電子郵件社交工程與防護

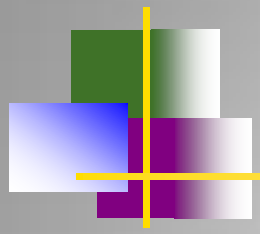
計算機與通訊中心
網路系統組 陳怡碩
E-mail：yschen@cc.nthu.edu.tw
分機：31234

大綱

- 新聞事件
- 資訊安全
- 社交工程介紹
- 教育部演練計畫
- 電子郵件社交工程的防護
- 相關資訊
- Q & A

新聞事件

- 社交網站成為網路犯罪目標
- Fortinet 7月網路威脅報告
  - 電子賀卡垃圾郵件主要是利用直接連結、Google 網上論壇和 Tinypic 相片分享服務做為散佈工具
  - MS ActiveX Video 控制項弱點，微軟於 7 月 14 日發佈了修補程式 MS09-032
  - MS Office Web Components ，在本文撰寫之時修補程式尚未發佈。
- Twitter、Facebook遭駭客攻擊（「阻斷服務式攻擊」denial-of-service）8/5 —— 工商時報08/08/2009
  - 透過大量的「傀儡電腦」攻擊
- Flash 0day漏洞攻擊首現中國網際網路7/30 —— 鉅亨網新聞中心 30/07/2009
- 韓國主要網站同時遭攻擊：2萬電腦淪為肉雞 7/7 —— 新華網 10/07/2009



資訊安全

資訊安全的定義

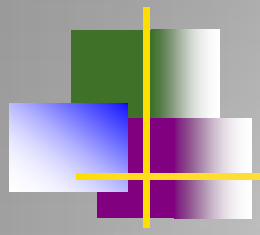
- 靜態資訊（電腦安全）
  - 根據電腦處理個人資料保護法之相關規定，需審慎處理及保護個人資訊。
  - 建立系統備援設施，定期執行必要的資料、軟體備份及備援作業，以便發生災害或儲存媒體失效時，可迅速回復正常作業。
  - ……
- 動態資訊（網路安全）
  - 與外界網路連接之網點，設立防火牆控管外界與內部網路之資料傳輸及資源存取，並執行嚴謹的身分辨識作業。
  - 機密性及敏感性的資料或文件，不存放在對外開放的資訊系統中，機密性文件不以電子郵件傳送；敏感性資訊如有電子傳送之必要，需經加密或電子簽章等安全技術處理後傳送。
  - ……

個人電腦安全的威脅

- 自然損害
  - 地震、颱風、水災...
- 電腦主機硬體損害
  - 不預期斷電、硬體故障...
- 人為損害
  - 駭客、內部人員、電腦病毒...

網路連線的安全

- 攻擊：外部駭客入侵及病毒散播
  - 電子郵件社交工程
  - USB病毒
  - …
- 防護：工具或網路技術建立安全通道
  - 工具：防火牆…
  - 網路技術：電子簽章、識別協定
  - …



社交工程介紹

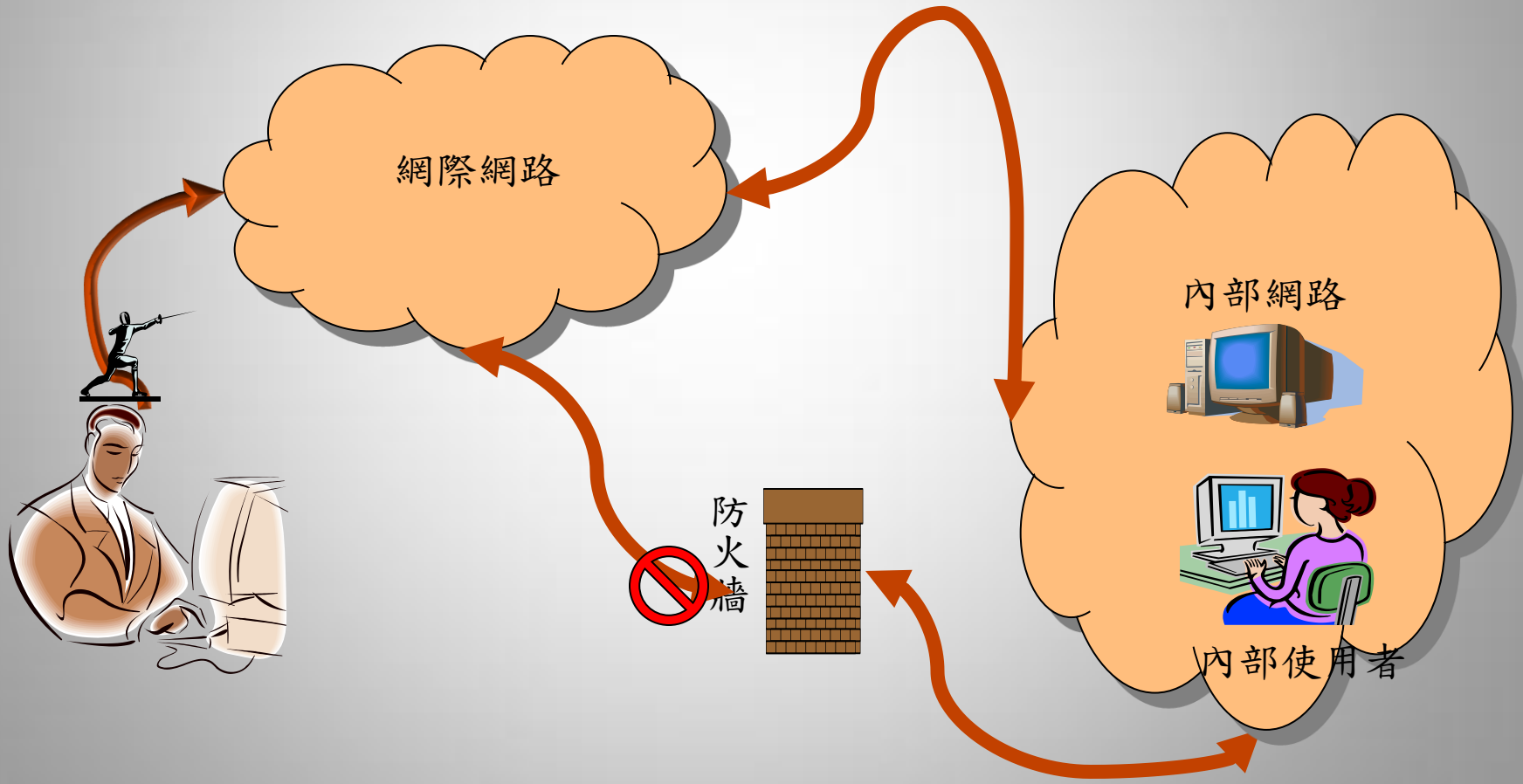
社交工程

- 社交工程的定義
  - 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。
  - 網路世界的數位安全(Secrets & Lies: Digital Security in a Networked World)的作者Bruce Schneier曾提到所謂社交工程，全都是由人性方面，也就是利用所謂的”信任”來進行。
  - 欺騙的藝術(The Art of Deception)的作者（Kevin Mitnick），更進一步的解釋到人類的天性就是很希望能幫助別人，因此也相當容易被欺騙。
  - 以人為本、騙術為主
  - 技術門檻低
  - 貪心、好奇
  - 缺乏警覺性：有那麼嚴重嗎？

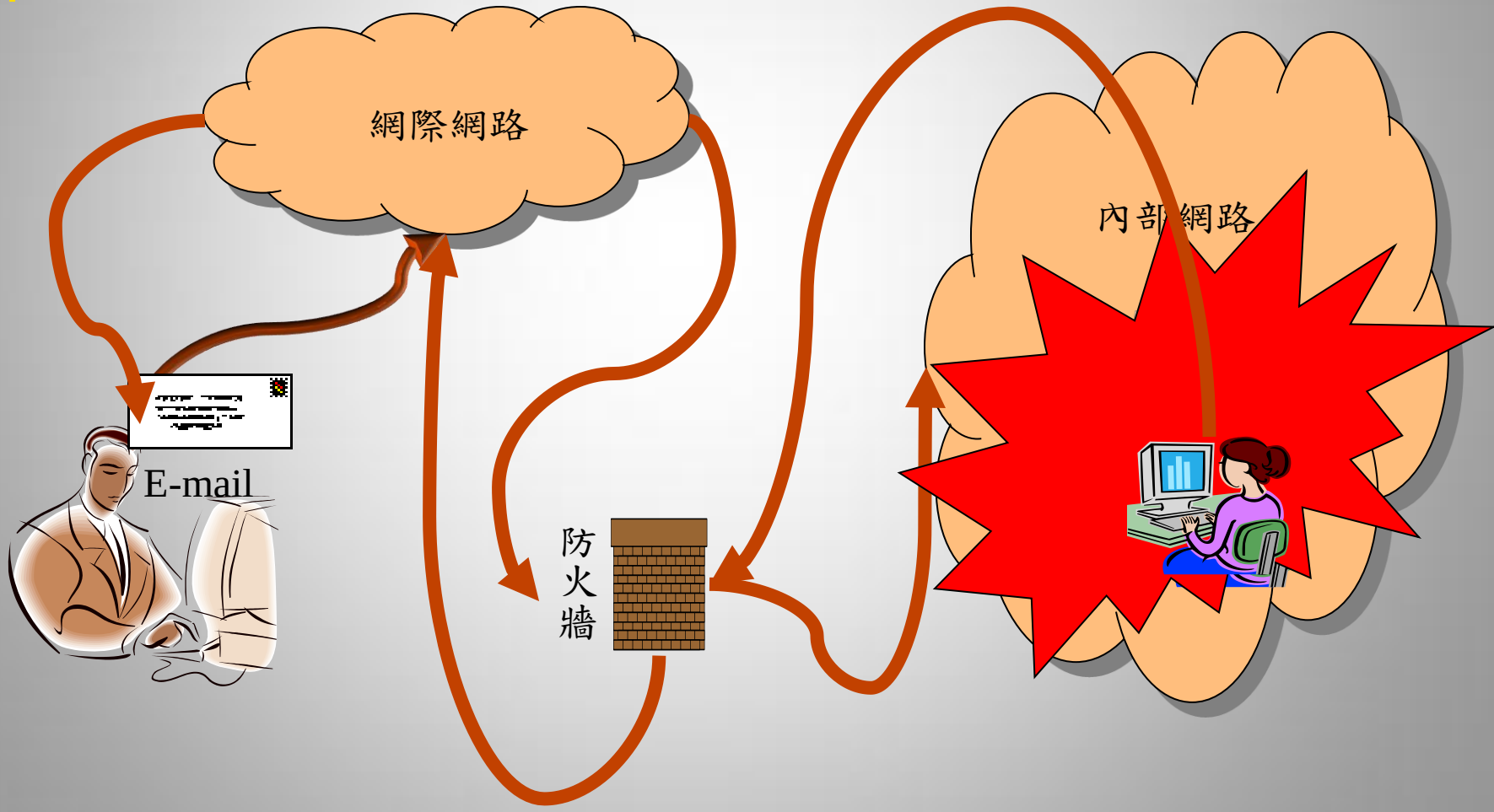
社交工程攻擊的定義

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

常見網路攻擊



現在網路攻擊模式



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
- 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
- 使用者開啟信件
- 啟動或下載有害程式
- 反向輸出使用者資料（轉眼變成受害者）

軟體弱點與零時差攻擊

- 只要是軟體就可能存在有弱點，未能及時修補的話，就可能遭利用被入侵成功。
- 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」。

常見被利用的軟體弱點

- 微軟的作業系統和文書軟體
  - Microsoft office（word）
- 常見的應用軟體
  - Winrar、adobe reader、flash player等軟體

電子郵件社交工程的手法

- 網路釣魚(Phishing)
  - 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。
  - 偽造網址：http://www.hinet.net ←→ http://www.hinet1.net
  - 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、天上掉下來的禮物...

教育部演練計畫

教育部電子郵件社交工程演練之信件主旨

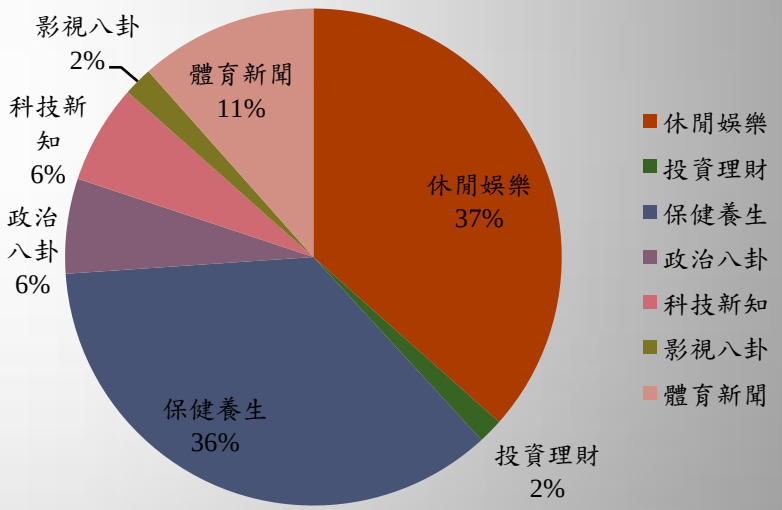
- 新流感 H1N1 大流行期間，個人保健注意事項
- 自行車旅遊私房路線
- 瑤瑤和舒舒，你喜歡誰
- 景氣復甦了嗎？
- 洋基球團虧待王建民
- 聯合報邀請您賞桐花
- 軍方賣官內幕
- 蛀牙不是病，痛起來要人命
- 蔡依林愛無赦+練舞功超神奇混音版
- USB成病毒溫床！台灣電腦今年Q1中毒率列入全球第四大

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

教育部電子郵件社交工程演練結果

- 本校排名為B級單位(全國102所大學)：第45名
- 參加人數：278
- 開啟信件：6.69%
- 點選連結：1.51%
- 平均：4.10%
- 未通過測試人數：90



演練郵件格式

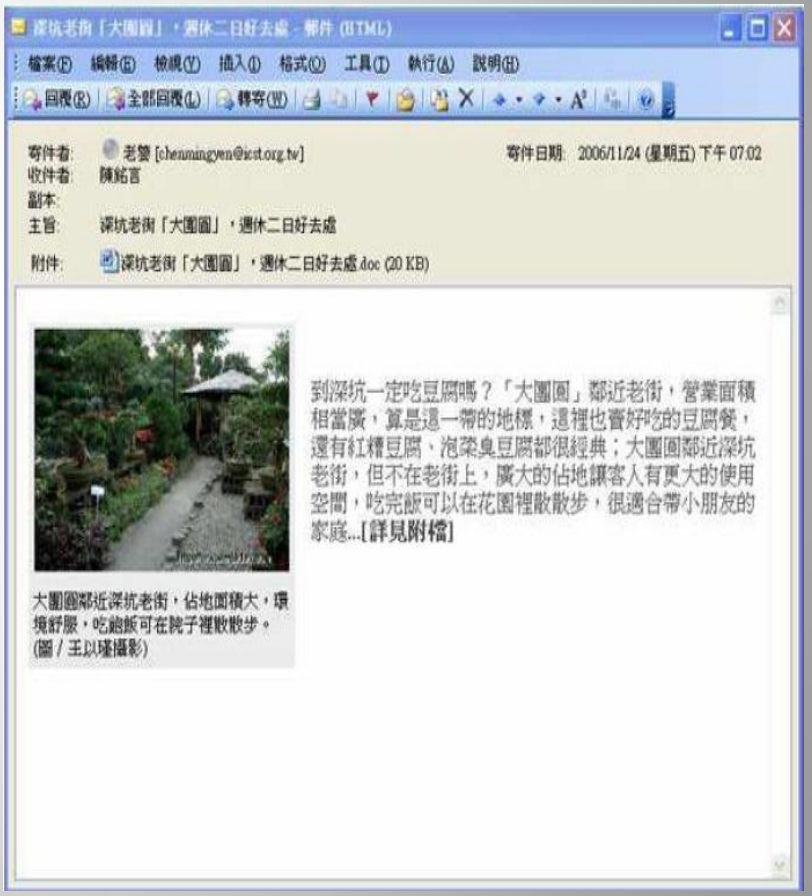
- 惡意網頁攻擊（八卦主旨）

演練郵件格式

- 惡意圖檔攻擊（情色主旨）

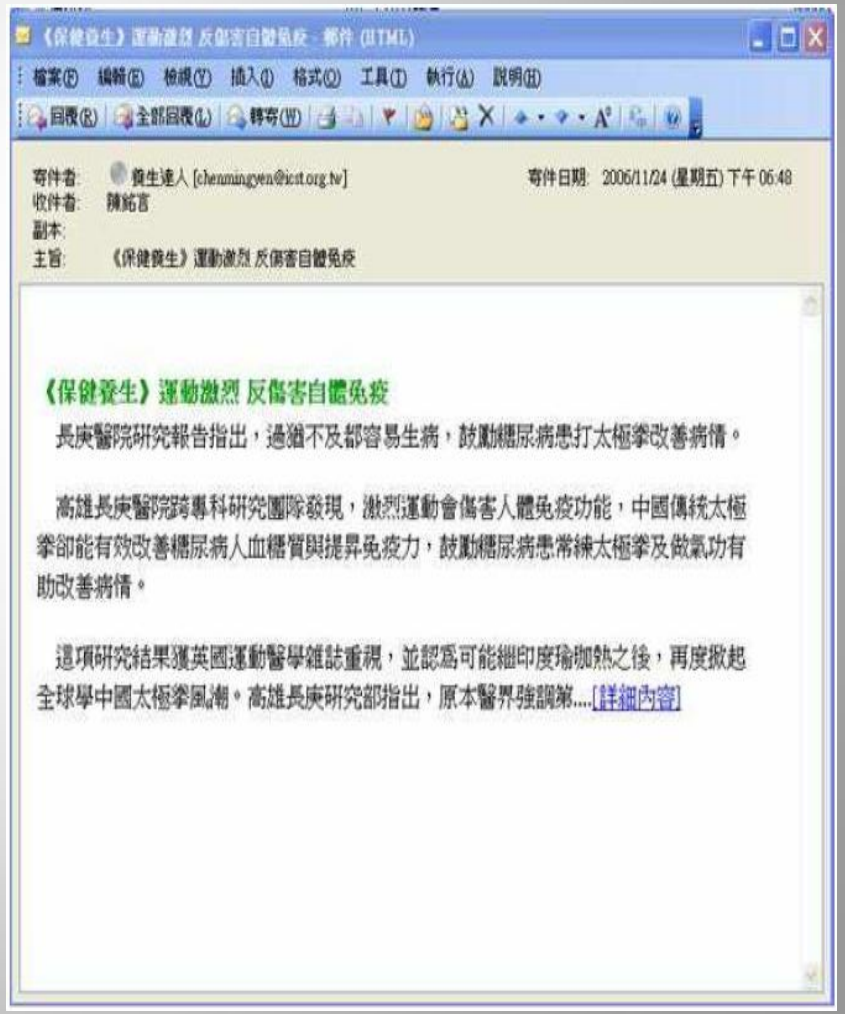
演練郵件格式

- 惡意word檔攻擊（休閒娛樂主旨）



演練郵件格式

- 惡意網頁攻擊（保健養生主旨）

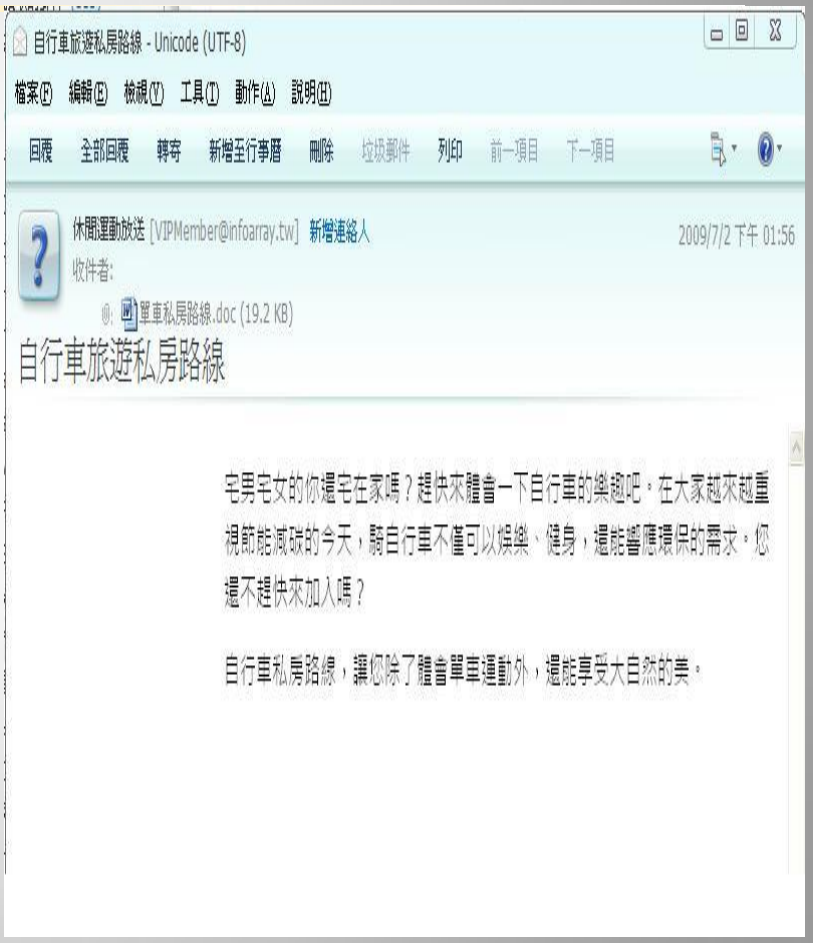


演練郵件格式

- 惡意word檔攻擊（公務人員相關主旨）

演練郵件格式

- 惡意word檔攻擊（休閒娛樂主旨）



電子郵件社交工程的防護

電子郵件社交工程的防護

- 基本的防護
  - 作業系統更新
  - 應用軟體更新
  - 防毒軟體、個人防火牆
- 再多一點的防護
  - 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
- 近乎完美的防護
  - 改變使用習慣

基本的防護

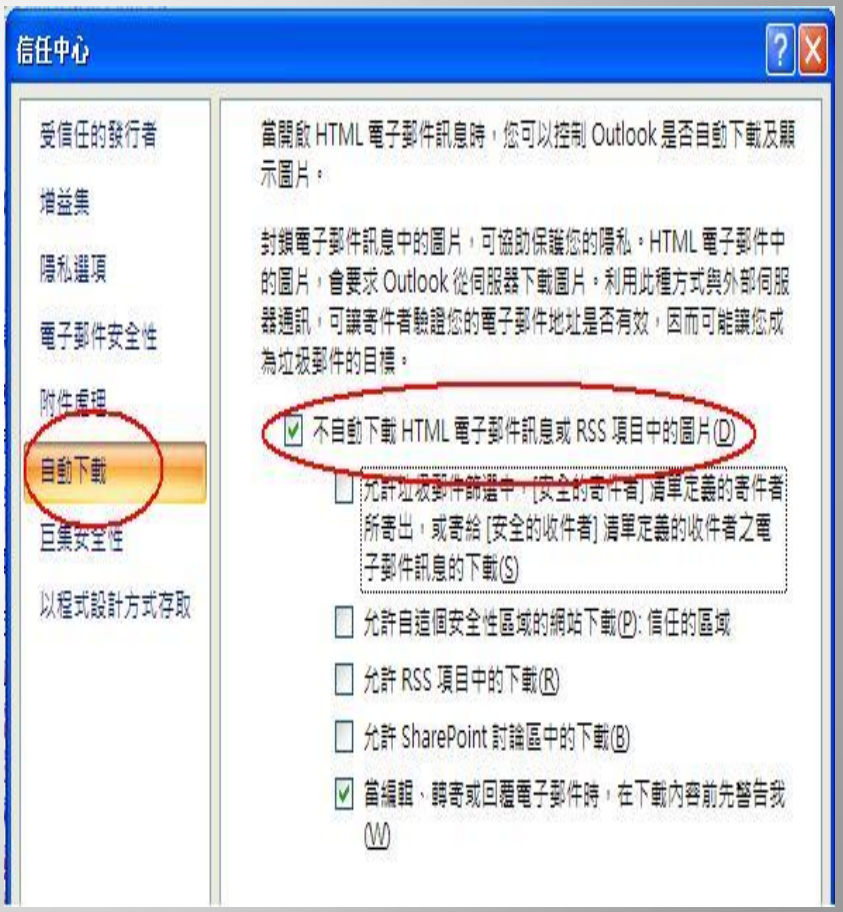
- 作業軟體更新
  - 設定自動更新 microsoft update
- 應用軟體更新
  - Adobe reader…等軟體
- 安裝防毒軟體、個人防火牆並更新病毒碼
  - 卡巴斯基、賽門鐵克、趨勢（學校授權）

再多一點的防護

- 變更看信軟體的設定，提高安全性
  - 不自動下載圖檔（強烈建議）
    - outlook 2007
    - outlook express
    - live mail
  - 關閉信件預覽功能（建議）
    - outlook 2007
    - outlook express
    - live mail
  - 以純文字開啟信件（建議）
    - outlook 2007
    - outlook express
    - live mail

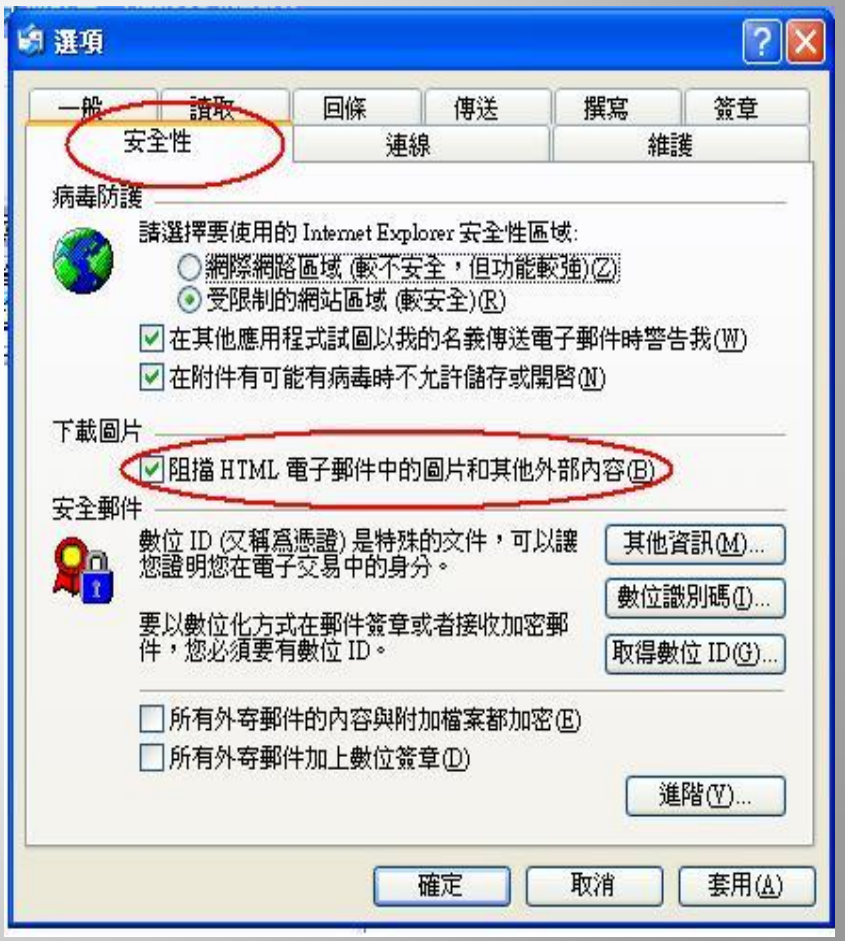
Outlook 2007

- 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



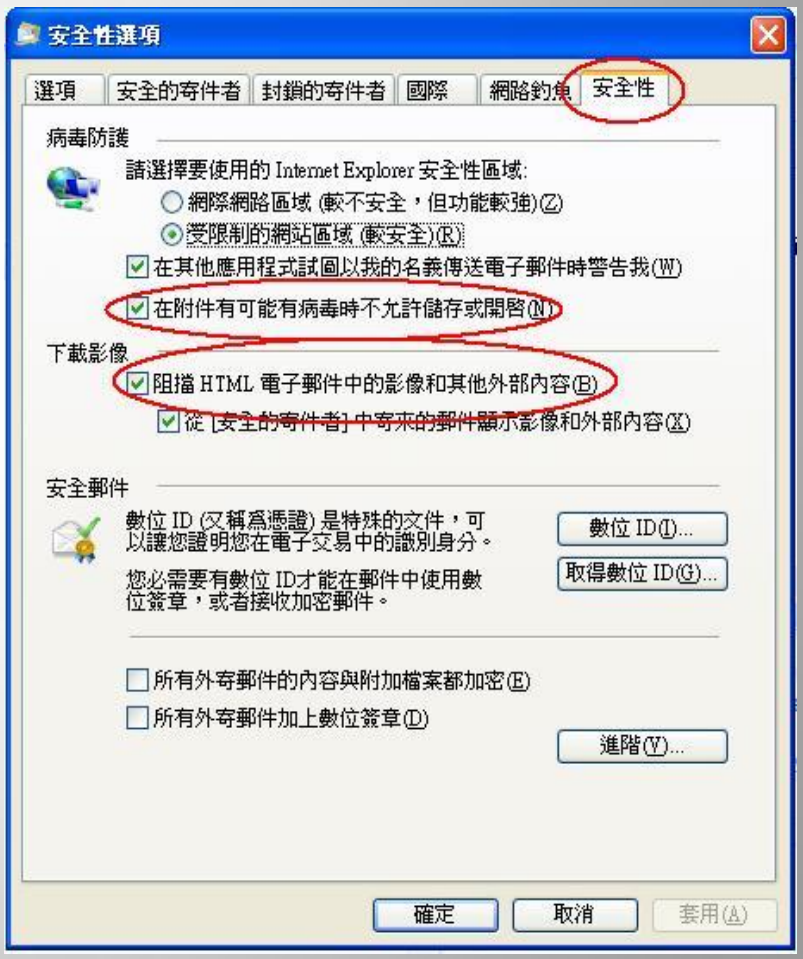
Outlook express

- 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



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

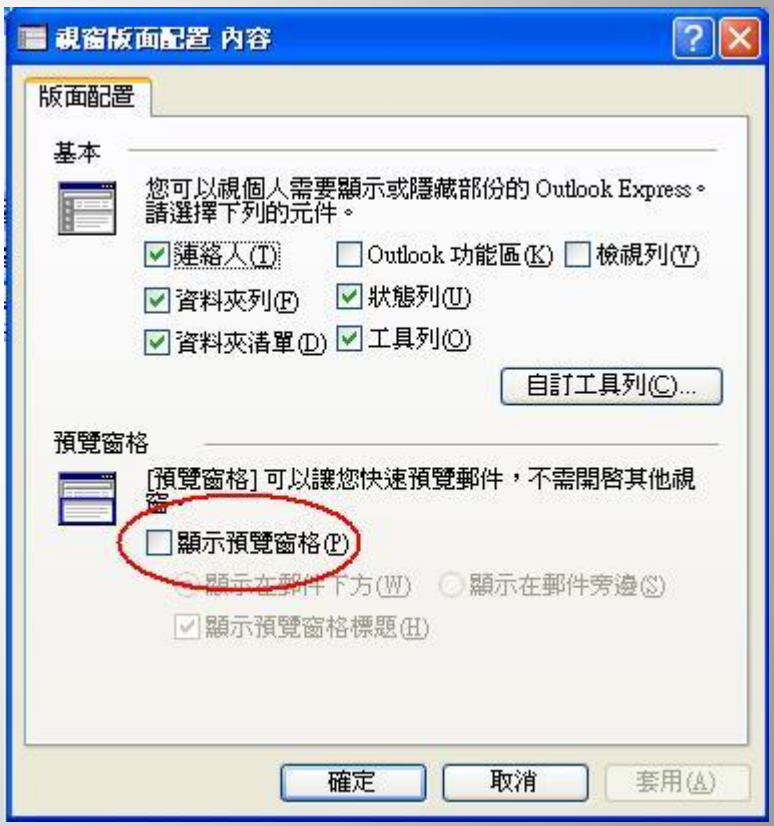


outlook 2007

- 開啟outlook 2007
- 選取【檢視】
- 選取【讀取窗格】
- 選擇【關】

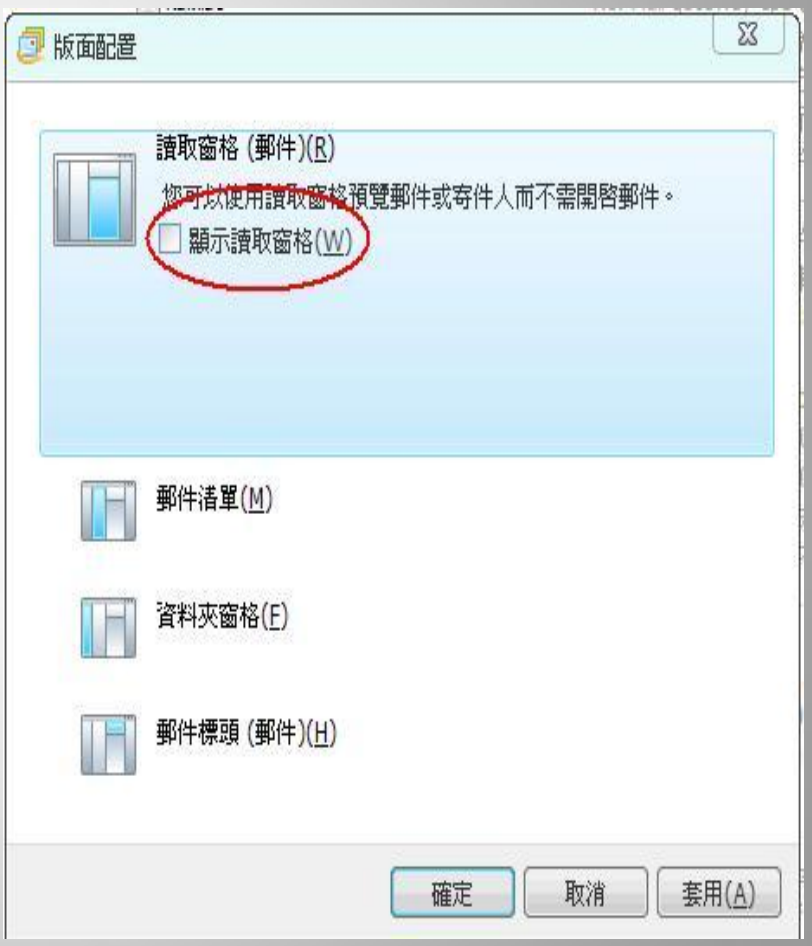
Outlook express

- 開啟 outlook express
- 選取【檢視】
- 選取【版面配置】
- 【顯示預覽窗格】不打勾



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

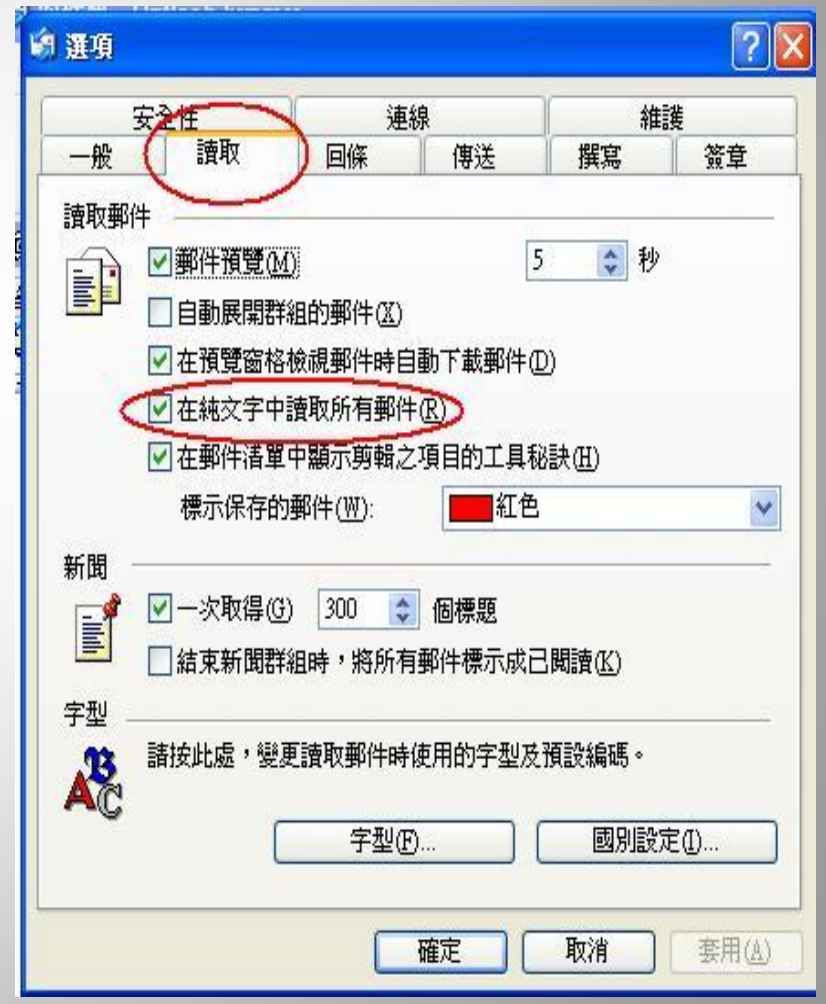


Outlook 2007

- 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

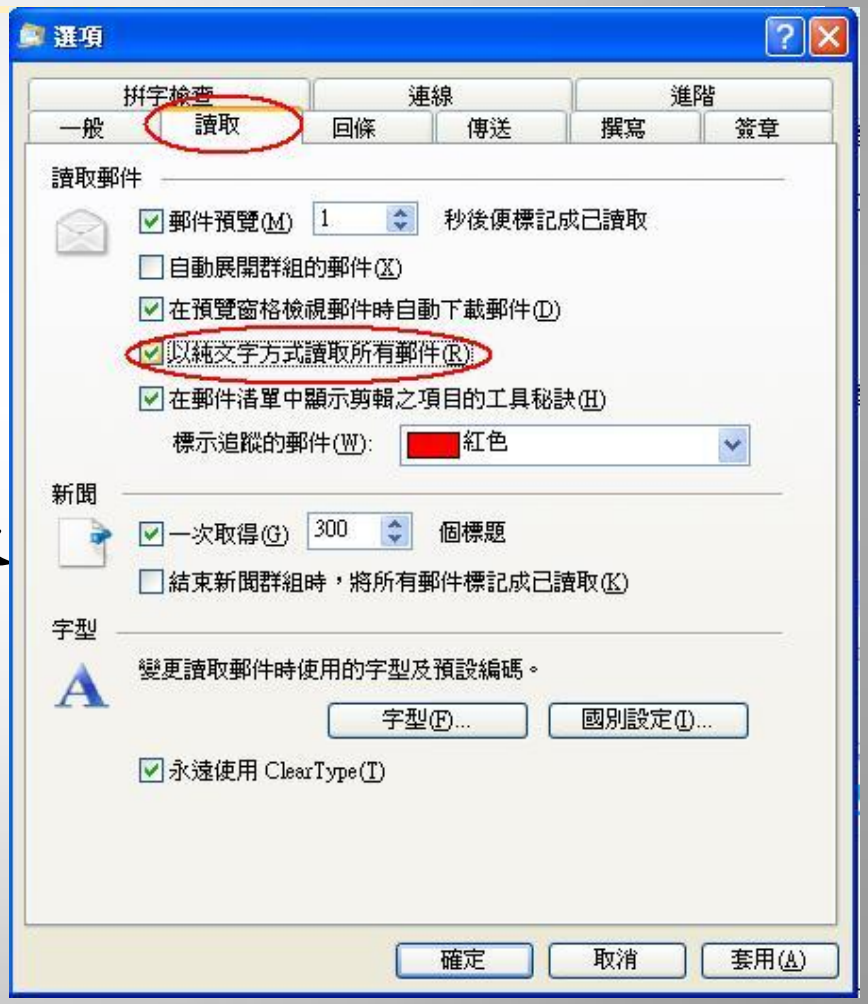
Outlook express

- 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



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



近乎完美的防護

- 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
  - 釐清寄件者身分
    - 以電話向寄件者確認
    - 郵件驗證機制
    - 附件加密
    - …

Mail header

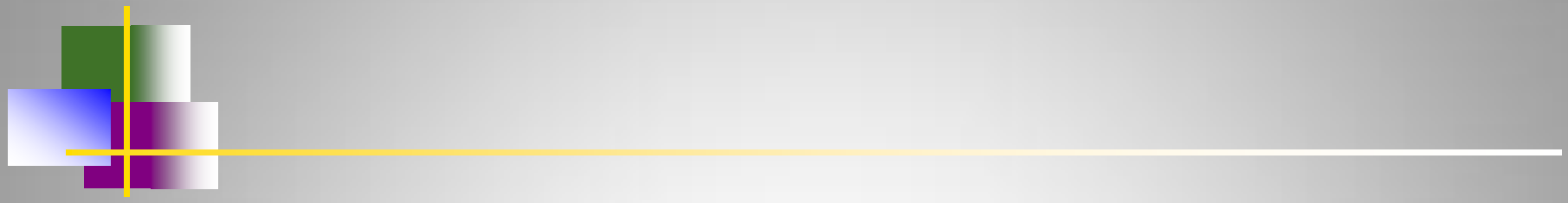
Return-Path: <vipmember@infoarray.tw>
X-Original-To: OOO@mx.nthu.edu.tw
Delivered-To: OOO@mx.nthu.edu.tw
Received: from cp1.oz.nthu.edu.tw (cp1.oz.nthu.edu.tw [140.114.63.141])
by cc.nthu.edu.tw (Postfix) with ESMTP id AA6BA56C76
for <ptlin@cc.nthu.edu.tw>; Thu, 2 Jul 2009 13:56:42 +0800 (CST)
parts
Received: from mail.communicatearea.tw [(210.67.251.27)] by
cp6.oz.nthu.edu.tw
(envelope-from <vipmember@infoarray.tw>)
(NTHUCCC AntiSPAM Mail Server with TLS)
with ESMTP id 577192816; Mon, 18 May 2009 06:55:06 +0800
Received: from mailsystem ([192.168.255.100])
by mail.communicatearea.tw (8.13.8/8.13.8) with ESMTP id
n4HMs4w7018426
for <OOO@mx.nthu.edu.tw>; Mon, 18 May 2009 06:54:06 +0800
X-ssage-ID: <7141115.1242600903628.JavaMail.SYSTEM@mailsystem>
Date: Mon, 18 May 2009 06:55:03 +0800 (CST)

結論

- 兩不看
  - 不認識寄件者不看
  - 來源不明的信不看
- 不心動、不衝動
  - 對於自己有興趣、有吸引力....等信件
- 要勤勞
  - 設定好郵件軟體
  - 更新作業系統和應用軟體弱點

相關資訊

- 資訊安全網頁
  - http://net.nthu.edu.tw/2009/security
- 電子報
  - http://list.net.nthu.edu.tw/
  - 電子報名稱：網路系統組電子報



Q & A