8/6 (週五) 下午 1...	7 KB
系統管理者	政大電算中心 MailGates Notification	2010/8/5 (週四) 上午 1...	17 KB
系統管理者	政大電算中心 MailGates Notification	2010/8/1 (週日) 上午 1...	17 KB

Outlook2007 設定純文字模式1

The screenshot shows the Microsoft Outlook 2007 interface. The 'Tools' menu is open, and the 'Trust Center (S)...' option is highlighted with a red rectangle. The main window displays a list of emails, with the selected email's content visible in the bottom pane. The email is from '系統管理者 [MAILER-DAEMON]' and is marked as '此郵件已轉換為純文字' (This message has been converted to plain text).

發件人	收到日期	大小	類別
政大電算中心 MailGates Notification	2010/9/3 (週五) 下午 3...	7 KB	
ilGates Notification	2010/9/3 (週五) 上午 1...	17 KB	
帳號到期通知	2010/9/2 (週四) 下午 3...	9 KB	
ilGates Notification	2010/8/31 (週二) 上午 ...	17 KB	
ilGates Notification	2010/8/30 (週一) 上午 ...	17 KB	
ilGates Notification	2010/8/26 (週四) 上午 ...	29 KB	
ilGates Notification	2010/8/25 (週三) 上午 ...	18 KB	
系統管理者 政大電算中心 MailGates Notification	2010/8/24 (週二) 上午 ...	17 KB	
系統管理者 政大電算中心 MailGates Notification	2010/8/23 (週一) 上午 ...	24 KB	
系統管理者 政大電算中心 MailGates Notification	2010/8/22 (週日) 上午 ...	36 KB	
系統管理者 政大電算中心 MailGates Notification	2010/8/21 (週六) 上午 ...	29 KB	
系統管理者 政大電算中心 MailGates Notification	2010/8/20 (週五) 上午 ...	22 KB	

政大電算中心 MailGates Notification

系統管理者 [MAILER-DAEMON]

此郵件已轉換為純文字。

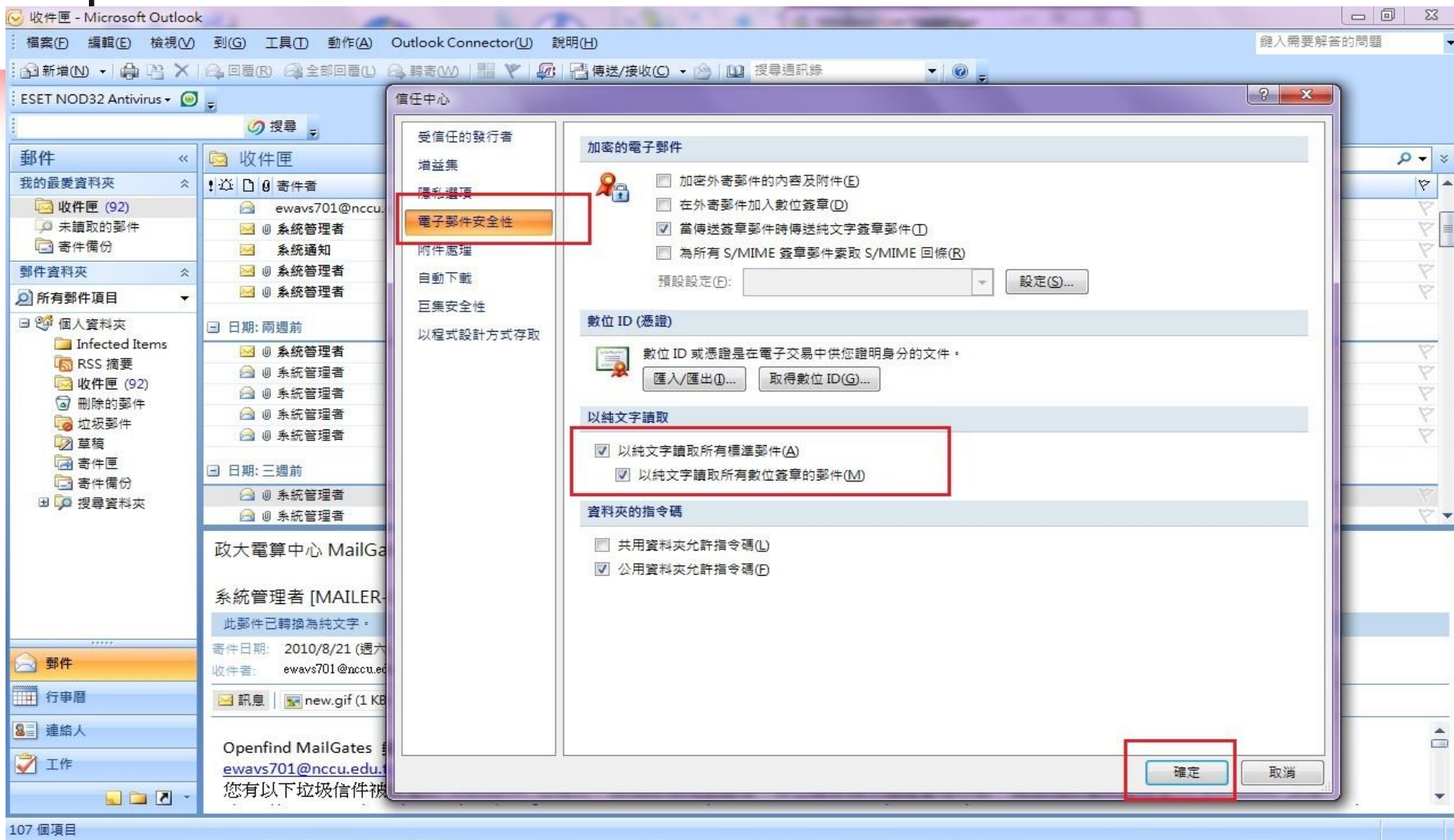
寄件日期: 2010/8/21 (週六) 上午 01:36
收件者: ewavs701@nccu.edu.tw

訊息 | new.gif (1 KB) | important.gif (197 B) | quarantine.html (10 KB)

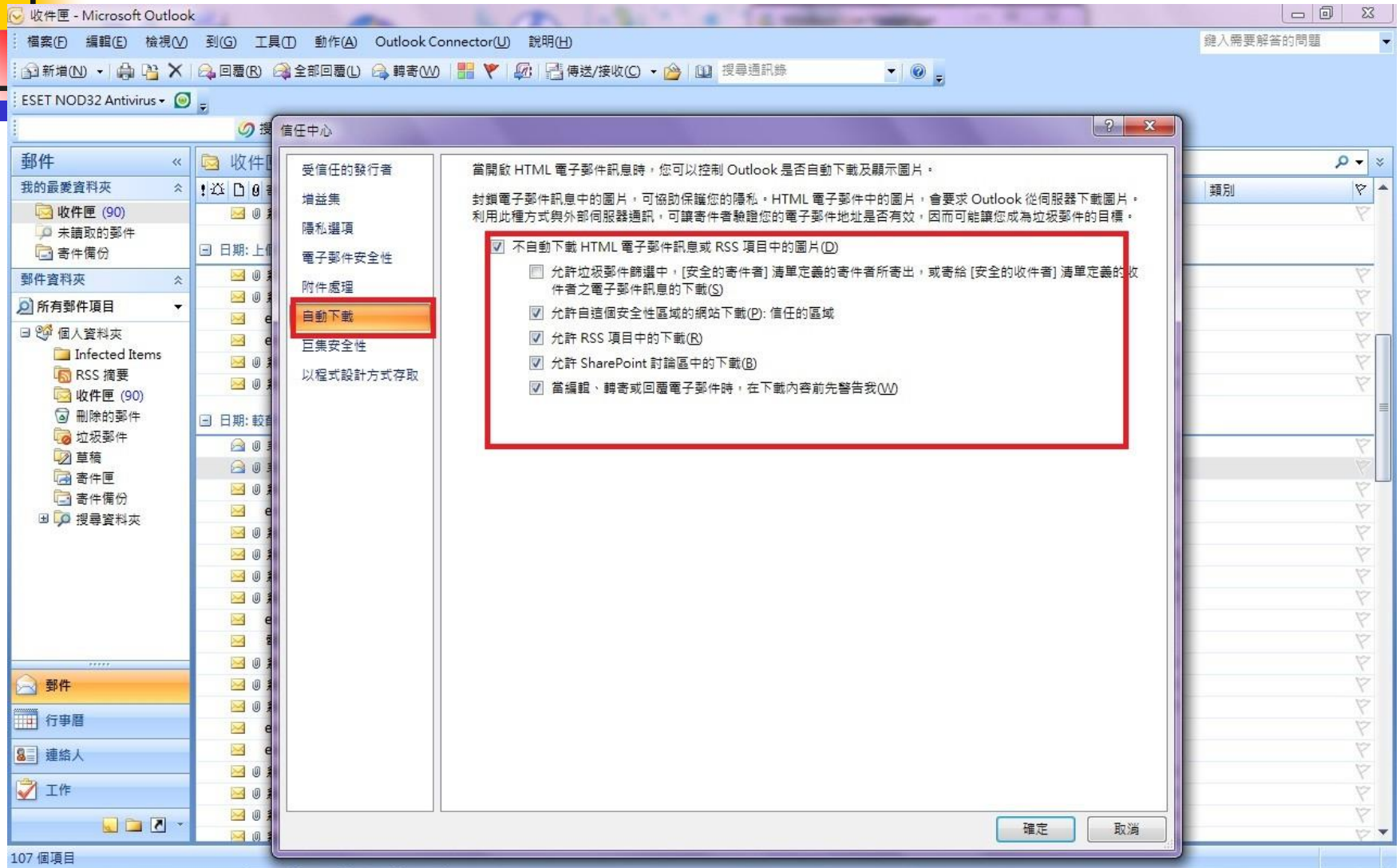
Openfind MailGates 郵件防護系統
ewavs701@nccu.edu.tw 您好:
您有以下垃圾信件被留置於 MailGates 主機上, 請協助檢視並處理。若您需要操作進階管理功能, 請檢視附檔或直接登入 MailGates 主機

107 個項目

Outlook2007 設定純文字模式2



Outlook2007 關閉自動下載



收件匣 - Microsoft Outlook

檔案(F) 編輯(E) 檢視(V) 到(G) 工具(T) 動作(A) Outlook Connector(U) 說明(H)

新增(N) 回覆(R) 全部回覆(L) 轉寄(W) 傳送/接收(C) 搜尋通訊錄

ESET NOD32 Antivirus

搜尋

郵件 收件匣 搜尋收件匣

我的最愛資料夾

- 收件匣 (89)
- 未讀取的郵件
- 郵件備份

郵件資料夾

- 所有郵件項目
- 個人資料夾
- Infected Items
- RSS 摘要
- 收件匣 (89)
- 刪除的郵件
- 垃圾郵件
- 草稿
- 寄件匣
- 郵件備份
- 搜尋資料夾

郵件

行事曆

連絡人

工作

107 個項目

政大電算中心 MailGates Notification - 郵件 (純文字)

郵件 增益集

回覆 全部回覆 轉寄 刪除 移動到 建立規則 其他動作 封鎖 寄件者 非垃圾郵件 分類 待處理 標記為 未讀取 尋找 相關 傳送至 OneNote 選取 尋找 OneNote

此郵件已轉換為純文字。

寄件者: 系統管理者 [MAILER-DAEMON] 寄件日期: 2010/7/24 (週六) 上午 01:35

收件者: ewavs701@nccu.edu.tw

副本:

主旨: 政大電算中心 MailGates Notification

new.gif (1 KB) quarantine.html (8 KB)

Openfind 檔案名稱: new.gif 檔案類型: GIF 檔案 檔案大小: 1 KB

郵件防護系統

ewavs701@nccu.edu.tw 您好:

您有以下垃圾信件被留置於 MailGates 主機上, 請協助檢視並處理。若您需要操作進階管理功能, 請檢視附檔或直接登入 MailGates 主機 <http://mg.nccu.edu.tw/mg-cgi/mg_login?HTTP_COOKIE=mg_uid%3Dewavs701@nccu.edu.tw;mg_skey%3D239826112.3904057600.ewavs701@nccu.edu.tw>, 謝謝。

* 垃圾信件 共 6 封
 新信 2 封 / 即將刪除 0 封 (保留期限 30 天)

旗標	信件處理	標題	寄件人	日期	預定刪除時間
新信	送信	< http://mg.nccu.edu.tw/mg-cgi/mg_sfm?			

政大電算中心 MailGates Notification 2010/3/30 (週二) 上午 ... 11 KB

政大電算中心 MailGates Notification 2010/3/23 (週二) 上午 ... 11 KB

Outlook 2010 關閉預覽

The screenshot shows the Microsoft Outlook 2010 interface. The title bar reads "收件匣 - ewavs701@nccu.edu.tw - Microsoft Outlook". The ribbon is set to "檢視" (View). The "預覽" (Preview) pane is active, and a context menu is open over it, with the "關閉" (Close) option highlighted. The main pane displays a list of emails from "政大電算中心 MailGates Notification". The taskbar at the bottom shows the system clock as "下午 04:53 2010/9/8".

日期	發件人	主旨	日期	時間	大小
今天	Microsoft Outlook	Microsoft Outlook 測試郵件			4 KB
昨天	@ 系統管理者	政大電算中心 MailGates Notification	2010/9/7 (週二)	上午 1:38	19 KB
上週	@ 系統管理者	政大電算中心 MailGates Notification	2010/9/4 (週六)	上午 1:37	18 KB
	ewavs701@nccu...	教育部網站應用程式弱點監測平台-政治大學電子計算機中心營運點-新增檢測網站通知	2010/9/3 (週五)	下午 3:27	7 KB
	ewavs701@nccu...	教育部網站應用程式弱點監測平台-政治大學電子計算機中心營運點-新增檢測網站通知	2010/9/3 (週五)	下午 3:27	8 KB
	@ 系統管理者	政大電算中心 MailGates Notification	2010/9/3 (週五)	上午 1:38	18 KB
	系統通知	單位公務用email帳號到期通知	2010/9/2 (週四)	下午 3:23	10 KB
	@ 系統管理者	政大電算中心 MailGates Notification	2010/8/31 (週二)	上午 1...	18 KB
	@ 系統管理者	政大電算中心 MailGates Notification	2010/8/30 (週一)	上午 1...	18 KB
兩週前	@ 系統管理者	政大電算中心 MailGates Notification	2010/8/26 (週四)	上午 1...	30 KB
	@ 系統管理者	政大電算中心 MailGates Notification	2010/8/25 (週三)	上午 1...	19 KB
	@ 系統管理者	政大電算中心 MailGates Notification	2010/8/24 (週二)	上午 1...	18 KB
	@ 系統管理者	政大電算中心 MailGates Notification	2010/8/23 (週一)	上午 1...	25 KB
	@ 系統管理者	政大電算中心 MailGates Notification	2010/8/22 (週日)	上午 1...	38 KB
三週前	@ 系統管理者	政大電算中心 MailGates Notification	2010/8/21 (週六)	上午 1...	30 KB
	@ 系統管理者	政大電算中心 MailGates Notification	2010/8/20 (週五)	上午 1...	23 KB
	@ 系統管理者	政大電算中心 MailGates Notification	2010/8/19 (週四)	上午 1...	23 KB
	@ 系統管理者	政大電算中心 MailGates Notification	2010/8/18 (週三)	上午 1...	22 KB
	@ 系統管理者	政大電算中心 MailGates Notification	2010/8/17 (週二)	上午 1...	18 KB
	@ 系統管理者	政大電算中心 MailGates Notification	2010/8/16 (週一)	上午 1...	18 KB
	@ 系統管理者	政大電算中心 MailGates Notification	2010/8/15 (週日)	上午 1...	18 KB

Outlook2010設定純文字模式1



Outlook2010設定純文字模式2

The screenshot shows the Microsoft Outlook 2010 interface with the Trust Center dialog box open. The dialog box is titled "Outlook 選項" and contains several sections. The "信任中心" (Trust Center) option is selected in the left-hand menu. The main content area displays a security warning and links to privacy and security information. A red rectangular box highlights the "信任中心設定(O)..." button at the bottom right of the dialog box.

Outlook 選項

協助您維護文件的安全，並讓您的電腦維持在安全和良好的狀態。

保護您的隱私權

Microsoft 關心您的隱私權，若需更多關於 Microsoft Outlook 如何保護您的隱私權之資訊，請查看隱私權聲明。

[顯示 Microsoft Outlook 的隱私權聲明](#)

[Office.com 隱私權聲明](#)

[客戶經驗改進計畫](#)

安全性和其他

從 Office.com 了解更多關於保護您的隱私權和安全性的資訊。

[Microsoft 可信度電腦遠算](#)

Microsoft Outlook 信任中心

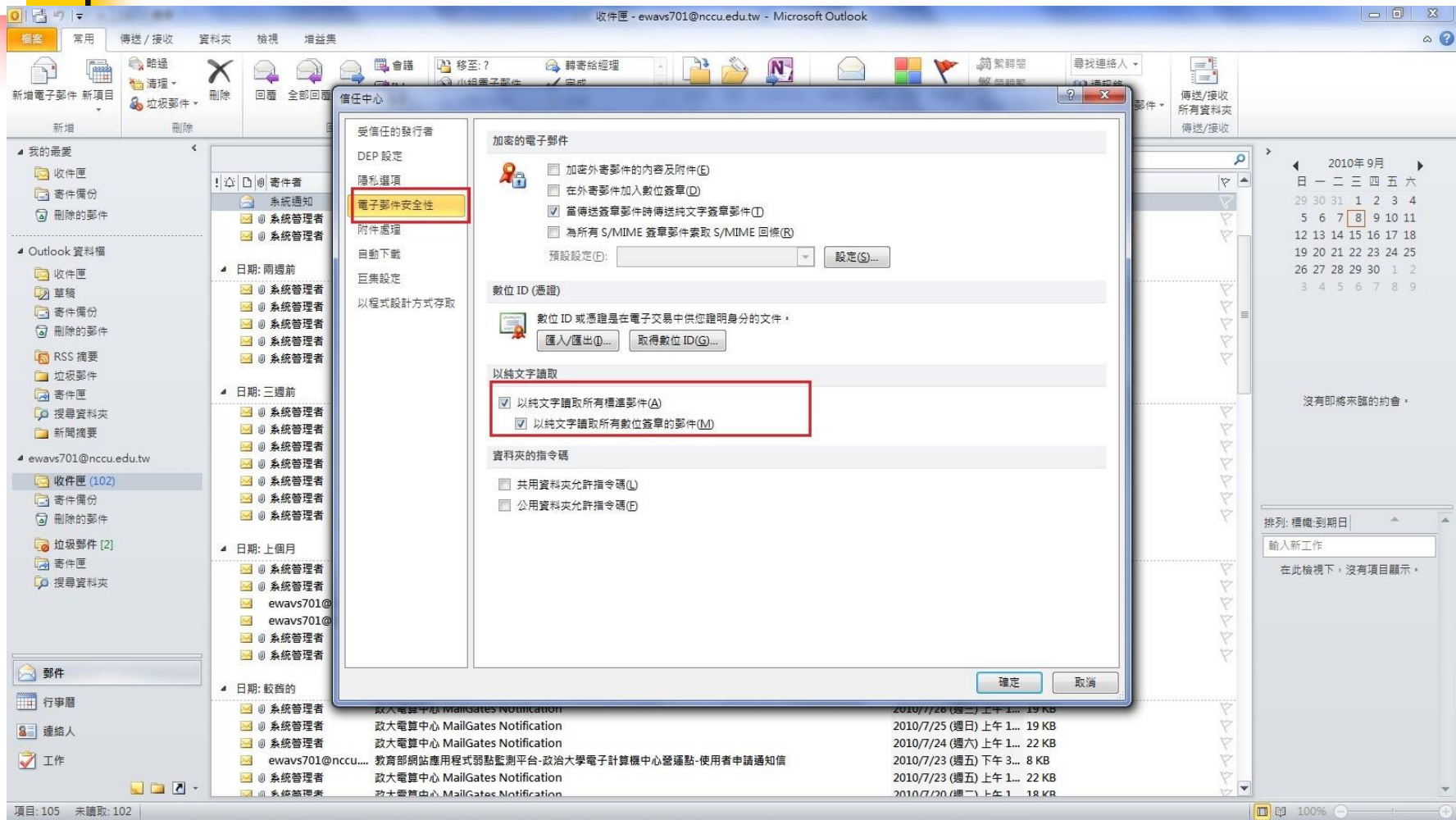
信任中心包含安全性和隱私權設定，這些設定將協助您保持電腦的安全性，我們建議您不要變更這些設定。

信任中心設定(O)...

確定 取消

項目: 105 未讀取: 102 100%

Outlook2010設定純文字模式3



Outlook2010 關閉自動下載

The screenshot displays the Microsoft Outlook 2010 interface. A 'Trust Center' dialog box is open, showing the 'Automatic Download' settings. The 'Do not automatically download HTML content or images in RSS feeds' option is checked. Below this, several other options are listed, including 'Allow automatic download of pictures in HTML e-mail messages from the Internet' (checked), 'Allow automatic download of pictures in HTML e-mail messages from intranet sites' (checked), 'Allow automatic download of pictures in HTML e-mail messages from the Internet' (checked), 'Allow automatic download of pictures in HTML e-mail messages from the Internet' (checked), and 'Warn me before automatically downloading pictures' (checked).

當開啟 HTML 電子郵件訊息時，您可以控制 Outlook 是否自動下載及顯示圖片。

封鎖電子郵件訊息中的圖片，可協助保護您的隱私。HTML 電子郵件中的圖片，會要求 Outlook 從伺服器下載圖片。利用此種方式與外部伺服器通訊，可讓寄件者驗證您的電子郵件地址是否有效，因而可能讓您成為垃圾郵件的目標。

- 不自動下載 HTML 電子郵件訊息或 RSS 項目中的圖片(D)
- 允許垃圾郵件篩選中，[安全的寄件者] 清單定義的寄件者所寄出，或寄給 [安全的收件者] 清單定義的收件者之電子郵件訊息的下載(S)
- 允許自這個安全性區域的網站下載(D): 信任的區域
- 允許 RSS 項目中的下載(R)
- 允許 SharePoint 討論區中的下載(B)
- 當編輯、轉寄或回覆電子郵件時，在下載內容前先警告我(W)

項目: 105 未讀取: 101

