電子郵件社交工程及網路資訊安全

瓏群資訊股份有限公司
業務經理 黃 傑 生
jason@lonchun.com.tw

綱要

- 為什麼要注重安全性
- 社交工程介紹
- 電子郵件社交工程的攻擊步驟
- 電子郵件社交工程的防護
- 了解資訊安全概念—學習保護自己
- 附件A--網路及病毒相關名詞解釋
- 附件B—校內Web Mail相關設定
  - 關閉自動預覽
  - 封鎖外部圖檔
  - 強制純文字轉換

為什麼要注重安全性

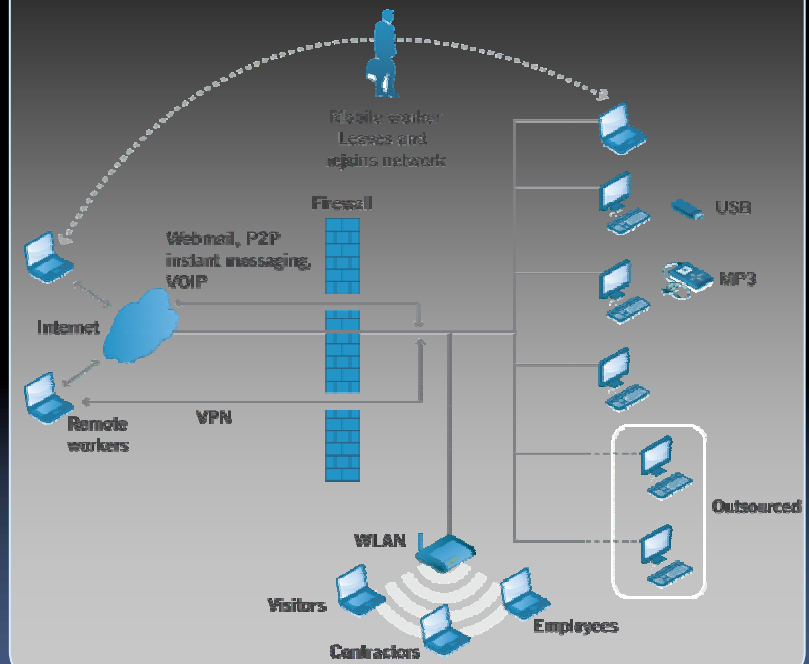
- 電腦安全性最大的問題之一，就是人們在問題發生前都不相信問題真的可能發生。
- 事實是問題的確存在，發生的次數更超出我們想像之外。
- 據美國 Computer Security Institute 及聯邦調查局（FBI）的調查估計，2002 年有九成的企業及政府機關偵測到電腦安全性方面的問題。這些企業和機關當中，有八成承認蒙受財務損失及工作受到影響。

資訊網路安全風險日漸升高

變化迅速的安全環境

從前	現在
惡作劇	有金錢目的
簡單	有智慧
散播緩慢	散播快速
無特定對象	有明確目標

網路邊界正在瓦解



終端電腦是安全防護最脆弱的一環

現有網路及系統可能面臨的資訊安全問題-1

- ・病毒防護： 電腦沒有病毒防護，電腦沒有最新的更新。一般而言，大部分的使用者已瞭解病毒的存在，但不太確定要怎麼預防。
- ・垃圾郵件篩選： 許多使用者總是抱怨垃圾郵件問題，但卻還沒有任何防護措施可以有效阻絕垃圾郵件。
- ・更新： 所有的 Windows XP Professional 或Vista系統都有最新的更新，因為系統會自動檢查並下載更新。 然而，因有些作業系非合法正版,所以未必有更新,包含 MicrosoftOffice 也是需要更新的，但有些電腦從未更新過。

現有網路及系統可能面臨的資訊安全問題-2

- ・密碼： 我們發現大部分的人根本沒用密碼，或是隨便記在電腦附近的便條紙上。 特別要注意的是，有設密碼卻太過簡單，容易被破解。

- ・網頁瀏覽： 大家都認為有快速的網際網路連線是個很好的福利，但大家整天使用它卻沒有仔細想過其風險。 經由內容篩選稽核，可以發現很多單位使用的網頁瀏覽大多都和公事無關。 並未針對可接受的使用方式設定原則或透過閘道過濾，甚而沒有採取任何資訊安全措施，於網頁上熱門的facebook執行小遊戲,易導致安全風險。

網路連線引發的安全課題

遭受攻擊：外部駭客入侵及病毒散播

- 病毒/後門程式 …
- 電子郵件社交工程(垃圾及惡意郵件攻擊)

防護措施：工具或網路技術建立安全通道

- 工具：防火牆/資安防護…
- 網路技術：電子簽章、識別協定

社交工程介紹

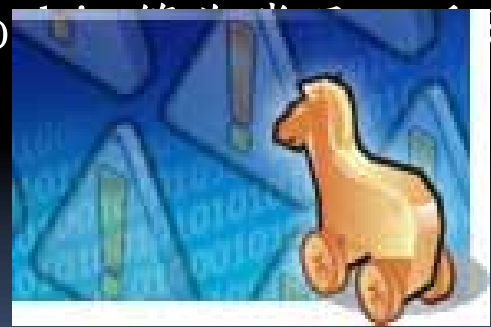
- 利用人性弱點或利用人際之信任關係來進行詐騙，是一種非“全面”技術性的資訊安全攻擊方式，藉由人際關係的互動進行犯罪行為。
- 所謂社交工程，全都是由人性方面為出發點，也就是利用所謂的”信任”來進行。
- 以人為本、騙術為主, 目的為取得重要個資。
- 技術及成本門檻低。
- 利用人性貪婪、好奇及貪小便宜的心理。

社交工程攻擊的定義

- 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。

  早期社交工程是藉由電話或假扮身份問些看似無關緊要的問題等各種方法來獲取所需資訊。

- 透過電子郵件進行攻擊或網頁暗藏木馬/roo[illegible]法



  1. 使用與業務相關或令人感興趣的郵件內容
  2. 含有惡意程式的附件或連結
  3. 假冒寄件者
  4. 利用應用程式之弱點(包括零時差攻擊*)

*針對軟體弱點未修補前，出現針對弱點的攻擊行為，即稱為「零時差攻擊」。

目前郵件威脅種類

Mail-in 郵件威脅種類

垃圾郵件 (Spam)
病毒郵件 (Virus)
間諜程式 (Spyware)
釣魚郵件 (Phishing)
轉嫁郵件 (pharming)
中繼跳板 (Relay)
DoS攻擊 (DoS)
郵件炸單 (Mail Bombing)
駭客入侵 (Hacking)
造假攻擊 (Faking Attacking)

電子郵件社交工程的攻擊步驟

- 有心人設計陷阱或後門程式(木馬)
- 在電子郵件內放置有害程式或連結
- 將信件寄給特定或不特定對象
- 使用者(收信後)開啟信件
- 啟動連結惡意網頁或下載有害程式
- 要求輸出使用者資料（轉眼資料外洩變成受害者）

電子郵件社交工程的手法

網路釣魚(Phishing)

1. 常見的社交工程，特別是利用email來欺騙，Phishing並不是一個新的攻擊手法，然而發生的頻率卻在過去幾年中逐漸增加。
2. 偽造網址：http://www.yahoo.com　　http://www.yah00.com
3. 偽造網頁：製作與原來完全一樣的頁面，以騙取重要的相關資訊。

利用郵件夾帶惡意程式或惡意連結進行攻擊。

運用各種人性弱點吸引使用者開啟有問題信件

- 興趣、貪心、關心的時事、免費的禮物…

網路拍賣實際案例

(4293 封未讀取的信件。) Yahoo!奇摩電子信箱 2.0, plus_jason - Windows Internet Explorer
YAHOO! 奇摩 電子信箱 2.0
您好，son
會員登出
Yahoo!奇摩
即時通
網頁搜尋
檢查新信
編寫新信
搜尋信件...
收件匣 (4293)
草稿匣 (1)
寄件備份匣
垃圾信件匣 (1461)
垃圾筒
通訊錄
信件匣
應用程式
Flickr
我的相片
我的硬碟
編輯相片
行事曆
記事本
最新訊息
收件匣 5738 封信件
Yahoo!奇摩拍賣 問題
刪除
回覆
轉寄
這是垃圾信
搬移
列印
更多選項
拍賣商品問題通知
親愛的 plus_jason 您好：
zxcvbn2974在2010-01-09 22:16針對您的拍賣商品：全新沐浴蓮蓬頭、龍頭、手持花灑 提出了一個問題囉！
請注意 若買方於問與答中提供釣魚連結(Phishing URL)，請勿點選或回覆。此連結將有可能導致您誤登入而使帳號遭到盜用，請您儘速刪除留有不明連結之問與答。如何刪除「問與答」的問題？
詳細內容
提出的問題
拍賣編號：d44380456
問題內容：
可以和這個一起買嗎
http://actionte.host01.chinac.net/tw/yahoo.com.tw/tw/actiion/d457854244
點選回覆此問題，在表格內填寫您回覆的內容，然後按一下「回覆」即可。
廣告
Yahoo!奇摩拍賣
輕秋冬完美保養
告別乾妹妹
保養全攻略
Model圖片由 I'Miusa提供
凡士林 潤膚乳液
足部滋潤系列
今天 1/20(三) - 2/12(五) 無新增事件
2/13(六) • 農曆除夕
2/14(日) • 春節 • 西洋情人節
2/15(一) - 2/27(六) 無新增事件
2/28(日) • 元宵節
完成
網際網路
100%

網路拍賣實際案例(續)

上網搜尋,發現真相

網路拍賣實際案例(續)

上網搜尋,發現真相(偽裝yahoo登入網站,竊取帳密)

網路拍賣實際案例(續)

上網搜尋,發現真相(請仔細確認網址)

怎麼會要我再登入呢？

頭腦尚未完全清醒的我，
於是輸入帳號密碼，
送出後，
又跳到yahoo的登入畫面，
這時候我完全醒了，
身為資訊人員的直覺跳了出來，
靠，
我的帳號密碼被騙了，
趕快回到正版yahoo的網站，
變更密碼，
並且第一時間，
在這裡發表這篇文章，
希望有看到的朋友小心Yahoo的登入面頁，
以免成為受害者。

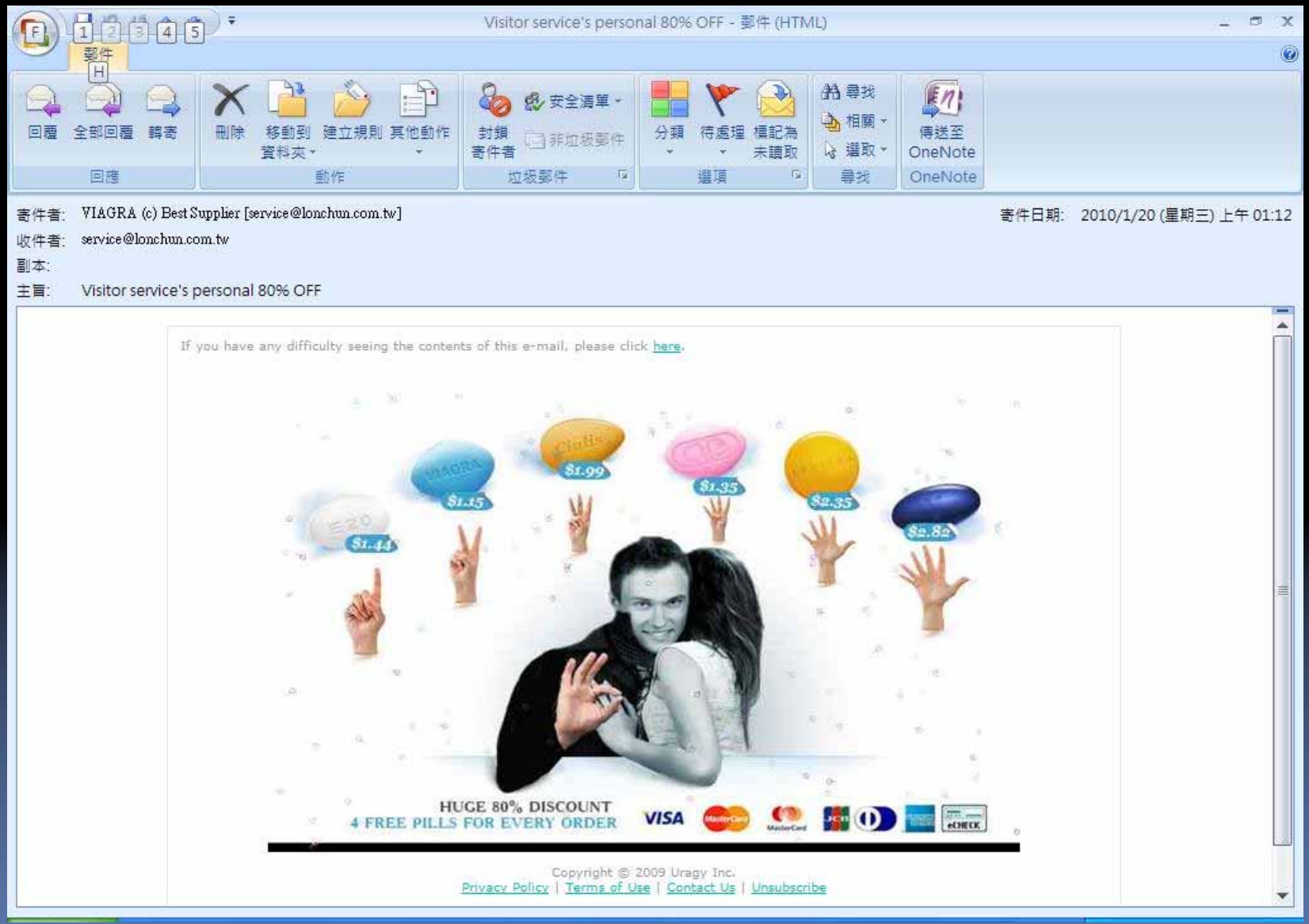
怎麼辨識是否位正版呢？
一律看網址，
正版網址開頭為
https://login.yahoo.com/config/login
看如
https://login.yahoo.com/config/login?.intl=tw&.pd=c%3d7pP3Kh2p2e4XklntZWWfDLAC8w--&.done=https://tw.login.yahoo.com/cgi-bin/kcookie.cgi/www/http://tw.yahoo.com

其他的都是釣魚網站要來騙帳號密碼的。

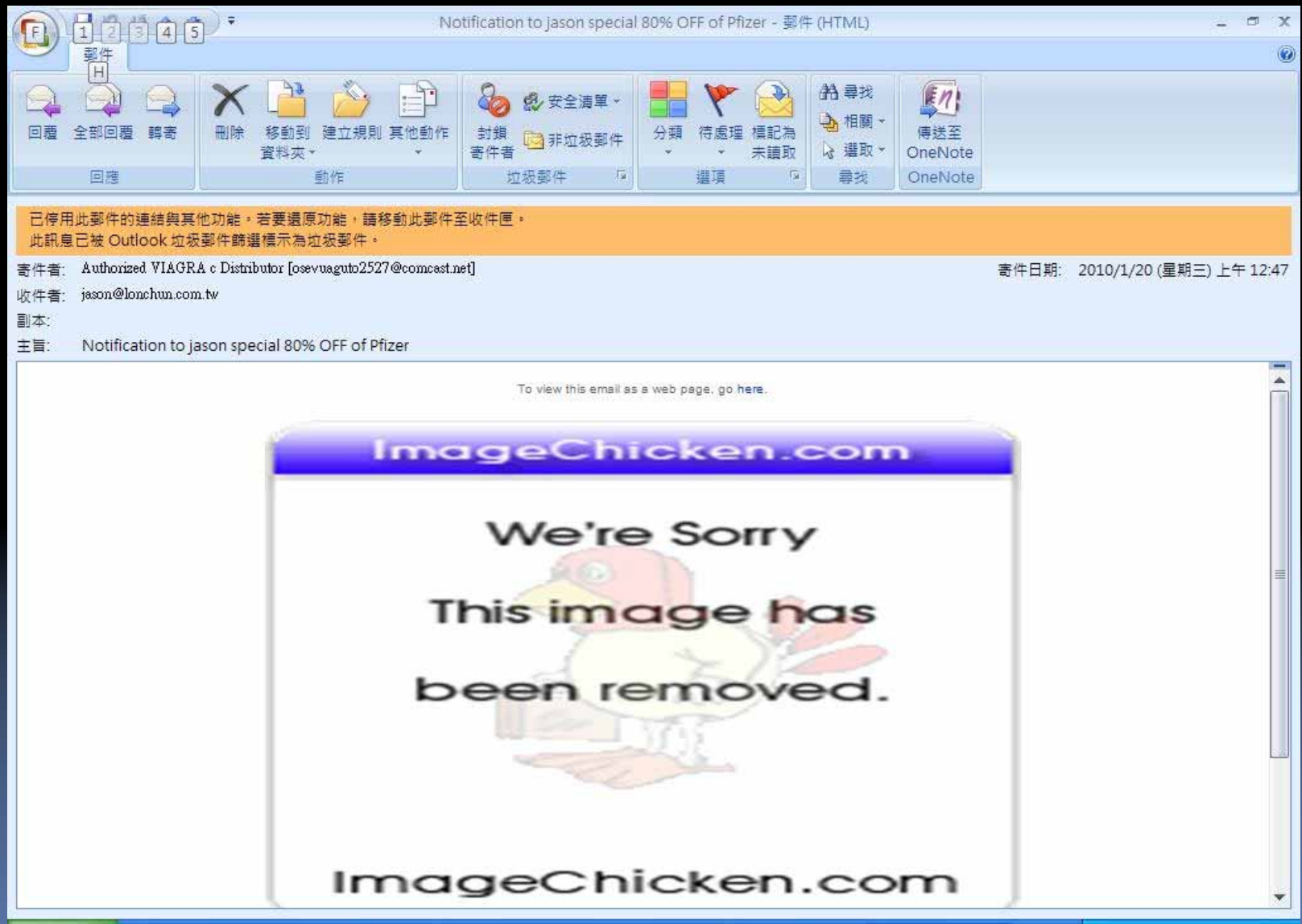
可疑電子郵件之特徵

- 陌生人或極少往來對象的來信
- 大量發送之擾人垃圾信
- 非正常的發信方式
- 非正常的發信時間
- 過於聳動的主旨
- 主旨不明或不符合發信者習慣
- 要求輸入敏感資料之郵件
- 內含不明檔案或鏈結之信件
- 假冒發佈訊息的信件
- 偽冒自己為寄件者的信件

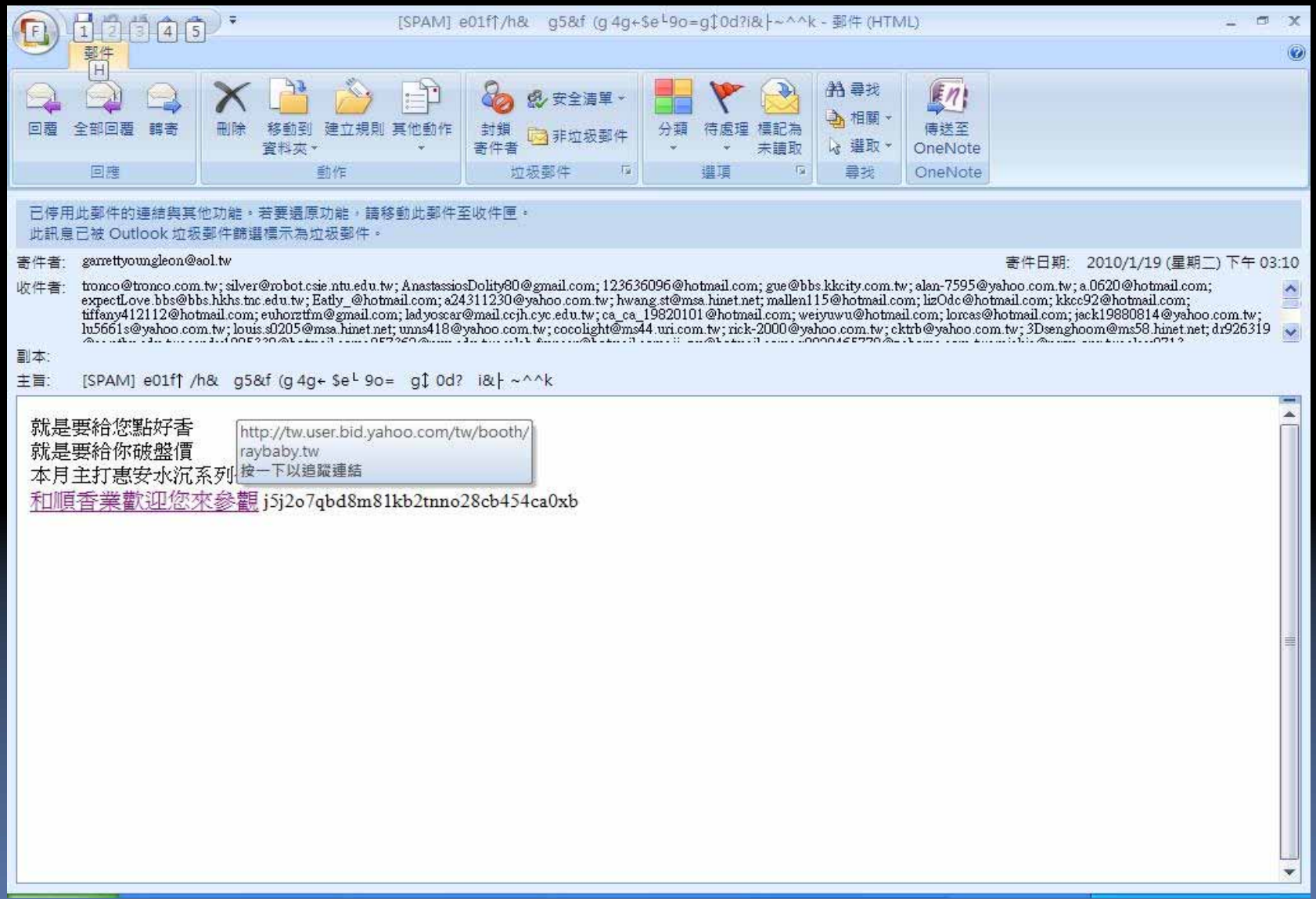
大量發送之擾人垃圾信


Visitor service's personal 80% OFF - 郵件 (HTML)
回覆
全部回覆
轉寄
刪除
移動到資料夾
建立規則
其他動作
封鎖寄件者
安全清單
非垃圾郵件
分類
待處理
標記為未讀取
尋找
相關
選取
傳送至 OneNote
寄件者: VIAGRA (c) Best Supplier [service@lonchun.com.tw]
寄件日期: 2010/1/20 (星期三) 上午 01:12
收件者: service@lonchun.com.tw
副本:
主旨: Visitor service's personal 80% OFF
If you have any difficulty seeing the contents of this e-mail, please click here.
$1.99
$1.35
$2.35
$2.82
$1.15
$1.44
HUGE 80% DISCOUNT
4 FREE PILLS FOR EVERY ORDER
VISA
Copyright © 2009 Uragy Inc.
Privacy Policy | Terms of Use | Contact Us | Unsubscribe

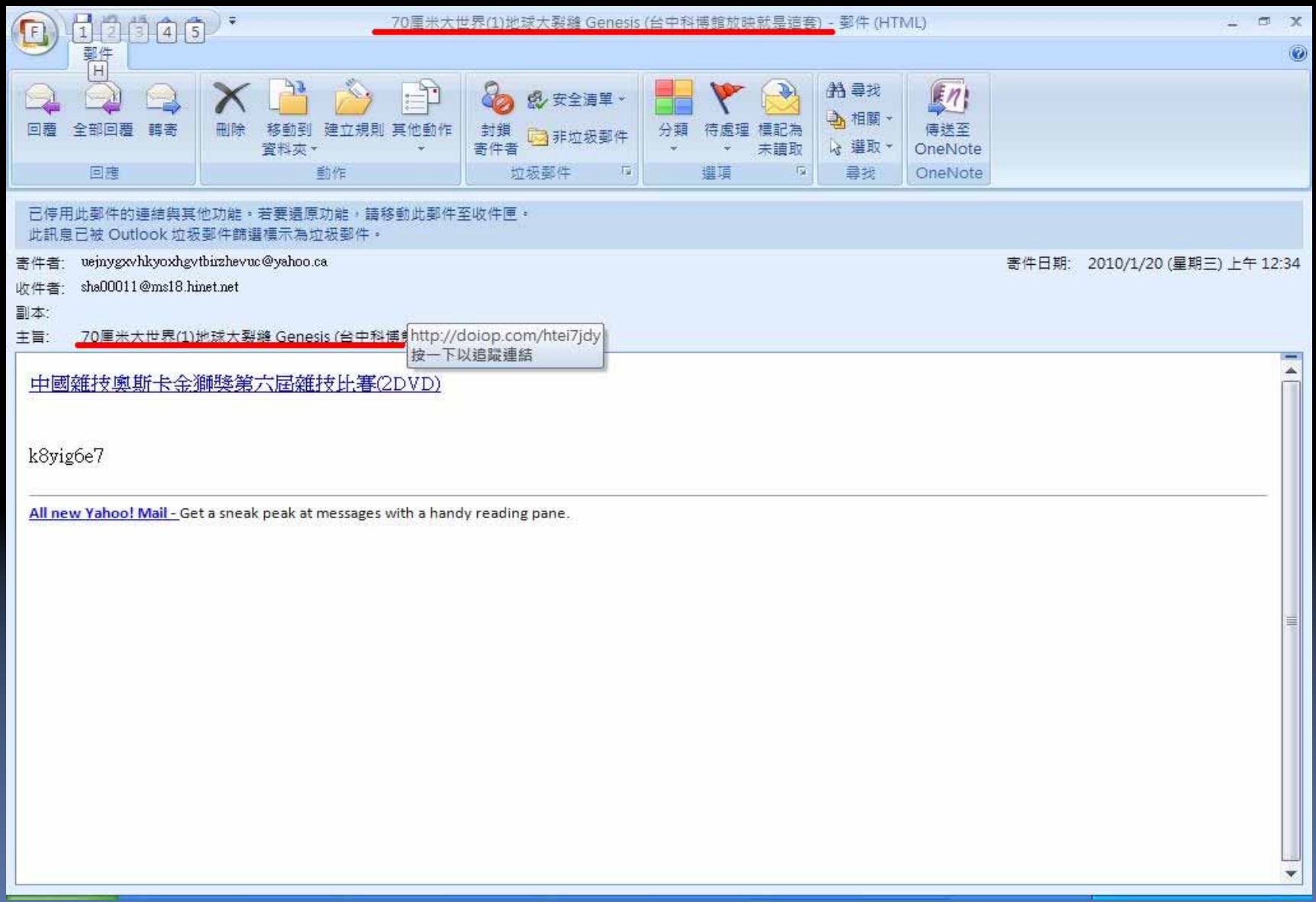
陌生人或極少往來對象的來信



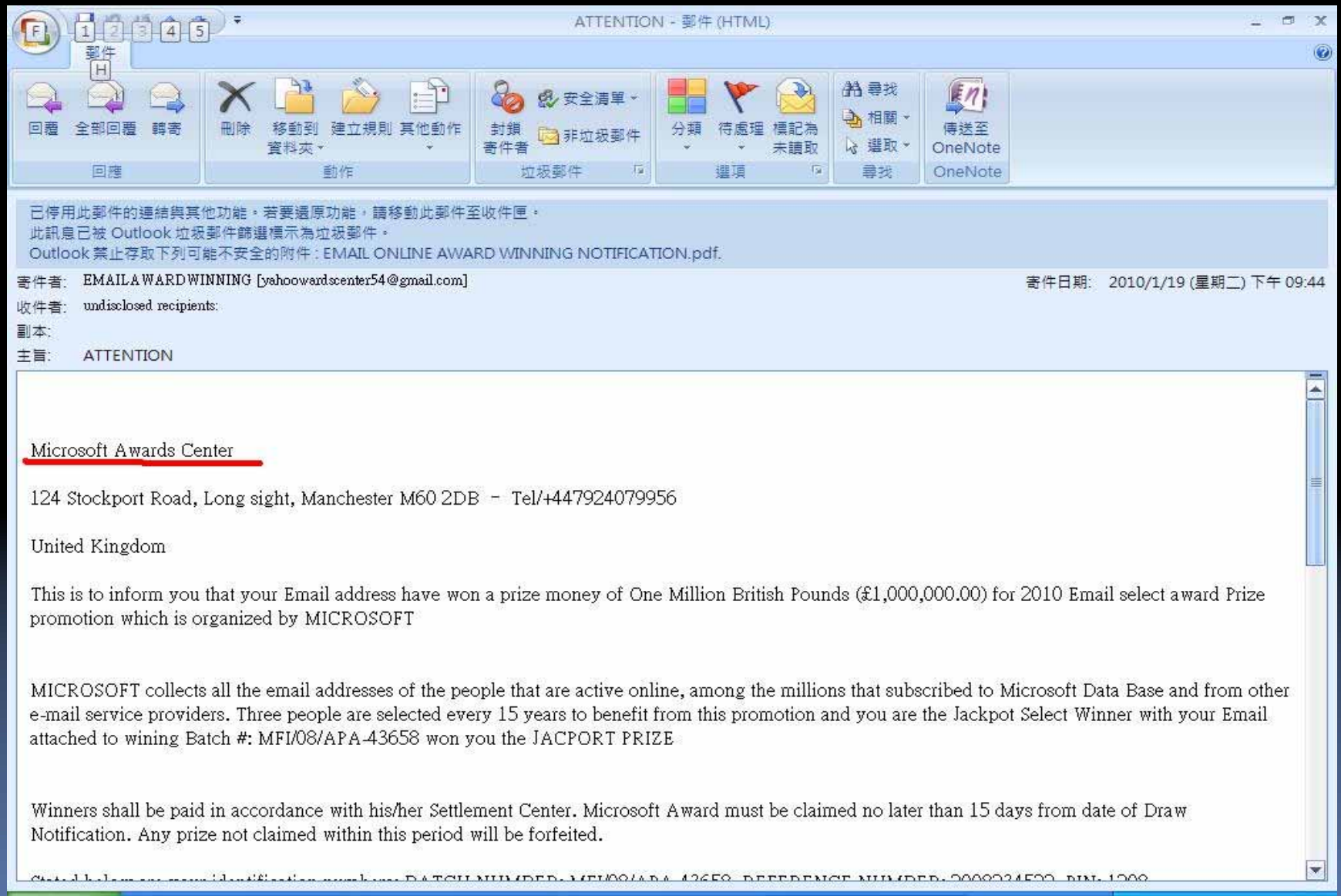
主旨不明或不符合發信者習慣



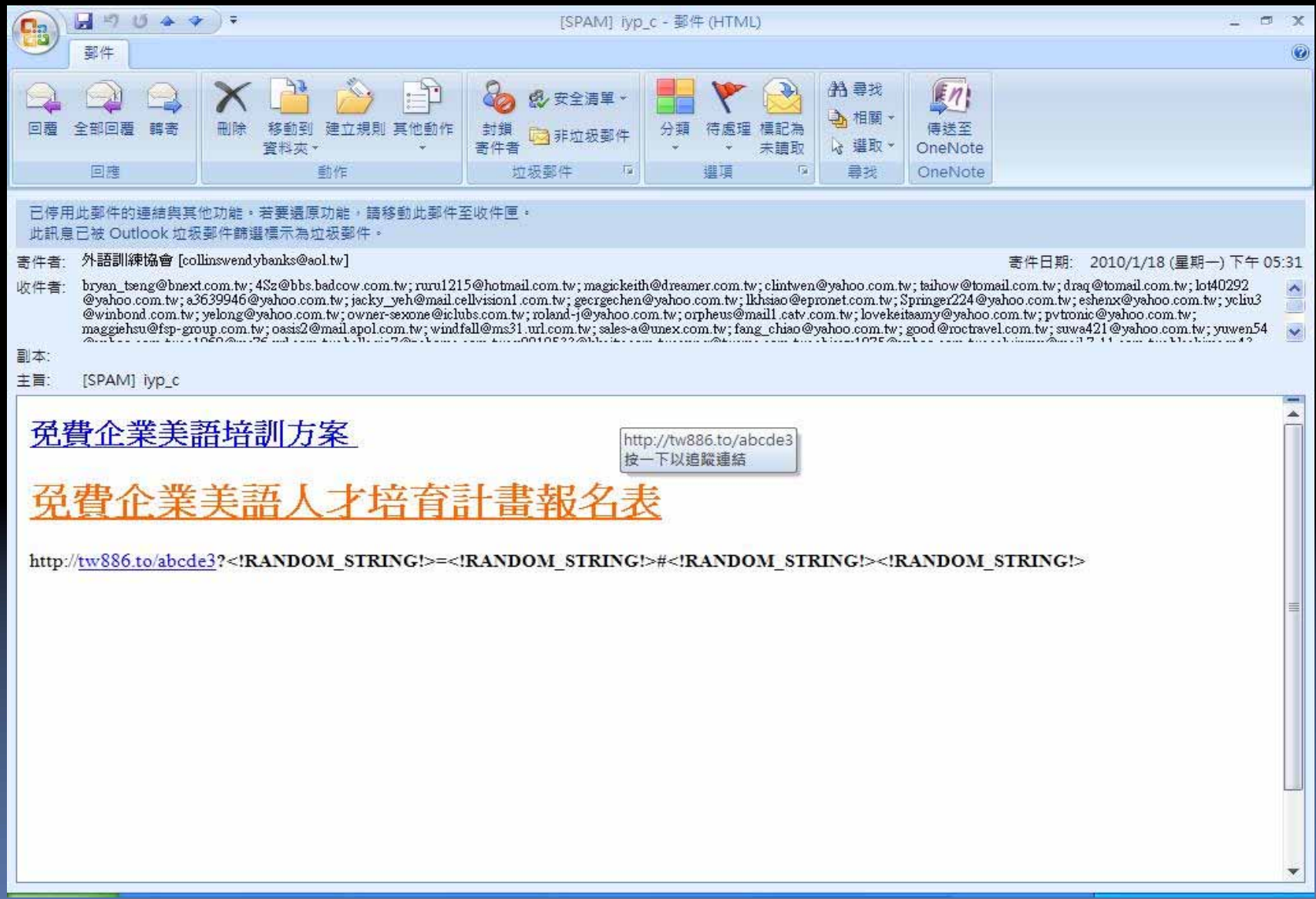
過於聳動的主旨


70厘米大世界(1)地球大裂縫 Genesis (台中科博館放映就是這套) - 郵件 (HTML)
郵件
回覆
全部回覆
轉寄
回應
刪除
移動到資料夾
建立規則
其他動作
動作
封鎖寄件者
安全清單
非垃圾郵件
垃圾郵件
分類
待處理
標記為未讀取
選項
尋找
相關
選取
傳送至OneNote
OneNote
已停用此郵件的連結與其他功能。若要還原功能，請移動此郵件至收件匣。
此訊息已被 Outlook 垃圾郵件篩選標示為垃圾郵件。
寄件者: uejnygxvhkyoxhgvtbirzhevuc@yahoo.ca
寄件日期: 2010/1/20 (星期三) 上午 12:34
收件者: sha00011@ms18.hinet.net
副本:
主旨: 70厘米大世界(1)地球大裂縫 Genesis (台中科博
http://doiop.com/htei7jdy
按一下以追蹤連結
中國雜技奧斯卡金獅獎第六屆雜技比賽(2DVD)
k8yig6e7
All new Yahoo! Mail - Get a sneak peak at messages with a handy reading pane.

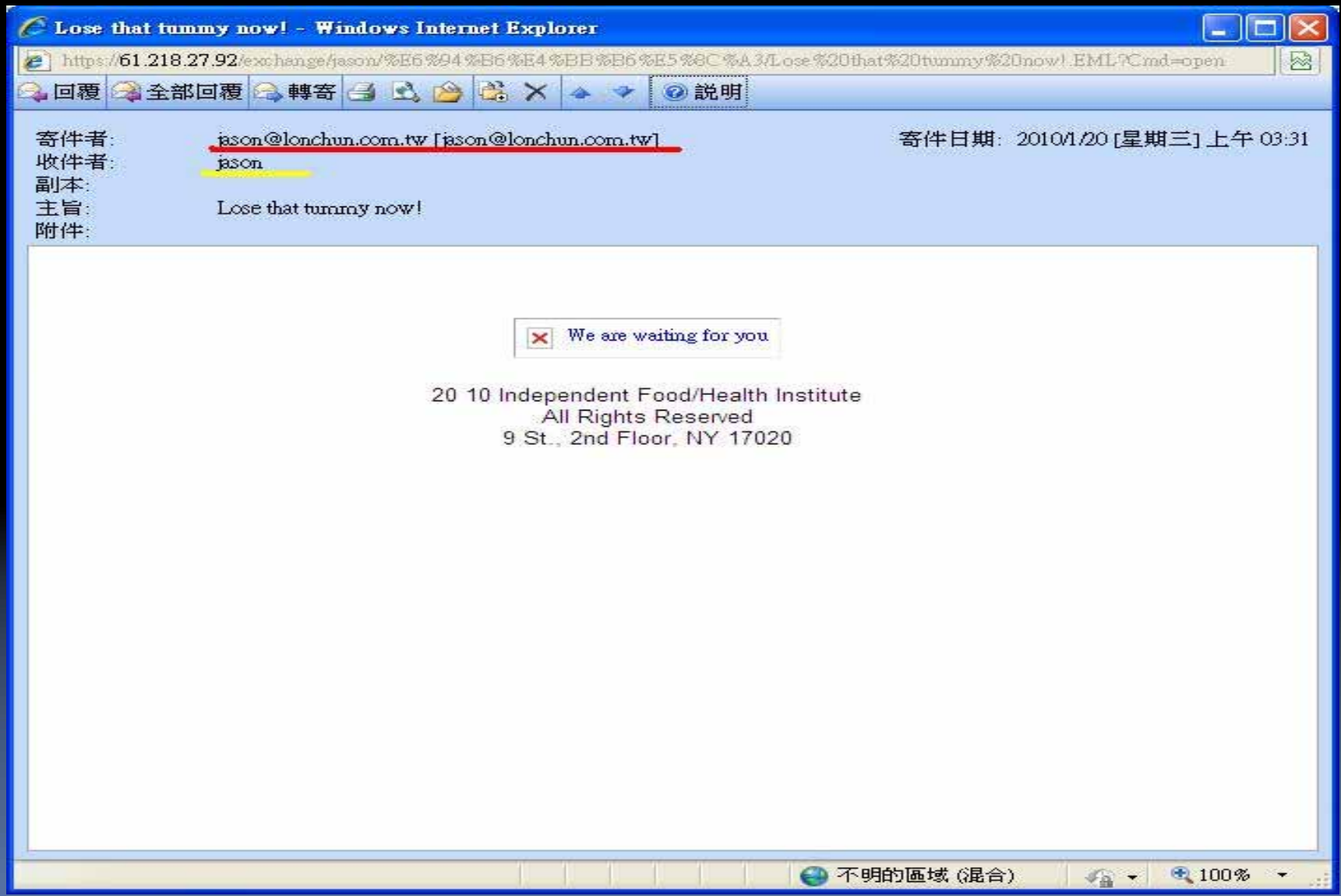
假冒發佈訊息的信件


ATTENTION - 郵件 (HTML)
已停用此郵件的連結與其他功能。若要還原功能，請移動此郵件至收件匣。
此訊息已被 Outlook 垃圾郵件篩選標示為垃圾郵件。
Outlook 禁止存取下列可能不安全的附件：EMAIL ONLINE AWARD WINNING NOTIFICATION.pdf.
寄件者: EMAILAWARDWINNING [yahoowardscenter54@gmail.com]
寄件日期: 2010/1/19 (星期二) 下午 09:44
收件者: undisclosed recipients:
副本:
主旨: ATTENTION
Microsoft Awards Center
124 Stockport Road, Long sight, Manchester M60 2DB - Tel/+447924079956
United Kingdom
This is to inform you that your Email address have won a prize money of One Million British Pounds (£1,000,000.00) for 2010 Email select award Prize promotion which is organized by MICROSOFT
MICROSOFT collects all the email addresses of the people that are active online, among the millions that subscribed to Microsoft Data Base and from other e-mail service providers. Three people are selected every 15 years to benefit from this promotion and you are the Jackpot Select Winner with your Email attached to wining Batch #: MFI/08/APA-43658 won you the JACPORT PRIZE
Winners shall be paid in accordance with his/her Settlement Center. Microsoft Award must be claimed no later than 15 days from date of Draw Notification. Any prize not claimed within this period will be forfeited.

內含不明檔案或鏈結之信件



偽冒自己為寄件者的信件



教育部電子郵件社交工程演練之信件主旨

- 新流感H1N1 大流行期間，個人保健注意事項
- 自行車旅遊私房路線
- 瑤瑤和舒舒，你喜歡誰
- 景氣復甦了嗎？
- 洋基球團虧待王建民
- 聯合報邀請您賞桐花
- 軍方賣官內幕
- 蛀牙不是病，痛起來要人命
- 蔡依林愛無赦+練舞功超神奇混音版
- USB成病毒溫床！台灣電腦今年Q1中毒率列入全球第四大

* 以上主旨的共同特色皆爲聳動之新聞事件或引人好奇之話題

測試定義

信件開啟：

受測人員開啟測試信件並且完成圖片下載之動作，因而被記錄者。

- 圖片下載

連結點選：

受測人員點選測試信件中之連結網址，因而被記錄者。

- 本文連結
- 附件連結

*透過社交工程之測試演練,強化教育單位之網路資安防護能力

電子郵件社交工程的防護

使用者注意事項

- 電子郵件社交工程型攻擊的目的在於誘騙收信者提供個人資料(如：帳號、密碼)，或**引誘收信者透過下載方式來執行以圖片、連結、夾檔所偽裝的惡意軟體**(malware)，讓電腦中毒成為入侵者所控制的殭屍網路電腦(botnet)。

  由於這類的攻擊，如：下載圖片、點選連結，實際惡意軟體的資料是由使用者電腦直接向提供者下載取得，並不會經過郵件伺服器的防毒機制，即使過濾夾檔也有零日病毒(zero-day virus)的問題，在郵件伺服器端僅能過濾已知的病毒，因此，**最佳防範這類社交工程型態攻擊的方法，就是使用者要有資安警覺**，收到電子郵件時，注意下列幾件事：

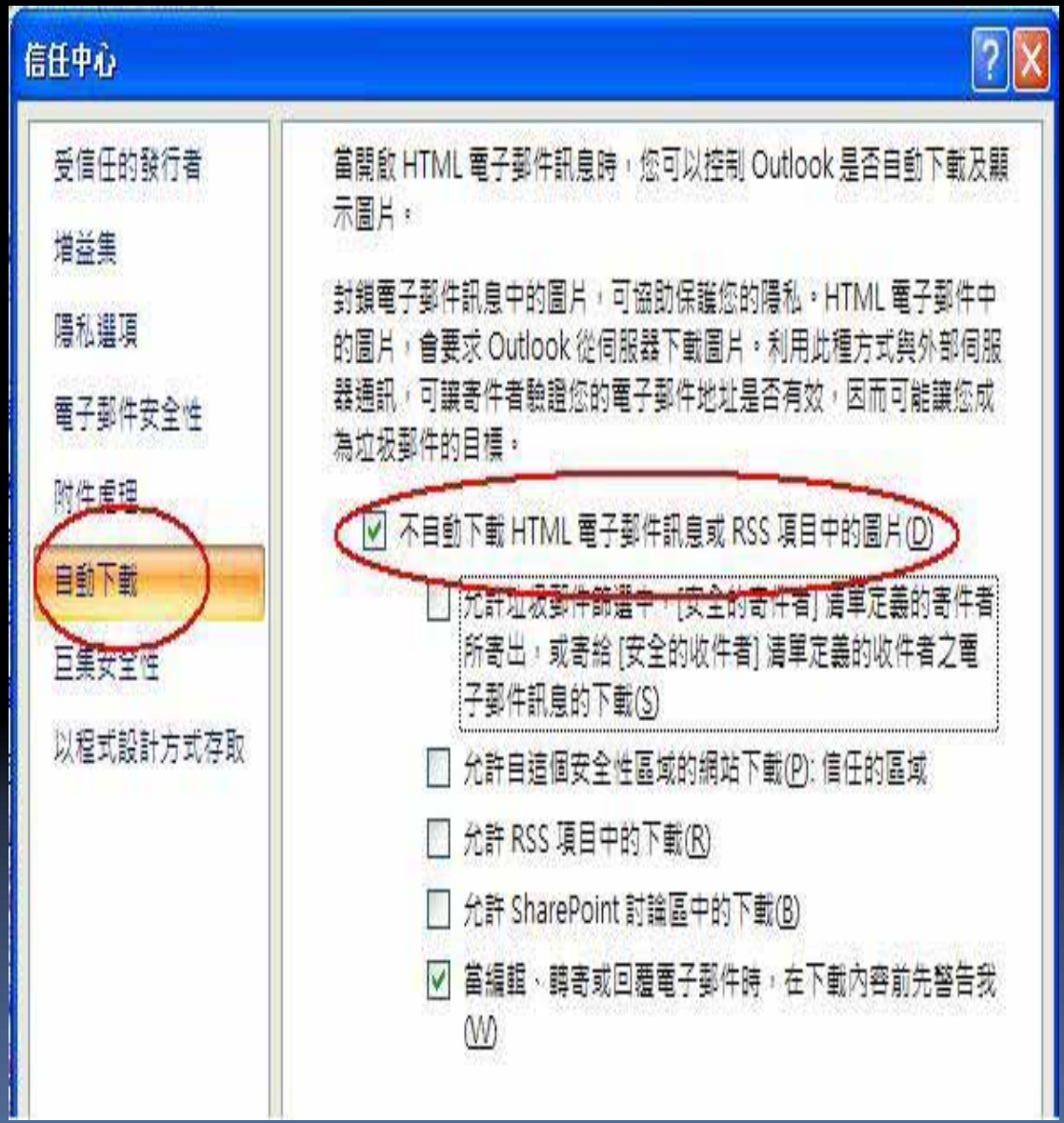
- **不要開啟不明信件**：開啟信件前，務必先檢視寄件者資料，如有疑問，千萬不要開啟。最好**設定郵件軟體安全性為「不要自動下載圖片」**，以免不小心按到開啟信件時，會自動下載到有問題的檔案，而讓電腦產生安全漏洞。
- **不點擊不明信件內的連結。**
- **不開啟不明信件的夾檔。**

電子郵件社交工程的防護措施

- 作業系統/應用軟體更新
- 防毒軟體更新、個人防火牆、端點安全　控制(USB/網路存取/應用程式控制)
- 調整收信軟體的部分設定（outlook 2007、outlook express、live mail）
- 熟悉所使用軟體基本設定及改善使用習慣
- 加強單位DLP(資料遺失保護/硬碟加密)等功能
- 增強閘道網頁安全(Web Security)過濾防護機制
- 採取行為模式分析之垃圾郵件稽核系統,降低收取垃圾郵件所造成之風險

調整收信軟體的設定，提高安全性

- 不自動下載圖檔（強烈建議）
  - outlook2007
  - outlook express
  - live mail
- 關閉信件預覽功能（建議）
  - outlook2007
  - outlook express
  - live mail
- 以純文字開啟信件（建議）
  - outlook2007
  - outlook express
  - live mail
- Web mail及Mail 2000之郵件設定注意事項



不自動下載圖檔 Outlook 2007

開啟outlook 2007

選取【工具】

選取【信任中心】

選擇【自動下載】

將【不自動下載HTML電子郵件訊息或RSS項目中的圖片】打勾

不自動下載圖檔

Outlook express

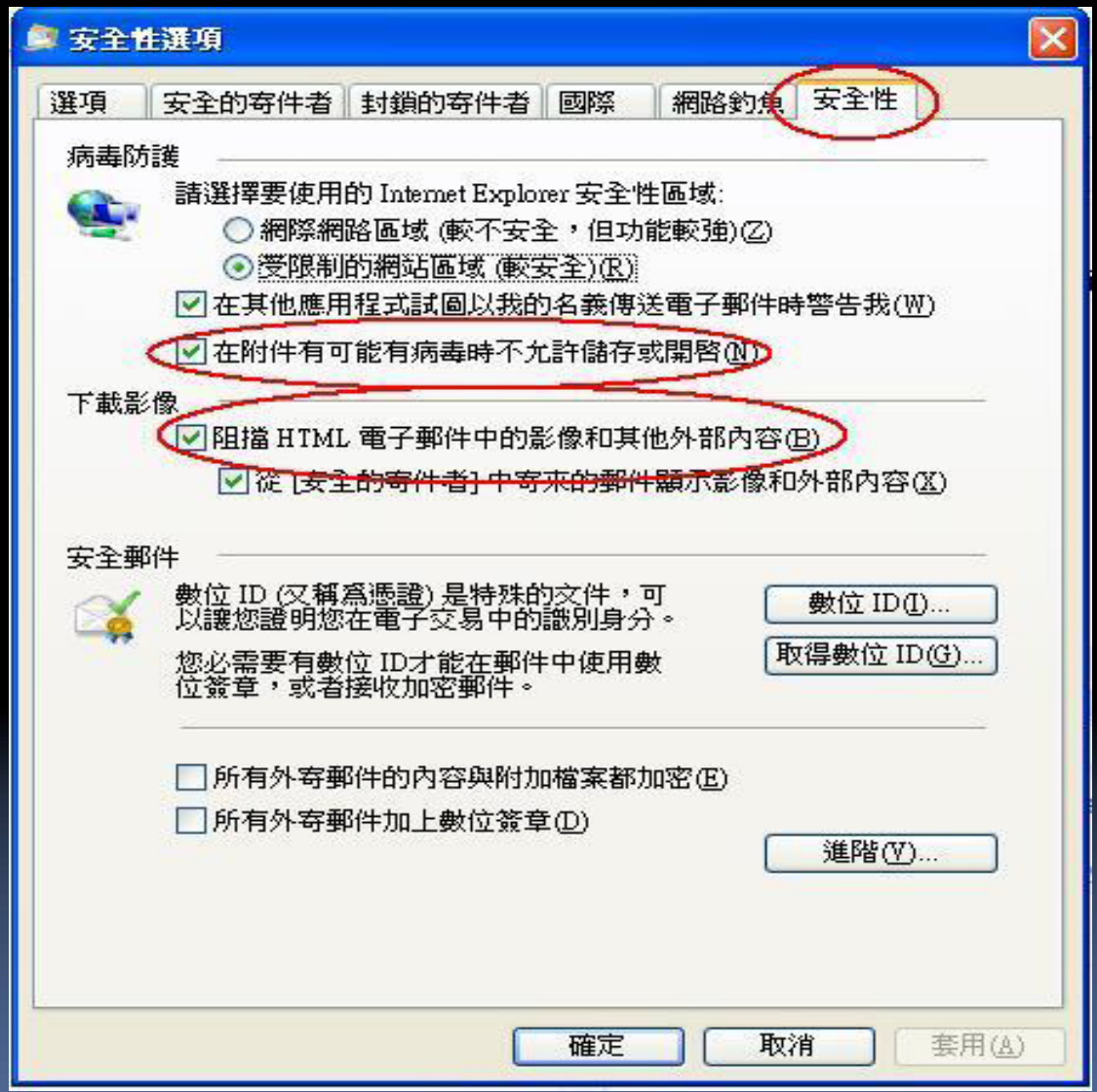
開啟outlook express

選取【工具】

選取【選項】

選取【安全性】

將【阻擋HTML電子郵件中的圖片和其他外部內容】打勾



不自動下載圖檔 live mail

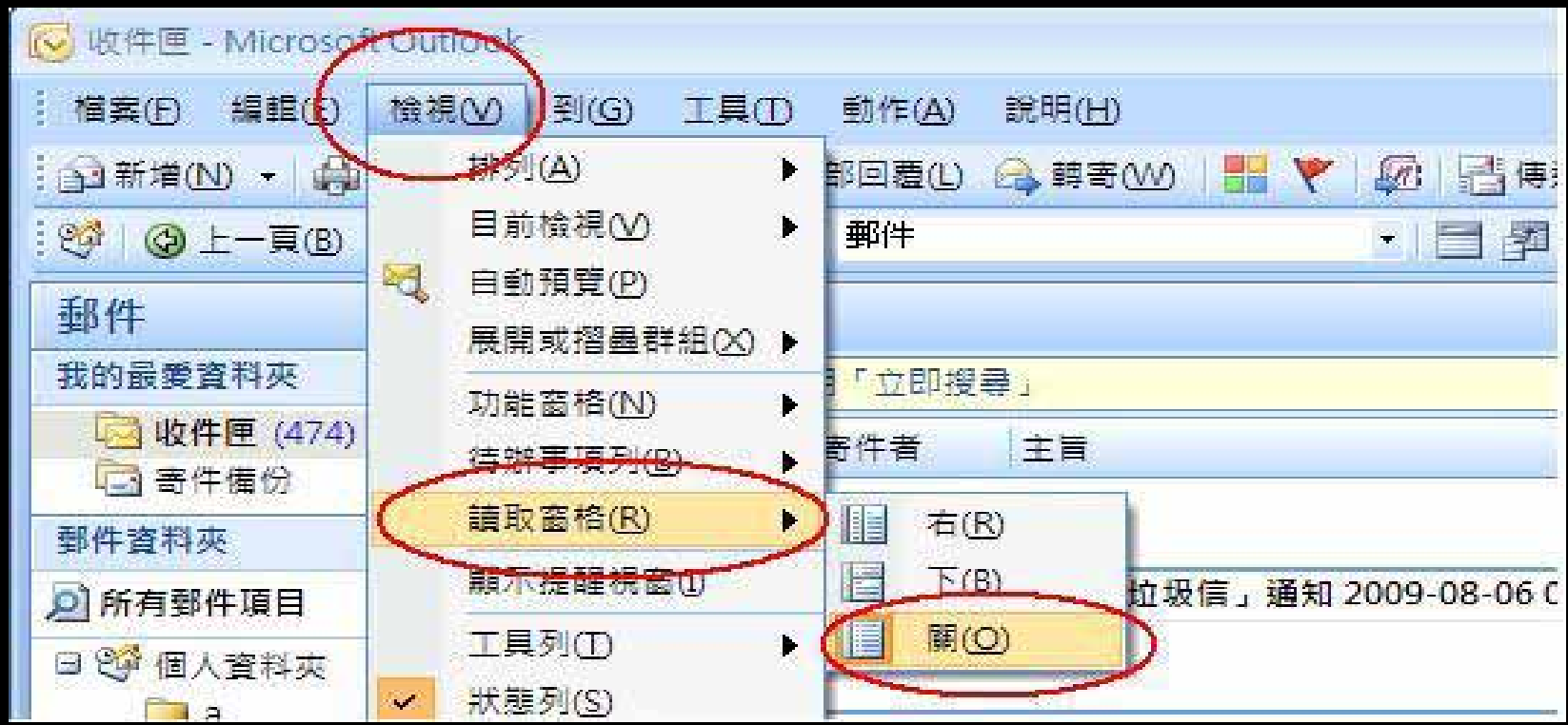
開啟live mail

選取【工具】

選取【安全性選項】

選取【安全性】

將【阻擋HTML電子郵件中的圖片和其他外部內容】打勾

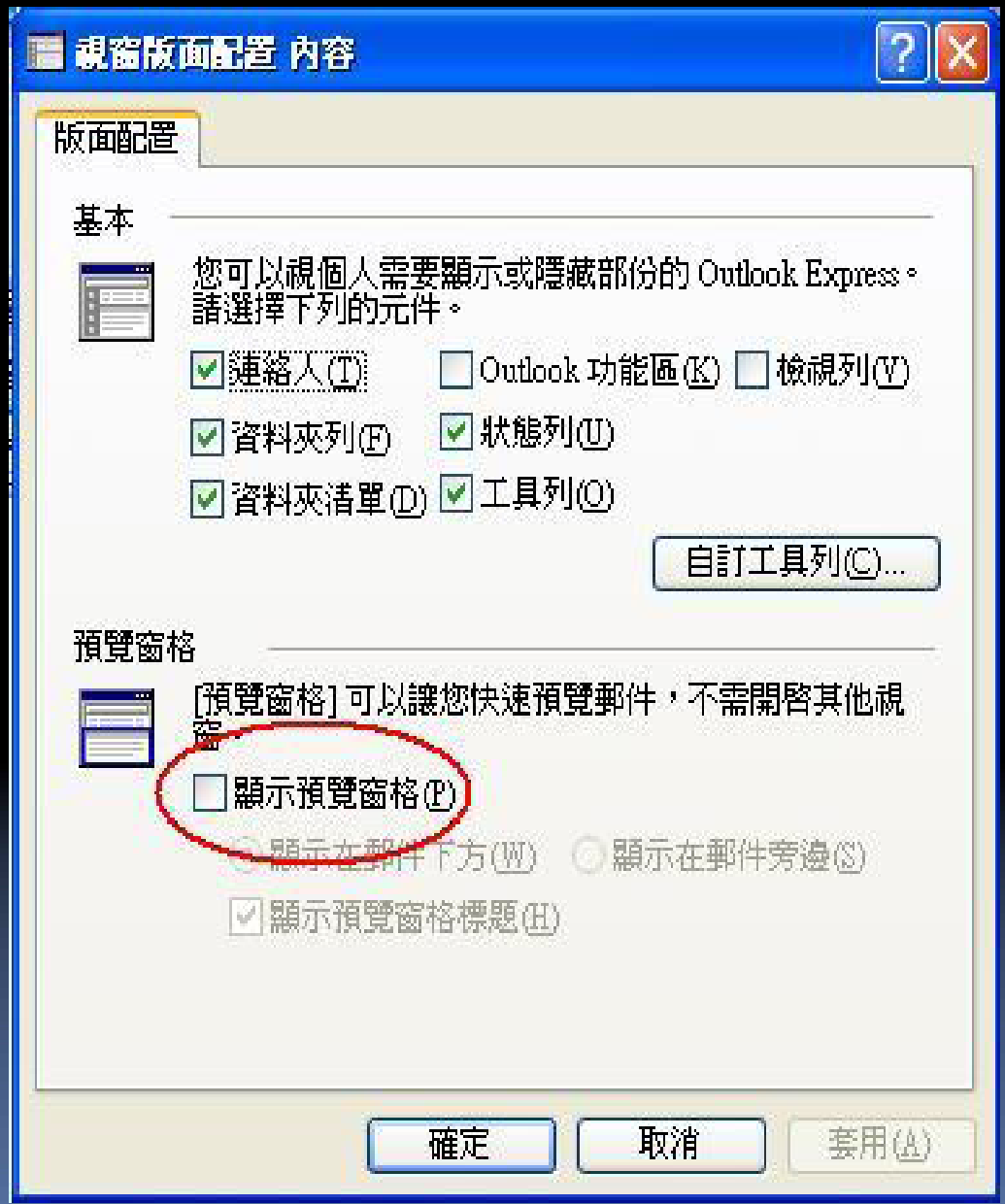


關閉信件預覽outlook 2007

開啟outlook 2007

選取【檢視】

選取【讀取窗格】



關閉信件預覽

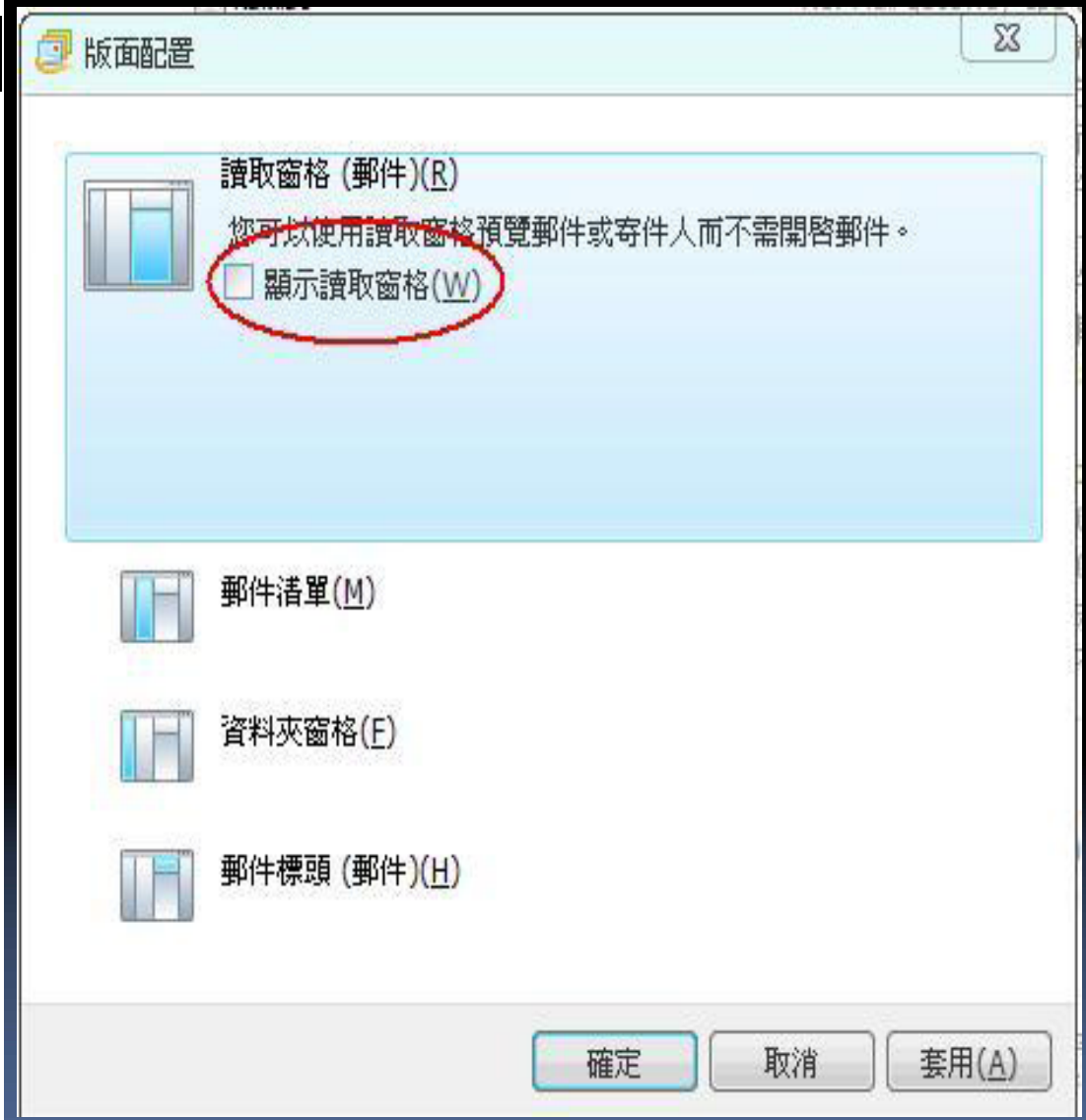
Outlook express

開啟outlook express

選取【檢視】

選取【版面配置】

【顯示預覽窗格】不打勾



關閉信件預覽

live mail

開啟live mail

選取【檢視】

選取【版面配置】

【顯示預覽窗格】不打勾

以純文字開啟信件 Outlook 2007

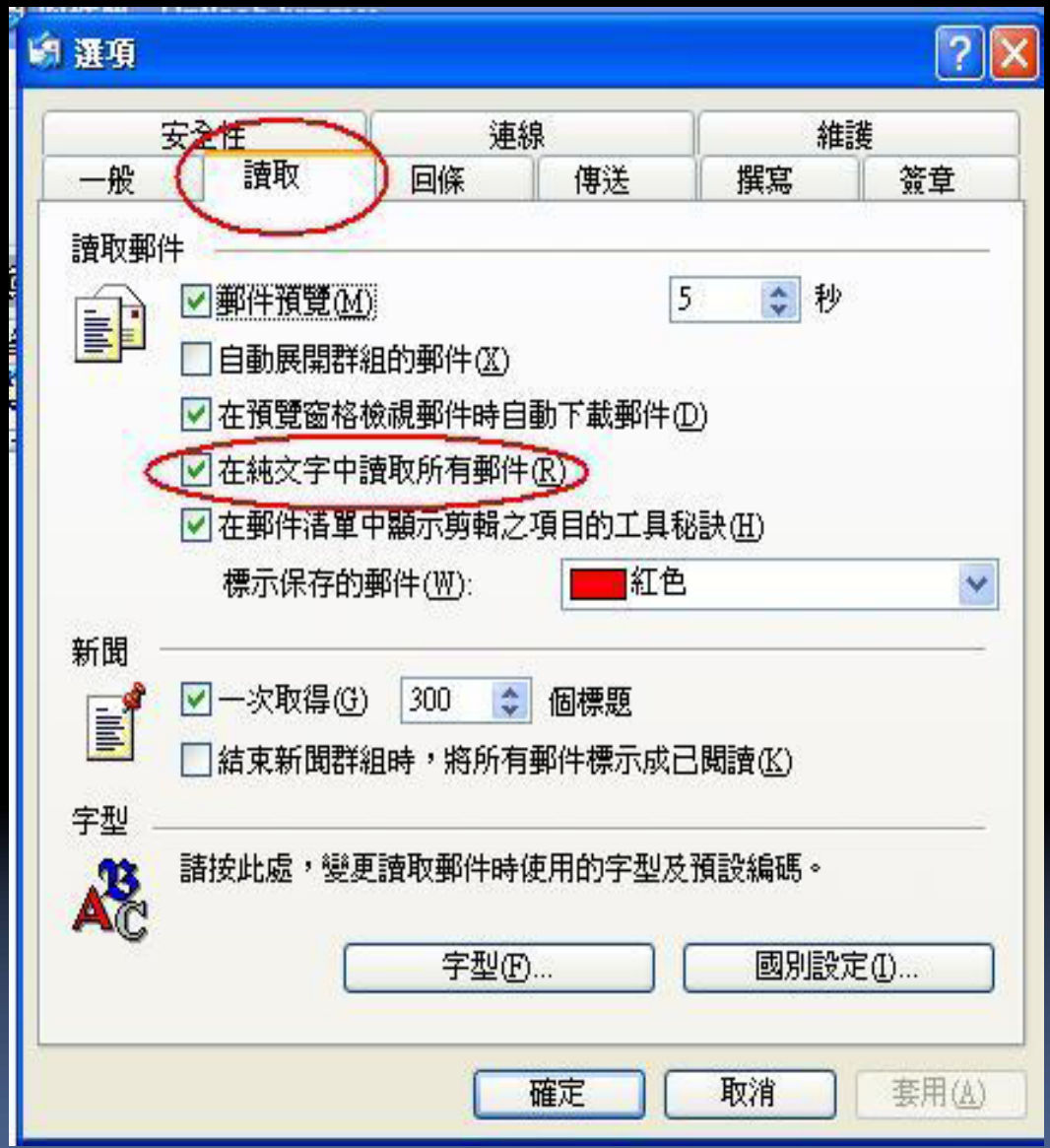
開啟outlook 2007

選取【工具】

選取【信任中心】

選擇【電子郵件安全性】

將【以純文字讀取所有標準郵件】打勾



以純文字開啟信件

Outlook express

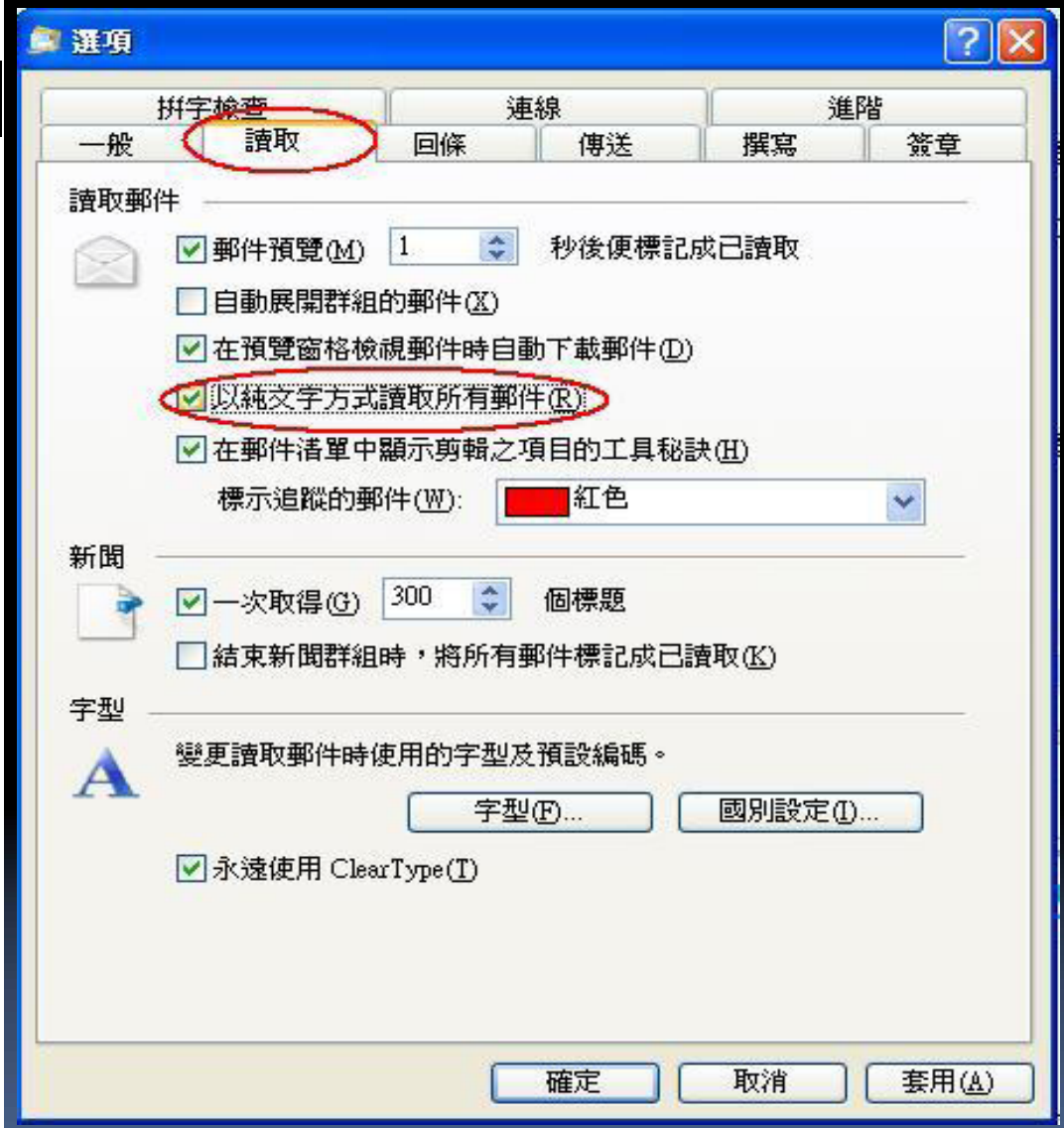
開啟outlook express

選取【工具】

選取【選項】

選取【讀取】

將【在純文字中讀取所有郵件】打勾



以純文字開啟信件 live mail

開啟live mail

選取【工具】

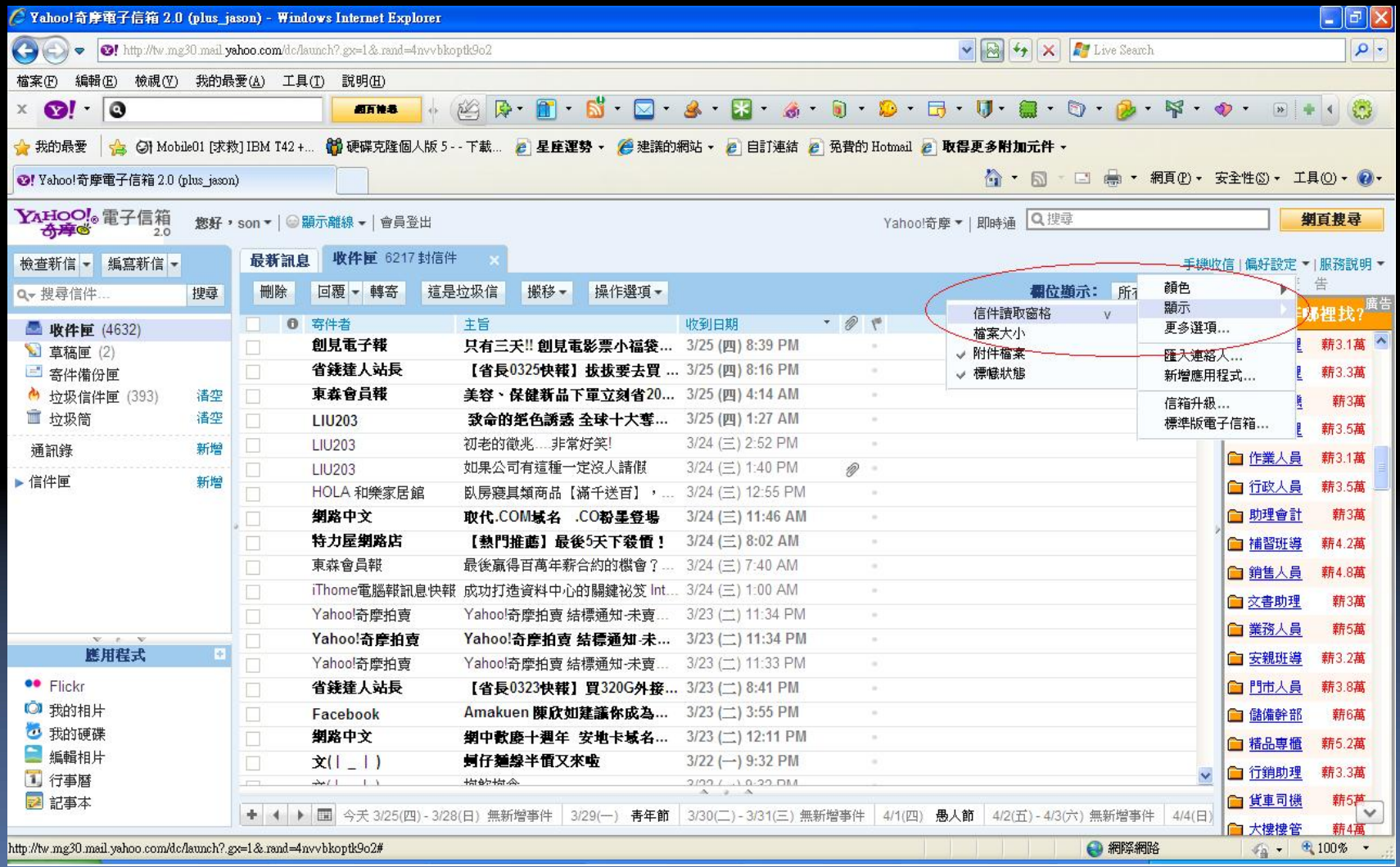
選取【選項】

選取【讀取】

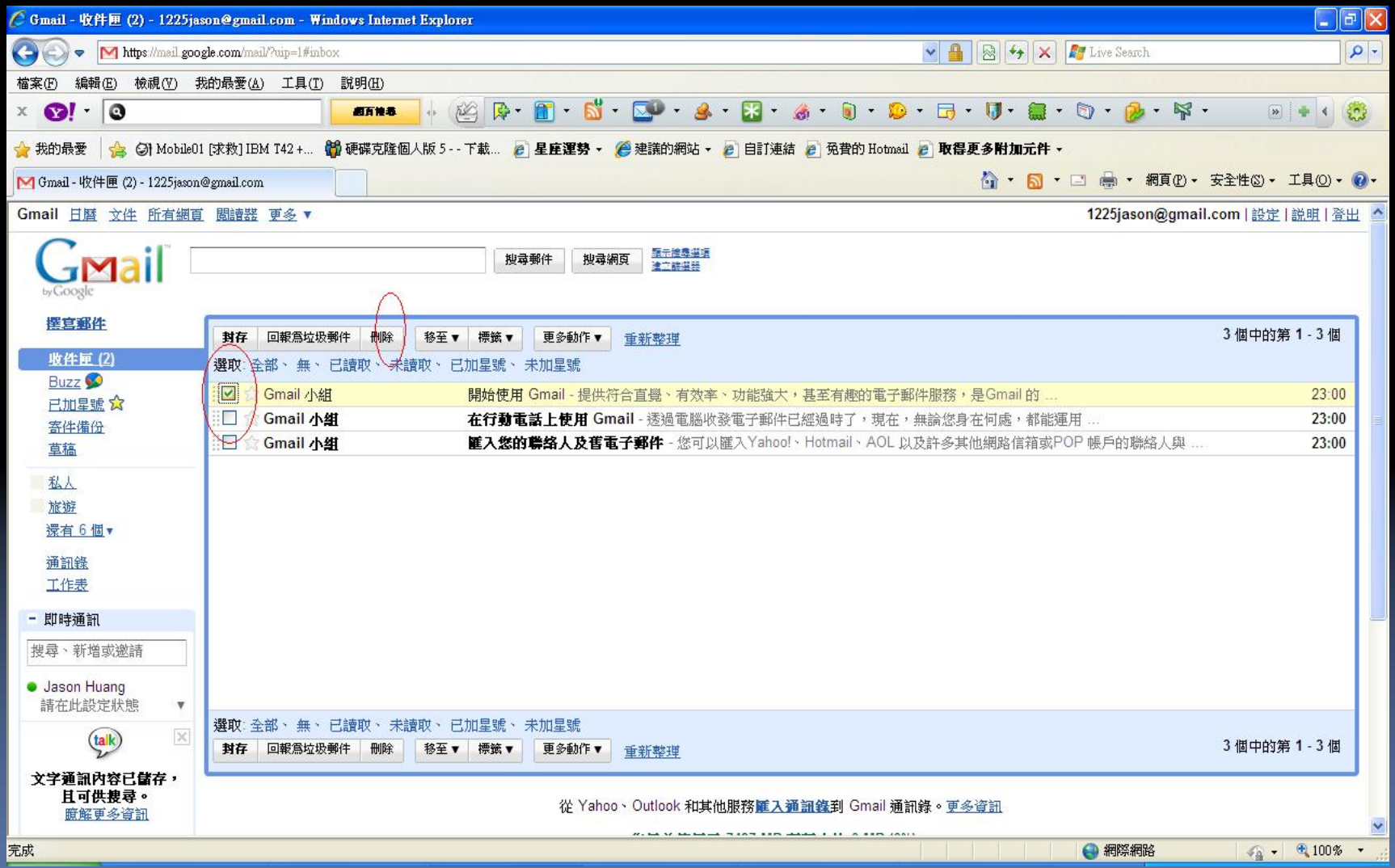
將【在純文字中讀取所有郵件】打勾

Web mail及Mail 2000
之郵件設定注意事項

Yahoo mail

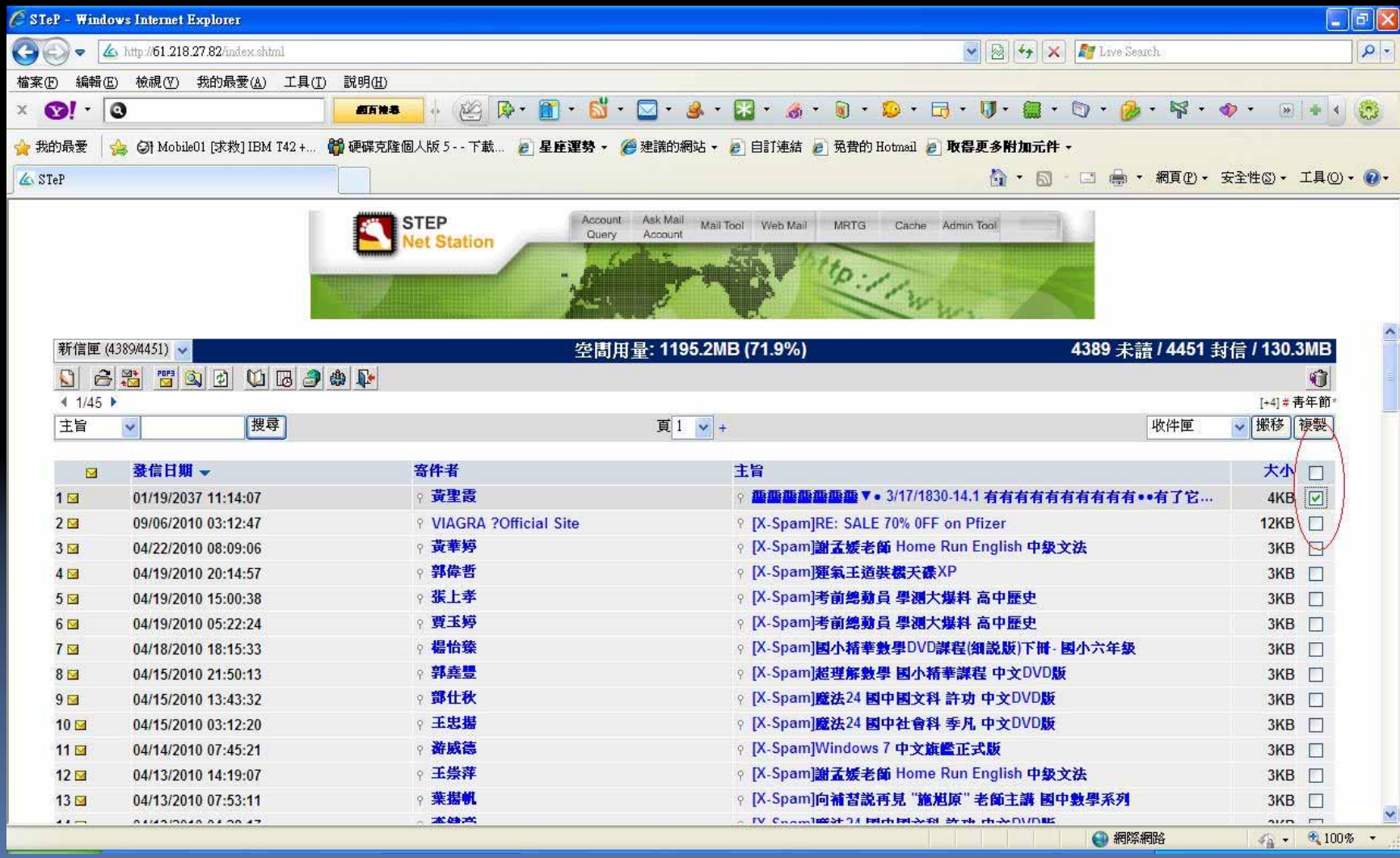

Yahoo!奇摩電子信箱 2.0 (plus_jason) - Windows Internet Explorer
收件匣 (4632)
草稿匣 (2)
寄件備份匣
垃圾信件匣 (393)
垃圾筒
通訊錄
信件匣
應用程式
Flickr
我的相片
我的硬碟
編輯相片
行事曆
記事本
最新訊息
收件匣 6217 封信件
刪除
回覆
轉寄
這是垃圾信
搬移
操作選項
寄件者
主旨
收到日期
創見電子報 只有三天!! 創見電影票小福袋... 3/25 (四) 8:39 PM
省錢達人站長 【省長0325快報】 扳扳要去買 ... 3/25 (四) 8:16 PM
東森會員報 美容、保健新品下單立刻省20... 3/25 (四) 4:14 AM
LIU203 致命的絕色誘惑 全球十大奪... 3/25 (四) 1:27 AM
LIU203 初老的徵兆....非常好笑! 3/24 (三) 2:52 PM
LIU203 如果公司有這種一定沒人請假 3/24 (三) 1:40 PM
HOLA 和樂家居館 臥房寢具類商品【滿千送百】，... 3/24 (三) 12:55 PM
網路中文 取代.COM域名 .CO粉墨登場 3/24 (三) 11:46 AM
特力屋網路店 【熱門推薦】最後5天下殺價！ 3/24 (三) 8:02 AM
東森會員報 最後贏得百萬年薪合約的機會？... 3/24 (三) 7:40 AM
iThome電腦報訊息快報 成功打造資料中心的關鍵祕笈 Int... 3/24 (三) 1:00 AM
Yahoo!奇摩拍賣 Yahoo!奇摩拍賣 結標通知-未賣... 3/23 (二) 11:34 PM
Yahoo!奇摩拍賣 Yahoo!奇摩拍賣 結標通知-未... 3/23 (二) 11:34 PM
Yahoo!奇摩拍賣 Yahoo!奇摩拍賣 結標通知-未賣... 3/23 (二) 11:33 PM
省錢達人站長 【省長0323快報】 買320G外接... 3/23 (二) 8:41 PM
Facebook Amakuen 陳欣如建議你成為... 3/23 (二) 3:55 PM
網路中文 網中歡慶十週年 安地卡域名... 3/23 (二) 12:11 PM
文(|_|) 阿仔麵線半價又來啦 3/22 (一) 9:32 PM
欄位顯示:
信件讀取窗格
檔案大小
附件檔案
標幟狀態
顏色
顯示
更多選項...
匯入連絡人...
新增應用程式...
信箱升級...
標準版電子信箱...
作業人員 薪3.1萬
行政人員 薪3.5萬
助理會計 薪3萬
補習班導 薪4.2萬
銷售人員 薪4.8萬
文書助理 薪3萬
業務人員 薪5萬
安親班導 薪3.2萬
門市人員 薪3.8萬
儲備幹部 薪6萬
精品專櫃 薪5.2萬
行銷助理 薪3.3萬
貨車司機 薪5萬
大樓樓管 薪4萬

Google mail-1

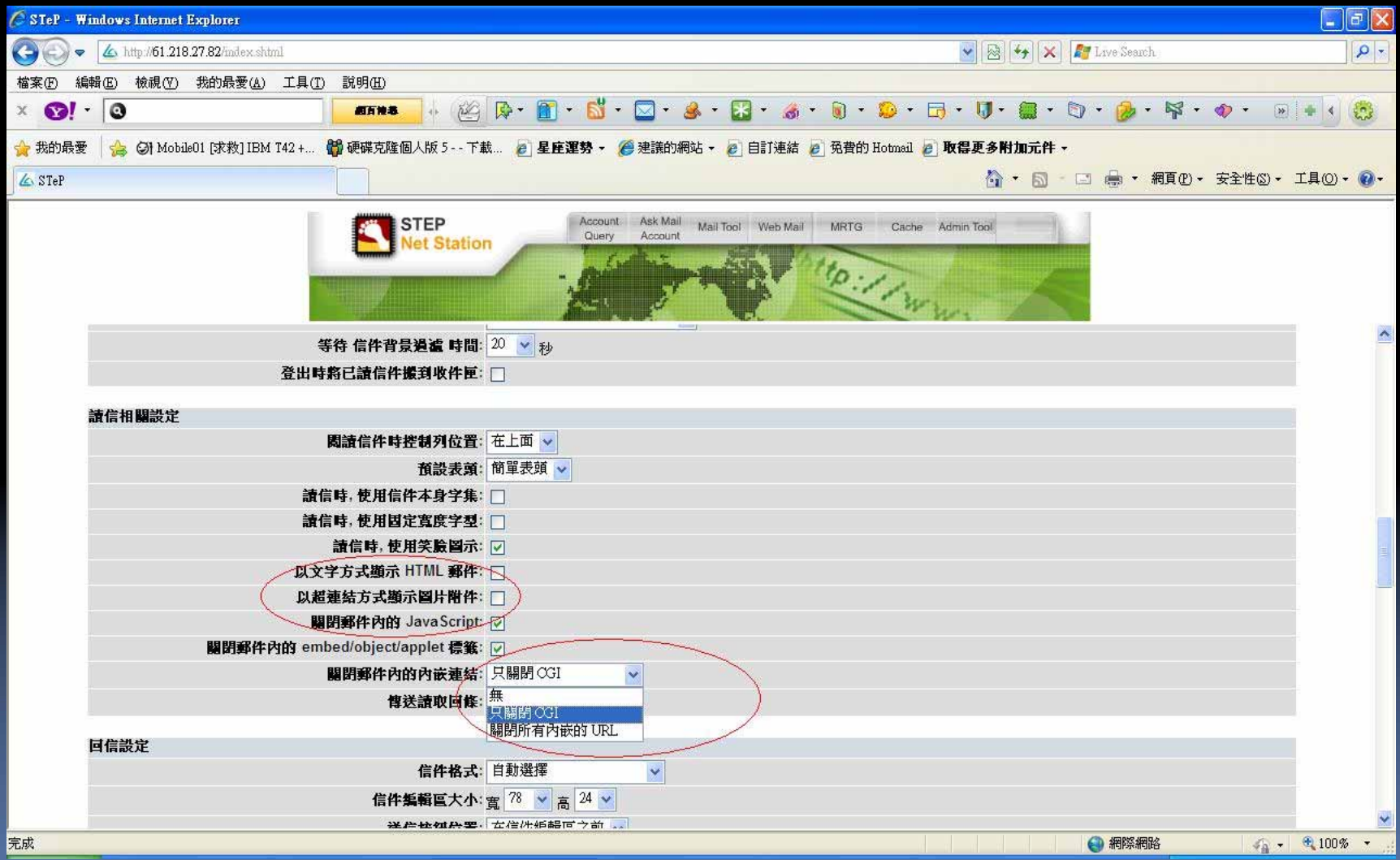


Google mail-2

OPEN Webmail-1



OPEN Webmail-2



如何預防垃圾郵件的打擾呢？

- 1. 自訂過濾規則：例如 Mail2000 可以讓使用者可以針對特定的信件欄位，像寄件人、標題、信件大小等等，再選擇符合條件郵件的處理方式。例如：如果「標題」「包含」「廣告」，則將此信件「刪除」如果「寄件人」「包含」「@openfind.com.tw」，則將此信件「放入收信匣」 Outlook 或 Outlook Express 也提供使用者類似的過濾功能。

- 2. 自訂黑、白名單：與之前提到ISP訂定的黑、白名單方法類似，讓使用者自行決定信件來源是否為垃圾郵件。例如 Mail2000 提供使用者自行建立「合法收、寄件人」以及排外名單的功能，再配合廣告信件匣搭配使用，就可以排除相當程度的垃圾郵件騷擾，而微軟的Exchange 2003 + Outlook 2003 也有類似的功能。

- 3. 慎用自動回覆功能：許多電子郵件服務提供商提供了很方便的「自動回覆」的功能，但鑒於垃圾郵件問題的日益嚴重，在使用上應該更加謹慎小心。因為許多垃圾郵件程序都利用了這一功能，在隨機測試寄送過程中，會有目的地搜索收集自動回覆郵件的有效email地址，然後建立email名單，以便進一步騷擾使用者。

如何預防垃圾郵件的打擾呢？--續

- 4. 不隨意回應垃圾郵件：不回應任何來歷不明的垃圾郵件，即使是修改或取消訂閱，絕對不可回覆，對此類郵件也不要簽收回條，否則等於在提示垃圾郵件發送者，您的信箱地址有效。

- 5. 對於在網路上的個人資料更謹慎：不隨便在公開的網路上留下自己的email地址，在填寫一些網站註冊的資料時要特別注意，要勾選不要洩漏email地址給別家廠商的選項，並且避免訂閱一些不熟悉的網站電子報。

- 6. 使用多重email帳號：在不熟悉的網站註冊時，最好使用無關緊要的email帳號。

- 7. 申請email帳號時，勿設定常見、簡短或有意義的英文單字組合：現在有許多有心人士會為了收集email名單，會選擇某些特定網域名稱，再以隨機的亂數法則組合產生數以百萬計可能的email帳號。例如：使用常見英文名字、簡短或有意義的單字，再將不同的網域名稱加上去。之後利用發信程式大量寄發垃圾郵件。因此，建議個人的email帳號避免設定過於容易被猜測到的組合。以這種方式寄發的垃圾郵件裡可能會藏有收集名單的陷阱，例如告訴收件者去取消訂閱、回覆信件、開啟附檔或點選連結等，其實是藉此確認並收集有效的email。

Mail2000 設定個人使用環境

- **如何設定個人使用環境？**

由於每個人希望信箱使用環境顯示或瀏覽的方式有不同的需求，故本系統提供此功能選項，讓您設定最舒適的個人使用環境。

1. 點選左側的目錄選單的「個人設定」選項，選擇「個人化設定」的「使用環境」進入使用環境設定頁面。

2. 選擇欲調整個人化設定項目，進行調整，調整完成後，選取〔確定〕按鈕。

Mail2000 設定外部圖檔封鎖-1

如何設定外部圖檔封鎖？

廣告信或不明來源的郵件，除了造成閱覽與整理信件的困擾外，其中所附加連結的圖檔，可能暗藏了病毒或者利用您開啓圖片的當時，確認了您信箱的有效性，繼而廣佈地寄送廣告信給您。

爲了保護您的隱私權不受垃圾郵件業者的侵犯，並避免開啓廣告郵件時觸目所及的盡是色情、暴力或血腥等不雅的圖片所帶來的不適感與尷尬。本系統提供了封鎖圖像的保護措施。 被封鎖的圖像會以灰色背景填滿原先圖片顯示的位置，除了給您一個清爽的看信環境外，更多了一層安全的保障。

1. 從左側功能選單中，點選「個人化設定」→「使用環境」→「封鎖外部圖檔」。
2. 您可以選擇封鎖的型態（全部／只封鎖廣告信匣／不封鎖）。
3. 此外，您更可以彈性的選擇（已讀信件不封鎖/好友信件不封鎖）。此一進階功能，可以幫助您封鎖住來信的外部圖檔，但已讀過與來自通訊錄的寄件人之來信將不會被封鎖的便利性。

祕訣

1. 點選「全部封鎖」：本系統將爲您封鎖全部信件匣的圖片。
2. 點選「只封鎖廣告信匣」：本系統只爲您封鎖廣告信匣裡的圖片。
3. 點選「不封鎖」：不封鎖任何信匣中的任何圖片。

Mail2000 設定外部圖檔封鎖-2

Mail2000 如何檢舉廣告信

- **如何檢舉廣告信？**

1. 請先勾選所要檢舉的信件。
2. 接著點選「廣告信」選單的→「廣告信檢舉」。
3. 點選後，系統會詢問您是否確定要檢舉這封信件爲廣告信，請按〔確定〕。
4. 檢舉動作完成後，系統會自動幫您將廣告信以代轉的方式寄給系統管理者，接著再詢問您是否要在檢舉之後順便 刪除這封廣告信。

Mail2000 如何設定排外名單

- **如何設定排外名單？**

1. 請先勾選所要檢舉的信件。
2. 接著點選「廣告信」選單的→「加入排外名單」。
3. 點選後，系統會自動列出欲拒絕的選項。

請注意： 加入 IP 會拒絕所有由該 IP 寄出或轉送信件，可能造成無法收信。 請務必確認該 IP 爲欲拒絕主機再加入。

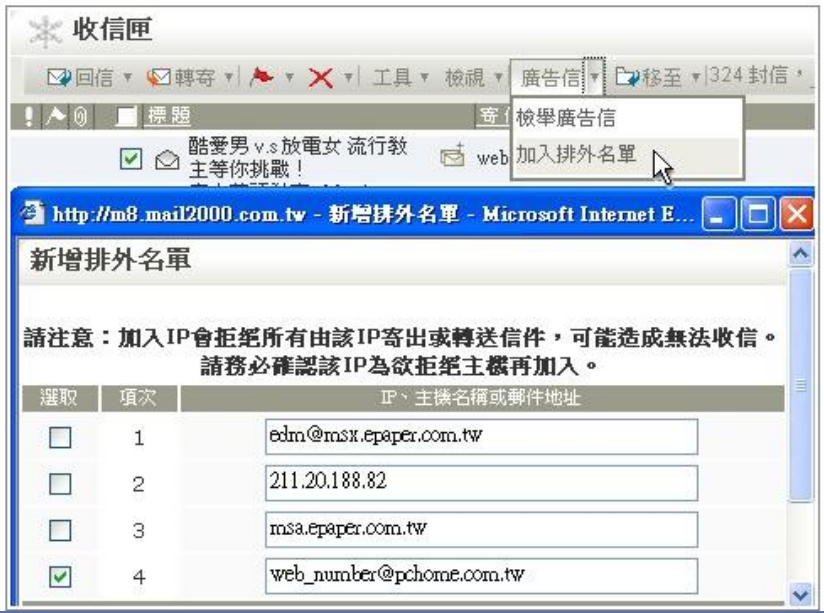
4. 選取確認要加入排外的項目後，再按〔確定〕即可。

5. 此設定支援萬用符號，若您確定要擋住某個 domain 可輸入：

*@aaa.com 或

*aaa.com 或

@.aaa.com



Mail2000 如何設定合法寄件人名

- **如何設定合法寄件人名單？**

為了避免漏接重要來信或訂閱的電子報，建議您將常往來的寄件者加入通訊錄並設定為合法寄件人。如果，因未加入通訊錄而被系統過濾至廣告信匣，請您將該信加入合法寄件人名單中，日後相同來源的信件便不會再被過濾到廣告信匣中了。

1. 先選取要加入的信件，接著進入「工具」→點選「加入合法寄件人」。

2. 選取要新增的IP、主機名稱或郵件地址，再按〔確定〕即可完成設定動作。

Mail2000 如何設定合法收件人名單-1

- **如何設定合法收件人名單？**

當您利用本系統收取外部郵件時，系統同時會檢查該封信件的收信人是否為目前系統的帳號，為了避免外部郵件、設定群組或設定自動轉寄郵件，被系統誤判而過濾至廣告信匣。建議您將外部郵件帳號、群組帳號或設定自動轉寄帳號加入合法收件人名單中，日後再收到相同來源的信件時就不會再被誤判而過濾到廣告信匣中了。

舉例說明：目前系統的帳號為 adm@openfind.com.tw，有設定外部信箱為 adm@pchome.com.tw，另外也會寄給mis@openfind.com.tw 也會自動轉寄過去。建議您將 adm@pchome.com.tw 及 mis@openfind.com.tw 加入合法收件人，以避免信件被誤判而過濾至廣告信匣。

1. 點選左側功能選單→「個人設定」→「廣告信管理」→「合法收件人」。

2. 在這裡能檢視全部的名單，您可視需要進行名單的新增、修改與刪除。

Mail2000 如何設定合法收件人名單-2

Mail2000 如何設定廣告信過濾等級

如何設定廣告信過濾等級？

廣告信過濾等級設定的邏輯正好與排外名單相反。過濾等級設定，係指限定通關者的身份，凡符合者才予放行，否則將視爲垃圾信。把關的標準由使用者自行設定分爲：關閉、低、中、高四個等級。

1. 關閉：不針對信件的寄收件人進行過濾。

2. 低：系統會自動判斷該信件中是否有包含寄件人或收件人，若無，則該封信件會被視爲垃圾郵件。

3. 中：系統會將來自通訊錄聯絡人及合法寄、收件人的信件放在收信匣中，另外也會將指定收信人是「您」的信件放在放信匣中，即使寄件人不在您的通訊錄或合法寄收件人名單裡，您也會收到該封信件。

4. 高：系統只會將通訊錄聯絡人及合法寄、收件人的信件放在收信匣中，其餘信件會被視爲垃圾郵件。

秘訣

除了加入排外名單、加入合法／收件人、調整廣告信管理等級之外，還可以透過關鍵字的設定，來過濾廣告信。

您可以 將含有特定的關鍵字的來信，如"免費"、"月入百萬" 等語詞指定過濾到回收筒裡。此功能的詳細設定操作，請參考「個人設定」→「信件過濾」。

Mail2000 刪除郵件

- **如何搬移信件？**

利用信件搬移功能，您可以將不同屬性的信件收藏在不同的信匣中，讓您更能系統化的讀信與快速取閱信函。

1. 在信件列表的頁面中，在需要搬移的信件標題前之空格內打勾。

2. 點選功能列的「移至」選項，並於選單中選擇要搬移到的信件匣名稱。

3. 直接點選目的信匣名稱，該信件即搬移至指定信件匣中。

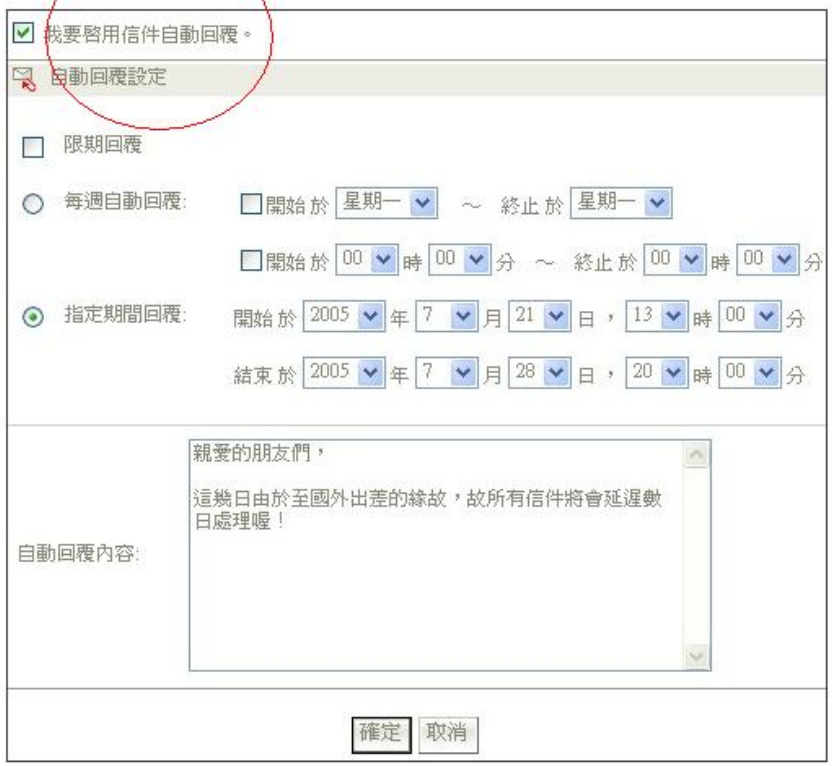
Mail2000 取消設定郵件自動回覆

- **如何設定郵件自動回覆？**

若您因出國旅遊或出差洽工，因而未能及時處理收發郵件時，您可於這段期間啓用「自動回覆」功能，提醒告知您的朋友或廠商，此郵件將會延遲數日才會處理，讓他們放心。

1. 點選左側目錄選單的「個人設定」選項，選擇「信件處理」的「自動回覆」進入信件自動回覆設定頁面。

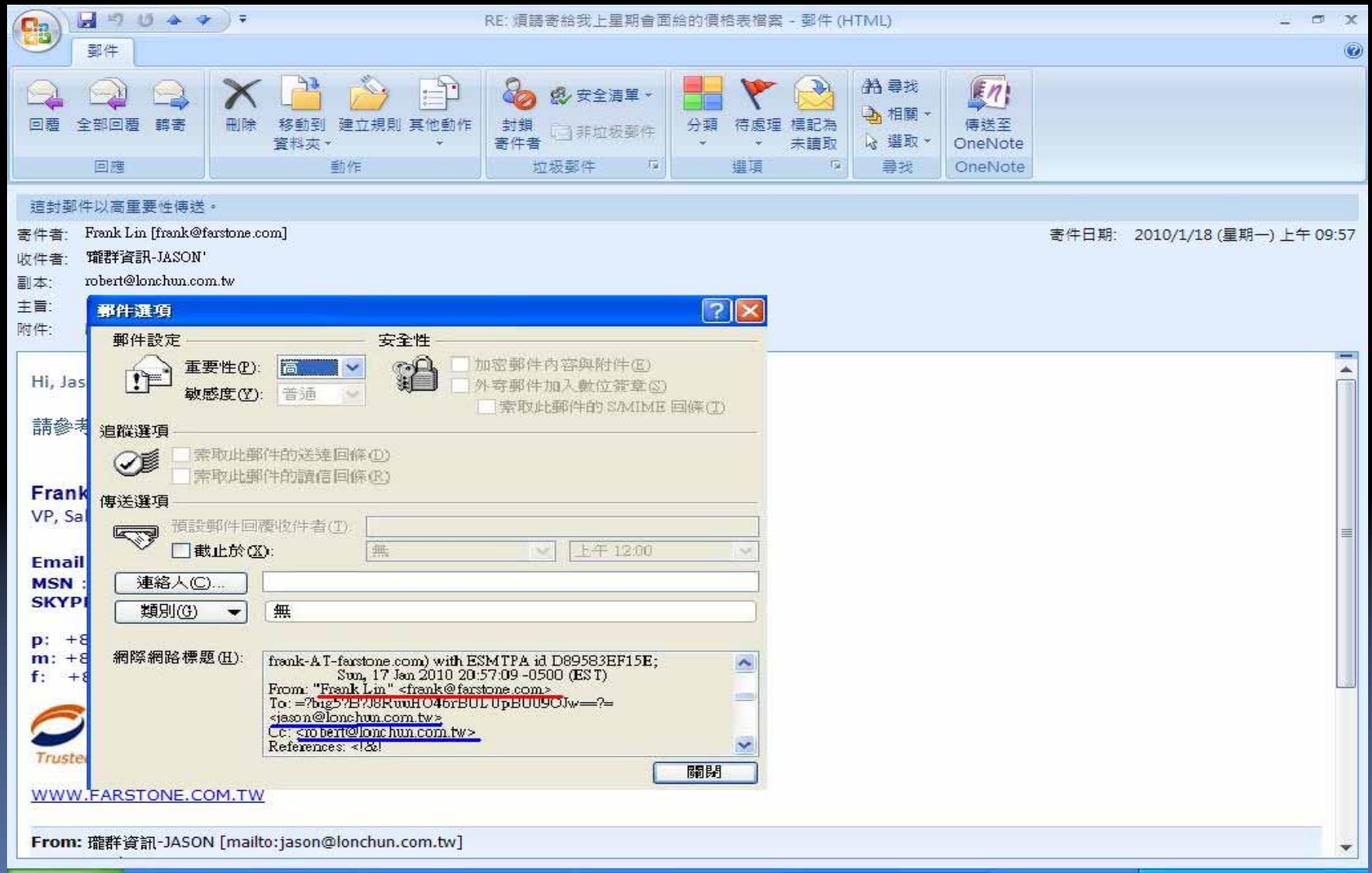
2. 選點〔我要啓用信件自動回覆〕功能，進行回覆時間設定及內容編輯。



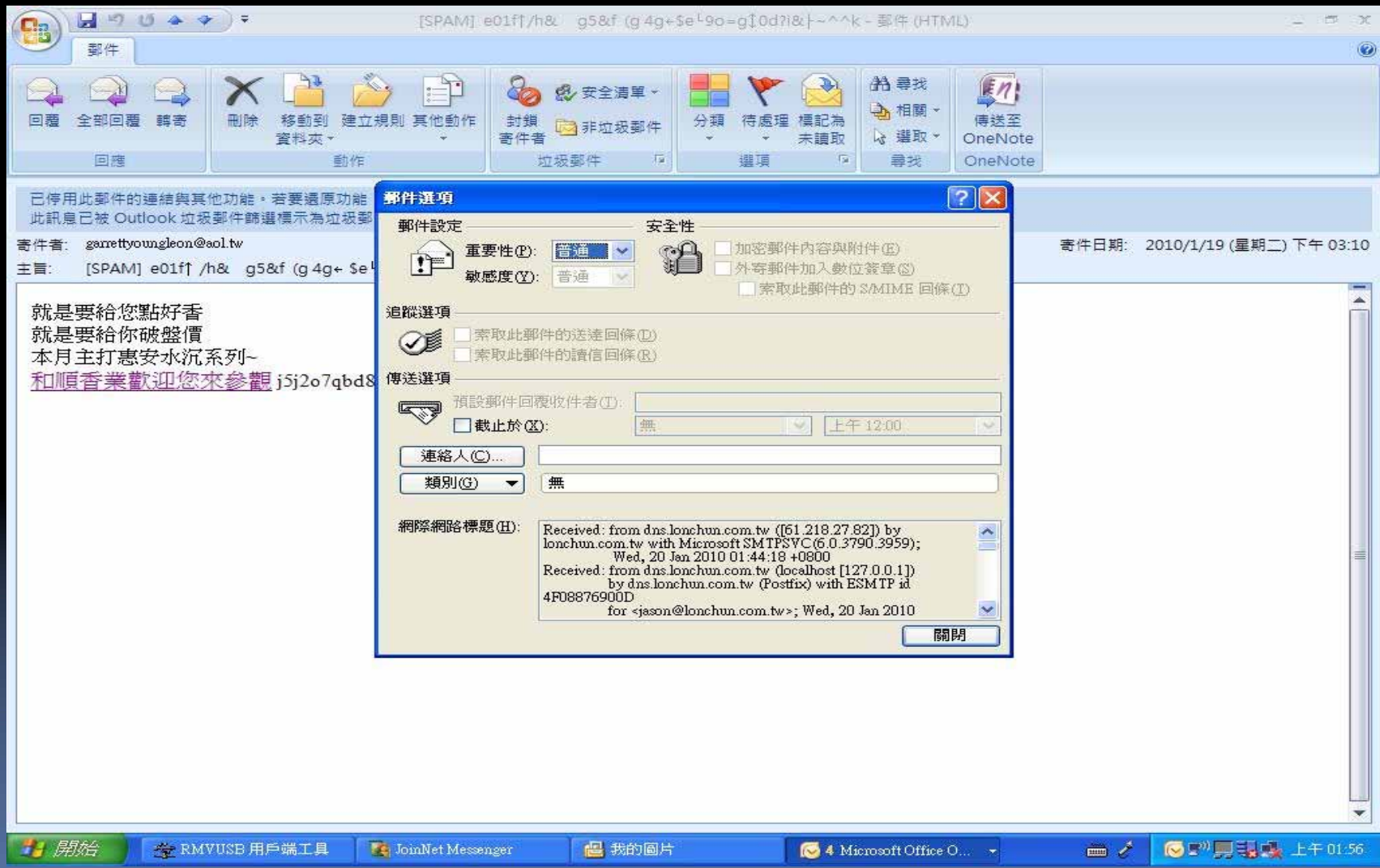
改變使用電子郵件的習慣

- 查明信件的來源
- 信件可由mail header查出所經的伺服器及收發信件者
- 釐清寄件者身分(避免開啟偽冒之信件)
- 若收到可疑信件,以電話向寄件者確認(避免誤觸惡意郵件)
- 郵件驗證機制(收發信採驗證方式或Domain KEY)
- 附件加密(避免誤寄或誤開啟惡意附件)

Mail header


RE: 煩請寄給我上星期會面給的價格表檔案 - 郵件 (HTML)
郵件
回覆
全部回覆
轉寄
刪除
移動到資料夾
建立規則
其他動作
封鎖寄件者
安全清單
非垃圾郵件
分類
待處理
標記為未讀取
尋找
相關
選取
傳送至OneNote
回應
動作
垃圾郵件
選項
尋找
OneNote
這封郵件以高重要性傳送。
寄件者: Frank Lin [frank@farstone.com]
寄件日期: 2010/1/18 (星期一) 上午 09:57
收件者: '瓏群資訊-JASON'
副本: robert@lonchun.com.tw
主旨:
附件:
郵件選項
郵件設定
重要性(P):
敏感度(Y):
普通
安全性
加密郵件內容與附件(E)
外寄郵件加入數位簽章(S)
索取此郵件的 S/MIME 回條(T)
追蹤選項
索取此郵件的送達回條(D)
索取此郵件的讀信回條(R)
傳送選項
預設郵件回覆收件者(T)
截止於(X):
無
上午 12:00
連絡人(C)...
類別(G)
無
網際網路標題(H):
frank-AT-farstone.com) with ESMTPA id D89583EF15E;
Sun, 17 Jan 2010 20:57:09 -0500 (EST)
From: "Frank Lin" <frank@farstone.com>
To: =?big5?B?J8RuuHO46rBUL0pBU09OJw==?=
<jason@lonchun.com.tw>
Cc: <robert@lonchun.com.tw>
References: <!&!
關閉
WWW.FARSTONE.COM.TW
From: 瓏群資訊-JASON [mailto:jason@lonchun.com.tw]

所經的伺服器資料


郵件選項
郵件設定
重要性(P):
普通
敏感度(Y):
普通
安全性
追蹤選項
傳送選項
連絡人(C)...
類別(G)
無
網際網路標題(H):
Received: from dns.lonchun.com.tw ([61.218.27.82]) by lonchun.com.tw with Microsoft SMTPSVC(6.0.3790.3959); Wed, 20 Jan 2010 01:44:18 +0800
Received: from dns.lonchun.com.tw (localhost [127.0.0.1]) by dns.lonchun.com.tw (Postfix) with ESMTP id 4F08876900D for <jason@lonchun.com.tw>; Wed, 20 Jan 2010
關閉
寄件者: garrettyoungleon@aol.tw
主旨: [SPAM] e01f† /h& g5&f (g 4g← $e
寄件日期: 2010/1/19 (星期二) 下午 03:10
就是要給您點好香
就是要給你破盤價
本月主打惠安水沉系列~
和順香業歡迎您來參觀 j5j2o7qbd8
開始
RMVUSB 用戶端工具
JoinNet Messenger
我的圖片
4 Microsoft Office O...
上午 01:56

了解

資訊安全概念—學習保護自己

了解

資訊安全概念—學習保護自己

- 保護自己不受網路詐騙之害
- 保護個人及電腦
- 防阻垃圾郵件
- 保護電腦免受病毒/蠕蟲或間諜程式的侵擾
- 讓電腦保持最新狀態

*以上相關資料參考節錄自臺灣微軟官方網站

保護自己不受網路詐騙之害

- 新型態的垃圾郵件，它們不僅是多餘且惱人的信件，這種新式垃圾郵件還可能會導致您的資料遭到竊取。點選假冒的網站連結將導致線上資料被竊取

- **什麼是網路詐騙？**

  網路詐騙是一種詐騙手法，目的在竊取您的身分資訊。在網路詐騙的詭計中，詐騙者會試圖以欺詐手段獲得您的信任，以取得您的個人資料（像是信用卡號碼、密碼、帳戶資料或其他資訊）。詐騙詭計可能由詐騙者親自進行、透過電話，或透過垃圾郵件或快顯視窗於線上進行。

- 釣魚的方式之一，就是使用誘餌。 在網站上詐騙的線上竊賊也會使用誘餌。

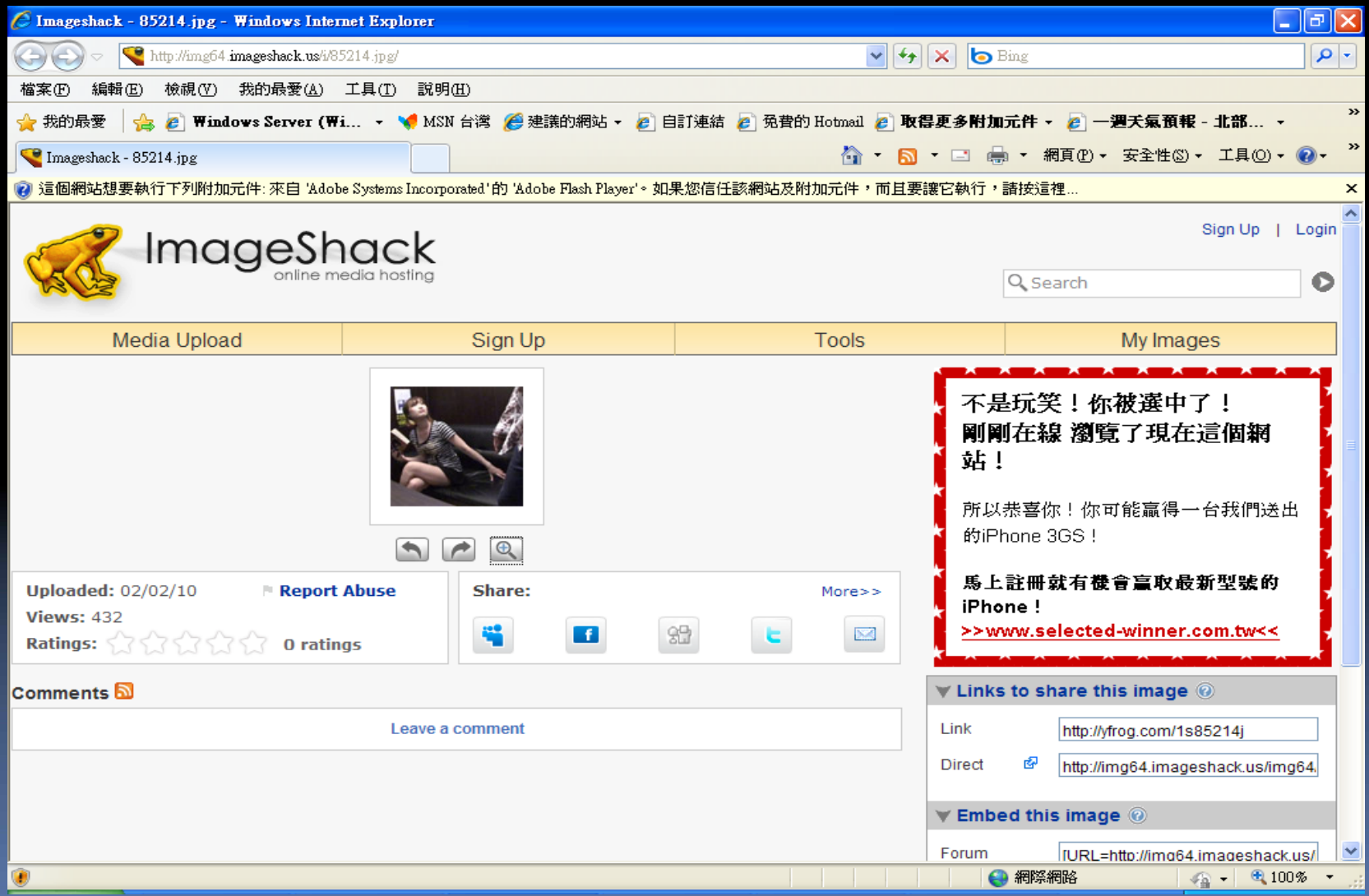
百万人疯狂下载 HOT!
桌面地图2007
最新版
免费使用 无限升级

網路詐騙的手法，是假冒真實且有信譽的公司發送電子郵件或即時訊息，但其實是出自竊賊之手。 使用這種伎倆的線上竊賊會企圖引誘閱覽者點選訊息中的連結。

詐騙廣告或網頁-1

FreakShare.net - Easy One-Click File Hosting - Windows Internet Explorer
http://freakshare.net/files/ufx47e9n/plus-Jessica.rar.html
Bing
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
我的最愛
Windows Server (Wi...
MSN 台灣
建議的網站
自訂連結
免費的 Hotmail
FreakShare.net - Easy One-Click File Hosting
網頁(P)
安全性(S)
工具(O)
這個網站想要執行下列附加元件: 來自 'Adobe Systems Incorporated' 的 'Adobe Flash Player'。如果您信任該網站及附加元件，而且要讓它執行，請按這裡...
FREAKSHARE
EASY ONE-CLICK FILE HOSTING
UNIVERSITY OF LIVERPOOL
New Online Programmes
Management
MBA International Business
plus-Jessica.rar
Download
不是玩笑！你被選中了！ 剛剛在線 瀏覽了現在這個網站！
所以恭喜你！你可能贏得一台我們送出的iPhone 3GS！
馬上註冊就有機會贏取最新型號的iPhone！ >>www.selected-winner.com.tw<<
網際網路
100%

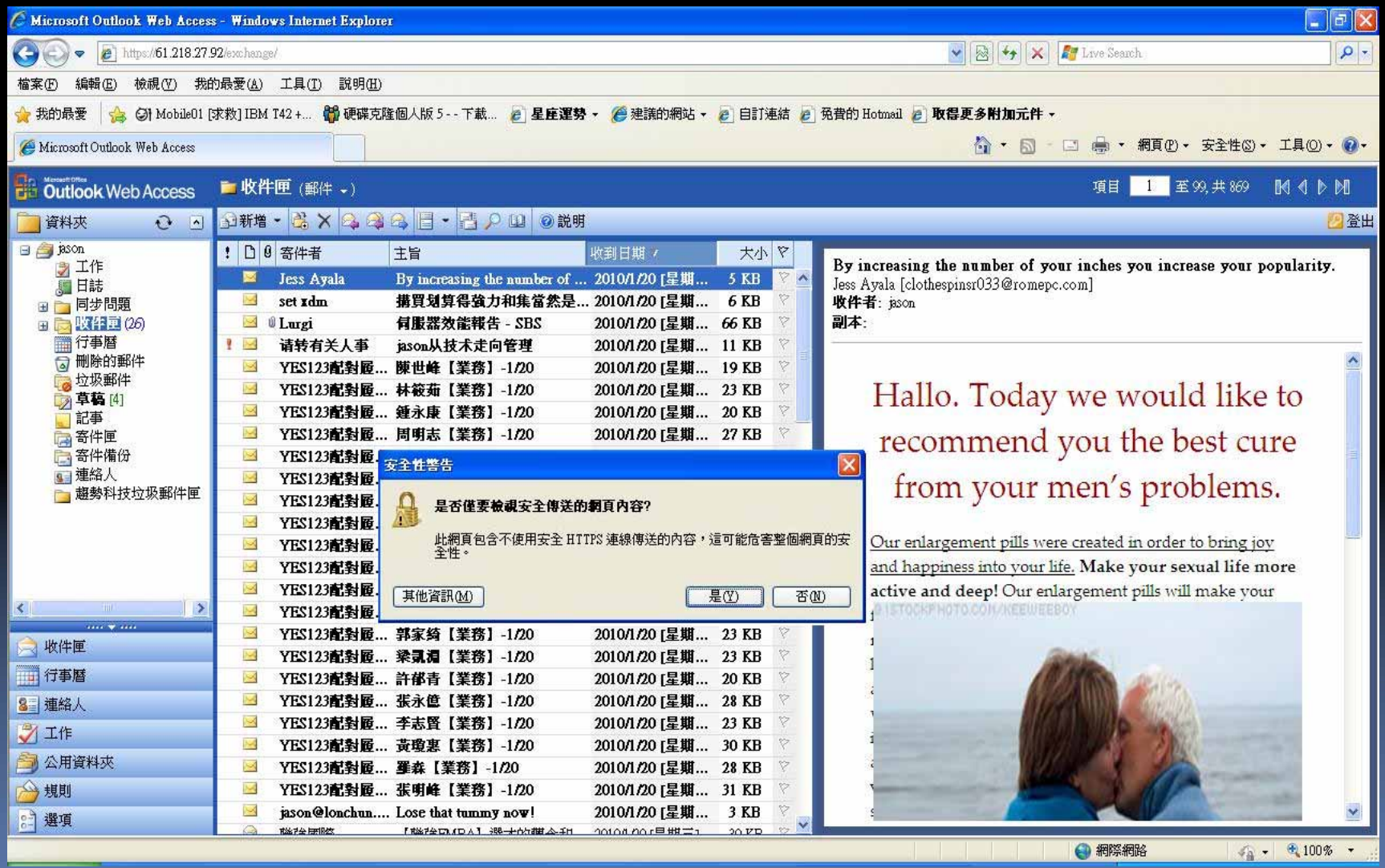
詐騙廣告或網頁-2


Imageshack - 85214.jpg - Windows Internet Explorer
http://img64.imageshack.us/i/85214.jpg/
Bing
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
我的最愛
Windows Server (Wi...
MSN 台灣
建議的網站
自訂連結
免費的 Hotmail
取得更多附加元件
一週天氣預報 - 北部...
Imageshack - 85214.jpg
網頁(P) 安全性(S) 工具(O)
這個網站想要執行下列附加元件: 來自 'Adobe Systems Incorporated' 的 'Adobe Flash Player'。如果您信任該網站及附加元件，而且要讓它執行，請按這裡...
ImageShack
online media hosting
Sign Up | Login
Search
Media Upload
Sign Up
Tools
My Images
不是玩笑！你被選中了！
剛剛在線 瀏覽了現在這個網站！
所以恭喜你！你可能贏得一台我們送出的iPhone 3GS！
馬上註冊就有機會贏取最新型號的iPhone！
>>www.selected-winner.com.tw<<
Uploaded: 02/02/10
Report Abuse
Views: 432
Ratings:
0 ratings
Share:
More>>
Comments
Leave a comment
Links to share this image
Link
http://yfrog.com/1s85214j
Direct
http://img64.imageshack.us/img64.
Embed this image
Forum
[URL=http://img64.imageshack.us/
網際網路
100%

以下是一個範例，說明詐騙電子郵件可能的外觀。

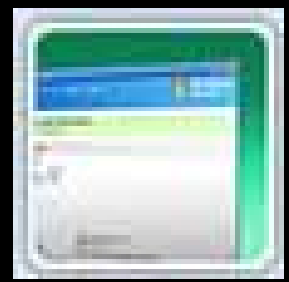
詐騙電子郵件範例，其中還有可以連至詐騙網站的假 URL 位址。

別以為SSL加密信件是安全的
（也是竊取機密資料手法之一）



不被欺騙的方法

如果有可能受害，就應該採取行動防止網路詐騙者傷害公司或單位。
以下有四種方式。



1. 確定電腦在最新狀態
   應該準備好基本的電腦及網路安全系統。
2. 減少暴露機會
   開始使用篩選科技，防止同仁接觸網路詐騙電子郵件訊息。
3. 教育工作同仁
   縱使是對付電子郵件詐騙的專家也很難區分製作精美的詐騙信件與真實郵件。 因此，為了避免同仁及單位因網路詐騙受害，必須提高警覺、做好防範措施，並進行教育。
4. 檢查網站是否保護敏感資料
   網路詐騙者可假造瀏覽器顯示的網址。 只要對該網站的合法性有些許懷疑，就應小心謹慎並馬上離開。

保護個人及電腦

- ## 機要文件的保密方式

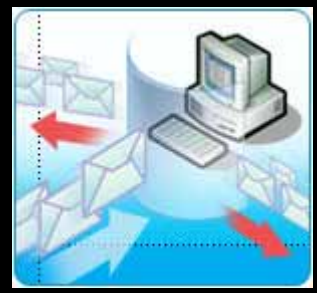
運用密碼、加密技術與常識來保護文件的隱私

- ## 保護文件的簡單方法

利用這些簡單的實務操作與隨手可得的科技工具，便可妥善保護文件：

1. **使用密碼保護。**
   - 可藉由要求開啟該文件的人輸入您所建立的密碼，以便限制能查閱文件的人。
2. **安裝防火牆。**
   - 安裝防火牆能減少駭客攻擊或掃描漏洞的機會，保護重要文件無疑是其中一個。更可以阻止網際網路入侵者存取電腦檔案及閱讀資訊。

防阻垃圾郵件



- 建立完善的垃圾郵件防制機制需要相關措施配合，茲列舉如下：
  - 自動確認電子郵件來自您經常往來的人士或公司
  - 容許未知的寄件人證明他們並非垃圾郵件寄件人
  - 不斷提升電子郵件過濾稽核機制
  - 預防垃圾郵件進入網路

不要輕易公開您的電子郵件信箱

更新防毒/資安軟體降低中毒風險

- 步驟 1：檢查電腦是否有防毒/資安防護軟體
- 步驟 2：選擇適合您的防毒/資安防護軟體將
- 步驟 3：防毒/資安防護軟體保持在最新狀態

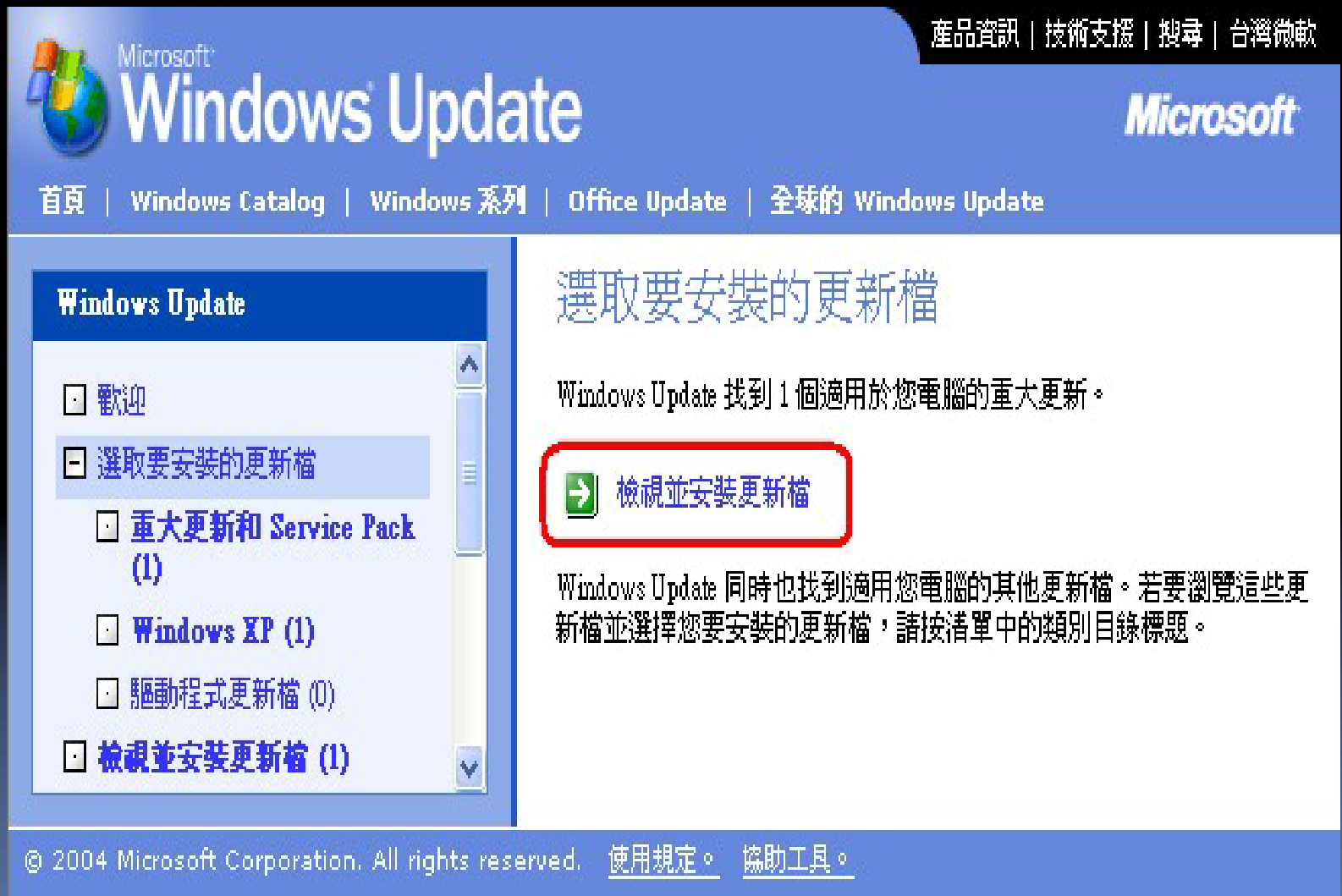
自動更新。

下載最新的更新是絕對必要的。許多公司的產品都提供此自動選項。

選擇聲譽良好的防毒/資安防護軟體。

您在網路上用心的搜尋或選購，必然會找到適當的防毒/資安防護軟體。

Windows Update更新



附件A--網路及病毒相關名詞解釋

- **Adware廣告軟體**

  廣告軟體是一個廣告的電腦程式，把廣告作爲目的，會不斷彈出視窗及造成系統效能低落。 並非所有的軟體內包含的廣告都是有害的，有時候內含廣告也只是單純營利的手段。不過有時候這些廣告的植入可能是使用者不願意的，並且會在執行過程來竊取使用者的資料。所以這也算是廣義下的一種間諜軟體。

- **Anti-Spyware反間諜軟體**

  反間諜軟體是用來清除間諜軟體、 廣告軟體、後門程式、鍵盤側錄程式及木馬程式等惡意程式的軟體，通常使用反間諜軟體皆需進行多次掃描及重啓電腦才可徹底清除惡意程式 。

- **Rootkit**

  是一種木馬或類似的技術，用以隱藏惡意程式的所在（執行程序、檔案、系統登錄碼、網路埠）之用，藉此躲過使用者或管理者的檢視。

- **Anti-Virus防毒軟體**

  透過即時監控的方式，掃描電腦裡執行的程式，並與病毒資料庫比對，若發現病毒時可將病毒的部分清除，或將可疑程式放入隔離區以免擴大感染。基本上目前的防毒軟體都具備即時清除病毒、木馬及惡意程式的功能，可於第一時間阻止電腦被感染或破壞。

- **Access control存取控制**

  是一種對於資料或資訊系統使用的安全控制措施。電腦系統管理者可利用密碼或其他身分驗證的方式，對使用者進行授權或拒絕存取與控管。換言之，存取控制在指派與控制使用者之權限（如使用者的身份、使用系統之時間等條件）。存取控管可提供資源系統使用安全功能，降低駭客入侵或資料不當外洩的風險。

- **Back door後門**

  指繞過軟體的安全性控制而從比較隱秘的通道獲取對程序或系統訪問權的駭客方法，包括了 不懷善意的後門程式或遠端管理程式 。在軟體開發時，設置後門可以方便修改和測試程序中的缺陷。但如果後門被其他人知道（可以是洩密或者被探測到有後門存在），或是在發佈軟體之前沒有移除後門，那麼它就對電腦系統安全造成了威脅。

- **BotNet傀儡網路攻擊**

  俗稱殭屍病毒，又稱機器人網路（ Robot Network ）或傀儡程式。受到 BotNet 感染的主機，會猶如殭屍般任由駭客控制，使用者上網連線速度會突然感覺變慢。駭客會以遠端控制受感染的主機，進行網路攻擊，包括竊取私密資料、網路釣魚、散布垃圾郵件、發動阻斷式服務等網路犯罪行爲。

- **Browser Hijacker瀏覽器綁架軟體**

  屬於流氓軟體的一種，會主動攻擊使用者瀏覽器，入侵後會改變電腦原先設定好的功能，讓使用者無法正常打開原先設定好的瀏覽器首頁業面，反而開啓了入侵者竄改後的不明網頁，強制要求使用者使用其設定的頁面。此類軟體多半是未經使用者許可的情形下植入。

- **Bulk Mail大量郵件**

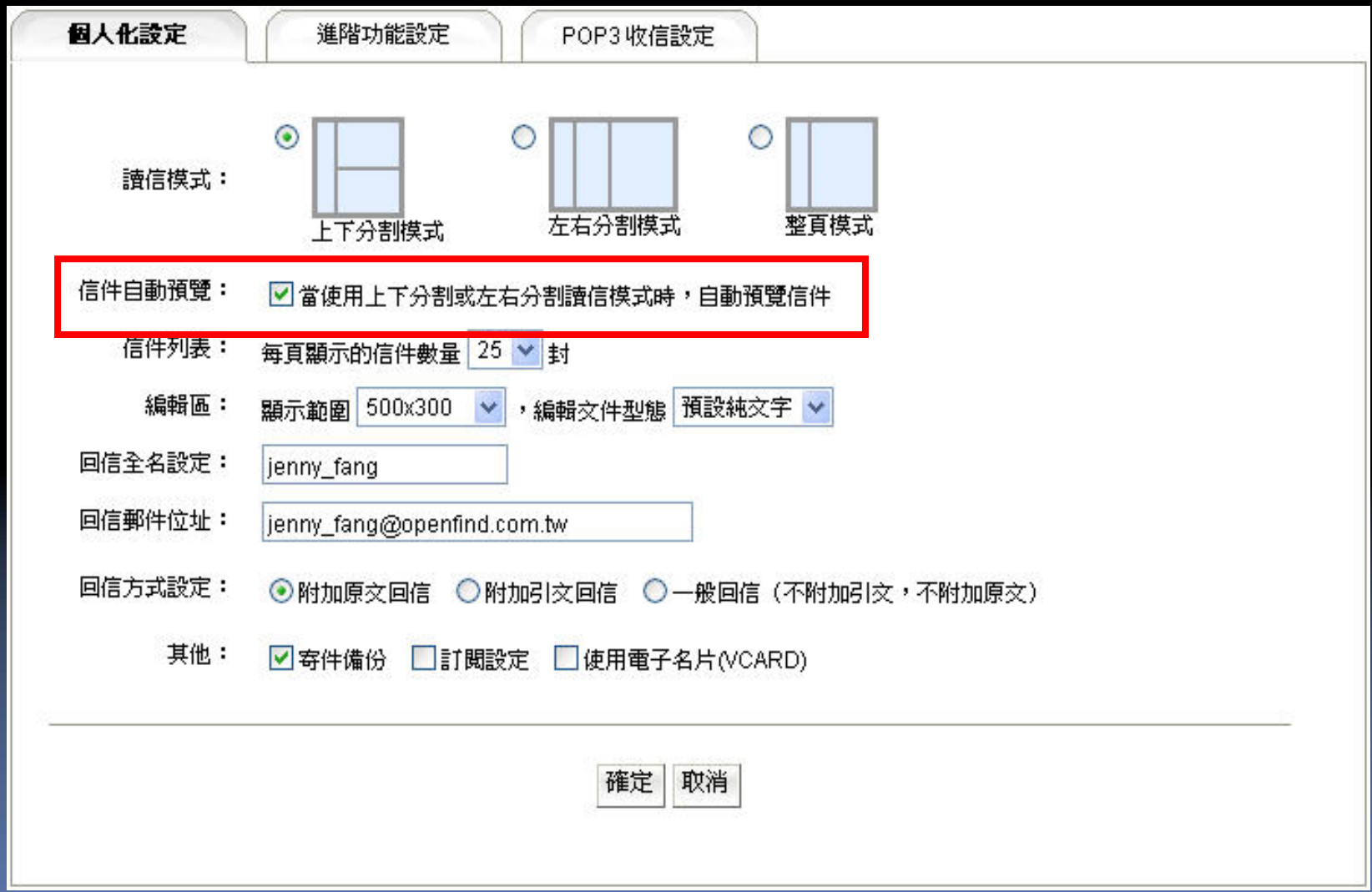
  指未經收件人許可，大量寄發的郵件，多以廣告信函與垃圾郵件爲主。如同住家信箱總是被大量的廣告宣傳單塞滿，電腦使用者的電子信箱也經常被大量垃圾郵件而嚴重影響使用效能；造成電腦使用者使用電子信箱與網際網路的困擾，同時也會降低網際網路使用的頻寬與效能。

更多資料可查詢<教育部 http://cissnet.edu.tw

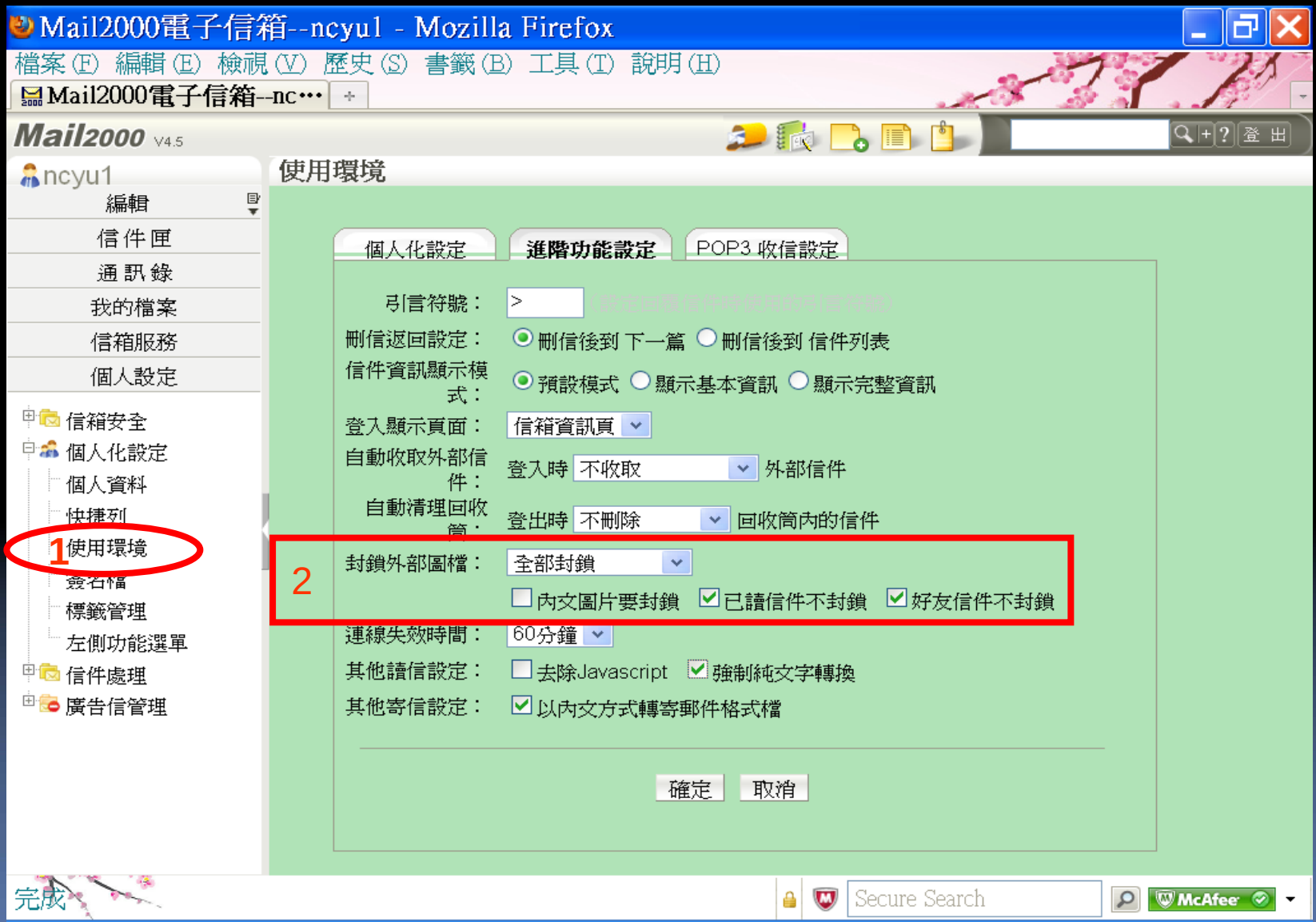
附件B—校內Web Mail相關設定

- 自動預覽的功能取消不允許使用 －「目前」設定以強制不允許使用

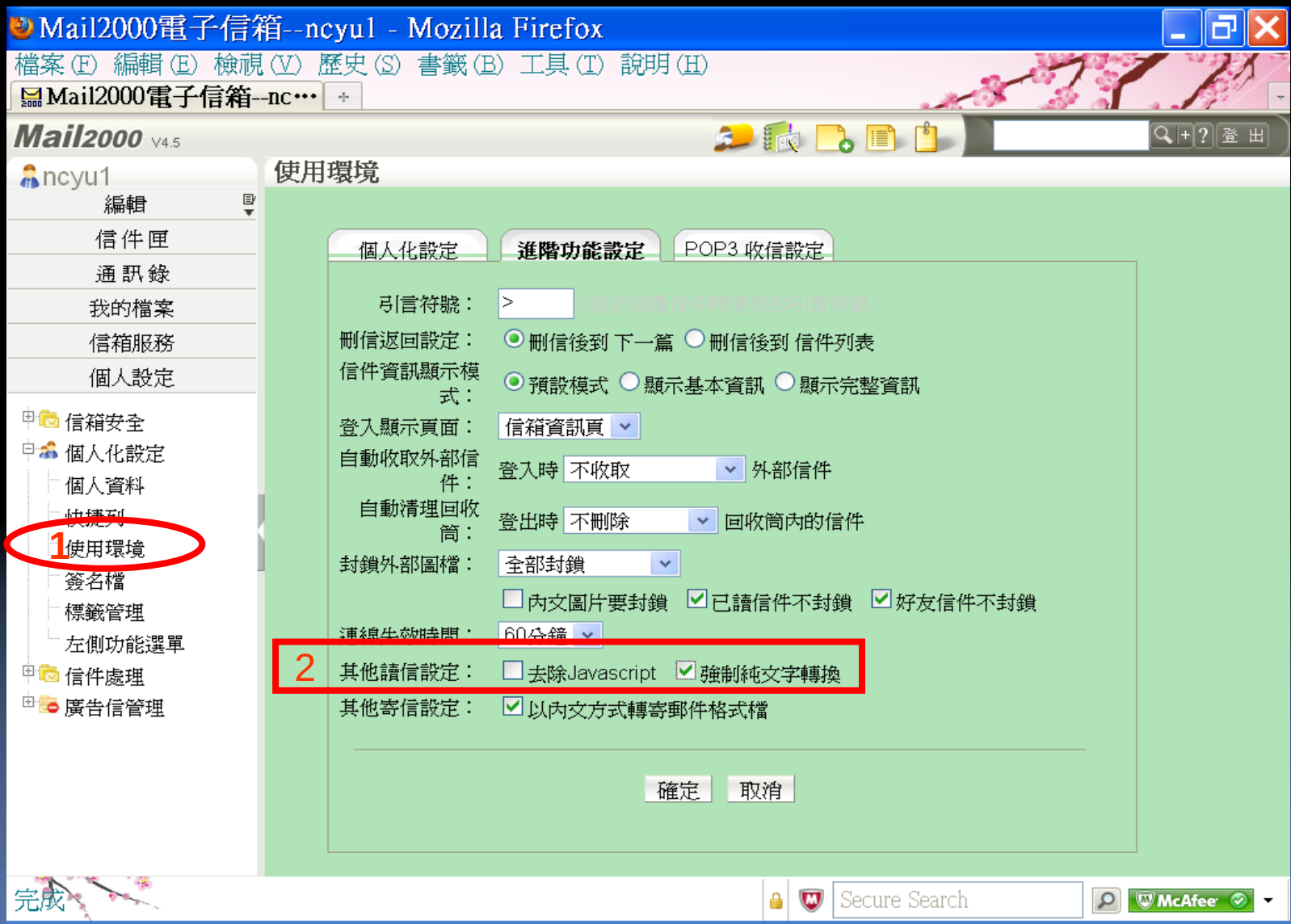
- 自動預覽「原始」設定


個人化設定
進階功能設定
POP3 收信設定
讀信模式：
上下分割模式
左右分割模式
整頁模式
信件自動預覽：
當使用上下分割或左右分割讀信模式時，自動預覽信件
信件列表：
每頁顯示的信件數量 25 封
編輯區：
顯示範圍 500x300 ，編輯文件型態 預設純文字
回信全名設定：
jenny_fang
回信郵件位址：
jenny_fang@openfind.com.tw
回信方式設定：
附加原文回信
附加引文回信
一般回信（不附加引文，不附加原文）
其他：
寄件備份
訂閱設定
使用電子名片(VCARD)
確定
取消

封鎖外部圖檔設定


Mail2000電子信箱--ncyu1 - Mozilla Firefox
檔案(F) 編輯(E) 檢視(V) 歷史(S) 書籤(B) 工具(T) 說明(H)
Mail2000電子信箱--nc…
Mail2000 V4.5
ncyu1
編輯
信件匣
通訊錄
我的檔案
信箱服務
個人設定
信箱安全
個人化設定
個人資料
快捷列
1
使用環境
簽名檔
標籤管理
左側功能選單
信件處理
廣告信管理
使用環境
個人化設定
進階功能設定
POP3 收信設定
引言符號：
>
刪信返回設定：
刪信後到 下一篇
刪信後到 信件列表
信件資訊顯示模式：
預設模式
顯示基本資訊
顯示完整資訊
登入顯示頁面：
信箱資訊頁
自動收取外部信件：
登入時 不收取 外部信件
自動清理回收筒：
登出時 不刪除 回收筒內的信件
2
封鎖外部圖檔：
全部封鎖
內文圖片要封鎖
已讀信件不封鎖
好友信件不封鎖
連線失效時間：
60分鐘
其他讀信設定：
去除Javascript
強制純文字轉換
其他寄信設定：
以內文方式轉寄郵件格式檔
確定
取消
完成
Secure Search
McAfee

強制純文字轉換


Mail2000電子信箱--ncyu1 - Mozilla Firefox
檔案(F) 編輯(E) 檢視(V) 歷史(S) 書籤(B) 工具(T) 說明(H)
Mail2000電子信箱--nc…
Mail2000 V4.5
登 出
ncyu1
編輯
信件匣
通訊錄
我的檔案
信箱服務
個人設定
信箱安全
個人化設定
個人資料
快捷列
1
使用環境
簽名檔
標籤管理
左側功能選單
信件處理
廣告信管理
使用環境
個人化設定
進階功能設定
POP3 收信設定
引言符號：
>
刪信返回設定：
刪信後到 下一篇
刪信後到 信件列表
信件資訊顯示模式：
預設模式
顯示基本資訊
顯示完整資訊
登入顯示頁面：
信箱資訊頁
自動收取外部信件：
登入時 不收取 外部信件
自動清理回收筒：
登出時 不刪除 回收筒內的信件
封鎖外部圖檔：
全部封鎖
內文圖片要封鎖
已讀信件不封鎖
好友信件不封鎖
60分鐘
2
其他讀信設定：
去除Javascript
強制純文字轉換
其他寄信設定：
以內文方式轉寄郵件格式檔
確定
取消
完成
Secure Search
McAfee