個人電腦安全之防護

台北海院 圖資中心

2010-09-07

個人電腦常見的被入侵方式

- 病毒(木馬、蠕蟲)感染、駭客的惡意攻擊。
  - 被他人盜取密碼。
  - 系統當機。
- 開啟不明伺服器網頁。
  - 瀏覽網頁時被惡意的java script程式攻擊。
  - 網頁綁架(Q播、百度…)。
- 系統存在漏洞使他人攻擊自己。
  - 已知系統漏洞未更新，而使得病毒透過特定方式(如網路或系統程式)入侵電腦。
- MSN、YAHOO即時通被攻擊或洩漏資訊。
- 分享網路連線卻未做相關防護措施。
- 執行來路不明的電子郵件。
- 下載安裝不明軟體。
- 下載或拷貝已中毒的可執行檔案。
- 使用已感染病毒之磁片、光碟等媒體。
- …..

常見電腦中毒或被入侵的症狀

- 系統目錄有奇怪的檔案、大小或某些檔案被損毀
- 電腦常當機
- 執行速度變慢
- 無法使用某些軟體
- 電腦無法開機
- 出現奇怪的對話窗
- 硬碟被重新格式化
- 電腦會自動傳送封包資料、訊息

常見電腦中毒或被入侵的後遺症

- 信箱帳號/密碼被盜
- 網拍帳號/密碼被盜
- 遊戲帳號/密碼被盜
- 網購帳號/密碼被盜
- 網路銀行帳號/密碼被盜
- 信用卡號被盜
- 網站帳號/密碼被盜
- MSN、YAHOO即時通帳號/密碼被盜
- 個人資訊檔案、私密照片被盜

防護電腦原則

1. Windows XP 網際網路連線防火牆設定:

開啟控制台→網路連線→區域連線→內容→進階→設定值，點選”開啟(建議選項)”，開啟Windows防火牆保護。

2. 作業系統相關程式更新:

- 打開IE瀏覽器，點選 工具→Windows Update。
- 為提供快速更新服務，本校建置有WSUS Server，相關服務請參閱中心網站→網路樂園→服務資源→微軟自動更新服務(WSUS)

3. 安裝防毒軟體

- 安裝前須確定電腦未受病毒感染
- 本校提供教職員在校NOD32、PANDA防毒軟體
  中心網站→網路樂園→服務資源→病毒防治服務(Virus)

保護電腦常要做的工作?

- **防病毒及防駭**
  - 定期更新掃毒軟體的「病毒碼」及「病毒掃瞄引擎」
  - 經常修正Windows 的漏洞
- **防制垃圾信(SPAM)**
  - 不任意開啟來路不明信件、檔案
  - 本校提供了垃圾郵件過濾系統
- **提高電腦的效率**
  - 移除及刪除沒用的軟體和檔案
  - 一段期間時執行「清理磁碟」及「磁碟重組」
- **備份**

如何處理中毒

- 將中毒的電腦網路線拔掉(避免散播病毒)
- 用其它安全、乾淨電腦上網，連線到信任的防毒公司網站，下載「檢查及移除工具」，用「檢查及移除工具」將病毒找出及清除掉
- 安裝防毒軟體，進行掃描、解毒，啟動防禦功能
- 如果沒裝防火牆, 安裝個人防火牆及啟動防駭功能
- 修正Windows 的漏洞
- 立即更新「病毒碼」及「掃瞄引擎」

如何自保？

- 隨時注意電腦使用狀況，一發覺有異常第一個懷疑的就是有沒有中毒。
  （事實上你的電腦送修，一般的工程師也會第一個想到這個原因）。
- 因為現在病毒更新的速度比防毒程式還快，舊一點的防毒程式可都抓不到新的病毒，請時常更新病毒碼。
  （有時候就算防毒程式是最新的也抓不到）。
- 中毒之後當然是要把毒解乾淨，解完毒的第一件事就是更換你的所有密碼。
  （毒沒解掉的話你換一百次也沒有用）。
- 多吸收防毒的知識，以及如何安全地使用電腦的知識。
  （請留意中心發佈之資訊安全訊息）。
- **不要用電腦了**。
  （哈哈 當然是不可能，所以**養成習慣，不要24小時掛網**囉!!）。

隨身碟病毒

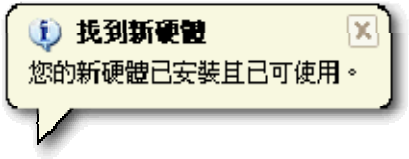
何謂隨身碟病毒？

- 隨身碟為什麼會傳播病毒？
  - 只因為一個功能：**自動播放。**
  - 自動播放的核心是一個檔名為autorun.inf的檔案，當你插入隨身碟時系統就會執行autorun.inf中所指定的程式。

- 隨身碟使用方式
  - 不管是「隨身碟」、「記憶卡」、「 MP3/MP4隨身聽」、「手機」、「相機」、「攝影機」和「外接式硬碟」等都適用，只要是插入電腦的USB連接埠會出現一台「卸除式磁碟機」的裝置都是相同的使用方式。

隨身碟正確的使用方法

- 當你插入這些USB裝置的時候，請先按住鍵盤的【Shift】鍵（**一直按著不要放開**）。
  - 如果這個裝置是第一次插入你的電腦的話，就會在右下角的系統圖示列出現以下的「找到新硬體」的提示，這個時候還是不要放掉【Shift】鍵。



- 等到右下角的 安全地移除硬體圖示出現後，你才可以放掉【Shift】鍵。

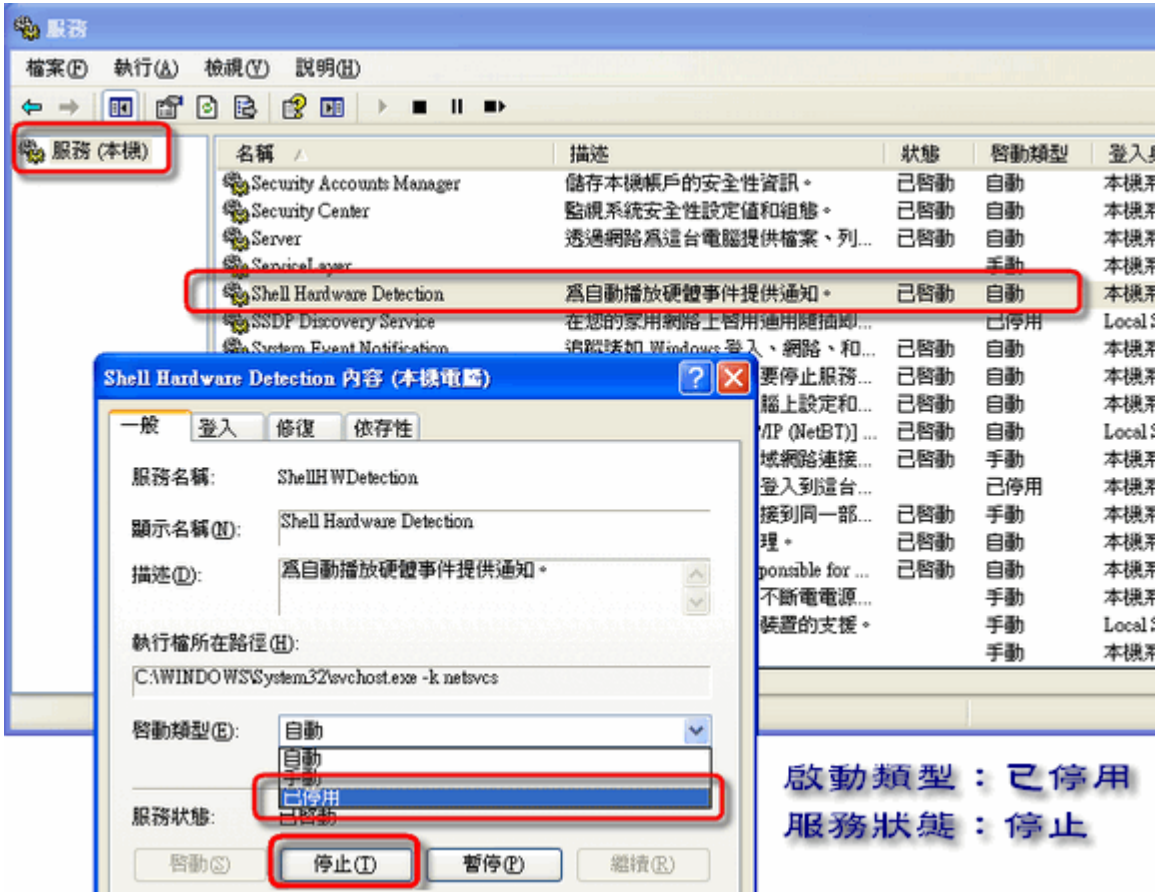
- 小提示：因為右邊的【Shift】鍵按8秒鐘內定會出現「篩選鍵」的選項，所以還是按**左邊的【Shift】鍵吧**！如果嫌一直按【Shift】鍵太麻煩，那請你將**隨身碟自動執行功能關閉**後就可以不用一直按【Shift】鍵。

關閉隨身碟(1) - 自動執行微軟更新

- 利用隨身碟的「自動執行AutoRun」來傳播病毒是最常見的方式，但是最根本解決之道就是**把隨身碟的「自動執行AutoRun」功能停用**，這樣子病毒就不會在你插入隨身碟的時候就被啟動，至少讓防毒程式有一個緩衝的機會。
- 如何關閉？
  - 微軟發佈了一個更新程式讓你來關閉Windows XP, Vista, Windows Server 2003等版本中的自動執行功能。
  - 微軟KB971029更新
    http://support.microsoft.com/?kbid=971029

關閉隨身碟(2) – 停用Shell Hardware Detection服務，取消自動播放的硬體通知

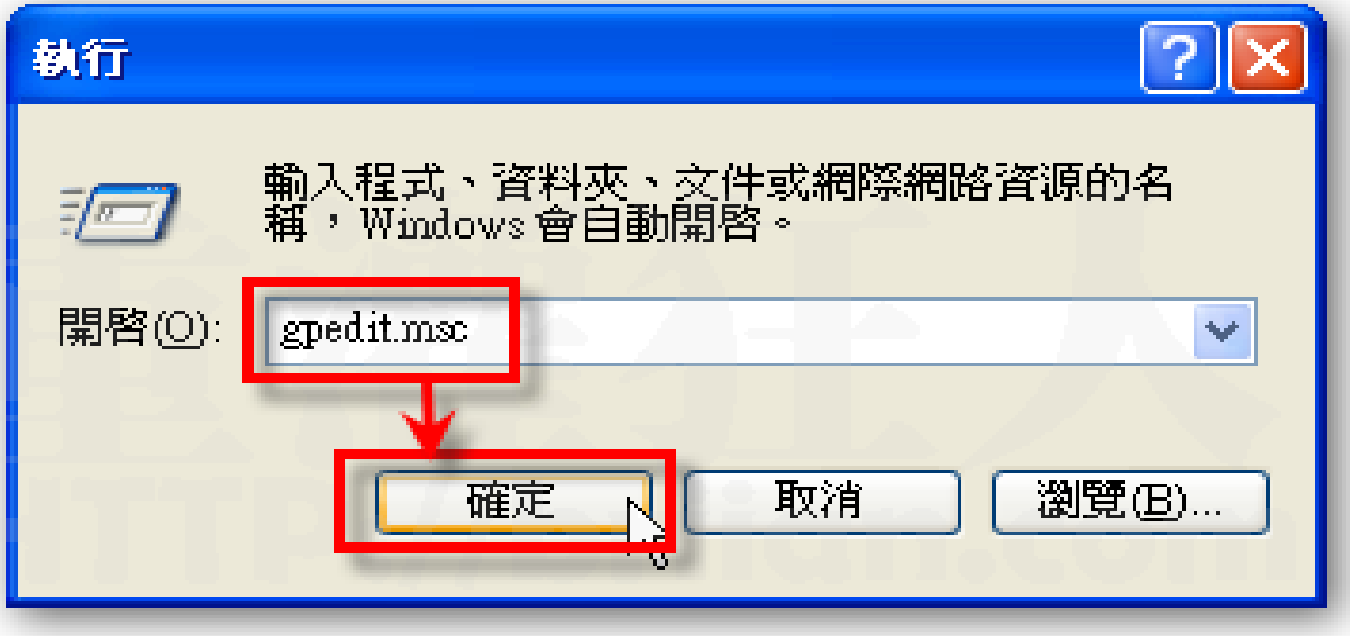
滑鼠點選「我的電腦」後按「 右鍵 」選擇「 管理 」→「 服務及應用程式 」→「 服務 」→ 於左邊視窗點選 「 **Shell Hardware Detection** 」→ 將啟動類型改為【已停用】後按「確定」鈕即完成。



關閉隨身碟(3) -修改「群組原則」，停用自動播放功能

—適用 Windows XP專業版

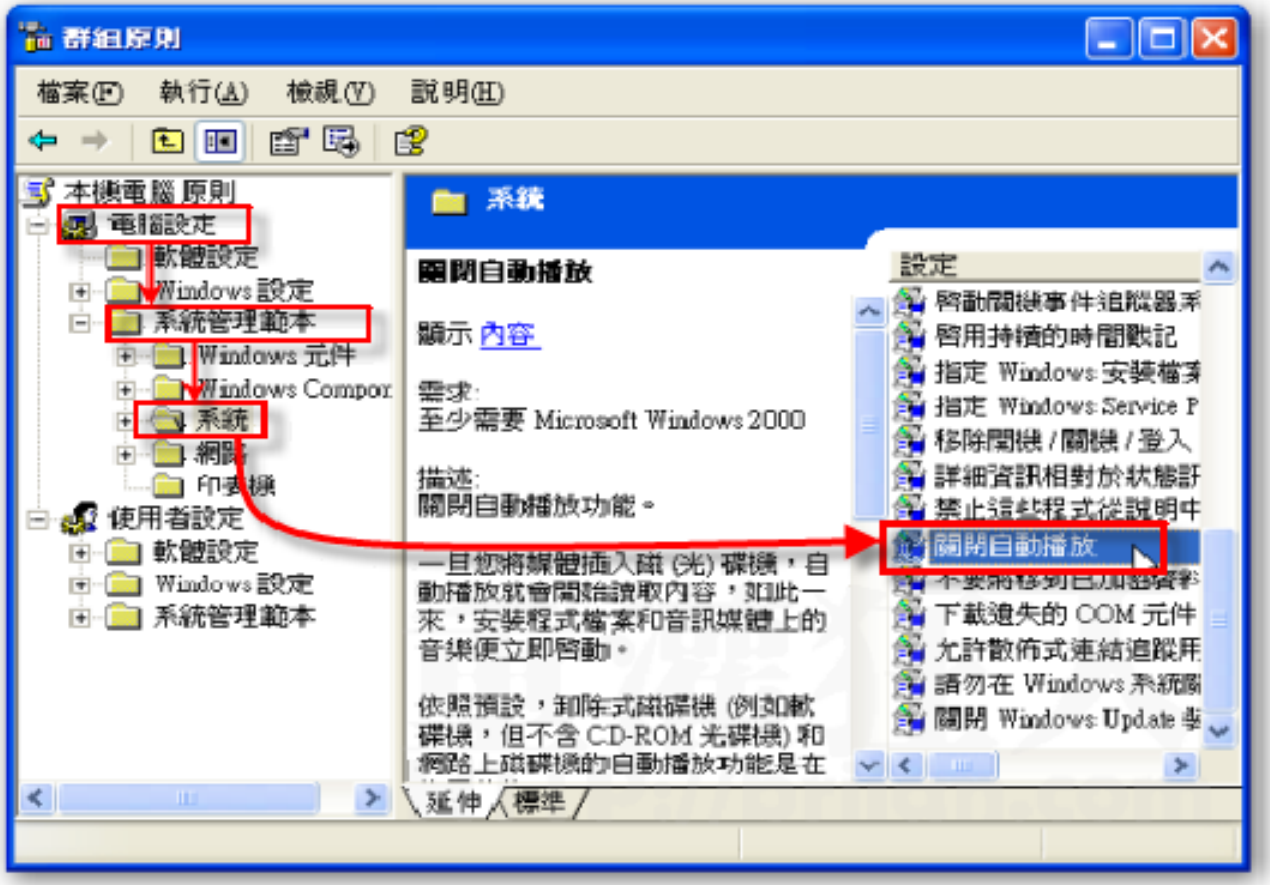
1. 點選〔開始〕→【執行】，開啟「執行」對話盒後請輸入「gpedit.msc」，再按一下〔確定〕按鈕，開啟群組原則設定頁面。



關閉隨身碟(3) -修改「群組原則」，停用自動播放功能

－適用 Windows XP專業版

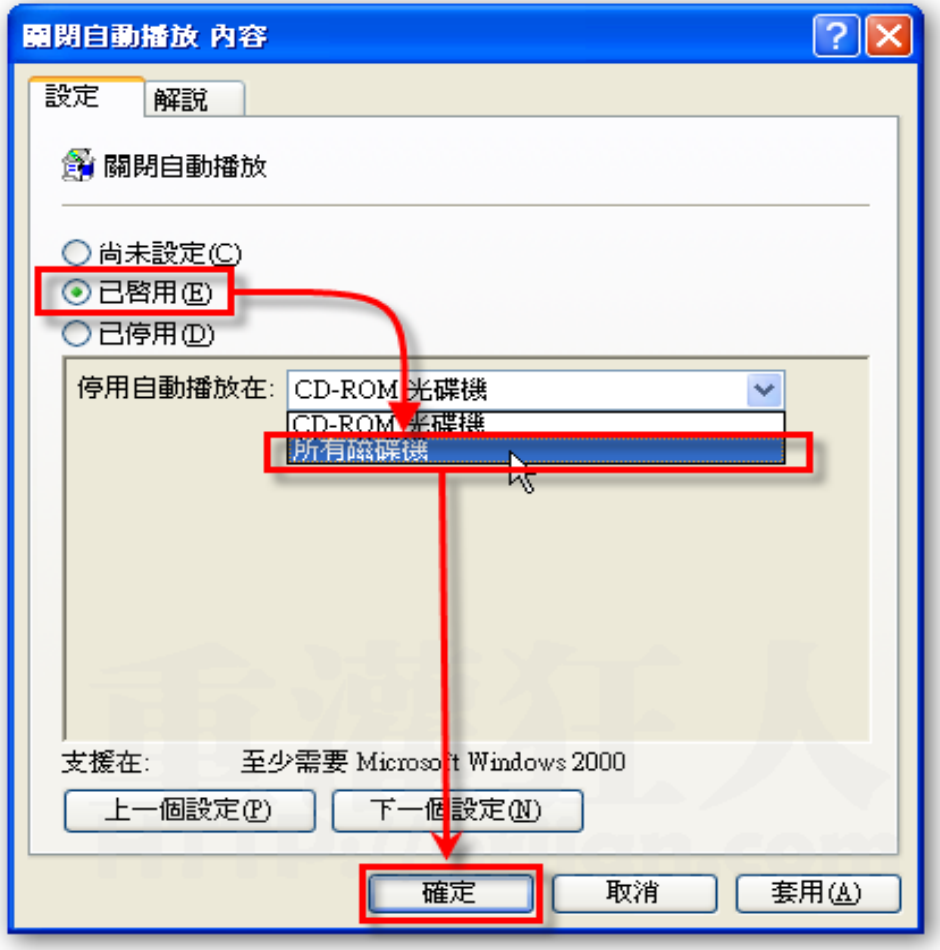
2. 如圖，先從左邊的目錄切換到「電腦設定」→「系統管理範本」→「系統」，在系統頁面中（右邊視窗）可以找到一個「關閉自動播放」的項目，請在上面按兩下滑鼠左鍵，開啟它。



關閉隨身碟(3) -修改「群組原則」，停用自動播放功能

－適用 Windows XP專業版

3. 接著先點選〔已啟用〕，然後在「停用自動播放在」下拉選單中點選【所有磁碟機】，然後再按下〔確定〕按鈕，即可設定完成，重開機後就可生效。

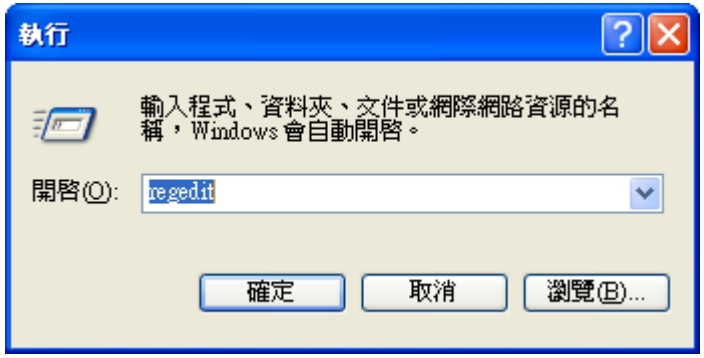


關閉隨身碟(4) –修改「登錄檔」

–適用Windows XP專業版與HOME家用版

- 若你的系統沒有 **gpedit.msc** 指令，例如 Windows XP Home，改用 **regedit** 處理。

1. 點選「開始」→「執行」，輸入「regedit」後按下「確定」鈕。

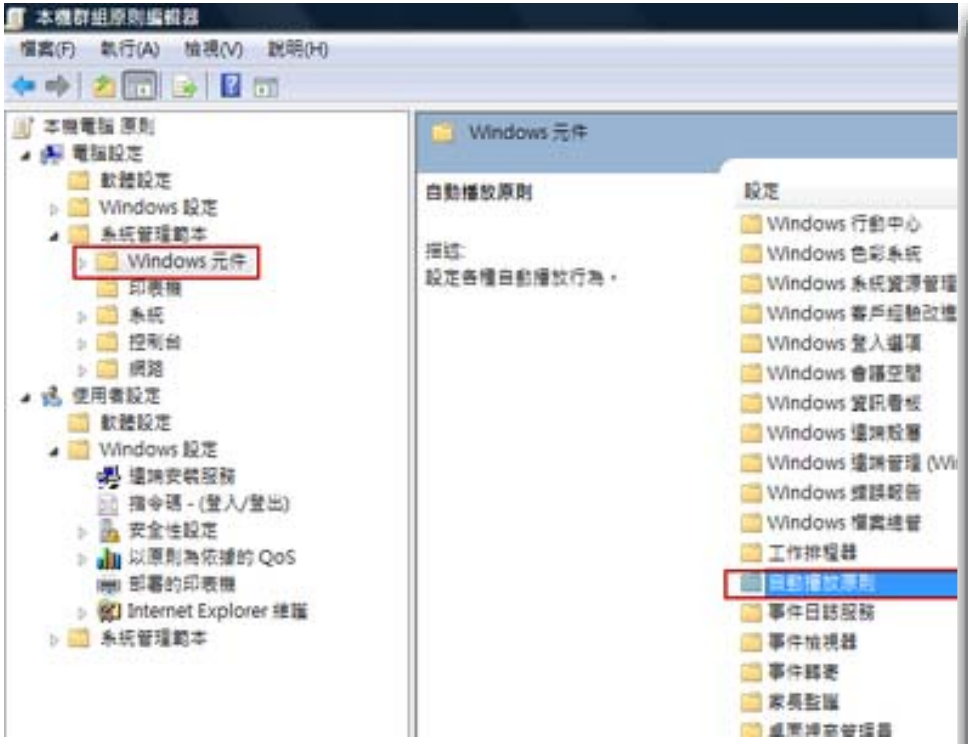


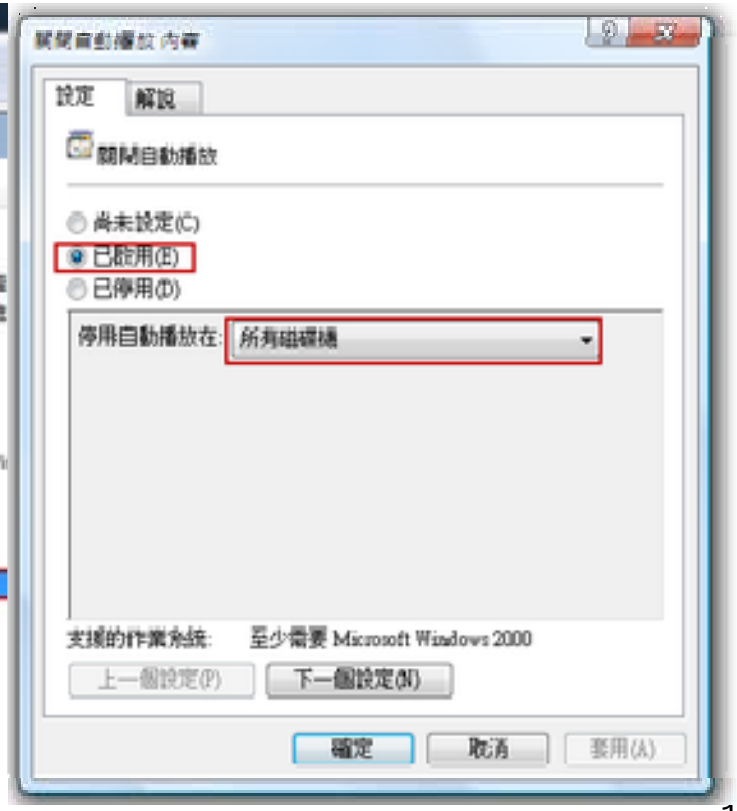
2. 請將 **HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDrive TypeAutoRun**值修改為「**255**」
3. 重新開機

關閉隨身碟(5) –修改「本機群組原則編輯器」

—適用Windows Vista

1. 點選「開始」→「執行」，輸入「gpedit.msc」後按下「確定」鈕。
2. 點選「群組原則」→「電腦設定」→「系統管理範本」→「Windows元件」→「自動播放原則」→ 關閉自動播放：【啟用】，並將停用自動播放在：【所有磁碟機】。





關閉隨身碟(5) –修改「本機群組原則編輯器」

—適用Windows 7

- 注意：儘管微軟在Windows 7版本已經不再針對卸除式磁碟進行自動執行(AutoRun)動作，但仍然會**針對光碟機(CD/DVD)進行自動播放功能**。

- 關閉光碟機(CD/DVD)自動執行動作：
  1. 點選「開始」→「執行」，輸入「gpedit.msc」後按下「確定」鈕。
  2. 點選「電腦設定」→「系統管理範本」→「Windows元件」→「自動播放原則」
     - **關閉自動播放**：點擊「已啟用」，並將「停用自動播放在:」項目調整為「所有磁碟機」。
     - **關閉「AutoRun的預設行為」**：點擊「已啟用」，再將「預設AutoRun行為」項目調 整為「不執行任何AutoRun命令」，即設定完成。

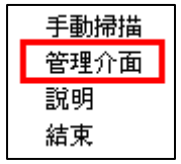
Wow! USB Protector 自動掃描隨身碟，輕鬆防毒！

- 隨身碟病毒的氾濫，常常讓你把隨身碟插入A電腦後不小心中了A電腦的毒，接著您又把隨身碟插入B電腦，將存在隨身碟內的病毒無意中便散佈到B電腦，使得B電腦也遭殃，正因為這樣，所以我們必須透過**有效的防堵**機制，做最前鋒的掃描與防堵。
- 中研院研發的「Wow! USB Protector」就可以主動偵測插入電腦的外接式裝置，做最前鋒的掃描與防堵。
  - 軟體下載

    圖資中心網站 → 下載專區 → 授權軟體 頁面
  - 官方下載

    http://of.openfoundry.org/download_path/wowusbprotector/0.80/WowUSBProtector-zh.exe

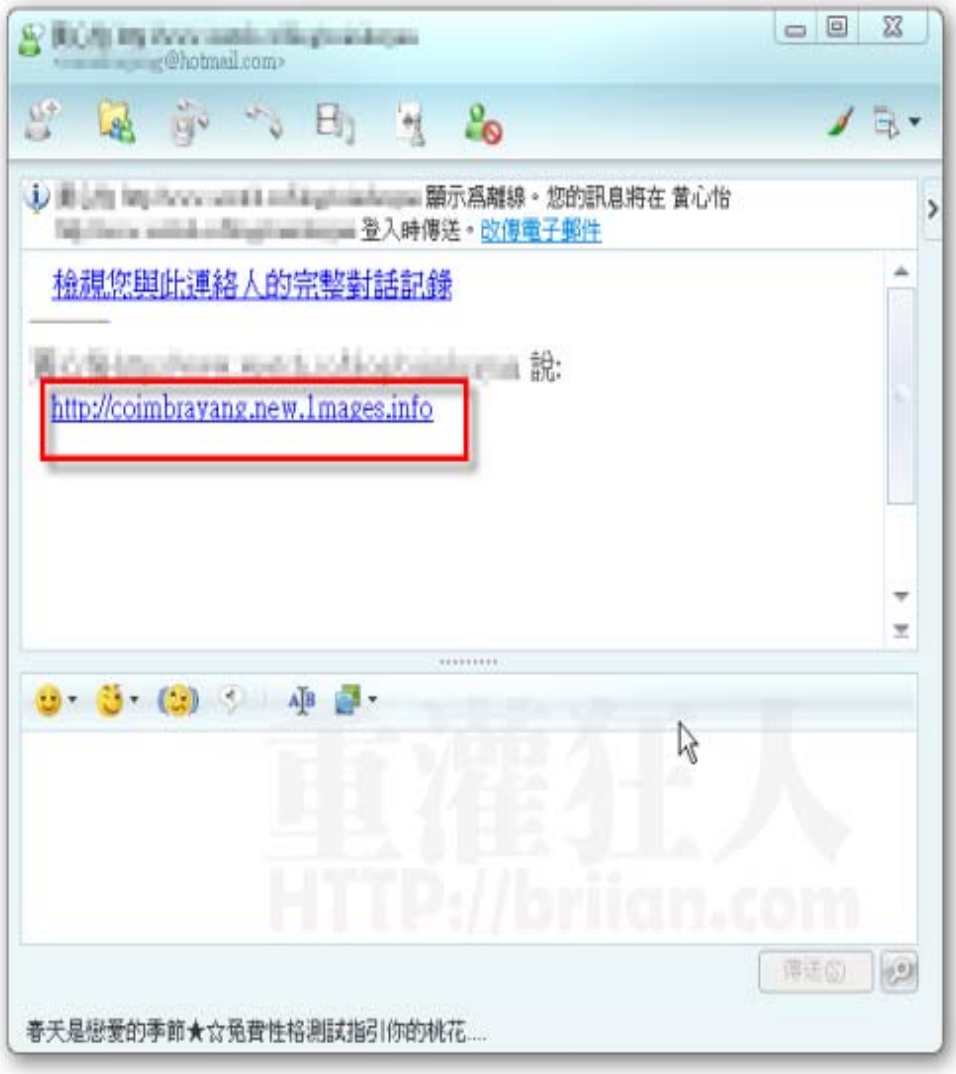
Wow! USB Protector

- 下載「Wow! USB Protector」並執行安裝，接著在桌面右下角點擊 後點右鍵 

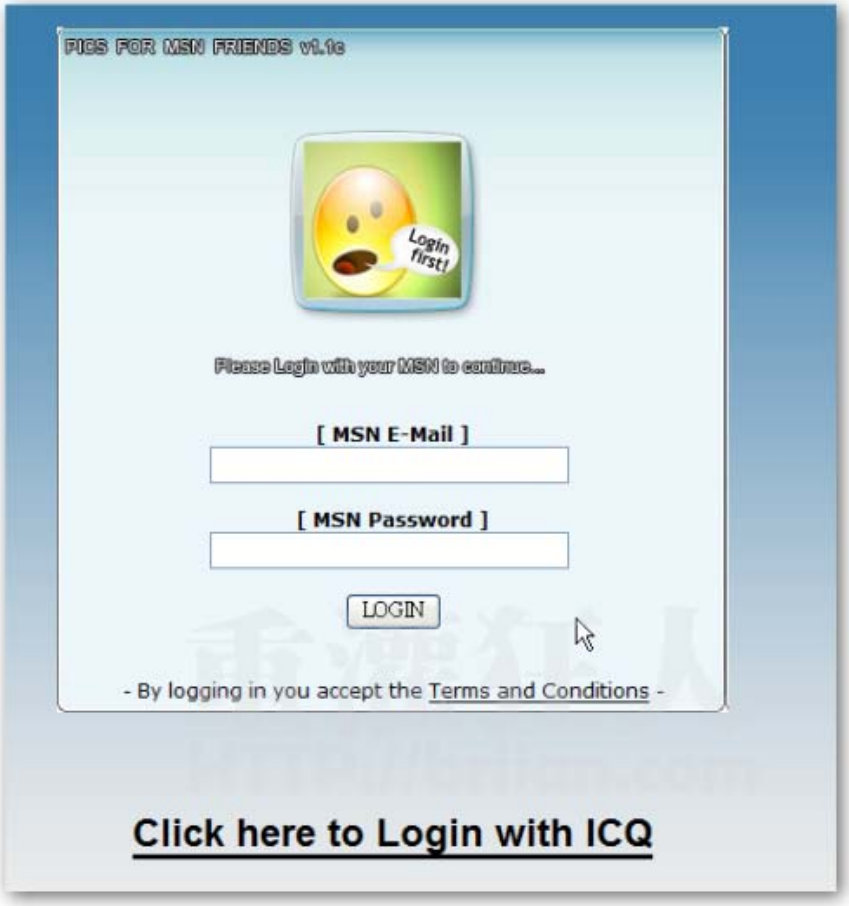
選擇「管理介面」，進入後會看到如下設定畫面。

MSN病毒

- 案例：通常在你的朋友未上線時，會丟一個網址給你後就離線，例如「**hxxp://xxxx.new.1mages.info/**」，其中「xxxx」會顯示你朋友的暱稱或帳號，讓你失去警戒心；「**1mages.info**」則會一直有新的網址代替。



- 當你按了那個網址進去，千萬別傻傻的看到登入MSN的帳號、密碼就很順手的輸入進去，要不然會被拿去做什麼壞事很難說。



常見MSN病毒感染方式

1. 傳送不知名檔案給你

- 身為你的好朋友，總是會傳個檔案給你，順便跟你說有精彩好康的，通常我們就會不疑地直接接收後趕緊打開，結果...就真的很精彩了。
- 一般收到檔案的副檔名大多是【 .scr .exe .rar .com .zip .jpg .pdf .pig .htm .doc .bat .sys 】，遇到上類型檔案千萬千萬要注意。

2. 傳送不知名連結

- 點選直接就中木馬，然後病毒就一傳十，十傳百。

  這種網頁上暗藏木馬的，必須要防毒軟體有網頁防護才有機會防到，由於不是每套防毒軟體都可以偵測，所以還是有不少人容易中獎。
- 另一種方式更奸詐，把網頁做的很像MSN或是Yahoo官方網頁，網站會要求你輸入帳號密碼，使用者不細查一輸入密碼後，就會發現自己的即時通訊帳號就被登出，這時候病毒的“伺服器”就會偽裝成你，繼續荼毒你的好友，更慘的是，很可能你的密碼就此被改掉，就永遠找不回來了，連要向朋友警告都沒機會。

  例如 ："**想知道哪些人把你封鎖了嗎?**"

MSN解毒參考資訊(1)

- MSN的蠕蟲病毒變型太多種，下列資料提供給大家參考。
  1. 不論如何先登出MSN，如果真的要用，可以先暫時使用Web MSN (http://webmsn.msn.com.tw/)
  2. 如果中的毒是會一直發送訊息給好友，先用以下這招先用看看
     - ① 利用「新增或移除程式」**移除 MSN主程式**
     - ② 刪除資料夾 **C:\ Program Files →MSN Messenger**
     - ③ 刪除 **C:\windows → system32 →msync.exe** (若查無此檔就算了)
       註:如果是接收檔案的病毒，記得在c:\windows\下順便把該檔案刪除)
     - ④ 從「開始」→「執行」→ 輸入「 **regedit**」
       - **HKEY_CURRENT_USER/Software/Microsoft/MSNMessenger** (全部刪除)
       - **HKEY_LOCAL_MACHINE/Software/Microsoft/MSNMessenger**(全部刪除)
     - ⑤ **重新安裝 MSN**

MSN解毒參考資訊(2)

3. 如果是帳號密碼被盜，記得趕緊改密碼，如果改不了，大概得重新申請帳號了吧。

   - 如何更改MSN Messenger密碼？

     ① 在登入MSN軟體時，**在MSN登入面板中按一下〔忘記密碼〕**；或者你也可以直接用瀏覽器**開啟「微軟重設密碼」網站**(https://account.live.com/ResetPassword.aspx?mkt=ZH-TW)，在「Windows Live ID」欄位中輸入你的MSN帳號，然後在下面輸入圖片驗證碼，再按〔繼續〕，進行下一步。

     ② 接著點選「**以電子郵件傳送密碼重設資訊給自己**」，然後再點選你的Email信箱後按下〔繼續〕，讓微軟將你的MSN密碼重設的網址傳送到你的Email信箱中。

     ③ 待「**密碼重設資訊已傳送**」畫面出現後，直接按一下〔確定〕。

     ④ 當收到「**重設您的Windows Live 密碼**」信件後，在「確認要求並重設密碼」下面的連結按一下，開啟重設密碼的網頁。

     ⑤ 接著在「Windows Live ID」填上你的MSN帳號，然後再下面**設定你的新密碼**，最後再按下〔繼續〕。

     ⑥ 全部完成後，會出現「**密碼已變更**」的畫面，此時我們便可直接用原本的MSN帳號跟你新設定的密碼來登入MSN，繼續聊天囉！

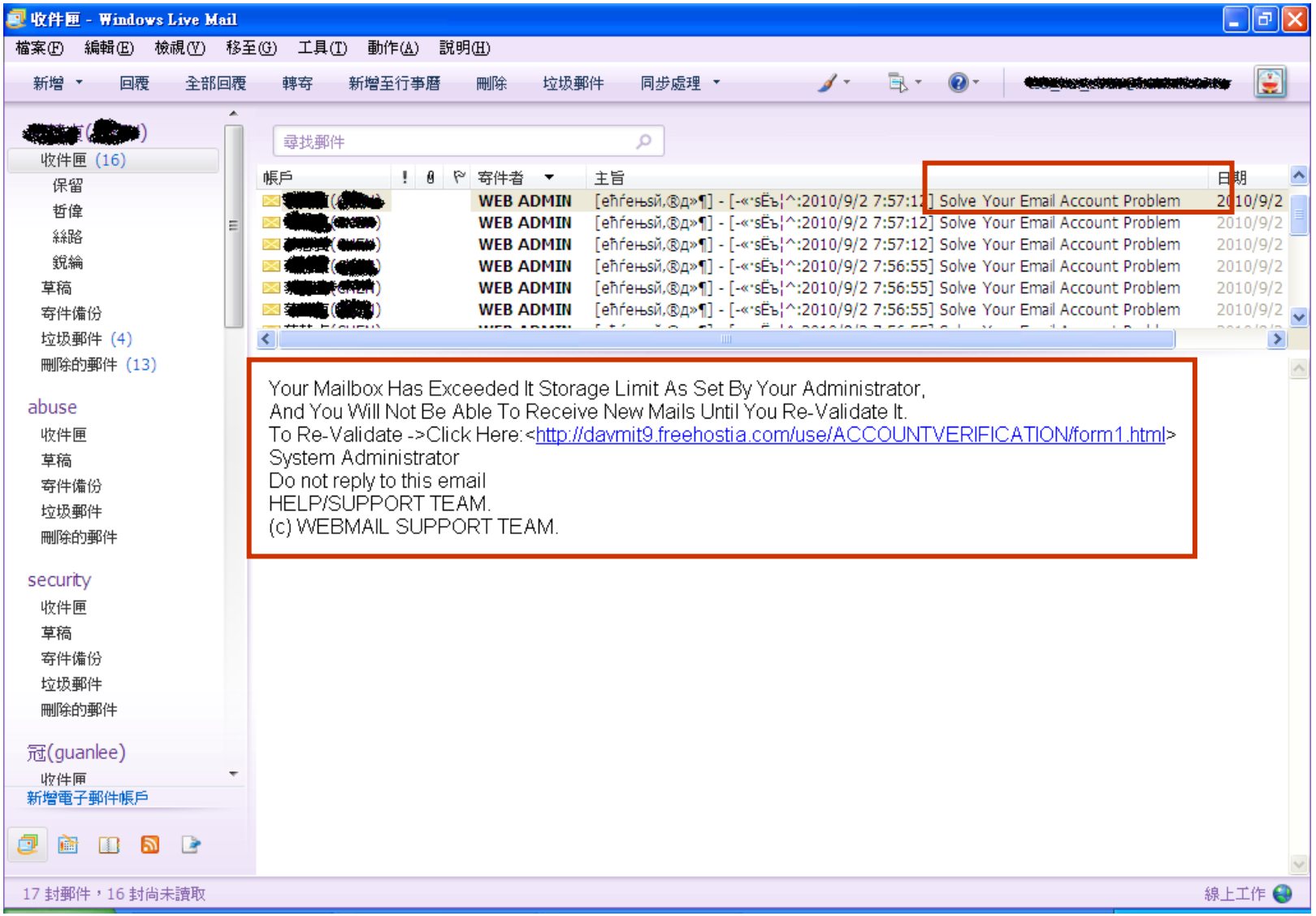
4. 若真的都不行，就只好重灌囉 ^^

要如何避免MSN中毒呢？

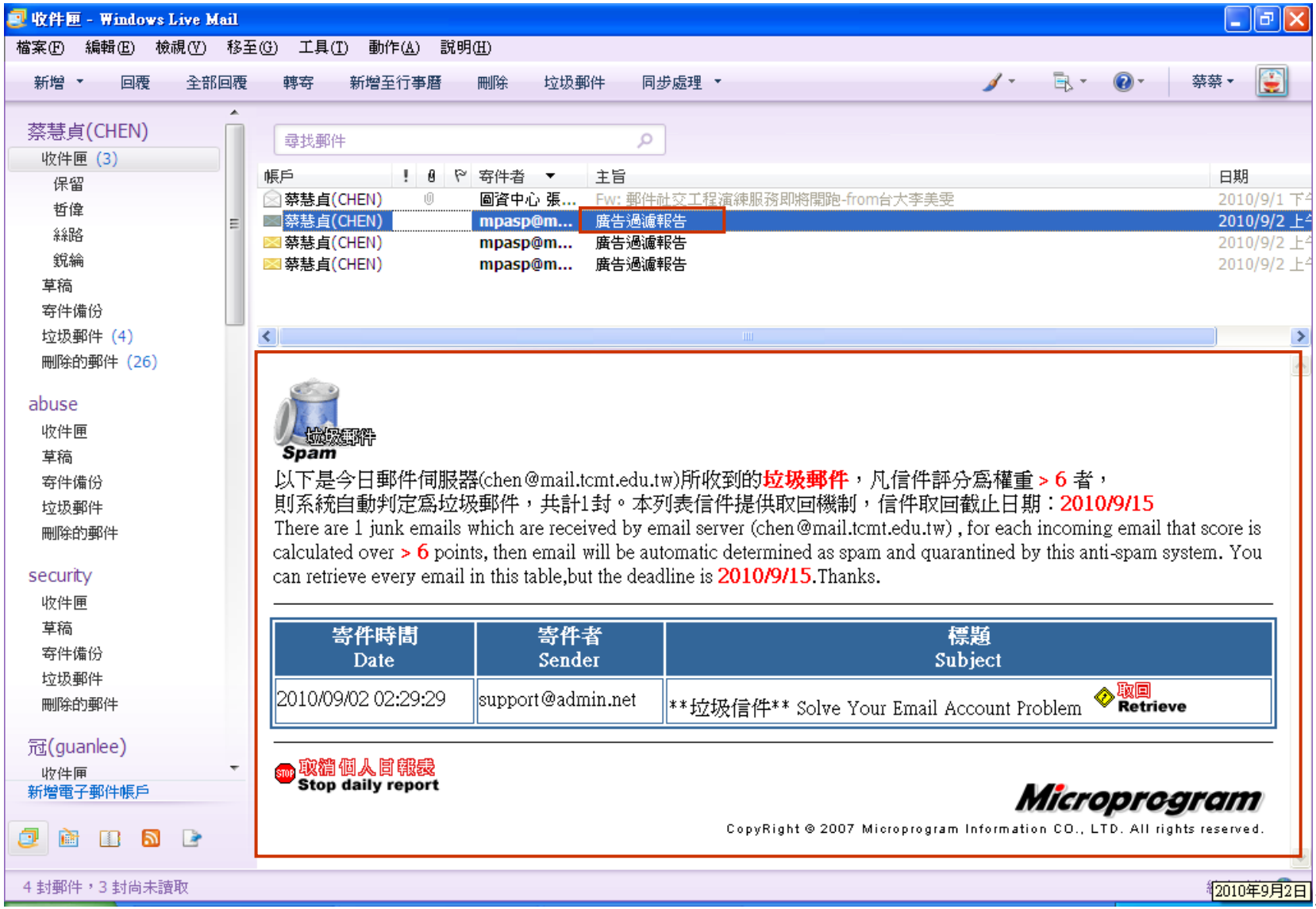
1. **不明的連結或檔案不要開**，這應該是最高指導原則，不過大家都喜歡和朋友分享有趣的網站，所以如果收到連結，可以問一下朋友這是甚麼!如果朋友都不回，那就真的有問題!! (不過聽說新品種的病毒，還會自動回覆訊息，所以還是得注意啊)
2. 如果想開連結或檔案，又不想問人，至少靠自己判斷一下到底有沒有危險
   - **很久不丟訊息的朋友忽然丟個連結給你**:除非算命說你今天犯桃花，人緣奇佳不然還是問一下好了。
   - **訊息是簡體字或是英文**，這兩種語言的人口多，所以病毒大多以這兩種語言為主，遇到這兩種語言的還是小心點。
   - **朋友訊息丟完就離線**:這朋友大概凶多吉少，很有可能就是中了病毒趕緊離線怕害到朋友。
3. **收到連結或檔案時，謹守「停看聽」原則**，先去泡杯咖啡，看個報紙，回來看看朋友有沒有在哀哀叫，千萬不要身先士卒。
4. **防毒軟體一定要裝**。
5. **記得要做Windows Update**。


郵件綁架

案例：釣魚信件— 竊取帳號、密碼



防堵：本校歸類垃圾信件，請不要取回。



Q：信件一直收不到？

近日上網(Webmail)收信或利用Outlook Express、Outlook收信總是收不到信？

A：登入本校Webmail系統(http://mail.tcmt.edu.tw) 查看是否因近日電腦中毒被駭客修改了信件轉寄功能。

① 點選「個人設定」→「信件處理」→「自動轉寄」。

② 取消勾選「我要啟用信件自動轉寄信件功能。

③ 刪除電子郵件欄位中填寫之E-MAIL位址。

垃圾郵件範例(1)

- 斧神工！你相信這全都是蛋糕嗎??
- 小心！雷射當保養 護膚不成反毀容！！
- 眩暈患者苦不堪言 如何面對眩暈?
- 上班累了嗎?放鬆一下，輕鬆的冷笑話:)
- 印度的九九乘法表是從1背到19?
- 讓你忘不了的安全帶宣導影片！

注意：好奇心是會要人命的!!

因為：傷神(擔心檔案不見了)又傷時(修電腦)

貼心小叮嚀

- 當您無法透過學校網站/教職員資訊網 進入 WEBMAIL系統收發信時，請直接打開IE瀏覽器，輸入 http://mail.tcmt.edu.tw登入。

免費個人防護

免費電腦安全掃描，防護個人資訊安全(1)

- Windows Live OneCare 安全掃描工具是全新的免費服務，協助您全方位防護個人資訊安全。
  - 針對電腦病毒、安全漏洞、間諜軟體，提供創新全方位掃描與清除服務
  - 偵測與移除老舊無用檔案，並搭配硬碟重組功能，大幅提升電腦系統執行效能
  - 有效強化資訊安全，提供個人用戶高效能的資訊安全防護新體驗
- 完整掃瞄服務網址
  http://onecare.live.com/site/zh-tw/default.htm

免費電腦安全掃描，防護個人資訊安全(2)

- 趨勢科技提供了免費的網頁過濾(WTP Add-on)及清毒工具(解毒快手iClean)，即使您不是趨勢用戶也可以使用，加強保護您電腦的安全!!

  - **WTP Add-On 網頁威脅防禦工具**

    這套輕盈的網頁威脅防禦工具，能有效且主動防護您的電腦，使您遠離網頁威脅和僵屍Bot 程式的攻擊。

    http://www.trendmicro.com.tw/wtp/micro/index.asp

  - **iClean解毒快手 清毒工具**

    趨勢科技 iClean解毒快手，能有效清除近期台灣地區常見的木馬、病毒及惡意程式，讓您輕鬆、快速地為電腦進行急救。

    http://www.trendmicro.com.tw/iclean/index.htm

貼心小叮嚀

- 現在病毒的更新速度比防毒程式還快，所以沒有一種防毒程式能100%有效的防範。
- 隨時注意你電腦的「隱藏檔選項」，這是一個很有效的指標。
- 隨身碟在別的電腦使用過之後，一定要再三檢查確認無毒。
- 電子郵件的毒也要小心，就算是朋友寄來的也很可能有毒，下載任何附加檔案或是點選連結之前請三思。

電子郵件社交工程演練

99 年度學術機構分組防範惡意電子郵件社交工程第一次演練成果

- 演練期間：99.09.02 - 99.09.06
- 參加人數：本教職員100位(隨機抽取)
- **信件開啟率：33%**
- **點擊郵件所附連結率：3%**
- **點擊郵件所附檔案：1%**

類別	郵件主旨	開啓率	開啓人數	附檔點擊率	點擊人數	URL連結點擊率	點擊人數
科技類 iphone4預購	Iphone4預購 仍有機會最快拿到最新的Iphone4！	5%	5	-	-	-	-
趣味類 冷笑話	**上班累了嗎?放鬆一下，輕鬆的冷笑話:)**	**18%**	**17**	**-**	**-**	**1%**	**1**
情色類 大陸美女	大陸版取經妹~挑戰尺度演出！	8%	6	1%	1	1%	1
美容類 雷射	**小心！雷射當保養 護膚不成反毀容！**	**15%**	**10**	**2%**	**2**	**3%**	**3**
知識類 99乘法	**印度的九九乘法表是從1背到19?**	**13%**	**11**	**1%**	**1**	**1%**	**1**
時事類 塑膠水壺	你家小孩的水壺安全嗎?	12%	7	2%	2	3%	3
健康類 眩暈	眩暈患者苦不堪言 如何面對眩暈?	8%	8	-	-	-	-
趣味類 蛋糕	鬼斧神工！你相信這全都是蛋糕嗎??	10%	8	1%	1	1%	1
旅遊類 觀光局	綠島低碳單車遊 2天1夜四大主題	11%	9	1%	1	1%	1
生活類 安全帶	讓你忘不了的安全帶宣導影片！	11%	8	1%	1	3%	3
平均		11%	8.9	1%	0.9	1%	1.4

電子郵件社交工程演練 (1)

- 目的

  為強化教職員資安意識，降低社交工程攻擊風險，教育部將於9月開始進行不定時郵件社交工程演練。

- 什麼是社交工程

  社交工程是惡意人士就使用者於防範詐騙沒有足夠的認知情況下，以輕易地避過了軟硬體安全防護，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，所造成的損害與威脅。

- 小叮嚀

  教育部與國家資通安全會報每年會定期與不定期寄送惡意電子郵件至教職同仁信箱，如果無警覺性打開電子郵件所提供的檔案或是連結，即會被記點，然後會統計各單位被記點的次數，做為未來教育訓練與獎懲標準。**請大家使用電子郵件時，務必小心，不要開啟看起來很可疑的電子郵件。可疑的電子郵件都是和公務沒有關係的郵件。**

電子郵件社交工程演練 (2)

- 電子郵件社交工程的攻擊手法：
  - 假冒寄件者
  - 使用讓人感興趣的主旨與內文
  - 含有惡意程式的附件
  - 利用零時差攻擊
  - 網路釣魚
- 可疑電子郵件之自我保護措施：
  - 關閉預覽窗格。
  - 非必要閱讀之郵件逕行刪除。
  - 設定為純文字讀取模式再開啟郵件閱讀。
  - 開啟郵件內含之超連結時先確認連線網址之網域名稱(Domain Name)是否足以識別？
  - 若為數字IP之網址勿輕易開啟。不隨意輸入資料送出，傳送私密資料時確認是否有啟動加密機制。
  - 分辨電子郵件的真偽。

電子郵件社交工程演練 (3)

- 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，確認對應軟體都保持在最新的修補狀態
  - 提高警覺，加強危機意識

電子郵件社交工程演練 (4)

- 電子郵件社交工程防範：
  - 注意可疑電子郵件之特徵
    - 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。
  - 可疑電子郵件之自我保護措施
    - 關閉預覽窗格
    - 非必要閱讀之郵件逕行刪除
    - 設定為純文字讀取模式再開啟郵件閱讀。
    - 不隨意輸入資料送出，傳送私密資料時確認是否有啟動加密機制。

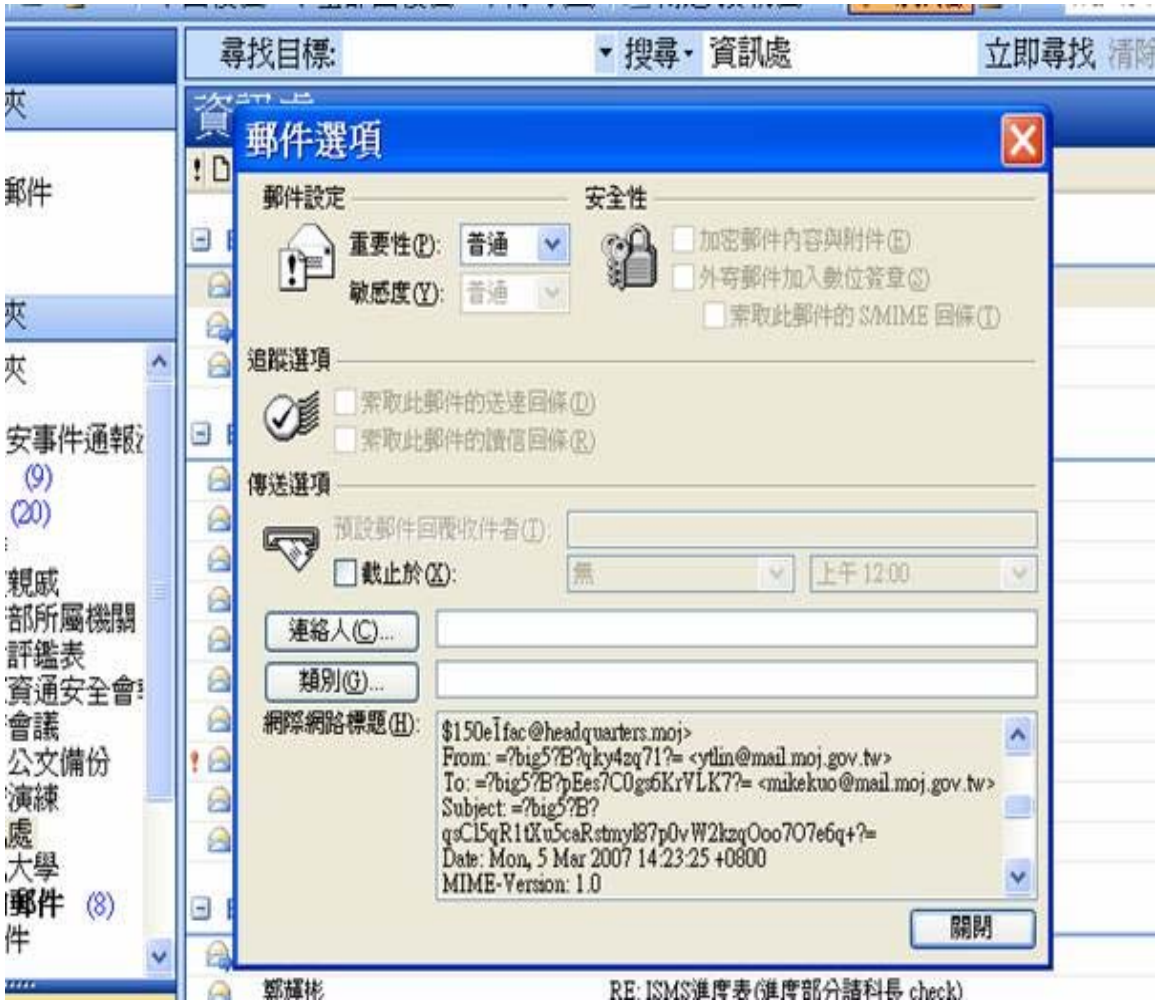
電子郵件社交工程演練 (6)

- 關閉預覽窗格

電子郵件社交工程演練 (7)

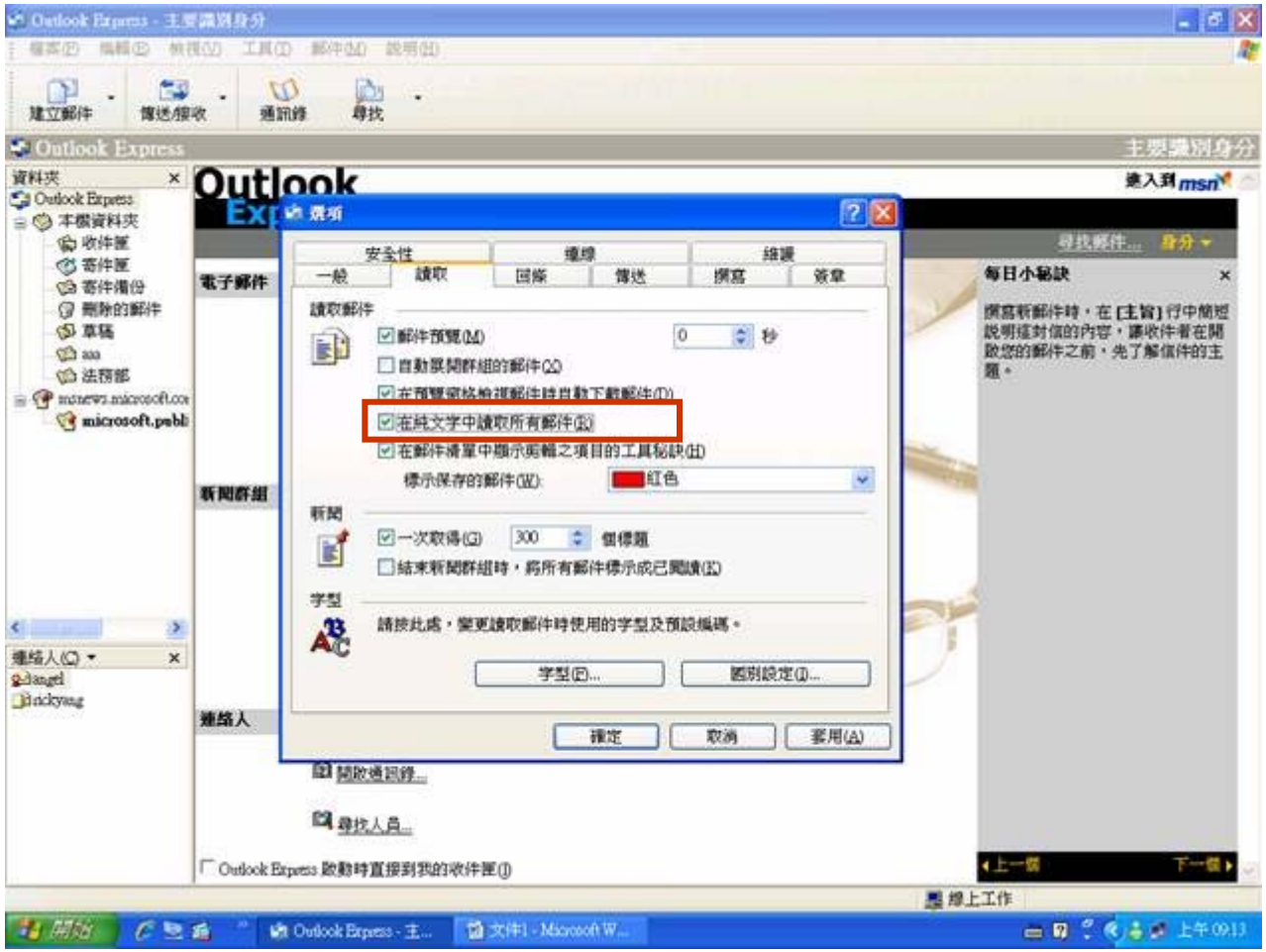
- **非必要閱讀之郵件逕行刪除 / 確定發信者電子郵件帳號**

於該信件按滑鼠右建，點選【內容】->【詳細資料】(Outlook Express)或點選【郵件選項】(Outlook)確任發信者電子郵件帳號，惟發信者電子郵件帳號仍有被偽冒的機率，必要時直接與寄信者連絡確認是否來信。



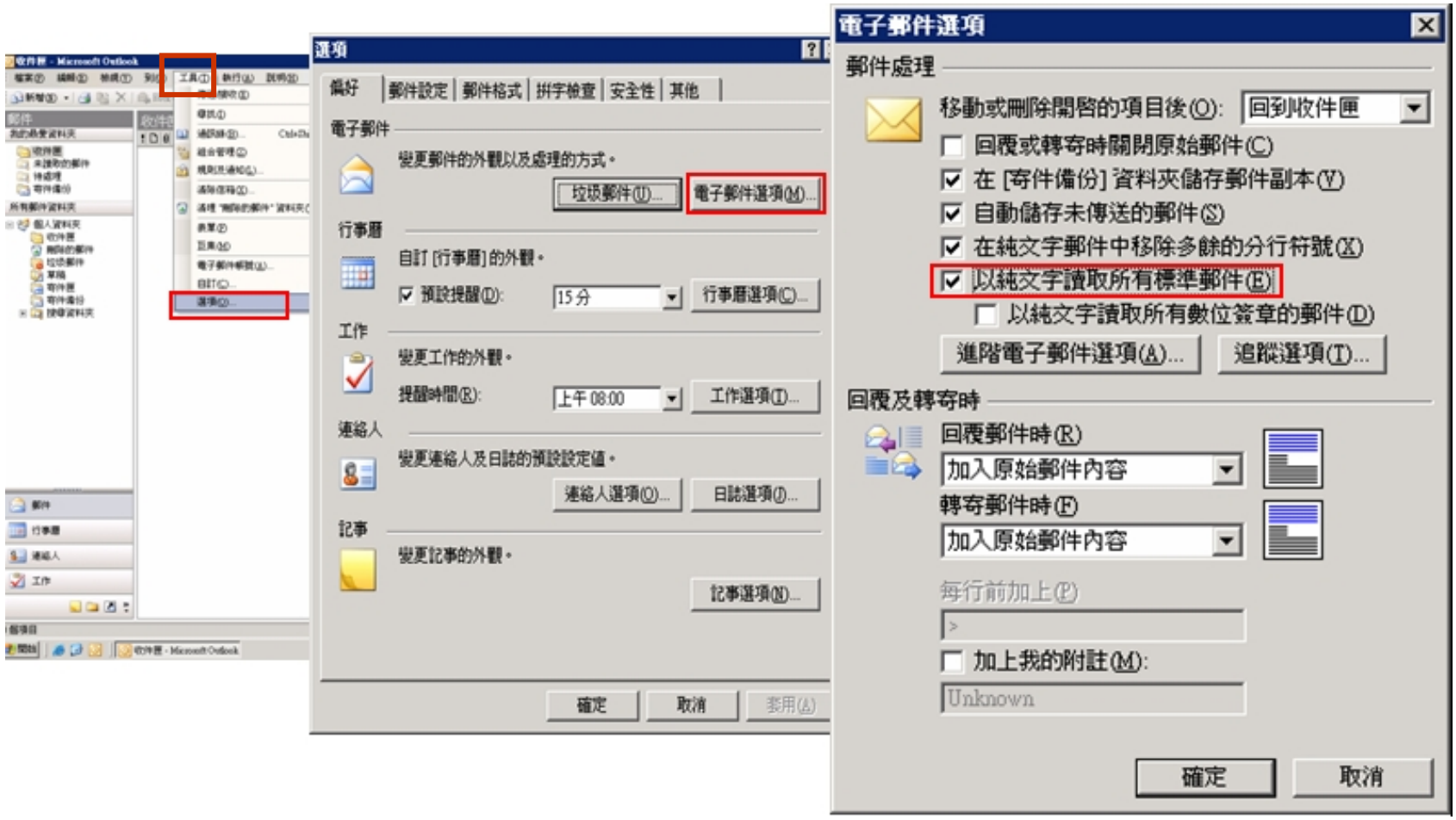
電子郵件社交工程演練 (8)

- 設定純文字讀取模式(Outlook Express)



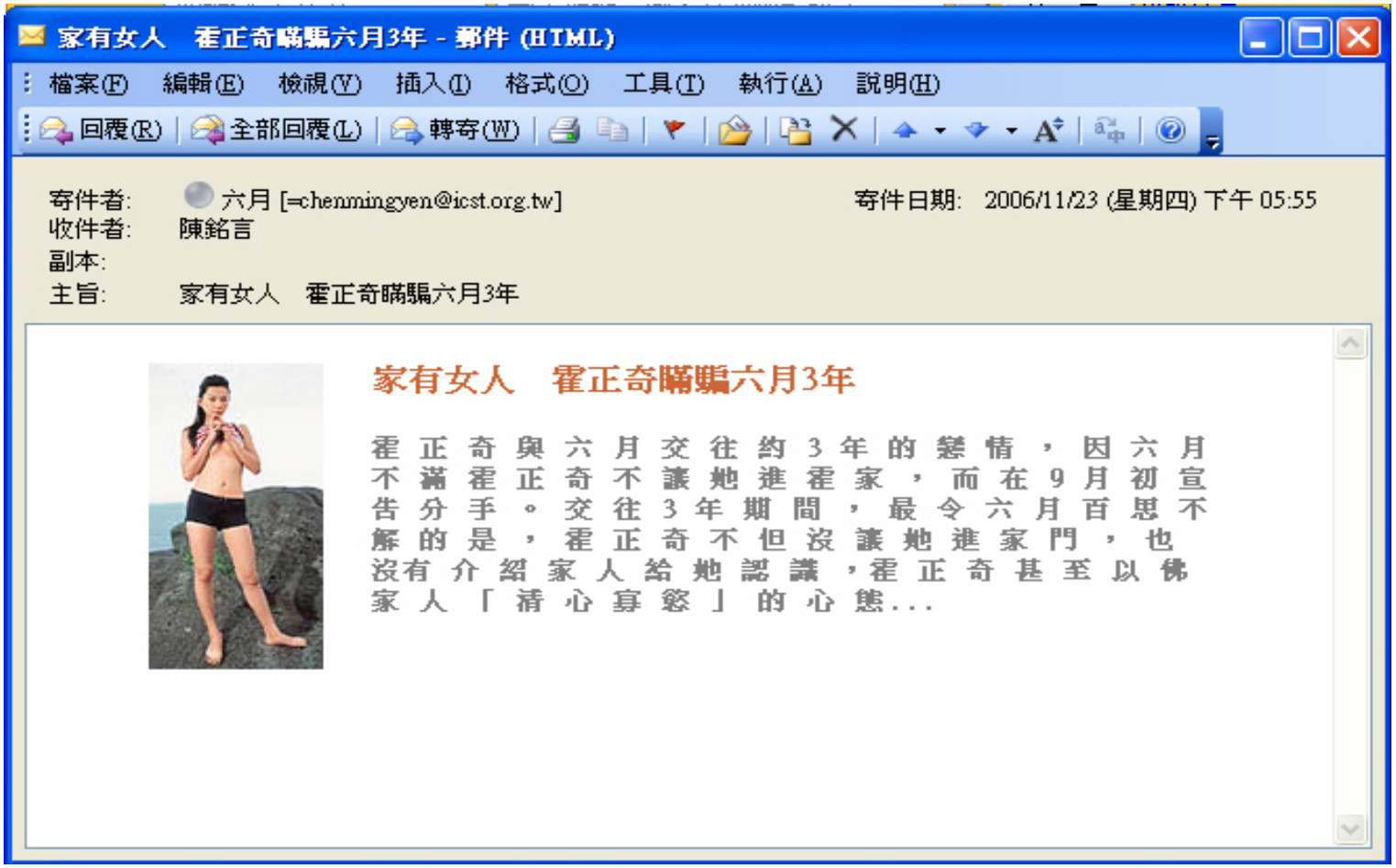
電子郵件社交工程演練 (9)

- 設定純文字讀取模式(OFFICE Outlook)



電子郵件社交工程演練 (10)

- **範例1 惡意網頁攻擊(八卦主旨)**



以上資料來源爲法務部全球資訊網http://elearning.nat.gov.tw/

電子郵件社交工程演練 (11)

- **範例2 惡意圖檔攻擊(情色主旨)**

以上資料來源爲法務部全球資訊網http://elearning.nat.gov.tw/

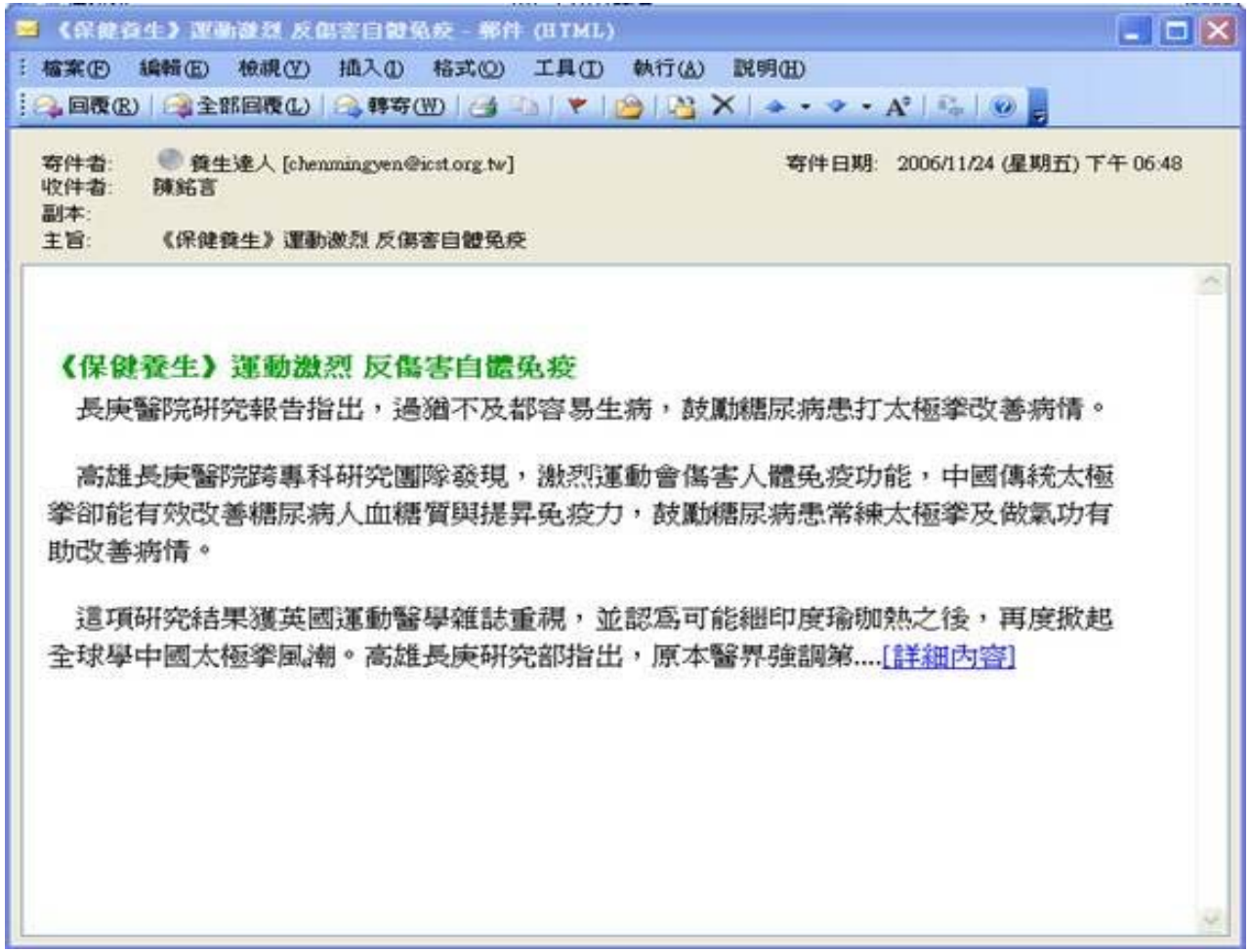
電子郵件社交工程演練 (12)

- **範例3 惡意word檔攻擊(休閒娛樂主旨)**

以上資料來源爲法務部全球資訊網http://elearning.nat.gov.tw/

電子郵件社交工程演練 (13)

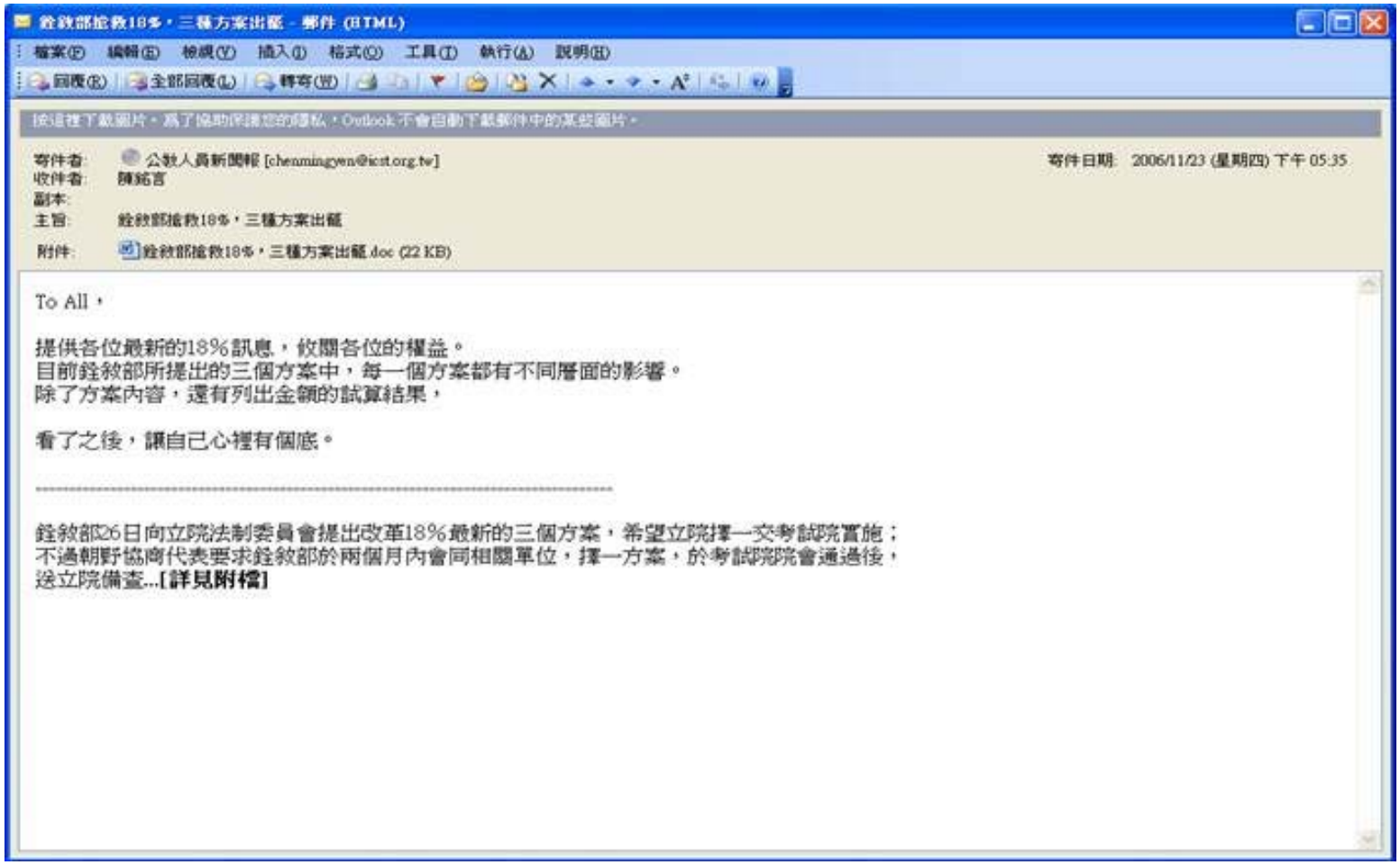
- **範例4 惡意網頁攻擊(養生保健主旨)**



以上資料來源爲法務部全球資訊網http://elearning.nat.gov.tw/

電子郵件社交工程演練 (14)

- **範例5 惡意word檔攻擊(公務人員相關主旨)**



以上資料來源爲法務部全球資訊網http://elearning.nat.gov.tw/

預告

99 年度學術機構分組防範惡意電子郵件社交工程第二次演練成果

演練期間：99.09.14 - 99.09.16

問題與討論