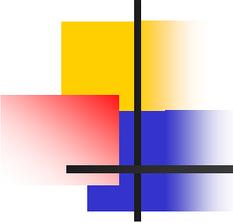


# 資訊安全認知與導入

---

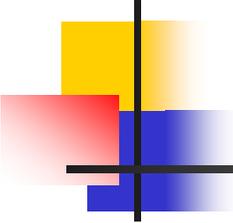
南投縣教育網路中心  
蔡昆穎、王登儀



# 課程綱要

---

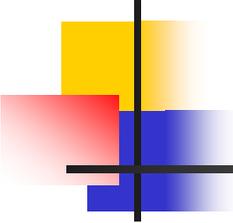
- 資訊安全簡介
- 資訊安全威脅
- 學術單位資安規劃推動概況
- 電子郵件社交工程技術、p2p簡介
- 木馬後門與病毒蠕蟲的清除與練習
- 案例探討
- 資通安全法令
- 資安實做



# 何謂資訊安全？

---

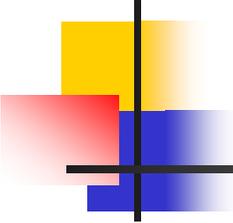
- 資訊對組織而言就是一種資產，和其它重要的營運資產一樣有價值，因此需要持續給予妥善保護。資訊安全可保護資訊不受各種威脅，確保持續營運、將營運損失降到最低、得到最豐厚的投資報酬率及商機。



# 資訊價值

---

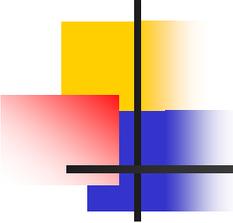
- 資訊的價值
  - 直接可衡量
  - 間接可衡量
- 爲了發揮資訊的最大價值，就必須有效的防止資訊遭竊取、竄改、毀損、滅失或遺漏，簡言之，就是確保資訊的：
  - 機密性
  - 完整性
  - 可用性



# 資訊安全三要素

---

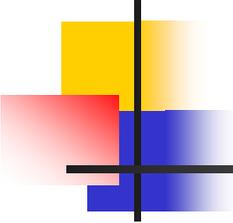
- Confidentiality 機密性
  - 保護資訊不被非法存取或揭露
- Integrity 完整性
  - 確保資訊在任何階段沒有不適當的修改或損毀
- Availability 可用性
  - 經授權的使用者能適時的存取所需資訊



# 資訊安全維護

---

- 機密性：確保只有經授權的人才能存取資訊。
- 完整性：保護資訊與處理方法的正確性與完整性。
- 可用性：確保經授權的使用者在需要時可以取得資訊及相關資產。

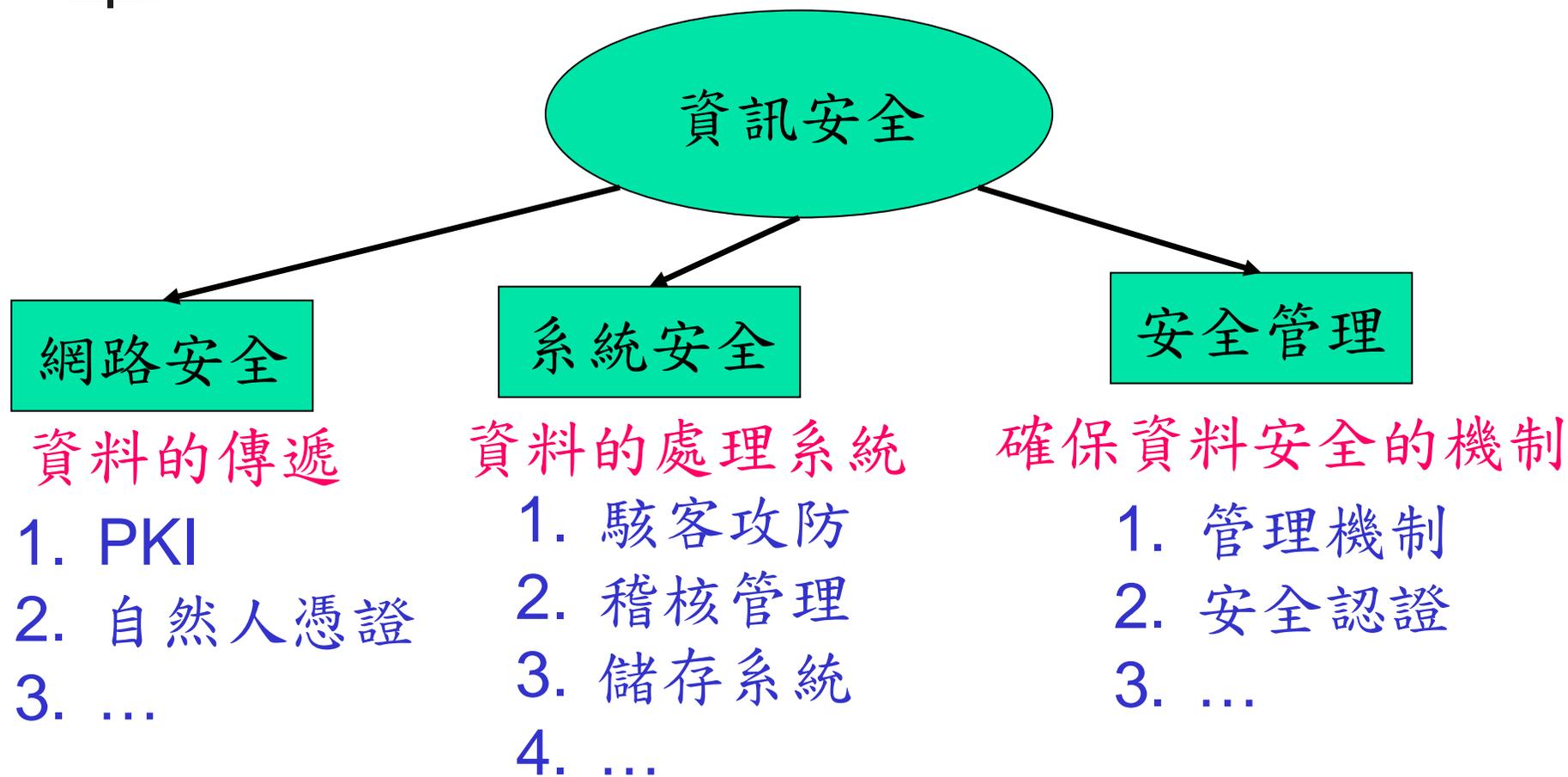


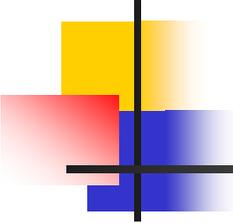
# 資訊安全的範圍(1/2)

---

- 定義保護及維護資料的安全，包含：
  - 資料的使用
  - 資料的傳遞
  - 資料的處理
  - 資料的儲存
- 網際網路加入後
  - 資料的傳遞安全變得愈來愈重要

# 資訊安全的範圍 (2/2)





# 目前的網路安全技術

---

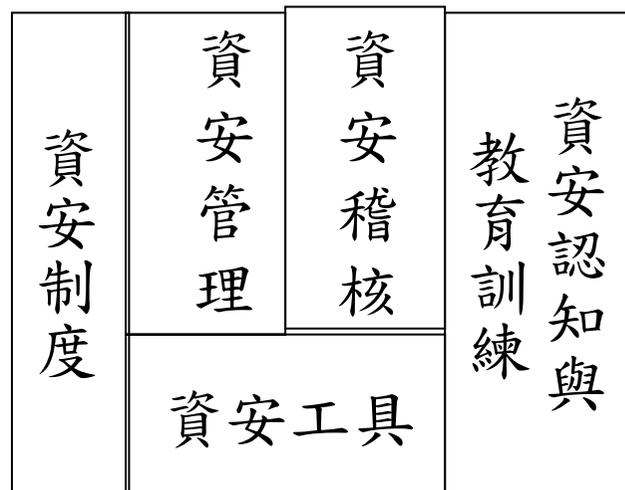
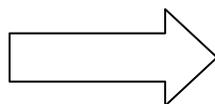
- 加密技術
  - 傳輸資料加密
  - 通道加密(SSL、VPN、IPsec)
- 身分認證
  - 電子簽章
  - 憑證(透過公正第三者做身份識別及確認)
    - GCA憑證
    - 自然人憑證

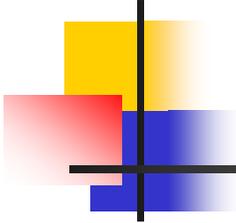
# 系統安全的定義

- 資料在處理過程中的安全

- 威脅

- 黑客入侵
- 木馬屠城
- 安全弱點
- 病毒蠕蟲

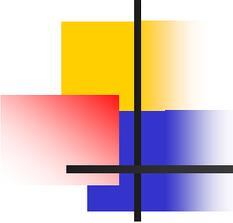




# 目前的系統安全安全管理技術

---

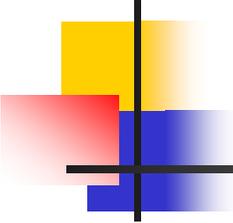
- 系統安全需要以全面的觀點來看，制度與管理、技術與工具、訓練(人)缺一不可。
- 資安制度：CNS17799、ISO 27001
- 資安管理：資安政策、ISMS
- 資安稽核：內部與外部稽核
- 資安工具：Firewall、IDS/IPS、
- 資安認知與教育訓練：提升資安意識與觀念。



# 資訊安全的實施-稽核

## 國際與國內資訊安全標準與法令

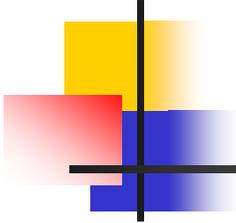
BS7799 / ISO17799	英國國家標準協會, 資訊安全管理機制 <a href="http://www.bsi.org.uk/">http://www.bsi.org.uk/</a>
COBIT	國際電腦稽核協會, 資訊技術控制架構, <a href="http://www.isaca.org/">http://www.isaca.org/</a>
NIST	美國國家標準與技術協會, <a href="http://csrc.nist.gov/nistpubs/800-14.pdf">http://csrc.nist.gov/nistpubs/800-14.pdf</a>
BIS Basel II	國際清算銀行/新巴塞爾資本管理協定 New Basel Capital Accord
我國政府規範	『行政院所屬各機關資訊安全管理實施基準/要點』 『財政部暨所屬機關資訊安全管理基準』 『金融機構辦理電子銀行業務安全控管作業基準』
我國法令要求	銀行法, 營業秘密法, 個資法, 刑法電腦犯罪
Electronic Banking Control	美國聯邦存款保險公司電子銀行控制架構評估—稽核規範



# 資訊安全事件定義

---

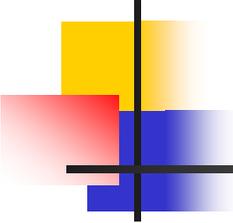
- 資訊安全事件指的是任何違反常軌的異常行爲，其可能造成資訊系統及網路的安全威脅。
- 經證明可能導致資訊系統運作錯誤事件或事故之情形及其後續所產生之故障效應等。
- 從設備故障、人員差錯、人爲事件或自然事件之類的單一事件到各種事件的複雜組合均屬於資安事件範疇內的事件案例。



# 資訊安全事件等級

---

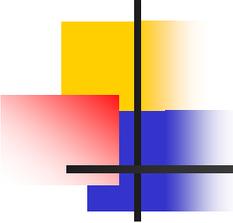
- 依據91年06月06日行政院資通安全會報，第二次修訂之「建立我國通資訊基礎建設安全機制計畫」，資通安全事件等級概分為四級
  - A 級**：影響公共安全、社會秩序、人民生命財產
  - B 級**：系統停頓，業務無法運作
  - C 級**：業務中斷，影響系統效率
  - D 級**：業務短暫停頓，可立即修復



## 資安事件的類型---內部事件

---

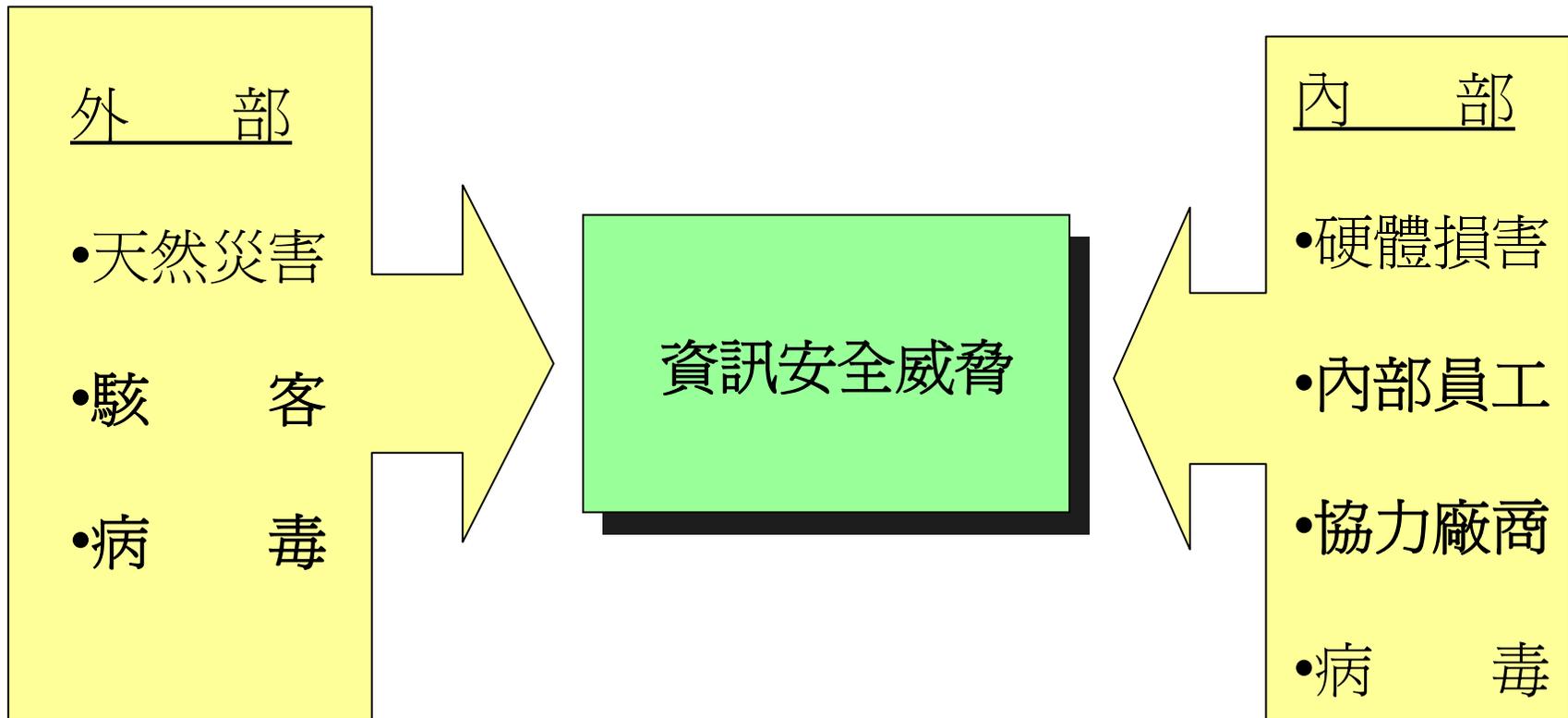
- 遭人爲惡意破壞毀損、作業不慎等危安事件。
- 設備故障：能直接或間接影響機房安全資訊系統的各個設備的故障可視爲資通事件。
- 人員差錯：錯誤或不良的維護、錯誤設定和操作員的其他錯誤行爲等。
- 其他內部事件：內部原因所引起的火災、爆炸等對機房安全可能產生重要之影響。



## 資安事件的類型---外部、自然事件

- 因外部事件或自然事件所引起某一安全重要系統、元件或建築物故障的可能性，可經由設計和建造中所採取的因應措施，將其風險降低至可接受的程度。
- 病毒感染事件
- 駭客攻擊（或非法入侵）事件
- 天然災害：颱風、水災、地震
- 重大突發事件：火災、爆炸、核子事故

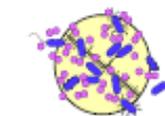
# 資訊安全的威脅來自



# 資訊安全威脅與來源---1



好奇的人士可能剛學會入侵電腦的方法，就應用書本上寫的方法當起駭客



病毒



蠕蟲



木馬



社交工程

# 資訊安全威脅與來源---2



內部員工也有可能是**潛在的威脅**，尤其對單位有不滿情緒及抱怨的人



# 資訊安全威脅與來源---3



預謀犯罪的歹徒是大家最熟悉的，會透過各種方式竊取單位機密、牟取暴利，如：  
販賣個人資料



# 資訊安全威脅與來源---4



間諜也是資安威脅的一種，因為商業上或政治上的因素，以各種滲透入侵技術，取得企業機密文件

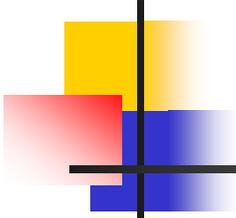


# 資訊安全威脅與來源---5



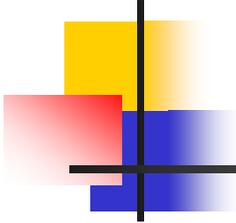
組織型駭客一般都扮演入侵者的角色，主要以竊取或破壞單位內部電腦機敏檔案資料為主，是以刺探、布建、竊取為目的





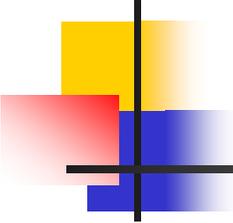
# 資訊安全風險---環境風險

風險的類型	範例
天災與實體	火災、水災、風災、地震 停電
非蓄意	未被告知的員工 未被告知的客戶
蓄意	駭客、恐怖份子、工業間 諜、政府、惡意的程式



# 資訊安全風險---潛在的弱點

風險的類型	範例
實體	門未鎖
天然	消防系統失效
硬體與軟體	軟體版本過期、韌體過舊
媒體	電子干擾
通訊	沒有加密傳輸
人為因素	疏忽



# 來自網路的威脅

---

- 有線網路

利用線路找尋設備資訊，封包加密較完整，若有人自線路中竊取資訊，至少還有軌跡可尋，無論是管理、安全、記錄資訊等較為方便。

- 無線網路

安全問題最令組織擔心，由於無線電波透過空氣傳遞訊號，只要在無線基地台訊號範圍內，都能擷取訊號資訊，故而管理無線網路資訊安全比有線網路更為困難。

# 來自離職員工的威脅

離職員工 犯案 - Google 搜尋 - Mozilla Firefox

離職員工 犯案

所有網頁 圖片 新聞 網上論壇 更多

離職員工 犯案 搜尋 進階搜尋 | 使用偏好

搜尋:  所有網頁  中文網頁  繁體中文網頁  台灣的網頁

所有網頁 約有6,370項符合離職員工 犯案的查詢結果, 以下是第 1-10項, 共費0.23秒。

**高鐵電纜遭竊五座101長度高能 離職員工偷拔軌道接地線-台灣新聞**  
雖然高鐵表示地線被偷不會影響行車安全, 但就怕沒地線後, 遇到雷雨來襲會受電擊破壞樁柱影響營運, 這次抓到離職員工犯案, 高鐵希望可以嚇阻這類犯罪再度發生。 ...  
[www.ttv.com.tw/096/05/0960522/09605224596904L.htm](http://www.ttv.com.tw/096/05/0960522/09605224596904L.htm) - 類似網頁

**E!Today**  
高鐵苗栗段電纜線頻頻失竊, 警方今日抓到兩名竊賊, 兩人是高鐵離職員工, 穿上高鐵背心和識別證佯裝修護工人, 到鐵道旁偷剪電纜線變賣, 去年至今已犯案將近50起, 偷 ...  
[www.ettoday.com/2007/05/22/545-2100548.htm](http://www.ettoday.com/2007/05/22/545-2100548.htm) - 104k - 頁面存檔 - 類似網頁

**E!Today**  
新竹某一交通公司離職員工徐水偉異想天開, 竟然以備份鑰匙將遊覽車開走, 將遊覽車 ... 可能是兩岸聯手犯案的機車勒贖集團犯案, 1名戴姓男子向警方自首, 坦承協助犯案, ...  
[www.ettoday.com/2007/04/22/138-2085337.htm](http://www.ettoday.com/2007/04/22/138-2085337.htm) - 103k - 頁面存檔 - 類似網頁

**犯案者在現場點名勸違與**  
檢警方面也不排除對勸違與公司離職與現職員工中的可疑對象, 採集毛髮、唾液或血液 ... 從容昨天再度犯案, 竟燈留下諸多線索, 勸違與員工認為應是想讓檢警辦案方向。 ...  
[tw.epochtimes.com/bt/5/0/13/n1050439.htm](http://tw.epochtimes.com/bt/5/0/13/n1050439.htm) - 16k - 頁面存檔 - 類似網頁

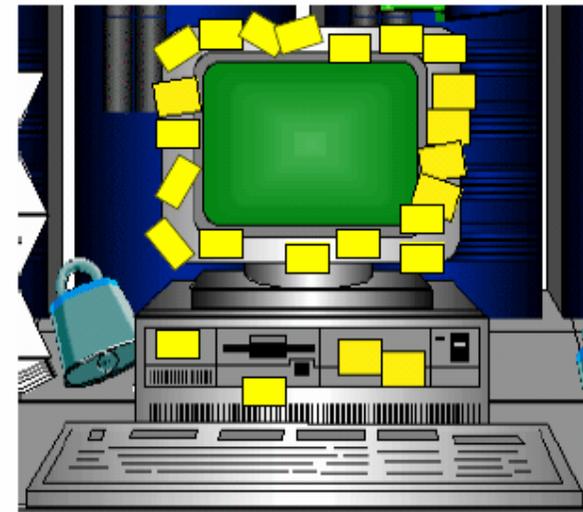
**威盛離職員工竊密案19日開庭王雪紅否認指控 華界 威盛 天極ChinaByte - 簡 - [轉為繁體網頁]**  
威盛竊密, 威盛離職員工竊密案19日開庭王雪紅否認指控, 友訊控告威盛員工竊密案, 今(19)日第1次開庭, 據了解, 威盛董事長王雪紅與總經理陳文琦當庭皆否認犯案, 威盛離職 ...  
[news.chinabyte.com/478/1763478.shtml](http://news.chinabyte.com/478/1763478.shtml) - 20k - 頁面存檔 - 類似網頁

完成

# 來自內部粗心員工的威脅

- 不規避旁人，如重要資料或密碼輸入
- 不隨手關機
- 隨時討論業務機密
- 使用者帳號隨便借給他人
- 印出的報表隨手亂放
- 檔案資料未事先分類
- 硬碟存放私人資料

密碼輸入？明碼張貼！！



# 即時通軟體的安全隱憂

- 常見的即時通軟體



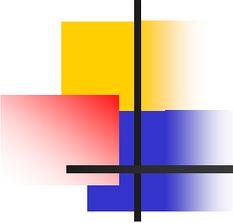
# 免費的網路資源

- 免費的電子郵件空間，高達2G
- 免費的網站空間，100M

我是唯一的  
管理者嗎？



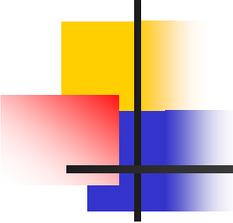
The screenshot shows the Gmail login page. At the top, there is a navigation bar with the Gmail logo and the text "歡迎使用 Gmail". Below this, there is a section titled "Google 在電子郵件上的革新" (Google's innovation in email). This section lists several features, with the second item, "不要捨棄任何郵件。" (Don't lose any mail), circled in red. The text for this item states: "超過 2675.532960 MB (還在增加中) 的免費儲存空間，讓您不需要再刪除其他郵件。" (Over 2675.532960 MB (still increasing) of free storage space, so you don't need to delete other mail). To the right of the features list is a "Gmail 登入" (Gmail login) form with fields for "使用者名稱" (Username) and "密碼" (Password), a checkbox for "在輕台電腦上記得我" (Remember me on this computer), and a "登入" (Login) button. Below the login form is a link for "忘記您的使用者名稱或密碼?" (Forgot your username or password?) and a button for "瞭解更多關於 Gmail 的資訊。" (Learn more about Gmail). At the bottom, there is a link for "參觀我們的新功能!" (Visit our new features!).



# 學術單位的資訊安全

---

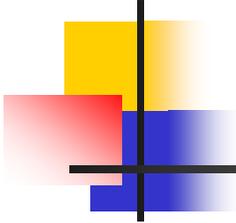
- 爲什麼學校單位需要資訊安全
  - 學生學籍資料
  - 成績資訊
- 學校單位所擁有的資訊設色
  - 非機密性
  - 具敏感性且涉及隱私及個人資料保護法相關規定



## TANet連線學校資通安全管理規範計劃

---

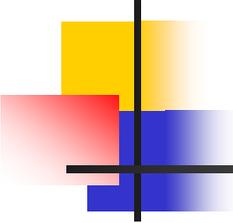
- 政府爲了滿足各行政單位之需求，民國88年制定了「行政院及所屬各機關資訊安全管理規範」。
- 由於學術單位與政府機關的屬性不同，雖然行政院已有頒布可依循之規範，但無法適用於TANet連線學校，因此實有必要研擬一套專屬的資通安全管理規範。



## 規劃目標(1/2)

---

- 籌劃權責組織架構與內容，協助政府的政策推動以及資安防護的落實。
- 參考ISO 27001:2005(E)、ISO 17799:2005、CNS 17800以及我國政府規範等法令標準，訂定出適用於TANet連線學校之管理規範；並在成大計中心建立試作點，檢測規範之適用性，作為日後相關單位的參考。
- 將此資安規範與實施之經驗推行到各校中，強化TANet中各連線學校的資通安全。

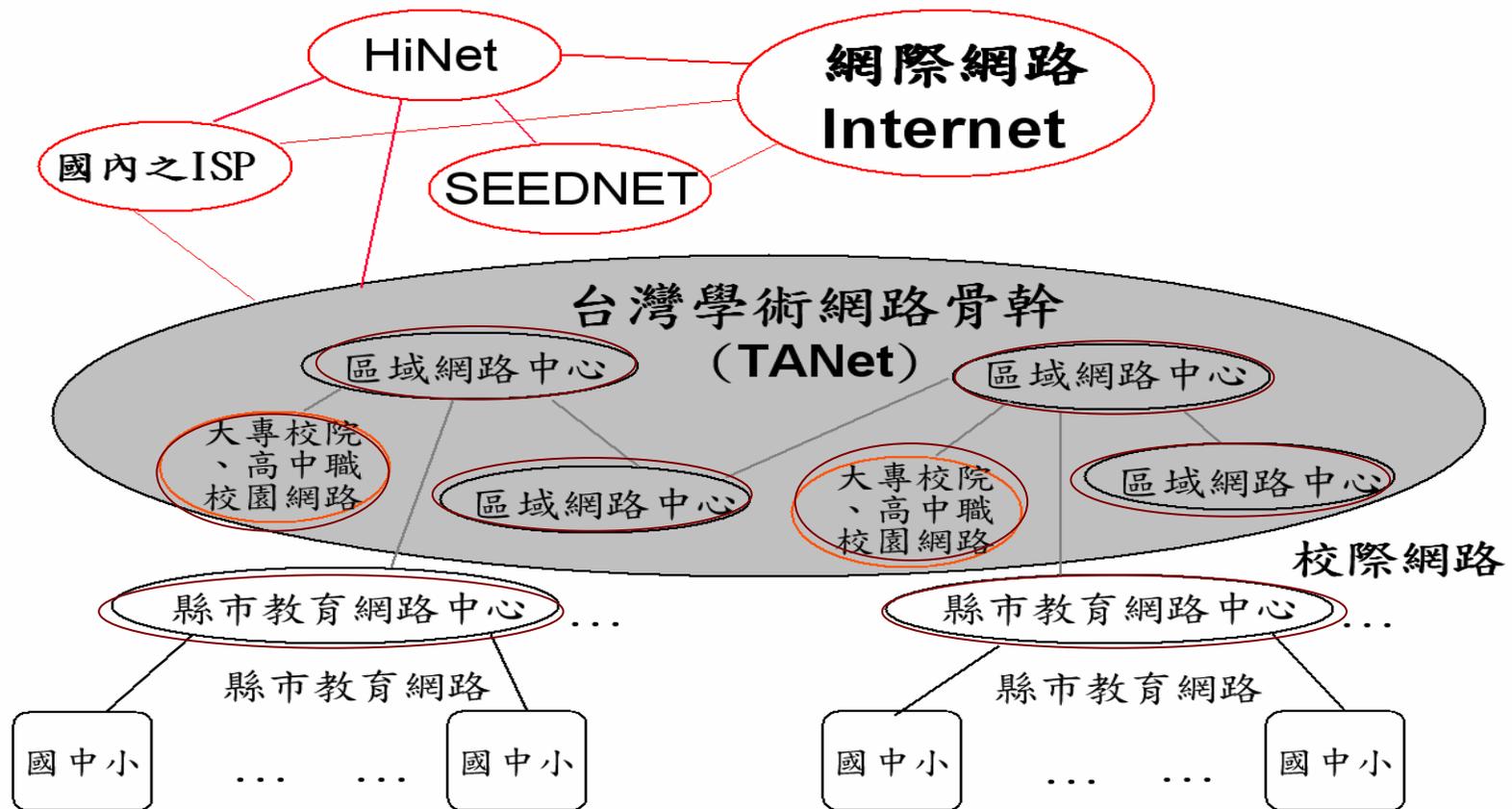


## 規劃目標(2/2)

---

- 使各連線單位能以最低的成本與時間，採用漸進的方式，建構嚴謹、合適之資訊安全管理系統。
- 配合教育部另外委託國家資訊基本產業發展協進會(NII)執行之25縣市網與國中小學網路資通安全環境與機制規劃，即可構成完整的學術網路資通安全系統，以確保學術網路使用的安全性。

# 適用對象



# 推動步驟

了解政府需求



進行任務分組



制定權責組織架構與  
任務草案



訂定規範及相關參考  
文件



準備階段  
2006年5月

- 規範宣導
- 教育訓練
- 試作點建立



以成大計中為試作點，進行  
ISMS建構與規範檢測之工作

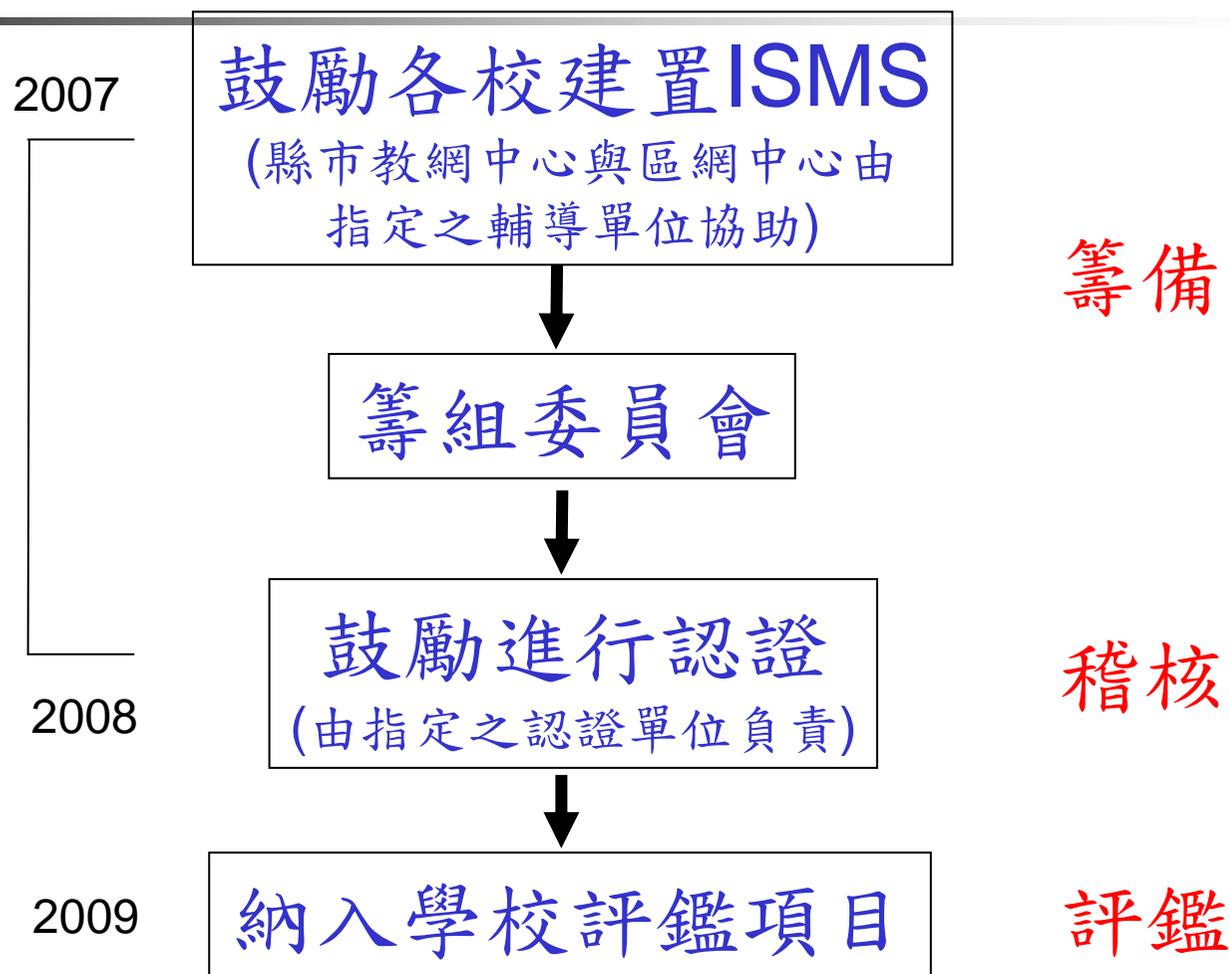
執行階段  
2007年~

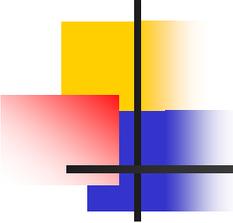
- 提交各項成果予教育部
- 落實於各 TANet 連線學校



稽核服務

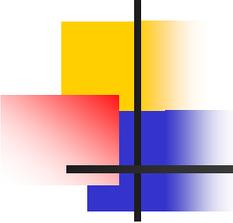
# 教育體系資通安全管理規範推行方式





# 教育部目前的推動規劃---1

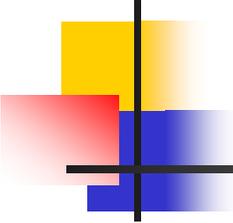
- 規劃成立資安規劃組織及營運，包含教育體系「第三者驗證」機制並推廣認證標章。
- 規劃資安通報處理組織及營運，建立教育體系通報應變網站。
- 試辦教育體系各級單位資訊安全管理系統（ISMS）及推廣，包含部屬管所與各級學校共8單位。



## 教育部目前的推動規劃---2

---

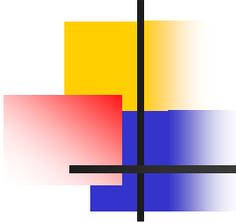
- 導入全部區、縣市網路中心資安管理制度、取得教育體系「第三者認證」。
- 公私立大學（B級）導入資安管理制度，由各校自行推動導入。
- 規劃辦理教育體系A、B、C級單位人員教育訓練，並取得資訊安全證照200人（AB級優先）。



## 教育部目前的推動規劃---3

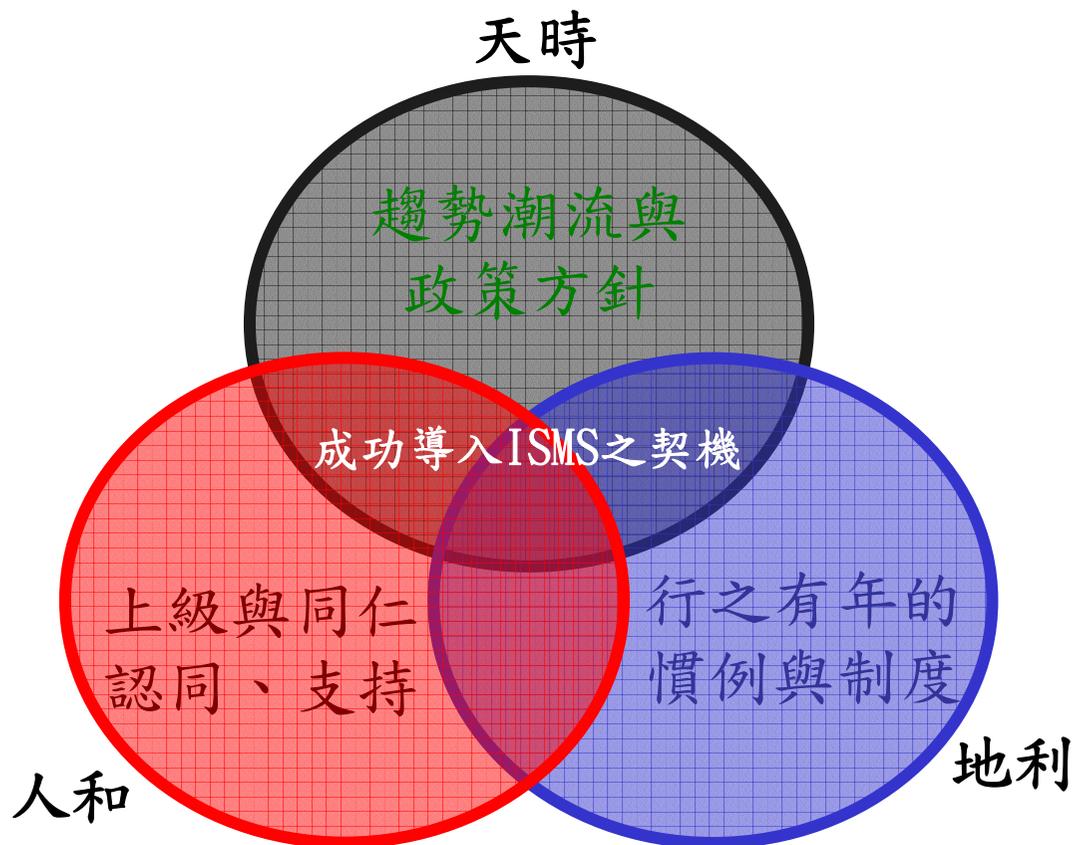
---

- 資安教育訓練－針對教育體系主官、主管、資訊技術人員、及一般教師。
- 針對教育體系學生規劃與執行資安認知推廣活動



# 如何成功導入ISMS

---



# 導入之流程

專家、顧問

單位內部達成共識

定義導入的範圍

判斷以往有無落實執行

Yes

風險評估

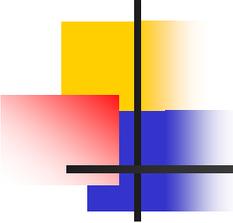
No

補強

(文件化、落實執行...等)

建置

(程序、執掌責任、文件化...等)



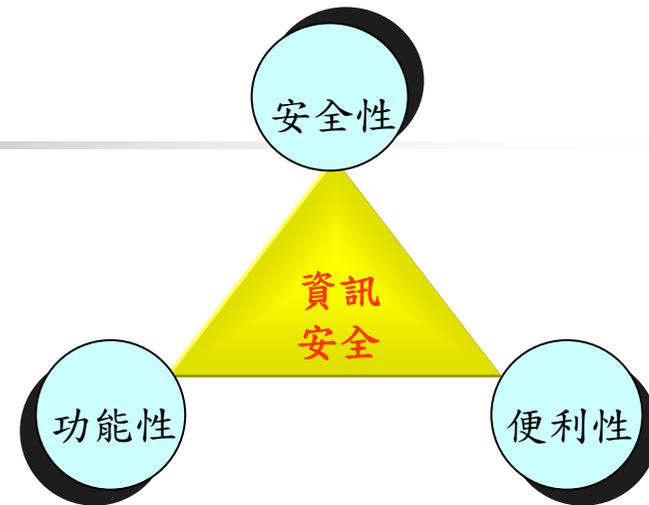
# 學術單位資訊安全政策

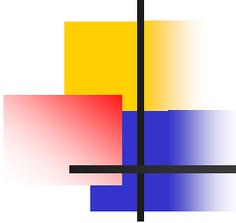
---

- 教育部未來推動規範將可滿足政府政策上的需求，成爲最基本的底限。
- 在資源許可下，各校可尋求更高標準的認證。各校ISMS之推動已不可不爲，越早進行可避免時程過於急迫的挑戰。
- 建立一完善之資安環境，可有效降低風險，避免各項資安的威脅。

# 重要資安觀念

- 資訊安全——
  - 說起來.....重要!
  - 做起來.....次要!!
  - 忙起來.....不要!!!
- 由全球推動ISMS的過程經驗中，最基礎且最重要的便是人員的資安觀念與管理知識
- 資通安全 = 技術 + 管理 + 稽核
  - 應達到“均衡”管理
  - “七分管理，二分技術，一分稽核”



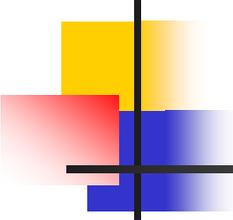


# 重要資安觀念

---

- 人為疏失造成的飛機失事，你會怪罪波音設計不良？
- 酒醉駕車造成的車禍意外，福特需要負擔必要賠償？

根據過去的統計，資安威脅來自  
天然威脅僅15%~17%，  
人為威脅達83%~85%。



休息一下！

---

# 案例探討

惡意活動密度 台灣全球第二高 - Yahoo! 奇摩新聞 - Microsoft Internet Explorer

檔案(E) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

網址(O) http://tw.news.yahoo.com/article/url/d/a/070605/2/fe2.html

新聞首頁 政治 社會 地方 國際 財經 科技 運動 健康 教育 藝文 影劇 旅遊 生活

資訊3C | 科學發展 | 自然環境 | 照片故事 | 專輯 | 民調中心 | 液晶螢幕

2007/06/08(星期五) 農曆(丁亥) 四月廿三日

新聞首頁 > 科技 > 資訊3C > 聯合新聞網

寄給朋友 | 友善列印 | 字級設定: 小 中 大 巨

## 惡意活動密度 台灣全球第二高

聯合新聞網 udn.com 更新日期: 2007/06/06 07:20 記者: 記者許韶芹 / 台北報導

全球駭客猖獗, Google 調查, 全球平均每十個網頁, 就有一個被植入惡意程式碼。賽門鐵克發現, 以上網人口數和惡意活動數量計算, 台灣是全球惡意活動密度第二高地區, 排名僅次於伊斯蘭恐怖分子環伺的以色列。

根據賽門鐵克最新的「全球網路安全威脅研究報告」, 只看惡意活動總量, 美國排名第一, 數量占全球總量三成; 中國大陸排名第二; 台灣排名第九, 比率占全球總量百分之三。

報告以最近前五十個惡意程式碼為樣本, 發現目的為竊取使用者個人資訊的高達卅三個, 其他則以破壞電腦性能為主。

台灣賽門鐵克技術總監王岳忠觀察, 過去網友認為只有到非法網站才危險, 但現在就連上合法網站也可能遭殃, 瀏覽某電影院網站就可能被植入一個後門程式, 駭客可從遠端操控使用者的電腦。Google 先分析全球上億網站中的四百五十萬個網頁, 發現四十五萬個藏有惡意程式碼。

請輸入搜尋關鍵字 搜尋新聞

廣告

Yahoo! 奇摩購物通

盛夏學顏美妝養顏班

每到夏天, 油光滿面, 閃閃動人?

痘痘粉刺 毛孔保養

毛孔粉刺無蹤 7件組

市價 5590

特惠價 1599 元

黃耀主 醫師

台灣英雄揚威

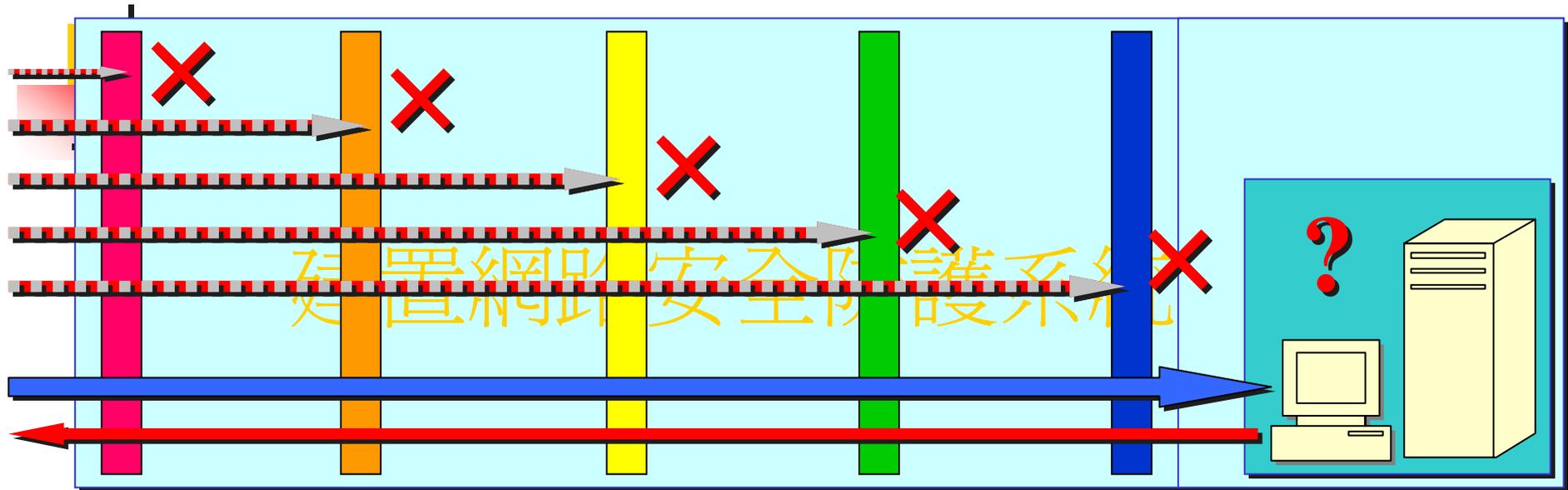
2007 美國職棒大聯盟專輯

Special Feature of Major League Baseball

網際網路

在駭客攻擊下, 如何安心上網?

# 如何偵測『已知型態攻擊』？



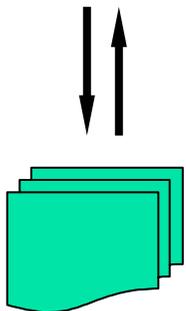
防火牆  
Firewall

入侵偵測系統  
IDS

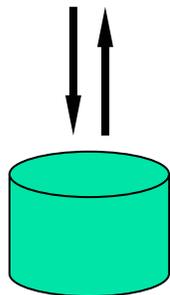
入侵防護系統  
IPS/IDP

防毒系統  
Viruswall

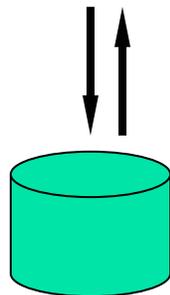
授權認證系統  
Authority



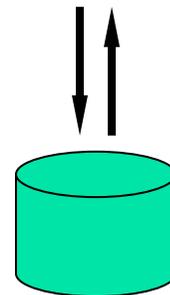
通訊服務  
開放政策  
Policy



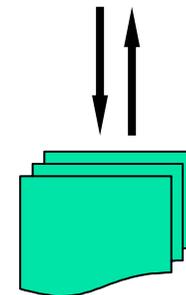
攻擊封包  
特徵規則  
Rules



攻擊封包  
特徵規則  
Rules



病毒蠕蟲  
識別檔案  
Pattern



帳號密碼  
存取控制  
ID/PWD ACL

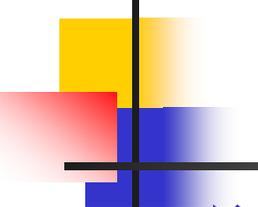
•如果攻擊者採用自己開發的木馬後門程式，並且偽裝成爲IE或MSN程式，從TCP-80或是TCP-1864送出資料，能夠察覺他嗎？

# 甚麼是 電子郵件 社交工程？

## ■ Email Social Engineering

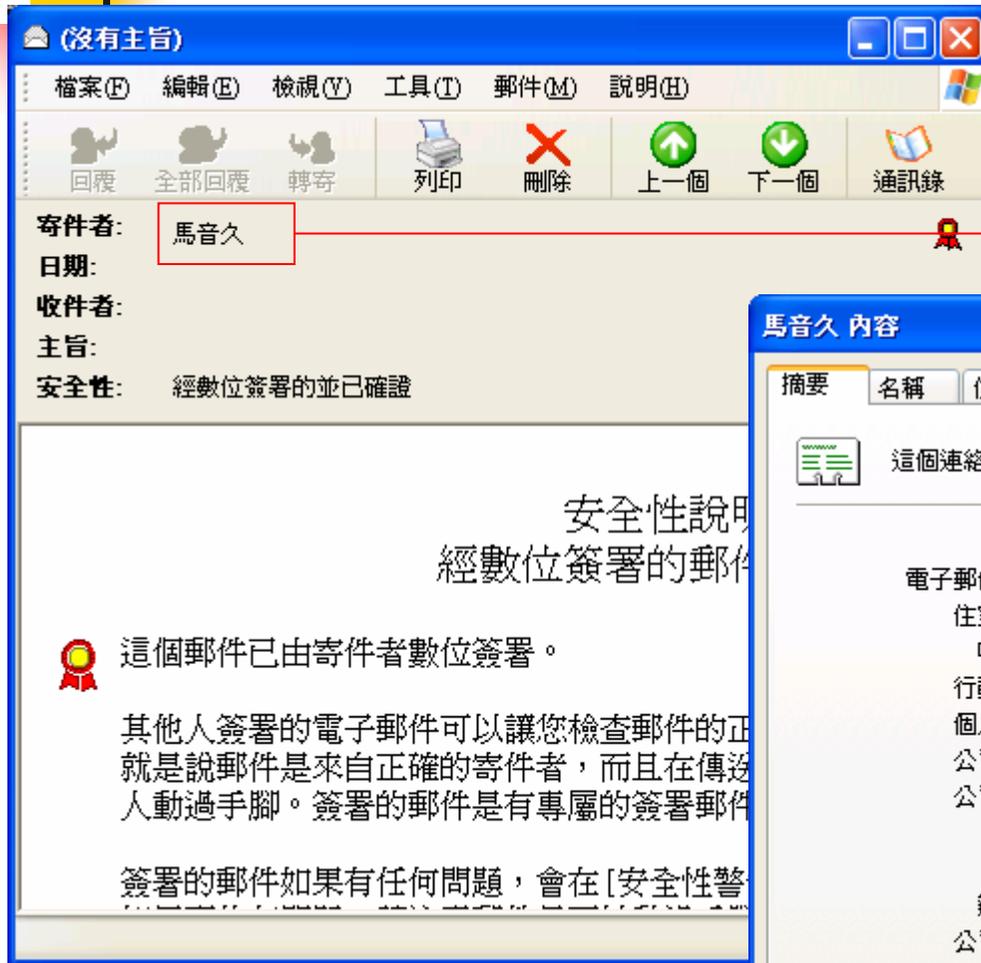
- 傳送電子郵件方式，騙取收件者信任，進而開啓郵件內容的駭客攻擊模式。
- 透過電子郵件，可以讓收件者
  - (1)誘騙進入假網站(網路釣魚)。
  - (2)開啓惡意檔案(木馬後門)。
  - (3)下載問題檔案(木馬後門)。
- 常見發燒話題：政治新聞、色情圖片、休閒養生。
- 網路郵件與網站詐騙技術演進，從錯字連篇到真假難辯。
  - 詐騙文字 更正式：書寫格式為正式商業通知，文筆愈來愈好。
  - 詐騙技術 更真實：大量使用圖片與其他能讓郵件顯得更真實的元素，包括使用銀行的標誌與公司名稱，以及版權與「註冊商標」符號，連最小的細節都不會遺漏。
  - 詐騙目標 更準確：更精確鎖定目標，只傳送給銀行真正的顧客。
  - 詐騙分工 更專業：目前的網路釣魚詐騙行動是由組織化的犯罪集團所為，大多運用有系統的方法來收集、核對、運用竊取到的資訊，以換取最大的利益。
  - 詐騙內容 更虛偽：故意加上針對網路釣魚攻擊所發出的警告！

# 電子郵件 社交工程 - 假冒寄件者

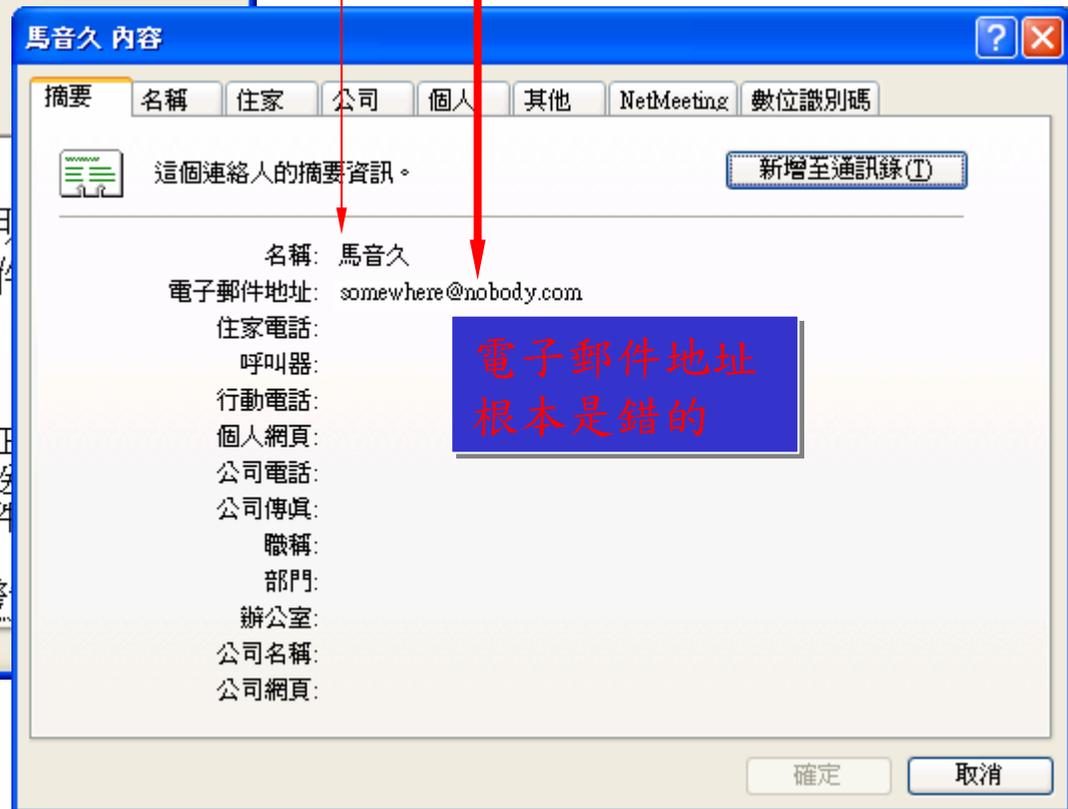


- 駭客會假冒成使用者信任的人，進而讓使用者相信而去開啓郵件及含惡意程式之附件或超連結
- 假冒寄件者方式
  - 顯示寄件者名稱，是假冒的身分
  - 電子郵件帳號，是假冒的資料
  - 傳統寄送電子郵件，預設值，無須帳號密碼
- 真假寄件者資料難以分辨

# 電子郵件 社交工程 - 假冒寄件者

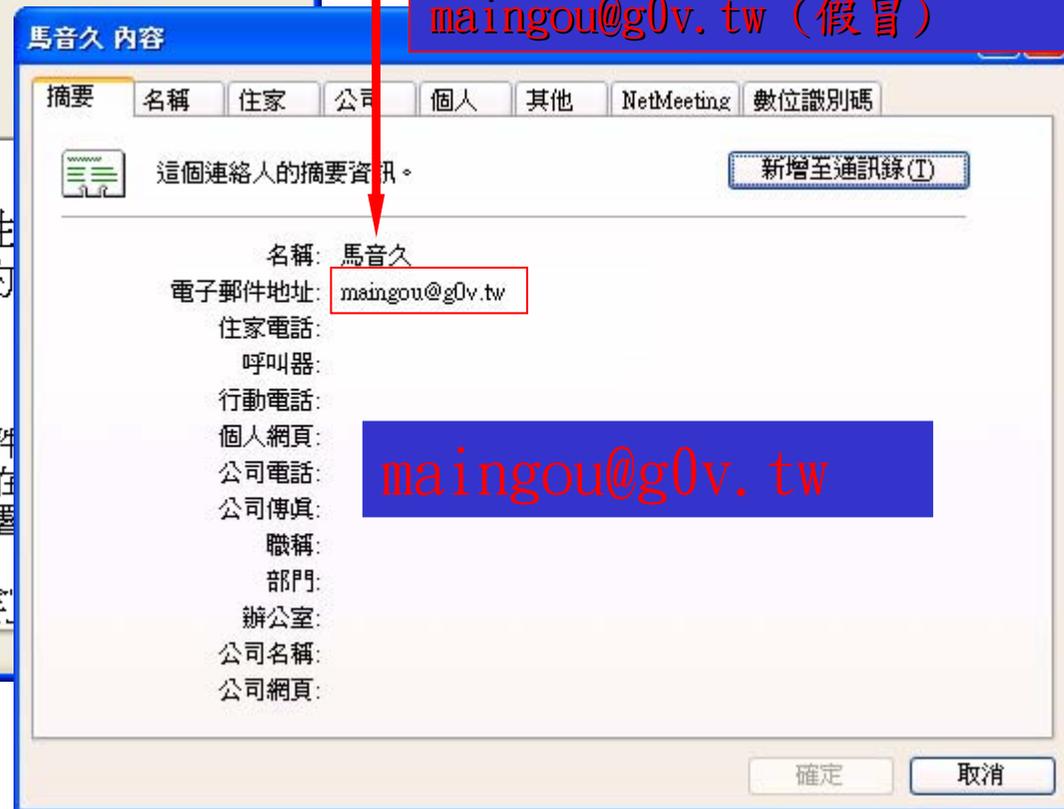
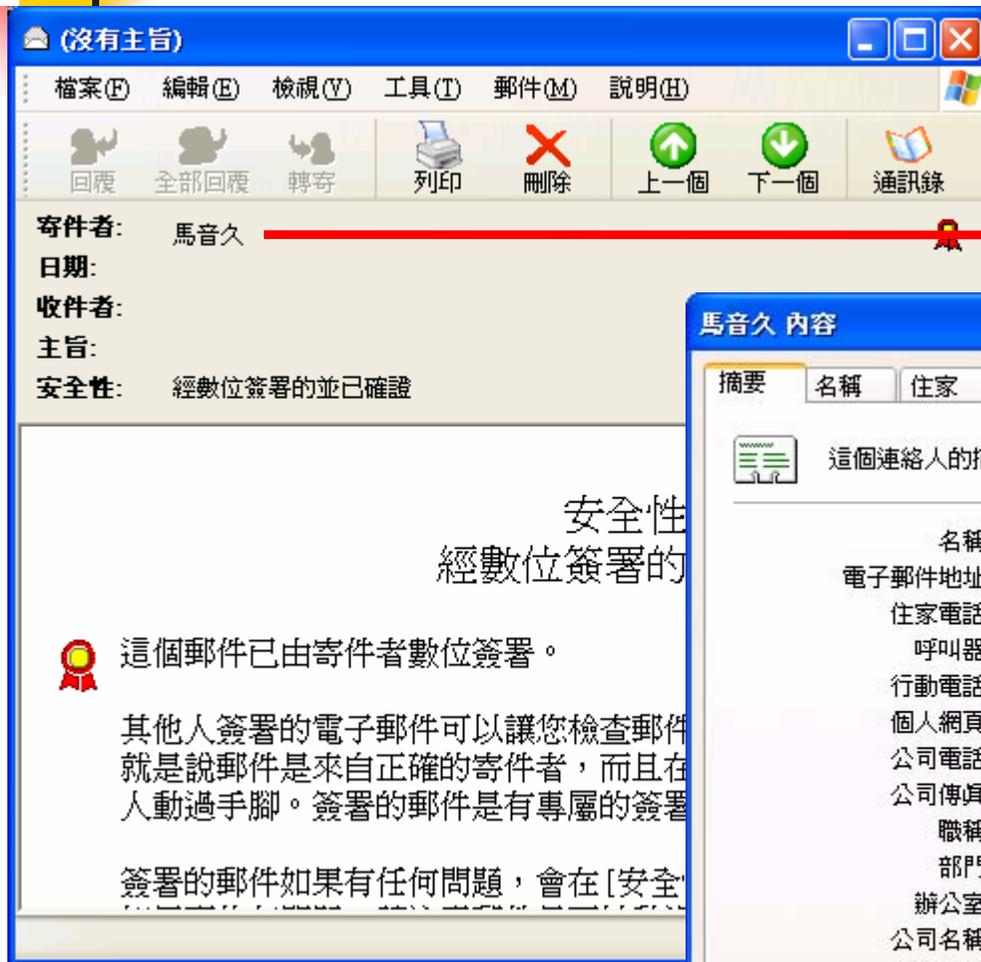


馬音久真正的帳號應該是  
maingou@gov.tw



# 電子郵件 社交工程 - 假冒寄件者

用數字0的零來假冒成英文的o  
用數字1的零來假冒成英文的l  
用數字6的零來假冒成英文的G  
maingou@gov.tw (真正)  
maingou@g0v.tw (假冒)



# 電子郵件 社交工程 - 含有惡意程式附件

- 電子郵件附件檔含有**惡意程式**
- 附件檔案型態不一定是**執行檔(.exe)**，可能是各種類型檔案(.doc、.ppt、.mdb等)，甚至是壓縮檔(.rar)

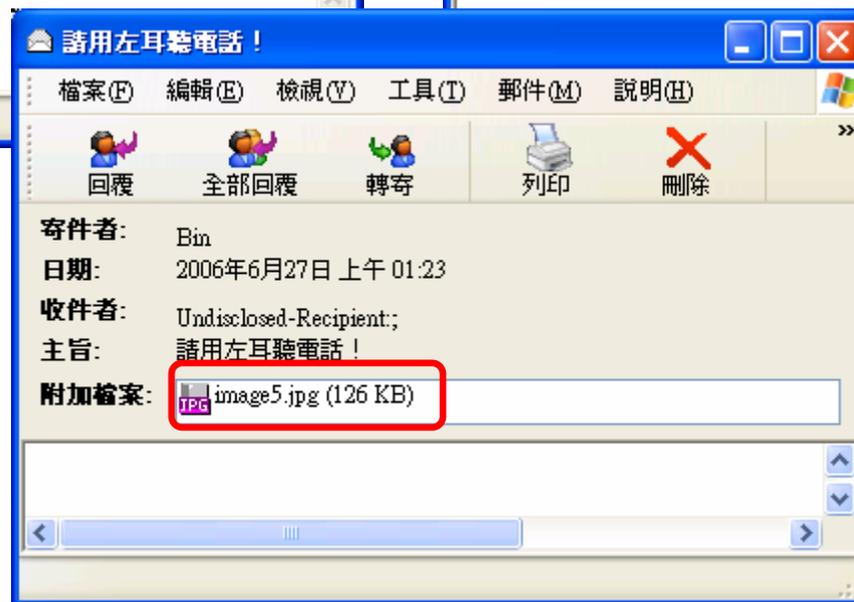
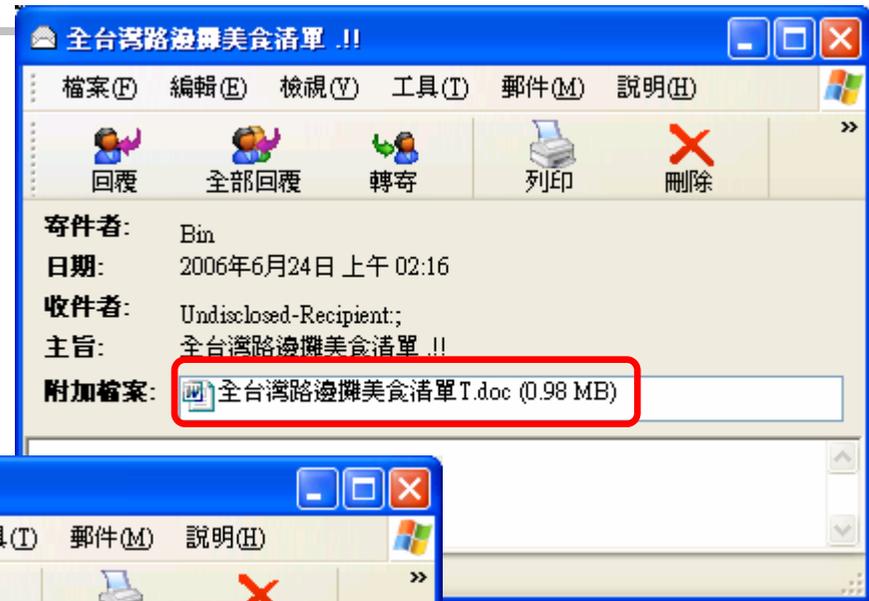
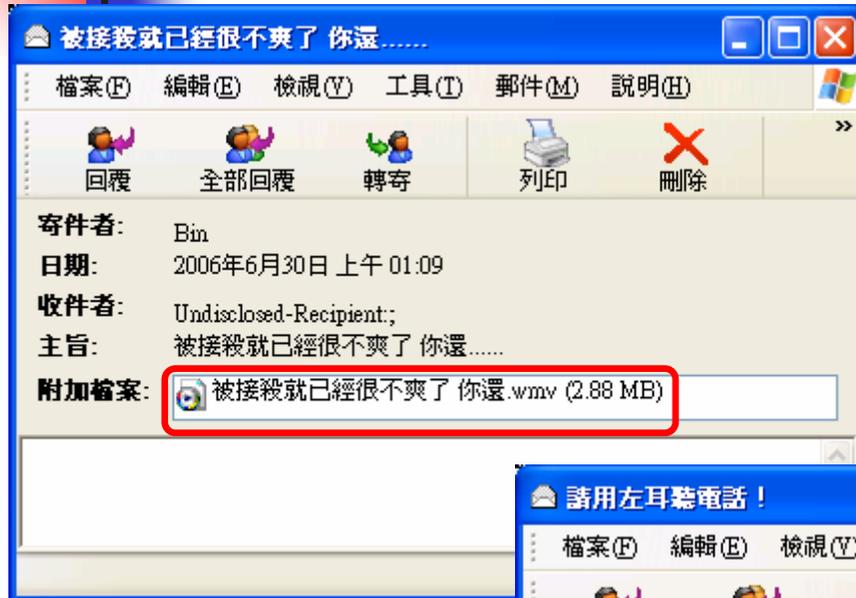
高危險檔案類型名稱

.exe	.com	.scr
.pif	.bat	.cmd
.doc	.xls	.pps,t
.reg	.lnk	.hta

中危險檔案類型名稱

.zip	.rar	.swf
.html	.pdf	.mdb

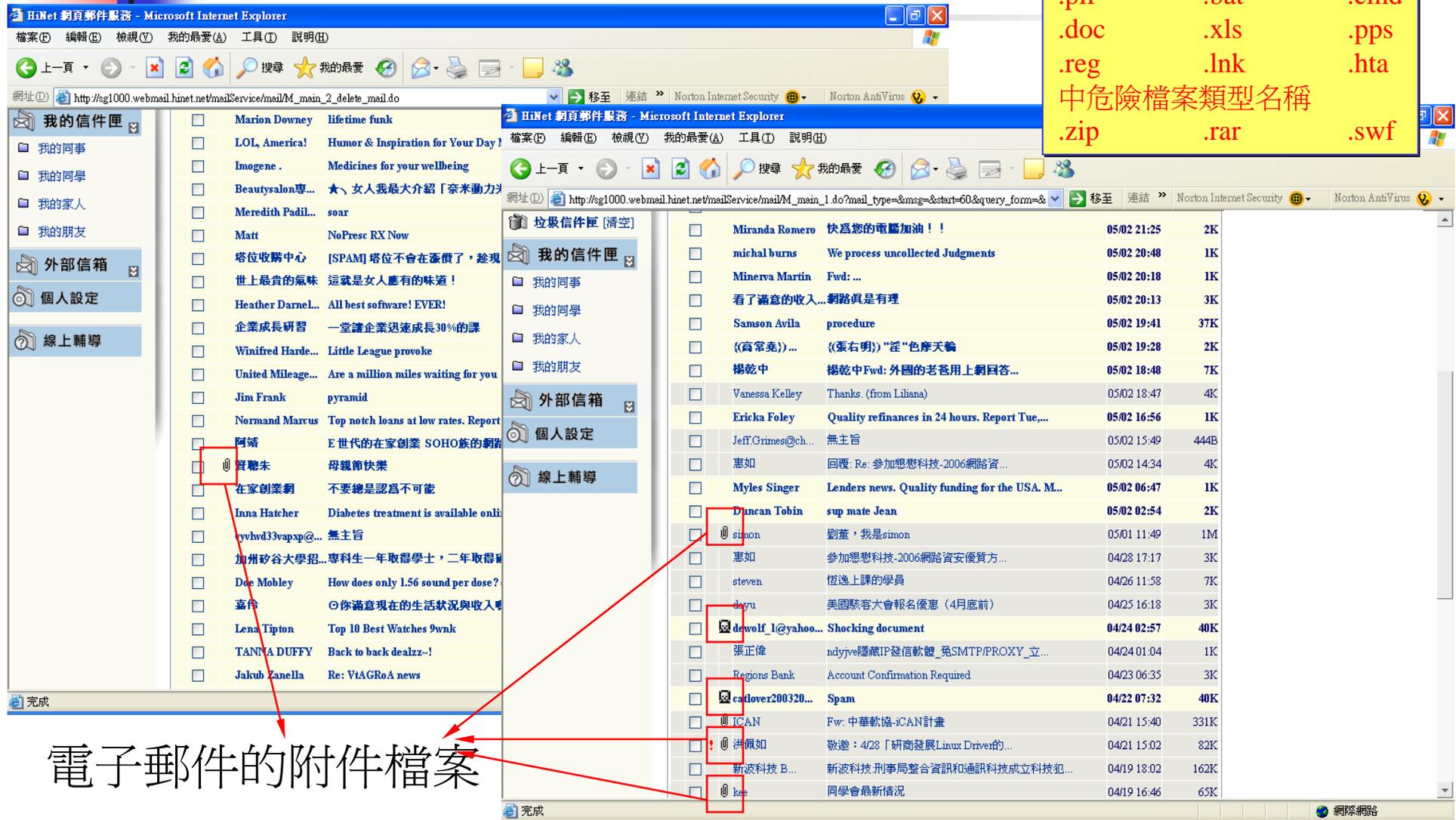
# 電子郵件 社交工程 含有惡意程式附件範例



# 如何檢查郵件是否夾帶木馬後門程式？

請您檢查電子郵件是否夾帶檔案？檔案名稱的尾碼是否為異常名稱？  
如果有異常名稱，請勿直接開啓執行。

高危險檔案類型名稱		
.exe	.com	.scr
.pif	.bat	.cmd
.doc	.xls	.pps
.reg	.lnk	.hta
中危險檔案類型名稱		
.zip	.rar	.swf



# 如何檢查郵件是否遭到網路釣魚詐騙？

檢查電子郵件是否遭到網路釣魚詐騙的方式很簡單，請從電子郵件所指向的網頁超連接網址，比較真正網址與郵件網址，兩者是否相同？

HiNet 網頁郵件服務 - Microsoft Internet Explorer

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

網址(📍) [http://sg1000.webmail.hinet.net/mailService/mail/M\\_mail\\_1.do?mail\\_type=&msg=5268DDDC77F1177878A8](http://sg1000.webmail.hinet.net/mailService/mail/M_mail_1.do?mail_type=&msg=5268DDDC77F1177878A8) 移至 連結 >> Norton Internet Security Norton AntiVirus

展開功能列 回信 全部回信 轉寄 檢視信件原始檔 友善列印 下載信件 刪除

dmliu: 收件匣 上一封 | 下一封 | 返回

寄件人: Regions Bank <customer.support@regions.com> 加入通訊錄 檢舉垃圾信

收信人: dmliu@ms4.hinet.net

日期: Sun, 23 Apr 2006 01:35:00 +0300

主旨: Account Confirmation Required

[字體] [語系]

D  
W  
re

[http://hoolla.nafree.net/zboard/data/GGols/https://secure.regionsnet.com/EBanking/logon\\_user=default&affiliate/index.php](http://hoolla.nafree.net/zboard/data/GGols/https://secure.regionsnet.com/EBanking/logon_user=default&affiliate/index.php)

<https://secure.regionsnet.com/EBanking/logon/user?a=default&affiliate>

If your problem could not be resolved, your account will be terminated. For the User Agreement, section 9 we may issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your auctions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Regards,  
Regions Bank Service Department.

dmliu: 收件匣 上一封 | 下一封 | 返回

展開功能列 回信 全部回信 轉寄 檢視信件原始檔 友善列印 下載信件 刪除

[http://hoolla.nafree.net/zboard/data/GGols/https://secure.regionsnet.com/EBanking/logon\\_user=default&affiliate/index.php](http://hoolla.nafree.net/zboard/data/GGols/https://secure.regionsnet.com/EBanking/logon_user=default&affiliate/index.php) 網際網路

Hi, **dmlin**您目前在第**1369**封信

關閉 回覆 全部回覆 轉寄 上一封 下一封 列印 刪除 信件原始檔

日期	2005年01月24日 下午 12:21
寄件人	Citizens Bank <support@citizensbank.com>
收件人	Gforward <gforward@ms4.hinet.net>
副本	
信件標題	Important Online Banking Alert



Dear valued **Citizens®** Bank member,

Due to concerns, for the safety and integrity of the online banking community we have issued the following warning message.

It has come to our attention that your **Citizens®** account information needs to be updated as part of our continuing commitment to protect your account and to reduce the instance of fraud on our website. If you could please take 5-10 minutes out of your online experience and renew your records you will not run into any future problems with the online service. However, failure to confirm your records may result in your account suspension.

Once you have confirmed your account records your internet banking service will not be interrupted and will continue as normal.

**To confirm your bank account records please click here.**

Thank you for your time,

**Citizens® Financial Group.**

Hi, **dmliu**您目前在第**1368**封信

關閉 回覆 全部回覆 轉寄 上一封 下一封 列印 刪除 信件原始檔

日期	2005年01月23日 上午 09:43
寄件人	"Customer Support" <support@customers.eBay.com>
收件人	dmliu@ms4.hinet.net
副本	
信件標題	eBay Notification



It has come to our attention that your eBay billing updates are out of order. If you could please take 1-2 minutes out of your online experience and update your billing records you will not run into any future problems with the online service. However, failure to update your records will result in account termination. Please update your records.

Once you have updated your account records your eBay session will not be interrupted and will continue as normal. Failure to update will result in cancellation of service, Terms of Service (TOS) violations or future billing problems.

To update your eBay records now follow this link:

<https://signin.ebay.com/ws2/eBayISAPI.dll?SignIn>

收件匣 - Microsoft Outlook

檔案(F) 編輯(E) 檢視(V) 我的最愛(O) 工具(T) 執行(A) NOD32 說明(H)

新增(N) 回覆(R) 全部回覆(L) 轉寄(W) 傳送/接收(C) 尋找(I) 組合管理(O) 關閉(O)

outlook:\個人資料夾\收件匣

Outlook Today

收件匣 (14)

行事曆

連絡人

工作

記事

刪除的郵件 (35)

我的捷徑

其它捷徑

資料夾清單

- Outlook Today - [個人資料夾]
  - Infected Items
  - 工作
  - 日誌
  - 收件匣 (14)
    - AVON
    - BSI英國標準協會
    - Microsoft
    - TCA
    - 公司
    - 文件 (1)
    - 其他
    - 保險
    - 家庭
    - 旅行
    - 氣象
    - 航空
    - 銀行
    - 行事曆
    - 刪除的郵件 (35)
    - 草稿
    - 記事
    - 寄件匣
    - 寄件備份
    - 連絡人

收件者	寄件者	主旨	收到日期	寄件日期
rongjing@ms3.hinet.net	楊淑君	單一產品創造百...	2007/7/31...	2007/7/31...
ling@cres.tcc.edu.tw	經典童話故事書	百大排行榜的冠...	2007/7/31...	2007/7/31...
ling@mail.diamondinfotech...	資訊室 許雅玫	讀取:【新波科技...	2007/7/31...	2007/7/31...
service@mail.diamondinfote...	資訊融入競賽管理中心	百萬創意競賽!...	2007/7/31...	2007/7/31...
吳冠雲	電子時報網路報 (HTML 圖...	伺服器3強築高牆...	2007/7/31...	2007/7/31...
ling@mail.diamondinfotech...	網路行銷專員 - Alen Chen	用關鍵字行銷等...	2007/7/31...	2007/7/31...
service@mail.diamondinfote...	網路行銷專員 - 劉小姐	網路行銷廣告託...	2007/7/31...	2007/7/31...
ling@mail.diamondinfotech...	趙枝剛	《近親亂倫》最...	2007/7/31...	2038/1/19...
劉志龍	謝志龍	讀取的主旨:【新...	2007/7/31...	2007/7/31...
鄭婕妤	鄭婕妤	2008 TGS全新規...	2007/7/31...	2007/7/31...
support@mail.diamondinfote...	謝謝 (8 D V D)	Hello! 小姐 &P...	2007/7/31...	2007/8/2 (...)
roomac@ms3.hinet.net	還有信用卡未付餘額嗎 點看...	超低利率 代辦貸...	2007/7/31...	2007/8/2 (...)
ling@mail.diamondinfotech...	簡訊王 最專業的簡訊行銷團...	哇塞!《手機簡訊...	2007/7/31...	2007/7/31...
service@mail.diamondinfote...	賺不出錢來沒關係	銀行不當催收，...	2007/7/31...	2007/7/31...

寄件者: 楊淑君  
主旨: 單一產品創造百億營業額，值得您來參考!

收件者: rongjing@ms3.hinet.net  
副本:

台灣近視比例，世界第一!!!

電腦族的視力愈來愈差~~~~

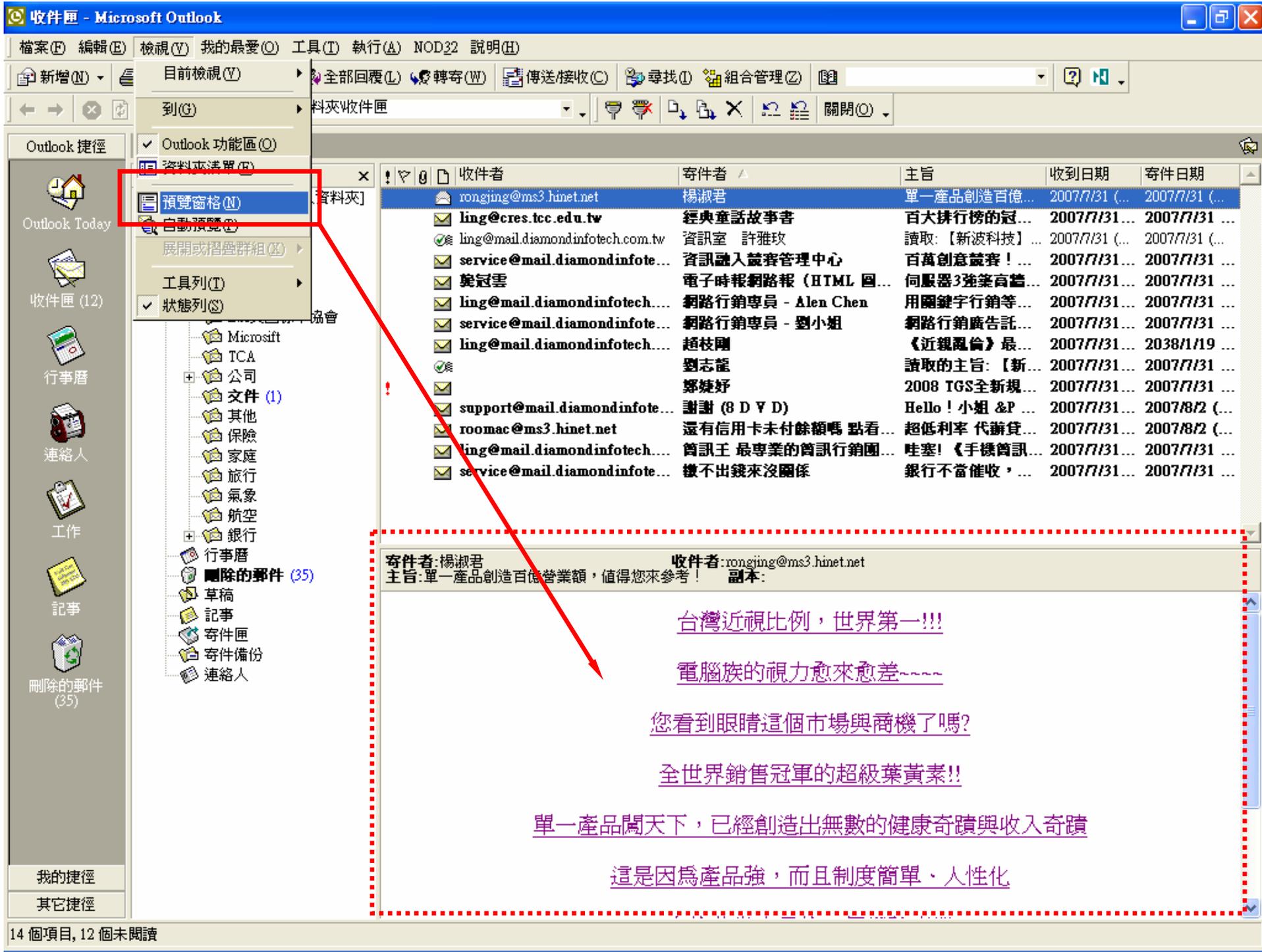
您看到眼睛這個市場與商機了嗎?

全世界銷售冠軍的超級葉黃素!!

單一產品闖天下，已經創造出無數的健康奇蹟與收入奇蹟

這是因為產品強，而且制度簡單、人性化

14 個項目, 14 個未閱讀



寄件者: 楊淑君  
 主旨: 單一產品創造百億營業額, 值得您來參考!

收件者: rongjing@ms3.hinet.net  
 副本:

台灣近視比例, 世界第一!!!

電腦族的視力愈來愈差~~~~

您看到眼睛這個市場與商機了嗎?

全世界銷售冠軍的超級葉黃素!!

單一產品闖天下, 已經創造出無數的健康奇蹟與收入奇蹟

這是因為產品強, 而且制度簡單、人性化

Outlook 捷徑

- Outlook Today
- 收件匣 (12)
- 行事曆
- 連絡人
- 工作
- 記事
- 刪除的郵件 (35)

我的捷徑

其它捷徑

資料夾清單

- Outlook Today - [個人資料夾]
  - Infected Items
  - 工作
  - 日誌
  - 收件匣 (12)
    - AVON
    - BSI英國標準協會
    - Microsoft
    - TCA
    - 公司
    - 文件 (1)
    - 其他
    - 保險
    - 家庭
    - 旅行
    - 氣象
    - 航空
    - 銀行
    - 行事曆
  - 刪除的郵件 (35)
    - 草稿
    - 記事
    - 寄件匣
    - 寄件備份
    - 連絡人

收件者	寄件者	主旨	收到日期	寄件日期
rongjing@ms3.hinet.net	楊淑君	單一產品創造百億...	2007/7/31 (...)	2007/7/31 (...)
ling@cres.tcc.edu.tw	經典童話故事書	百大排行榜的冠...	2007/7/31 ...	2007/7/31 ...
ling@mail.diamondinfotech.com.tw	資訊室 許雅玫	讀取:【新波科技】...	2007/7/31 (...)	2007/7/31 (...)
service@mail.diamondinfote...	資訊融入競賽管理中心	百萬創意競賽! ...	2007/7/31 ...	2007/7/31 ...
吳冠雲	電子時報網路報 (HTML 圖...	伺服器3強築高牆...	2007/7/31 ...	2007/7/31 ...
ling@mail.diamondinfotech....	網路行銷專員 - Alen Chen	用關鍵字行銷等...	2007/7/31 ...	2007/7/31 ...
service@mail.diamondinfote...	網路行銷專員 - 劉小姐	網路行銷廣告託...	2007/7/31 ...	2007/7/31 ...
ling@mail.diamondinfotech....	趙枝剛	《近親亂倫》最...	2007/7/31 ...	2038/1/19 ...
	劉志龍	讀取的主旨:【新...	2007/7/31 ...	2007/7/31 ...
	鄭婕妤	2008 TGS全新規...	2007/7/31 ...	2007/7/31 ...
support@mail.diamondinfote...	謝謝 (8 D V D)	Hello! 小姐 &P ...	2007/7/31 ...	2007/8/2 (...)
roomac@ms3.hinet.net	還有信用卡未付餘額嗎 點看...	超低利率 代辦貸...	2007/7/31 ...	2007/8/2 (...)
ling@mail.diamondinfotech....	簡訊王 最專業的簡訊行銷團...	哇塞!《手機簡訊...	2007/7/31 ...	2007/7/31 ...
service@mail.diamondinfote...	鑽不出錢來沒關係	銀行不當催收，...	2007/7/31 ...	2007/7/31 ...



- 資料夾
- Outlook Express
  - 本機資料夾
    - 收件匣 (1)
    - 寄件匣
    - 寄件備份
    - 刪除的郵件
    - 草稿

# Outlook Express

進入到 msn

尋找郵件... 身分 ▾

## 電子郵件

☑ [收件匣] 中有 **1 封未閱讀的郵件**

[設定郵件帳戶...](#)

## 新聞群組

[設定新聞群組帳戶...](#)

## 連絡人

連絡人(C) ▾  
沒有連絡人可以顯示。請按 [連絡人]，建立新的連絡人。

[開啓通訊錄...](#)

[尋找人員...](#)

Outlook Express 啟動時直接到我的收件匣(I)

**每日小秘訣** ×

要在新郵件中插入簽章，請從 [插入] 功能表選擇 [簽章]。

如果您建立了多個簽章，請從清單中選擇您要插入的簽章。

◀ 上一個      下一個 ▶

Outlook Express

檔案(F) 編輯(E) 檢視(V) 工具(T) 郵件(M) 說明(H)

建立郵件 傳送/接收

資料夾

- Outlook Express
- 本機資料夾
  - 收件匣 (1)
  - 寄件匣
  - 寄件備份
  - 刪除的郵件
  - 草稿

傳送至接收(S) 全部同步處理(Z) 同步處理資料夾(N) 標示成離線(K) 通訊錄(B)... Ctrl+Shift+B 新增寄件者至通訊錄(D) 郵件規則(R) 帳戶(A)... 選項(O)...

進入到 msn

尋找郵件... 身分

每日小秘訣 要在新郵件中插入簽章，請從 [插入] 功能表選擇 [簽章]。

[收件匣] 中有 1 封未閱讀的郵件

設定郵件帳戶...

新聞群組

設定新聞群組帳戶...

連絡人(C) 沒有連絡人可以顯示。請按 [連絡人]，建立新的連絡人。

連絡人

開啟通訊錄... 尋找人員...

Outlook Express 啟動時直接到我的收件匣(I)

選項

拼字檢查 安全性 連線 維護

一般 讀取 回條 傳送 撰寫 簽章

一般

- 啟動時直接進入 [收件匣] 資料夾(W)
- 如果有新的新聞群組就通知我(N)
- 自動顯示包含未閱讀郵件的資料夾(D)

傳送及接收郵件

- 新郵件送達時播放音效(P)
- 啟動時傳送及接收郵件(S)
- 每隔(C) 30 分鐘傳送及接收郵件(I)

如果我的電腦當時沒有連線(O):

不要連線

預設的訊息傳遞程式

- 這個應用程式是預設的郵件處理程式 設成預設(K)
- 這個應用程式是預設的新聞處理程式 設成預設(M)

確定 取消 套用(A)

讓您可以設定選項。

The image shows the Outlook Express interface with the 'Tools' menu open and the 'Options' dialog box displayed. The 'Options' dialog box has the 'Security' tab selected, and the 'Internet Explorer Security Zones' section is highlighted with a red dashed box. The 'Tools' menu has 'Options...' selected. The 'Options' dialog box has the 'Read' tab selected, and the 'Read Mail' section is highlighted with a red dashed box.

**Outlook Express 工具 (T) 郵件 (M) 說明 (H)**

- 傳送及接收 (S) >
- 全部同步處理 (Z)
- 同步處理資料夾 (N)
- 標示成離線 (K) >
- 通訊錄 (B)... Ctrl+Shift+B
- 新增寄件者至通訊錄 (D)
- 郵件規則 (R) >
- 帳戶 (A)...
- 選項 (O)...**

**選項**

拼字檢查 一般 **讀取** 回條 傳送 撰寫 簽章

讀取郵件

- 郵件預覽 (M) 5 秒
- 自動展開群組的郵件 (X)
- 在預覽窗格檢視郵件時自動下載郵件 (D)
- 在純文字中讀取所有郵件 (R)
- 在郵件清單中顯示剪輯之項目的工具秘訣 (H)

標示保存的郵件 (W): 紅色

新聞

- 一次取得 (G) 300 個標題
- 結束新聞群組時，將所有郵件標示成已閱讀 (K)

字型

請按此處，變更讀取郵件時使用的字型及預設編碼。

字型 (F)... 國別設定 (L)...

確定 取消 套用 (A)

**選項**

一般 讀取 回條 **安全性** 傳送 撰寫 簽章

拼字檢查 安全性 連線 維護

病毒防護

請選擇要使用的 Internet Explorer 安全性區域:

- 網際網路區域 (較不安全，但功能較強) (Z)
- 受限制的網站區域 (較安全) (R)

- 在其他應用程式試圖以我的名義傳送電子郵件時警告我 (W)
- 在附件有可能有病毒時不允許儲存或開啓 (N)

下載圖片

- 阻擋 HTML 電子郵件中的圖片和其他外部內容 (B)

安全郵件

數位 ID (又稱為憑證) 是特殊的文件，可以讓您證明您在電子交易中的身分。

要以數位化方式在郵件簽章或者接收加密郵件，您必須要有數位 ID。

- 所有外寄郵件的內容與附加檔案都加密 (E)
- 所有外寄郵件加上數位簽章 (D)

其他資訊 (M)...

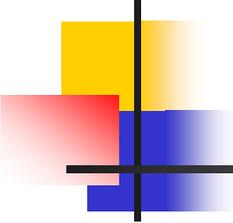
數位識別碼 (I)...

取得數位 ID (G)...

進階 (V)...

確定 取消 套用 (A)

讓您可以設定選項。



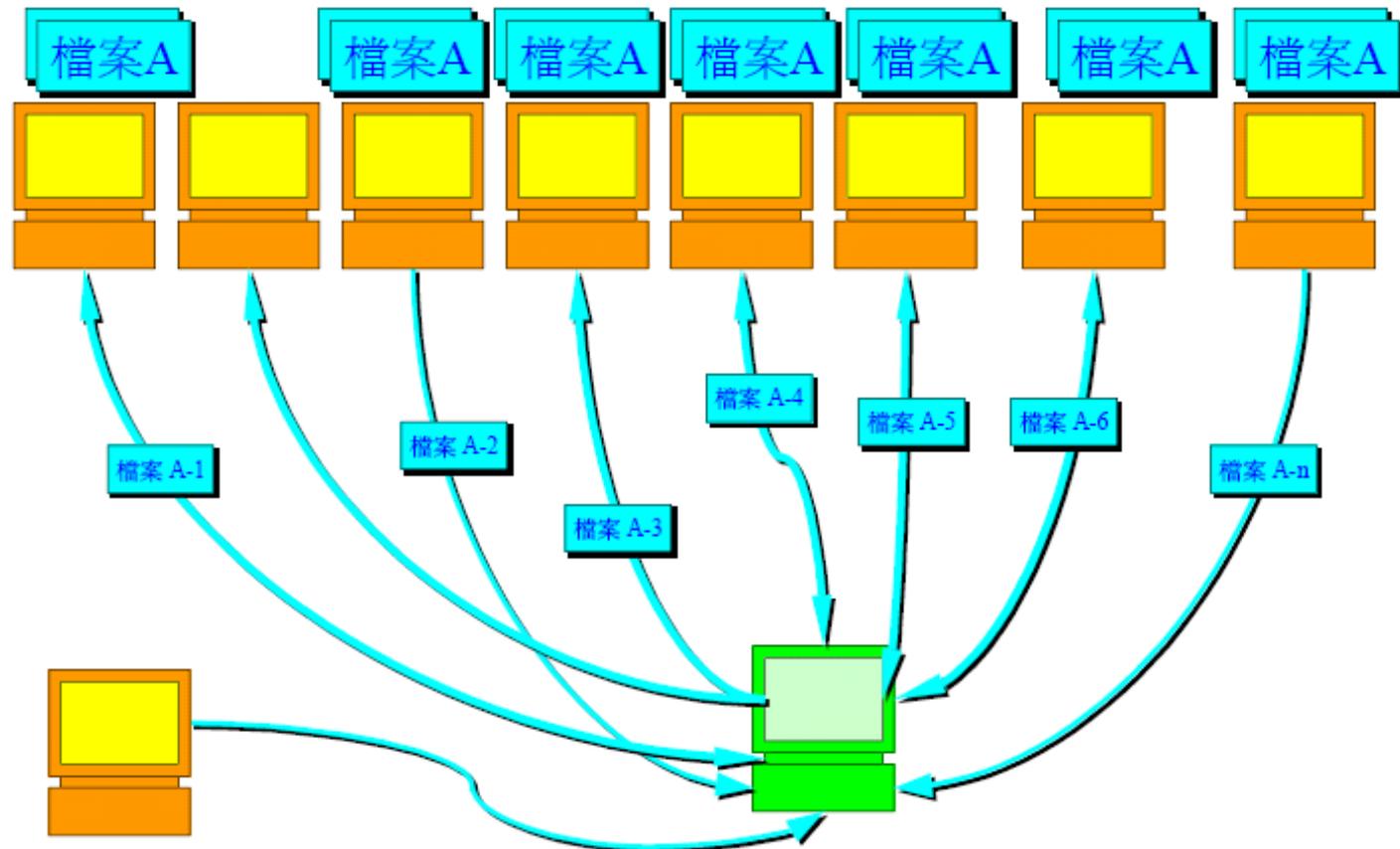
# 甚麼是P2P 軟體?

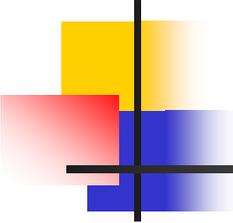
---

- P2P , Peer to Peer, 點對點通訊傳輸工具
- 傳統HTTP/FTP 傳送檔案方式，採取用戶與主機的通訊模式(Client-Server Mode)
- 新制P2P 檔案傳送，採取用戶與用戶的通訊模式，P2P傳送檔案的時候，可以同時連接多個下載點，分散式下載檔案。
- P2P可以快速完成檔案下載的目標。
- Skype也是P2P的一種應用工具。

# Peer to Peer, 點對點通訊傳輸

## 工具

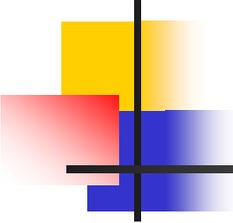




## P2P軟體的種類

---

- BitTorrent系列(BT) , BitTorrent 、 BitComet 、 BTspirit 、 BitTorando...
- eDonkey系列 , eDonkey, eMule...
- GnuTella系列 , GnuTella 、 ezPeer 、 Mxie 、 Foxy...
- FastTrack系列 , FastTrack 、 KaZaA...
- WinMx系列 , WinMx 、 Winny 、 NapMx...

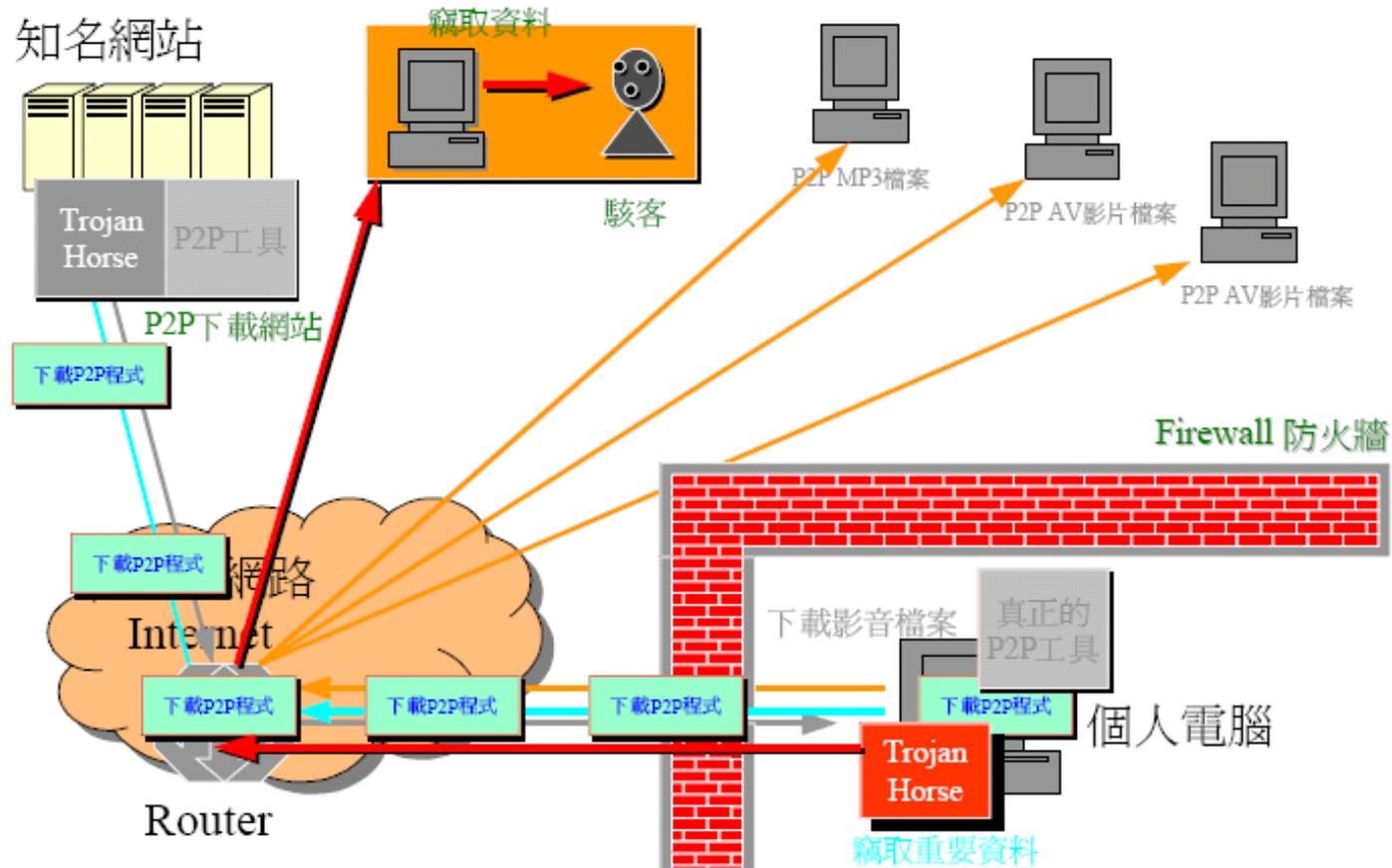


# P2P 軟體可能影響網路安全的問題

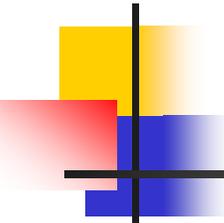
---

- P2P工具包，可能被惡意人員放置木馬後門程式，與病毒蠕蟲。
- P2P軟體本身的漏洞，造成駭客入侵。
- 使用P2P軟體時，誤將本機目錄開放共享。
- 使用P2P下載影音檔案，多半為mp3與mpeg、avi等等檔案，可能造成侵權行爲。
- 使用P2P下載色情影片，影響正常工作與政府形象。

# P2P工具包，可能放置木馬後門程式



# P2P 軟體可能影響網路安全的 問題



- 使用P2P軟體工具，誤將MyDocument目錄分享出來。
- 如果該主機登入帳號為空密碼(或簡單密碼)，對網路安全會產生立即危險。

# P2P 工具- Winny 嚴重事件資料

http://tw.news.yahoo.com/0605092151342gn.html

## 網路洩密：美軍曾訓練日本軍隊鎮壓暴動

【法新社 彭水芳】

（法新社東京八日電）根據日本自衛隊從網路中不小心洩漏的消息，美軍陸戰隊曾經訓練日本軍隊如何鎮壓在美國基地附近發生的群眾暴動活動。

這項鎮暴訓練是在去年日本南部的琉球群島進行。

美軍大部分的軍事設施都在琉球群島，當地居民與美軍經常發生衝突。



最近，每日新聞透過有線失的日本Winny軟體檔案的交換系統，從自衛隊網站滲透這項內幕消息，並且加以報導。

自衛隊證實，這項鎮暴訓練是在二〇〇五年三月二十一日至二十五日進行。

但自衛隊否認這項訓練是秘密性質。

一名自衛隊發言人說：「這項消息是透過檔案分享軟體洩漏的。但是我們的檔案並沒有任何不可告人的秘密。」

王者發威 建仔風雲

# P2P 工具- Winny 嚴重事件資料

日期	組織/個人	洩露資訊
03月03日	郵路審判情報局	114件分の顧客情報
03月02日	宮城県鹿島台小学校	700名分の個人情報
03月02日	さくらケーシーエス	55名分の社員情報
03月02日	富士宮信用金庫 NBC	13,619名分の法人・個人
03月02日	陸上自衛隊	報告書など
03月01日	航空自衛隊	60人分の隊員情報
03月01日	モスバーガー	234名分の顧客情報, 36名分の従業員情報
02月24日	宮崎地方検察庁	8名分の個人情報
02月24日	東京地方裁判所	149名分の個人情報
02月24日	NTT東日本	1,400件分の顧客情報
02月23日	海上自衛隊	海上自衛隊の機密情報

日本軍方機密 嚴重外洩

# P2P 工具- Winny 嚴重事件資料

The screenshot shows a news article from 'Internet Watch Japan' dated 2006/03/27. The article title is 'トレンドマイクロの営業資料がWinnyに流出' (Trend Micro's sales materials leaked to Winny). The text describes how Trend Micro's sales materials were leaked to the P2P network Winny. A red box highlights a specific entry in the list: '03月24日 ヤフー コーポド・ファン倶楽部 8,223件の顧客情報' (March 24, Yahoo! Corp. Fan Club, 8,223 customer records). Another red box highlights a blue box with the text '資安大廠與網路公司 仍然遭逢劫難' (Security giant and network company still face disaster). The article also mentions that Trend Micro employees had saved the data on their home PCs, which were then infected with a virus and leaked.

日付	組織名	流出情報
03月28日	FULLCA	フルキャストテクノロジー 128名分の個人情報
03月27日	トレンドマイクロ	報告書、資料
03月27日	三重県名張市立小学校	590名分の個人情報
03月25日	北海道セバタクロー協会	大会参加者の個人情報 ※調査中
03月24日	ヤフー	コーポド・ファン倶楽部 8,223件の顧客情報
03月23日	横浜市の事業委託団体	239名分の個人情報
03月22日	日本ソフトウェア協会	225名分の会員情報
03月22日	愛媛県立松山工業高校	1,625名分の個人情報
03月22日	新潟県立斎藤中学校	11名分の個人情報
03月20日	福井市営競技場「聖苑」	10,285名分の個人情報
03月20日	Yahoo! JAPAN	3,169社分の出店企業 228名分の社員情報

# P2P 工具- Winny 嚴重事件資料

2006年

報道日時	流出元	内容
06月23日	北九州市消防局	287名分の個人情報
06月19日	熊本県警	39件の警察資料 (Share)
06月12日	西日本プラント工業	差電所の資料
06月08日	石川県JAつるぎ郷	1,523名分の個人情報 (Share)
06月05日	J-COM ジェイコム	1万3,400名分の個人情報
06月02日	国土交通省	1,800名分の個人情報
06月02日	大庭府貝塚市消防本部	131名分の個人情報
06月02日	秋田県立横手高校	380名分の個人情報 (Share)
05月30日	愛知県西尾市立中学校	460名分の個人情報 (Share)

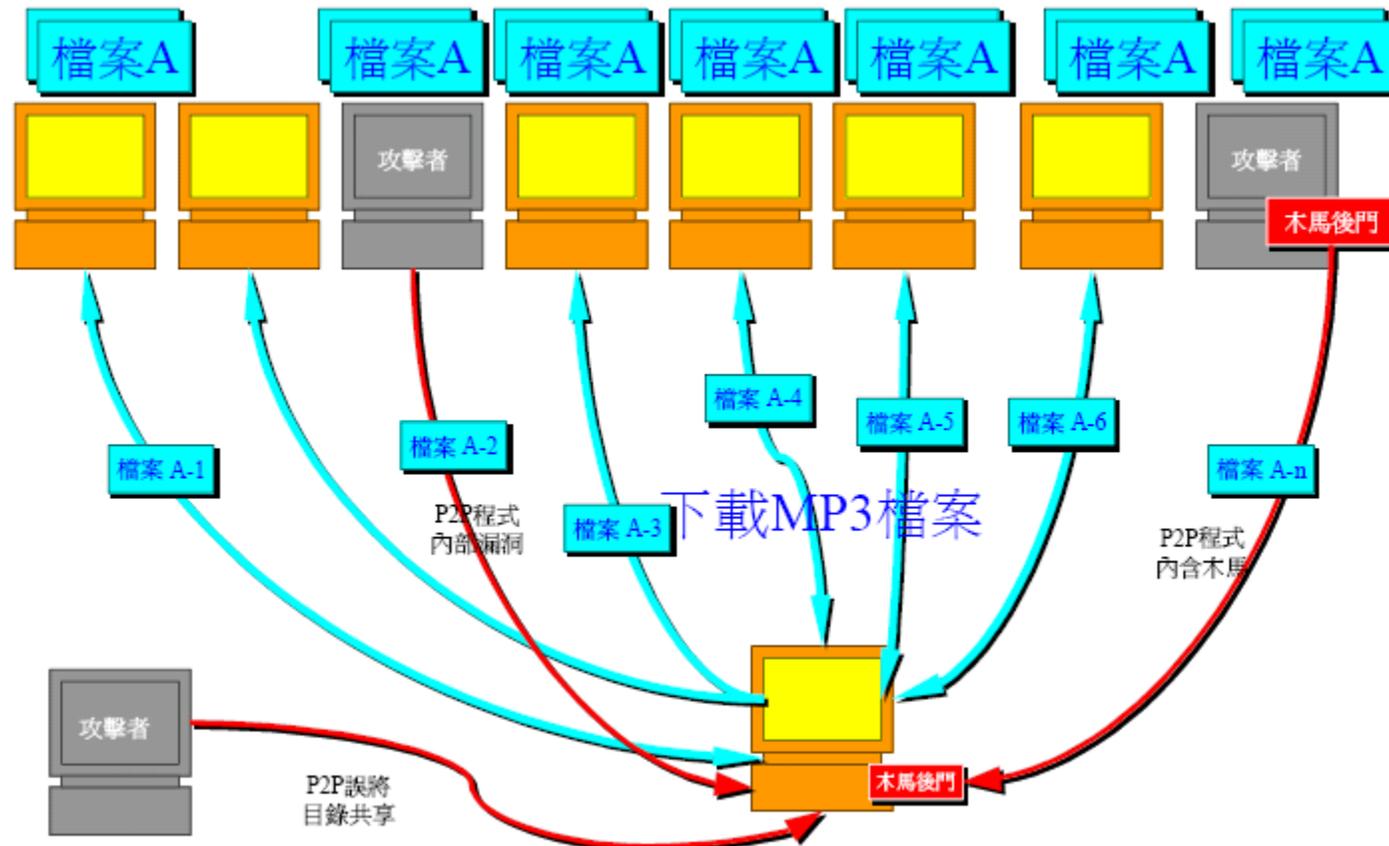
Links

- Winny?  
Winnyのインストール方法や設定、関連ツールの紹介。
- Share(版権)解説サイト  
Shareのインストール方法や設定、関連ツールの紹介。
- デジタルARENA  
Winnyの原理と情報流出の仕組みをわかりやすく解説。
- 仁義なきブログ  
その他、報道されていない流出。流出ファイルの詳細等。

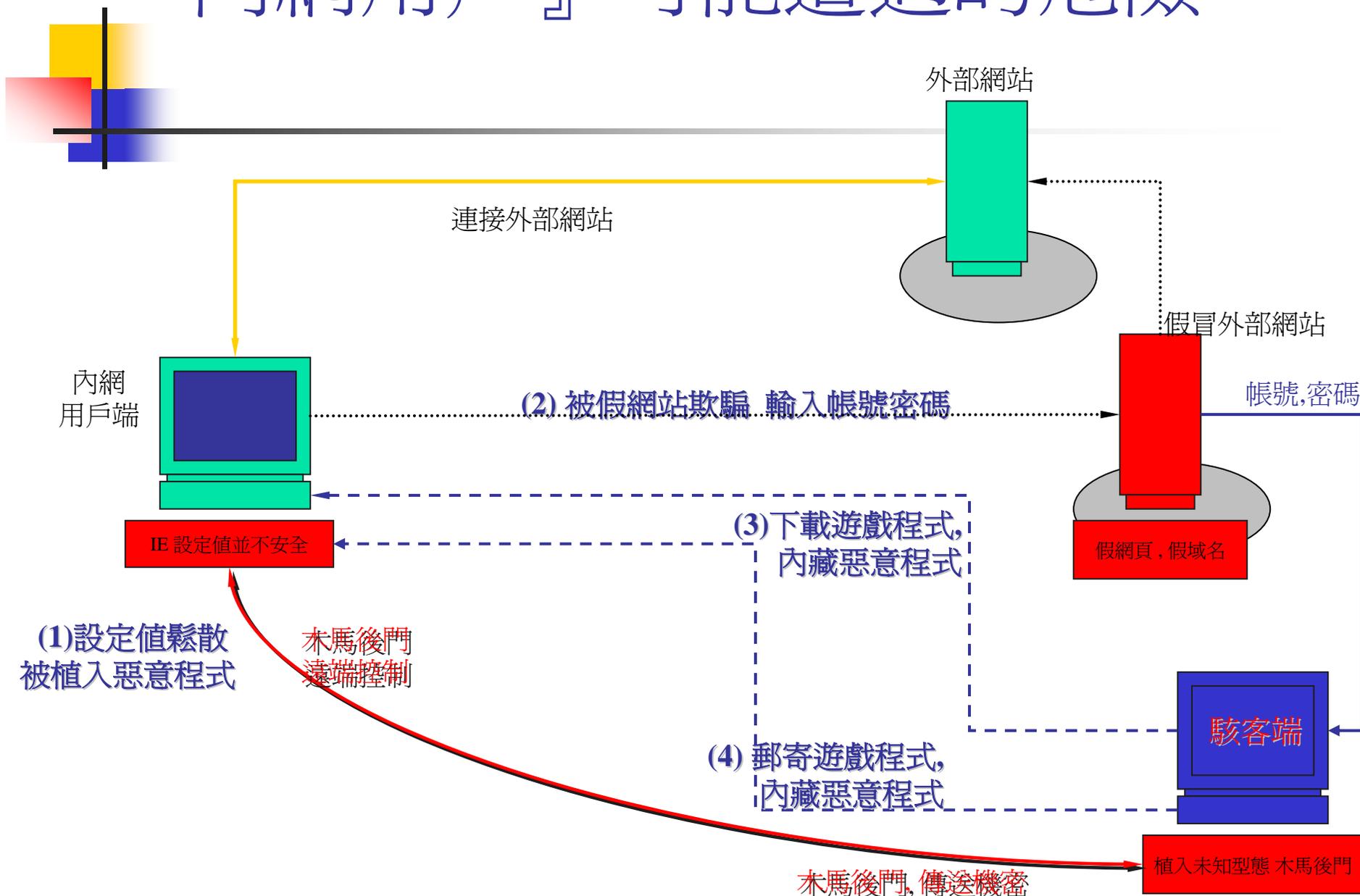
個人機密資料還在外洩

03月00日	NTT西日本	2,237名分の個人情報
02月24日	NTT東日本	1,400件分の顧客情報

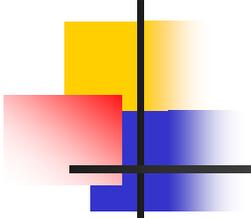
# P2P工具可能產生資安問題， 不易察覺



# 『內網用戶』可能遭遇的危險



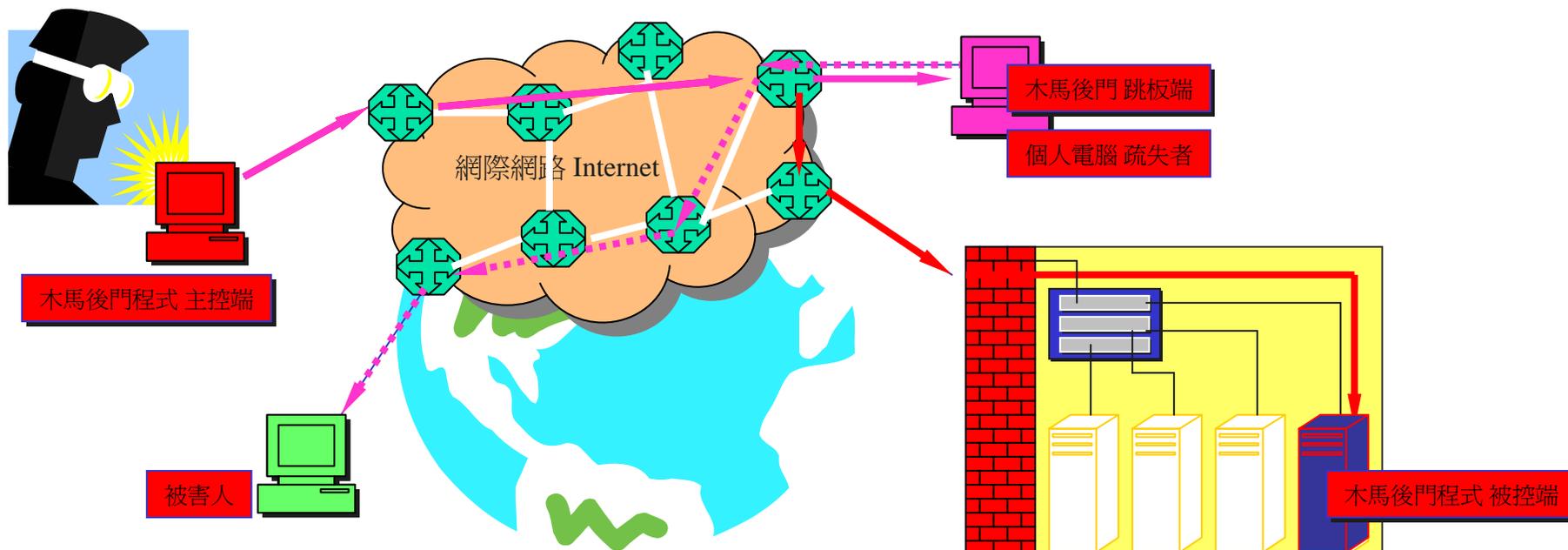
# 用戶開啓異常電子郵件的後果

- 
- 個人基本資料被盜用，金融密碼外洩。
    - 加害人立即更改密碼，受害者無法使用該帳戶。
    - 轉帳至臨時帳戶，或是冒用身份開假支票。
    - 盜刷信用卡，或是複製 ATM 提款卡。
    - 個人資料被地下交易，隱私權被侵犯。
  - 個人電腦被植入木馬後門程式
    - 電腦機密檔案被竊取，危駭他人安全。
    - 自身隱密照片外流，引發桃色糾紛。
    - 電腦做爲駭客跳板，攻擊政府部門。
    - 假借您的電郵帳號，寄送異常郵件給您的親朋好友。
  - 防火牆，防毒軟體僅能針對已知木馬後門防護。
  - 電子郵件與MSN最容易成爲駭客攻擊方式。

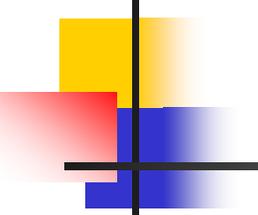
# 甚麼是木馬後門程式？

木馬後門程式是一種惡意通訊程式，這種惡意程式會在電腦使用者未授權的情況下，擅自對外連線通訊，接受外部控制者(駭客)的遙控指令，它的作用有下列幾種：(1) 可以作為網路跳板，轉攻其他電腦。(2) 竊取個人電腦的磁碟檔案，包括機密文件檔案與個人金融財務帳號。(3) 執行軟體程式，進行其他破壞行為。

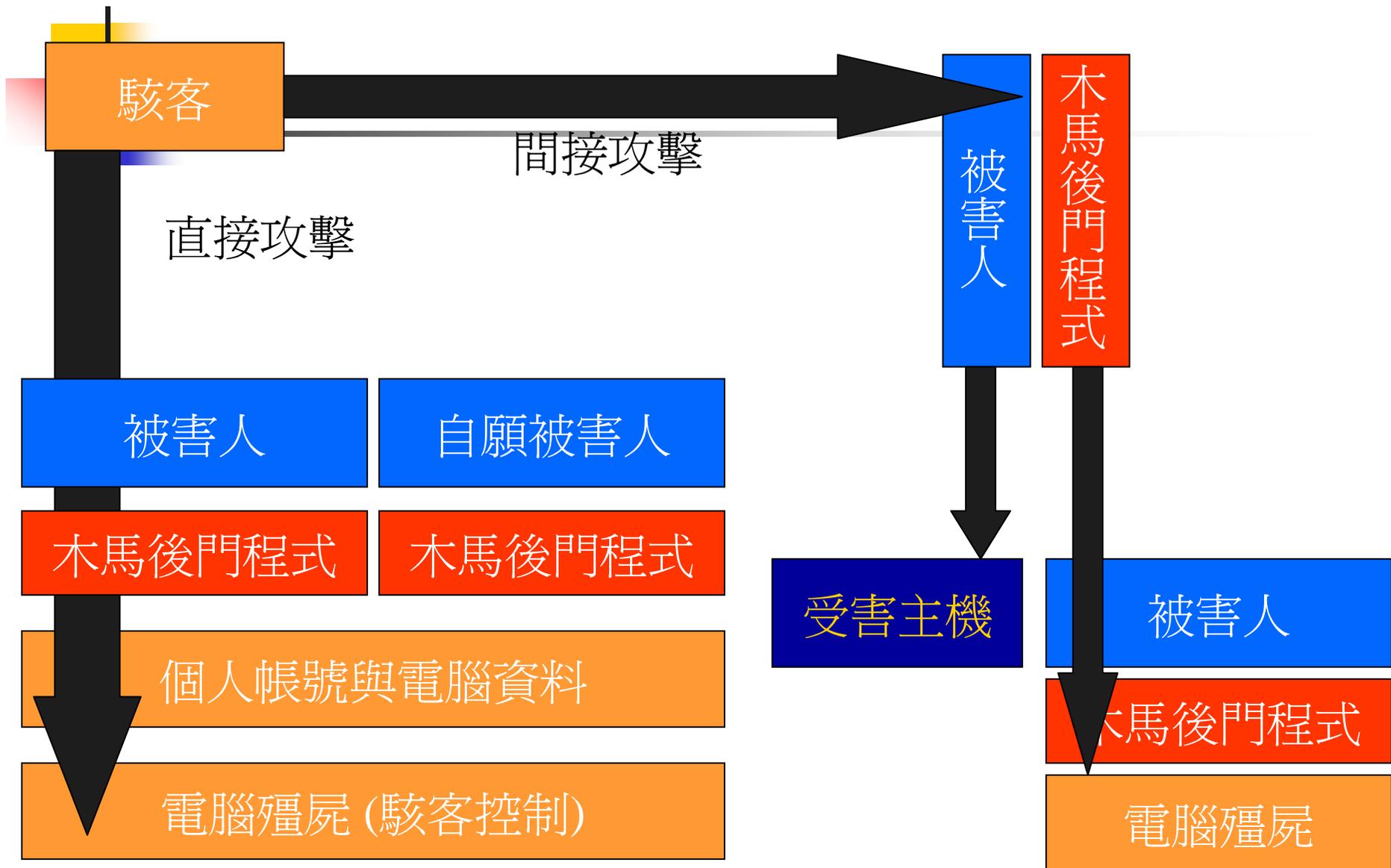
- 木馬後門程式與網路病毒蠕蟲不同之處，在於木馬後門程式背後隱藏著駭客遙控的因素。換句話說，病毒蠕蟲是漏洞感染傳播，而木馬後門則是駭客入侵的人為程式。關鍵是背後的駭客喔！
- PS: 題外話，木馬後門程式是採用古希臘的特洛伊戰爭，希臘人針對久攻不下的特洛伊城池，希臘人佯裝撤退，並呈獻木馬禮物給特洛伊人，卻將少數士兵藏裝於木馬之中，待特洛伊人將木馬拖入城市後，潛藏於木馬的希臘士兵將城門開啓，希臘大軍便毀滅了特洛伊國。您也許會好奇的問我：為甚麼是木馬？而不是木牛，或木雞木狗呢？因為特洛伊人位居商業貿易通道，而且該國的騎兵威震八方，它們的崇拜圖騰就是馬匹。



# 甚麼是木馬後門程式？



- 在電腦操作者(使用者)不知情的狀況，對外通訊的的程式，就可以稱為廣義的木馬後門程式。
- 狹義的木馬後門程式，是針對竊取電腦資料(帳號，密碼，檔案)與操控對方電腦(被控端)。
- 植入木馬後門程式的方式：  
主動植入：駭客利用漏洞入侵電腦。  
被動植入：將木馬後門程式與其他程式混合，等待用戶取回，常見方式有電子郵件，圖片下載，程式下載，破解軟體，等等。



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 → 搜尋 我的最愛 媒體

網址(D) http://tw.club.yahoo.com/clubs/MyDownload 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](#)  
[登出](#)

Yahoo!奇摩

### My Download 下載網

電腦通訊 > 軟體

建立家族不困難，家族教學讓你一目瞭然！ [加入此家族](#) [登出](#)

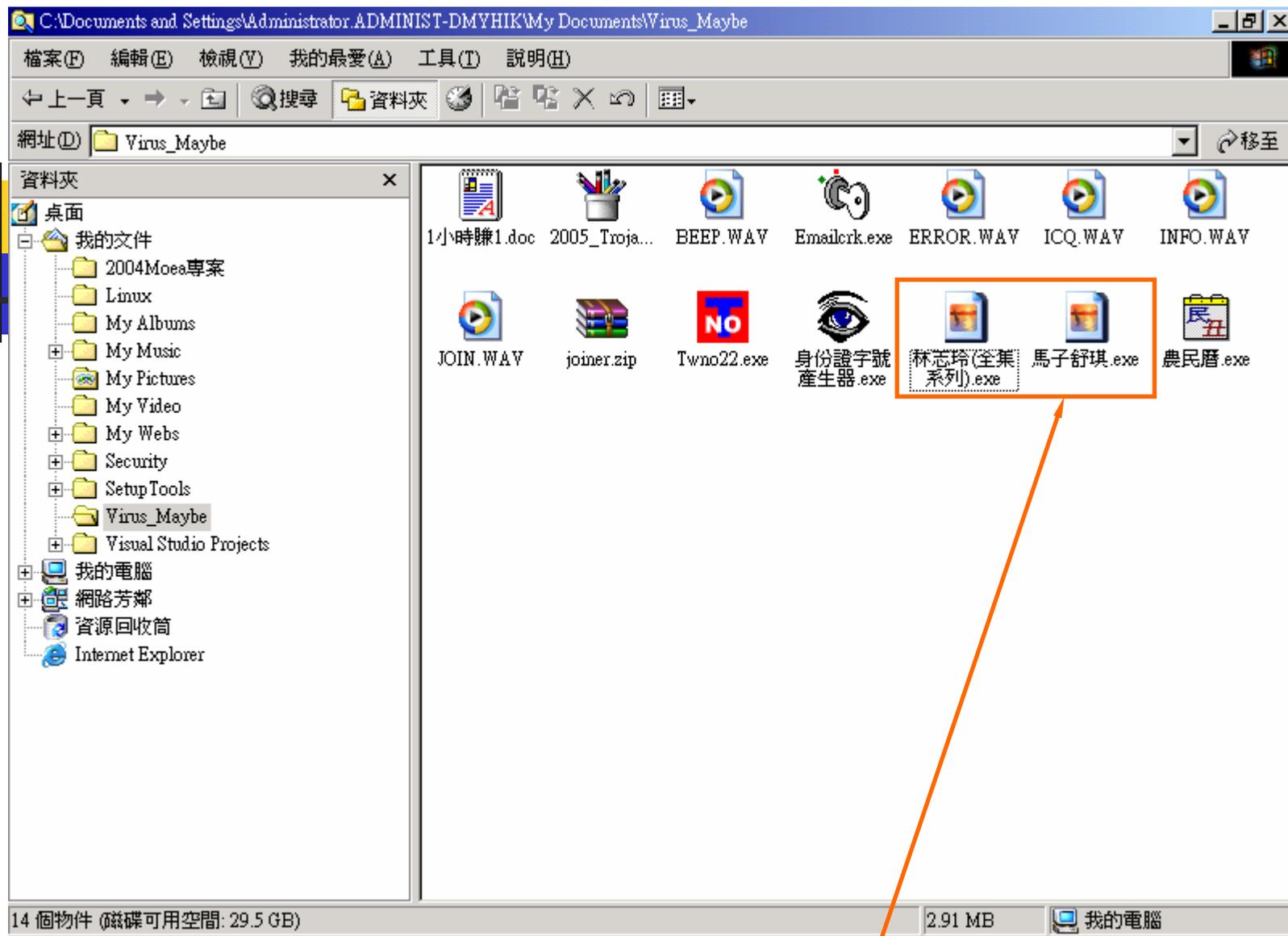
**檔案庫** [新增檔案](#) [精華區](#)

第 1-6 篇，共 6 篇 編輯管理

類別	檔案名稱	檔案大小	推薦人	日期
	<a href="#">我的馬子相舒琪,相似度80%</a> 天阿!我沒看錯吧!	160 K	☆☆~Mr.特務~☆☆ (abc8854120) <a href="#">留言給我!</a>	2005/03/27 18:18:32
	<a href="#">林志玲全裸寫真</a> 未成名前的照片(珍藏版)	264 K	豪!@#%^&*_{. (r123771481) <a href="#">留言給我!</a>	2005/02/14 02:02:45
	<a href="#">符號嚕~</a> 方便啦~!	11 K	Krista (happy-50033) <a href="#">留言給我!</a>	2005/02/02 11:09:06
	<a href="#">身分證字號產生器</a> 好用...我覺得... = =	340 K	Krista (happy-50033) <a href="#">留言給我!</a>	2005/02/02 11:08:28
	<a href="#">快速賺錢的好方法優!!</a> 好康給大家知...	10 K	為為 (love10250623) <a href="#">留言給我!</a>	2004/10/23 17:18:51
	<a href="#">信用卡產生器.rar</a> 如名	315 K	json800114 (json800114) <a href="#">留言給我!</a>	2003/09/25 17:16:42

網際網路

這些照片檔案，其實是EXE檔案  
 (可能是木馬加殼檔案)



這些EXE檔案，還故意使用XP圖片檔案的樣子喔!!

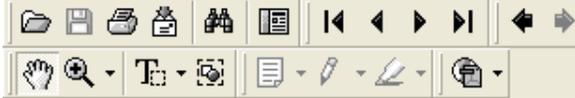


爲何防毒軟體不能救我的電腦呢？

# Trojan White Paper

Aelphaeis Mangarae [Igniteds.NET]

May 5<sup>th</sup> 2006



# 爲何防毒軟體不能救我的電腦呢？

## [Norton Anti-Virus (Symantec)]

Website: <http://symantec.com/>

Trojans Detected: 6 out of 8

Packers Detected: 3 out of 8

Heuristic Analysis:

To my knowledge Norton AV does not have Heuristic analysis.

General Comment:

Overall I think Norton AV is a very over hyped and very poor Anti-Virus software. Although it performed better than what I thought it would for the detection of Trojans, it's detection of file packers was poorer than expected.

原始木馬檔案 8 → 6  
壓縮組合檔案 8 → 3

## [McAfee Anti-Virus (Network Associates)]

Website: <http://www.mcafee.com/>

Trojans Detected: 8 out of 8

Packers Detected: 7 out of 8

Heuristic Analysis:

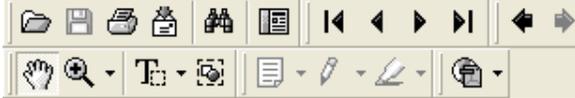
McAfee AV is not known to have Heuristic analysis.

General Comment:

Overall I thought McAfee AV performed rather well, and would be suitable as protection against Trojans and other malware.

原始木馬檔案 8 → 8  
壓縮組合檔案 8 → 7

Bookmarks  
Thumbnails  
Signatures



# 爲何防毒軟體不能救我的電腦呢？

## [Kaspersky Anti-Virus (Kaspersky Labs)]

Website: <http://kaspersky.com/>

Trojans Detected: 8 out of 8

Packers Detected: 7 out of 8

Heuristic Analysis:

Kaspersky Labs claims their latest Anti-Virus software has impressive Heuristics:

*Experts at Kaspersky Lab proudly present our second-generation heuristic virus analyzer that protects PCs from unknown viruses. This intricate and advanced technology detects almost 100% of previously undocumented viruses.*

However we did not see Kaspersky Labs heuristic analysis perform as well as it should of, and detect the last packer Kaspersky failed to detect.

General Comment:

Overall Kaspersky AV is a great Anti-Virus solution, I strongly recommend it.

原始木馬檔案 8 → 8  
壓縮組合檔案 8 → 7

## [NOD32 (ESET)]

Website: <http://www.nod32.com/>

Trojans Detected: 8 out of 8

Packers Detected: 6 out of 8

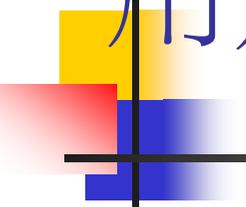
Heuristic Analysis:

NOD32 is known to have Heuristic Analysis and in the test we found that it's Heuristic managed to detect one of the packers.

General Comment:

Overall I was impressed by NOD32, but at the same time disappointed. I expected NOD32 to be able to detect all of the packers in the test, however NOD32 performed rather poorly.

原始木馬檔案 8 → 8  
壓縮組合檔案 8 → 6



# 用戶端電腦被植入木馬的後果

---

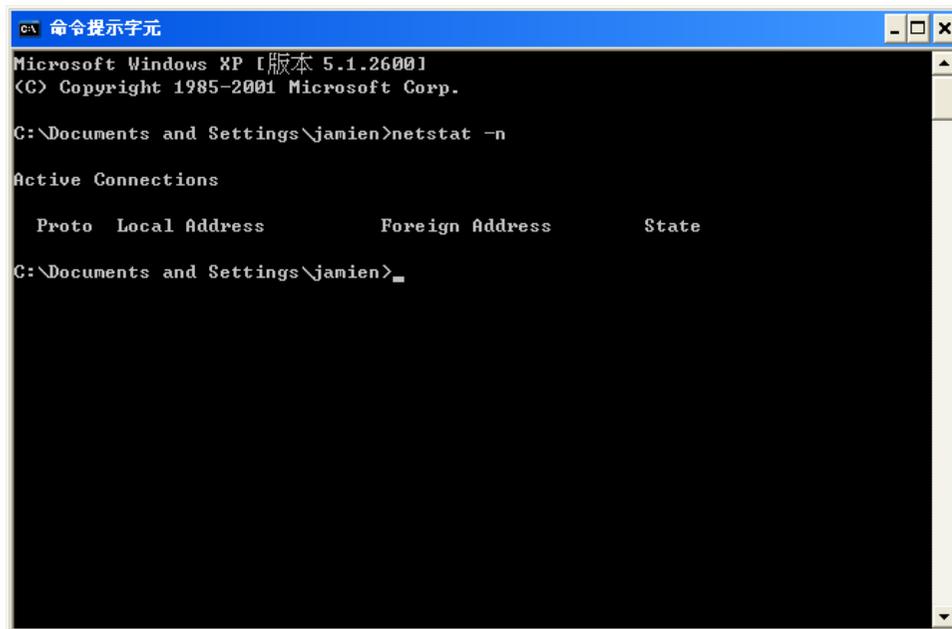
- 1.個人基本資料被盜用，金融密碼外洩。
- 2.電腦機密檔案被竊取，危駭他人安全。
- 3.自身隱密照片外流，引發桃色糾紛。
- 4.電腦做為駭客跳板，攻擊政府部門。
- 5.防毒軟體僅能針對已知木馬後門防護
- 6.使用者自行安裝軟體，屬『吳三桂模式』。



# 如何瞭解電腦是否被植入木馬後門程式？

電腦是否被植入木馬後門程式，請您執行下列簡單步驟，即可自我偵測。(1)將個人電腦重新開機，(2)家用電腦請撥接網路，一般電腦請連接網路，(3)請勿網頁瀏覽，或接收電子郵件，或開啓任何通訊程式(MSN,Skype,ezPeer,BT,eMule,eDonkey...)，(4)開啓命令列，執行netstat -n的指令，(5)如果出現左下角畫面，表示正常，無木馬後門程式。(6)如果出現右下角畫面，表示有異常通訊，可能有木馬後門程式。

- 請確定您在開機後沒有開啓任何通訊程式喔！這個檢查方式，是要檢查『沒有授權傳送資料的通訊程式』，正常情況下應該沒有任何通訊程式。少數情況會出現下列可能，(1)更新系統程式，連接到微軟網站。(2)更新病毒識別檔案，連接到防毒軟體公司。(3)微軟公司檢查您的軟體是否為盜版軟體，連接到微軟網站。(4)企業內部的其他應用程式，例如公文系統，會計軟體，出缺勤軟體等等。

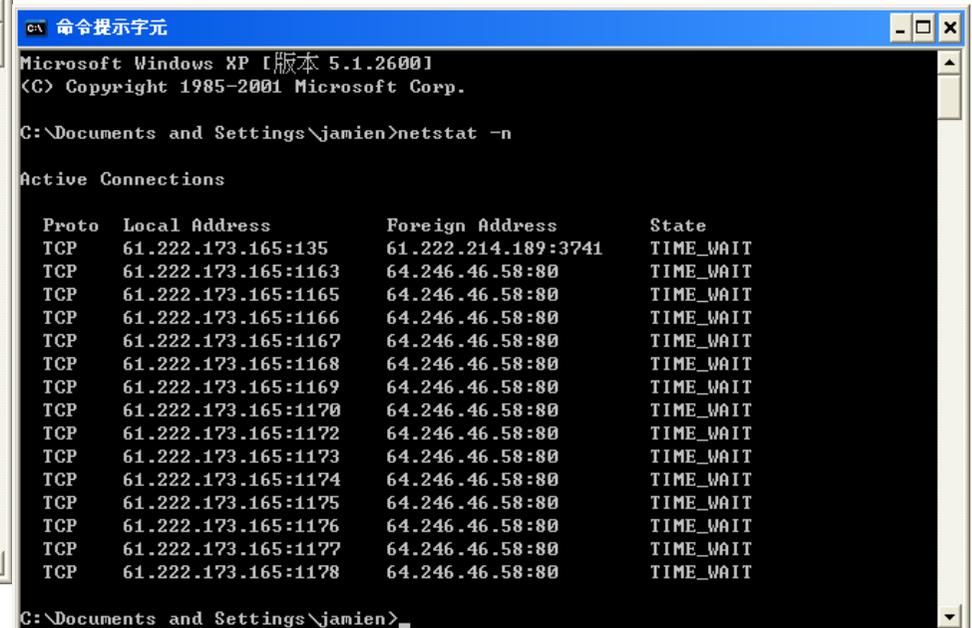


```
CA 命令提示字元
Microsoft Windows XP [版本 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\jamien>netstat -n

Active Connections

   Proto Local Address          Foreign Address         State
C:\Documents and Settings\jamien>
```

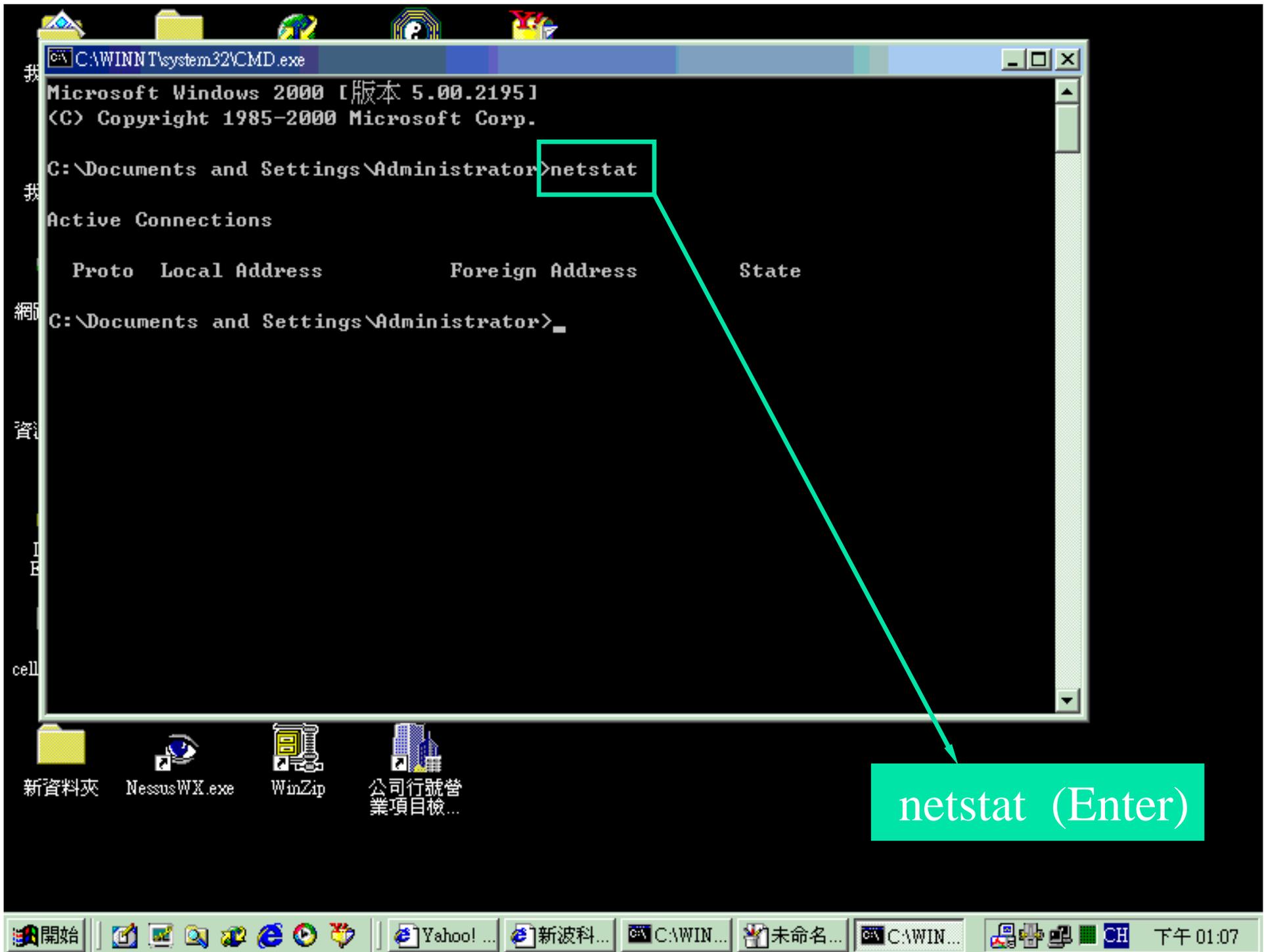


```
CA 命令提示字元
Microsoft Windows XP [版本 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\jamien>netstat -n

Active Connections

   Proto Local Address          Foreign Address         State
TCP    61.222.173.165:135     61.222.214.189:3741    TIME_WAIT
TCP    61.222.173.165:1163   64.246.46.58:80       TIME_WAIT
TCP    61.222.173.165:1165   64.246.46.58:80       TIME_WAIT
TCP    61.222.173.165:1166   64.246.46.58:80       TIME_WAIT
TCP    61.222.173.165:1167   64.246.46.58:80       TIME_WAIT
TCP    61.222.173.165:1168   64.246.46.58:80       TIME_WAIT
TCP    61.222.173.165:1169   64.246.46.58:80       TIME_WAIT
TCP    61.222.173.165:1170   64.246.46.58:80       TIME_WAIT
TCP    61.222.173.165:1172   64.246.46.58:80       TIME_WAIT
TCP    61.222.173.165:1173   64.246.46.58:80       TIME_WAIT
TCP    61.222.173.165:1174   64.246.46.58:80       TIME_WAIT
TCP    61.222.173.165:1175   64.246.46.58:80       TIME_WAIT
TCP    61.222.173.165:1176   64.246.46.58:80       TIME_WAIT
TCP    61.222.173.165:1177   64.246.46.58:80       TIME_WAIT
TCP    61.222.173.165:1178   64.246.46.58:80       TIME_WAIT
C:\Documents and Settings\jamien>
```



# 如何停止木馬後門程式的執行？

要停止木馬後門程式的執行，請先執行命令列，按照先前的檢測木馬後門程式的操作步驟，並且再執行工作管理員，從異常通訊程序的PID資料，對照於工作管理員的PID，然後終止該程序的執行。

```
C:\Documents and Settings\jamien>netstat -ano

Active Connections

Proto Local Address Foreign Address State PID
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 940
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING 4
TCP 61.222.173.165:139 0.0.0.0:0 LISTENING 4
TCP 127.0.0.1:1025 0.0.0.0:0 LISTENING 1508
TCP 127.0.0.1:1026 0.0.0.0:0 LISTENING 1188
TCP 127.0.0.1:1030 0.0.0.0:0 LISTENING 2116
UDP 0.0.0.0:445 **:* 4
UDP 0.0.0.0:500 **:* 688
UDP 0.0.0.0:4500 **:* 688
UDP 61.222.173.165:123 **:* 980
UDP 61.222.173.165:137 **:* 4
UDP 61.222.173.165:138 **:* 4
UDP 61.222.173.165:1900 **:* 1304
UDP 127.0.0.1:123 **:* 980
UDP 127.0.0.1:1900 **:* 1304
```

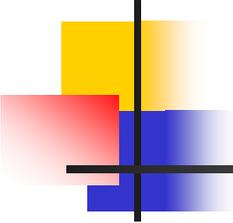
```
C:\Documents and Settings\jamien>netstat -ano

Active Connections

Proto Local Address Foreign Address State PID
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 940
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING 4
TCP 61.222.173.165:135 61.221.15.28:1844 ESTABLISHED 940
TCP 61.222.173.165:139 0.0.0.0:0 LISTENING 4
TCP 61.222.173.165:1041 59.120.215.160:1999 SYN_SENT 3460
TCP 127.0.0.1:1025 0.0.0.0:0 LISTENING 1508
TCP 127.0.0.1:1026 0.0.0.0:0 LISTENING 1188
TCP 127.0.0.1:1030 0.0.0.0:0 LISTENING 2116
UDP 0.0.0.0:445 **:* 4
UDP 0.0.0.0:500 **:* 688
UDP 0.0.0.0:1040 **:* 1208
UDP 0.0.0.0:4500 **:* 688
UDP 61.222.173.165:123 **:* 980
UDP 61.222.173.165:137 **:* 4
UDP 61.222.173.165:138 **:* 4
UDP 61.222.173.165:1900 **:* 1304
UDP 127.0.0.1:123 **:* 980
UDP 127.0.0.1:1900 **:* 1304
```

影像名稱	PID	使用者名稱	C...	CPU
GW-US54GZL.exe	2424	jamien	00	C
Hcontrol.exe	2196	jamien	00	C
iFmewrk.exe	2160	jamien	00	C
ISSVC.EXE	1604	SYSTEM	00	C
LSASS.EXE	688	SYSTEM	00	C
MSMSGs.EXE	2256	jamien	00	C
OProtSvc.exe	216	SYSTEM	00	C
POWERPNT.EXE	3072	jamien	00	C
RegSvc.exe	232	SYSTEM	00	C
S24EvMon.exe	1116	SYSTEM	00	C
SERVICES.EXE	676	SYSTEM	00	C
SMSS.EXE	536	SYSTEM	00	C
SNDSvc.exe	1632	SYSTEM	00	C
SoundMan.exe	800	jamien	00	C
SPOOLSVC.EXE	1992	SYSTEM	00	C
svchUst.exe	3460	jamien	00	C
SVCHOST.EXE	416	SYSTEM	00	C
SVCHOST.EXE	848	SYSTEM	00	C
SVCHOST.EXE	940	NETWORK SER...	00	C
SVCHOST.EXE	980	SYSTEM	00	C
SVCHOST.EXE	1208	NETWORK SER...	00	C
SVCHOST.EXE	1304	LOCAL SERVICE	00	C
SymIPEnh.exe	2100	jamien	00	C
SymIPLpr.exe	2088	jamien	00	C
System	4	SYSTEM	00	C
System Idle Process	0	SYSTEM	97	C
taskmgr.exe	1096	jamien	03	C
TosBtMngl.exe	2296	jamien	00	C
WCOURIER.EXE	2060	jamien	00	C
WDFMGR.EXE	452	LOCAL SERVICE	00	C
WINLOGON.EXE	632	SYSTEM	00	C
wuauclt.exe	3200	jamien	00	C
ZCfgSvc.exe	1256	jamien	00	C

netstat -ano (Enter)



# 偵測清除木馬後門的程序

---

- 1. 巡察異常執行通訊程式 (Hunting)
- 2. 尋找異常程式檔案位置 (Directory)
- 3. 挖掘程式啓動點 (Startup Position)
- 4. 檔案更名，重新開機 (Restart)

# 尋找異常程式檔案位置 (Directory)

The screenshot shows a Windows Explorer window titled "搜尋結果" (Search Results). The search criteria are: "部份或完整的檔案名稱(O): svchost.exe", "檔案裡的字或片語(W):", and "尋找在(L): 本機硬式磁碟機 (C;D:)". The search results table is as follows:

名稱	資料夾	大小	類型
svchost.exe	CAWINDOWS\system32	14 KB	應用程式
SVCHOST.EXE-2D5FBD18.pf	CAWINDOWS\Prefetch	20 KB	PF 檔案
svchost.exe	CAWINDOWS	244 KB	應用程式

A red arrow points from a text box to the "svchost.exe" file in the "CAWINDOWS" folder. The text box contains the following text:

相同檔案名稱，有兩各不同目錄位置，檔案大小也不相同，其中必定有假冒。

# Position)

The screenshot displays the Windows XP Registry Editor window titled "登錄編輯程式". The left pane shows the tree structure expanded to "Run". The right pane lists registry values with columns for Name, Type, and Data. An "執行" (Run) dialog box is overlaid on the bottom right, showing "regedit.exe" entered in the "開啓(O):" field.

名稱	類型	資料
(預設值)	REG_SZ	
ALCMTR	REG_SZ	ALCMTR.EXE
ALCWZRD	REG_SZ	ALCWZRD.EXE
ASUS Live Update	REG_SZ	C:\Program Files\ASUS\ASUS Live Update\ALU.exe
ATIPTA	REG_SZ	C:\Program Files\ATI Technologies\ATI Control Panel\atiptaxx.exe
ccApp	REG_SZ	"C:\Program Files\Common Files\Symantec Shared\ccApp.exe"
Demo Trojan_CTP	REG_SZ	C:\WINDOWS\svchost.exe
EOUApp	REG_SZ	C:\Program Files\Intel\Wireless\Bin\EOUWiz.exe
HControl	REG_SZ	C:\WINDOWS\ATK0100\HControl.exe
High Definition Audio 屬性頁捷徑	REG_SZ	HDASHCut.exe
IMJPMIG8.1	REG_SZ	"C:\WINDOWS\IME\imjp8_1\IMJPMIG.EXE" /Spoil/RemAdvDef /Migration32
IntelWireless	REG_SZ	C:\Program Files\Intel\Wireless\Bin\ifmewrk.exe /fi Intel PROSet/Wireless
PHIME2002A	REG_SZ	C:\WINDOWS\system32\IMEVIM\TLGNT\TINTSETP.EXE /IMEName
PHIME2002ASync	REG_SZ	C:\WINDOWS\system32\IMEVIM\TLGNT\TINTSETP.EXE /SYNC
Power_Gear	REG_SZ	C:\Program Files\ASUS\Power4 Gear\BatteryLife.exe 1
SoundMan	REG_SZ	SOUNDMAN.EXE
Symantec NetDriver Monitor	REG_SZ	C:\PROGRA~1\SYMNET~1\SNDMon.exe /Consumer
SynTPEnh	REG_SZ	C:\Program Files\Synaptics\SynTP\SynTPEnh.exe
SynTPLpr	REG_SZ	C:\Program Files\Synaptics\SynTP\SynTPLpr.exe
Windows Defender	REG_SZ	"D:\Program Files\Windows Defender\MSASCui.exe" -hide
Wireless Console	REG_SZ	C:\Program Files\ASUS\Wireless Console\wccourier.exe

執行

輸入程式、資料夾、文件或網際網路資源的名稱，Windows 會自動開啓。

開啓(O): regedit.exe

確定 取消 瀏覽(B)...

我的電腦\HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

# 檔案更名，重新開機 (Restart)

搜尋結果

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 資料夾 Norton AntiVirus

搜尋小幫手

用下列任何或所有的搜尋條件。

部份或完整的檔案名稱(O):  
svchost.exe

檔案裡的字或片語(W):

尋找在(L):  
本機硬式磁碟機 (C::D:)

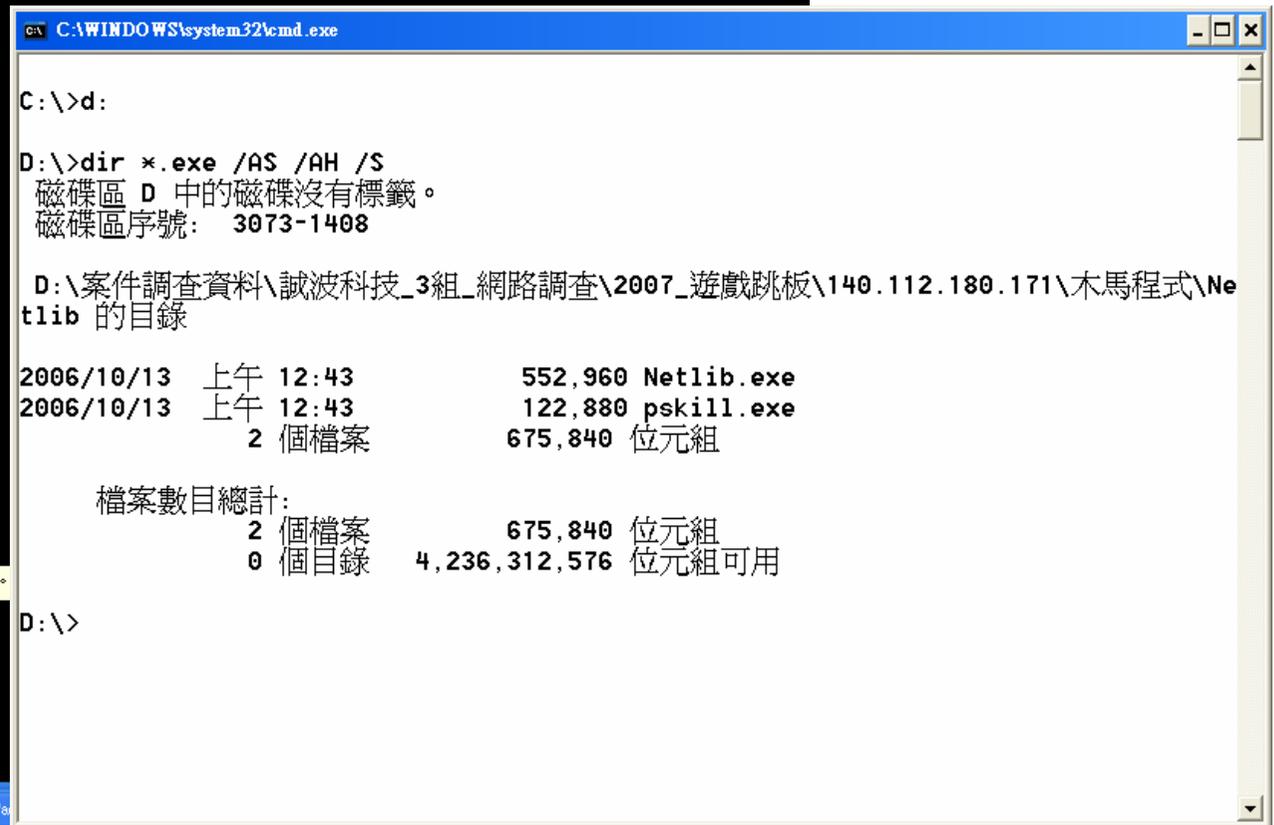
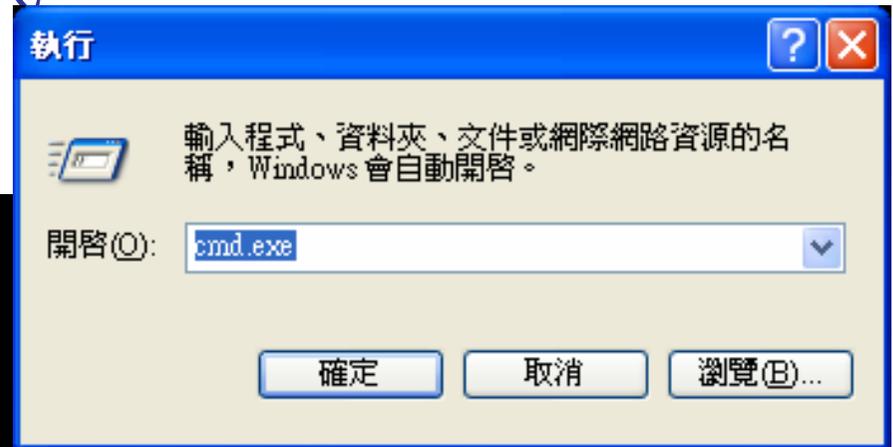
什麼時候修改的? 大小是? 進階選項

上一部(B) 搜尋(R)

名稱	資料夾	大小	類型
svchost.exe	C:\WINDOWS\system32	14 KB	應用程式
SVCHOST.EXE-2D5FBD18.pf	C:\WINDOWS\Prefetch	20 KB	PF 檔案
svchost.exe.bct	C:\WINDOWS	244 KB	應用程式

名稱	資料夾	大小	類型
svchost.exe	C:\WINDOWS\system32	14 KB	應用程式
SVCHOST.EXE-2D5FBD18.pf	C:\WINDOWS\Prefetch	20 KB	PF 檔案
svchost.exe.bct	C:\WINDOWS	244 KB	文字文件

# 顯示隱藏檔案的方式



# 自製USB病毒清除程式

找不到檔案，才是沒有USB病毒

PS:要記得先停止檔案總管桌面的執行 (explorer.exe)

```
C:\WINDOWS\system32\cmd.exe

D:\>type Clean_Kavo_Virus.bat
attrib -S -H -R autorun.inf
attrib -S -H -R ntdelect.com
del autorun.inf
del ntdelect.com
D:\>Clean_Kavo_Virus

D:\>attrib -S -H -R autorun.inf
找不到檔案 - autorun.inf

D:\>attrib -S -H -R ntdelect.com
找不到檔案 - ntdelect.com

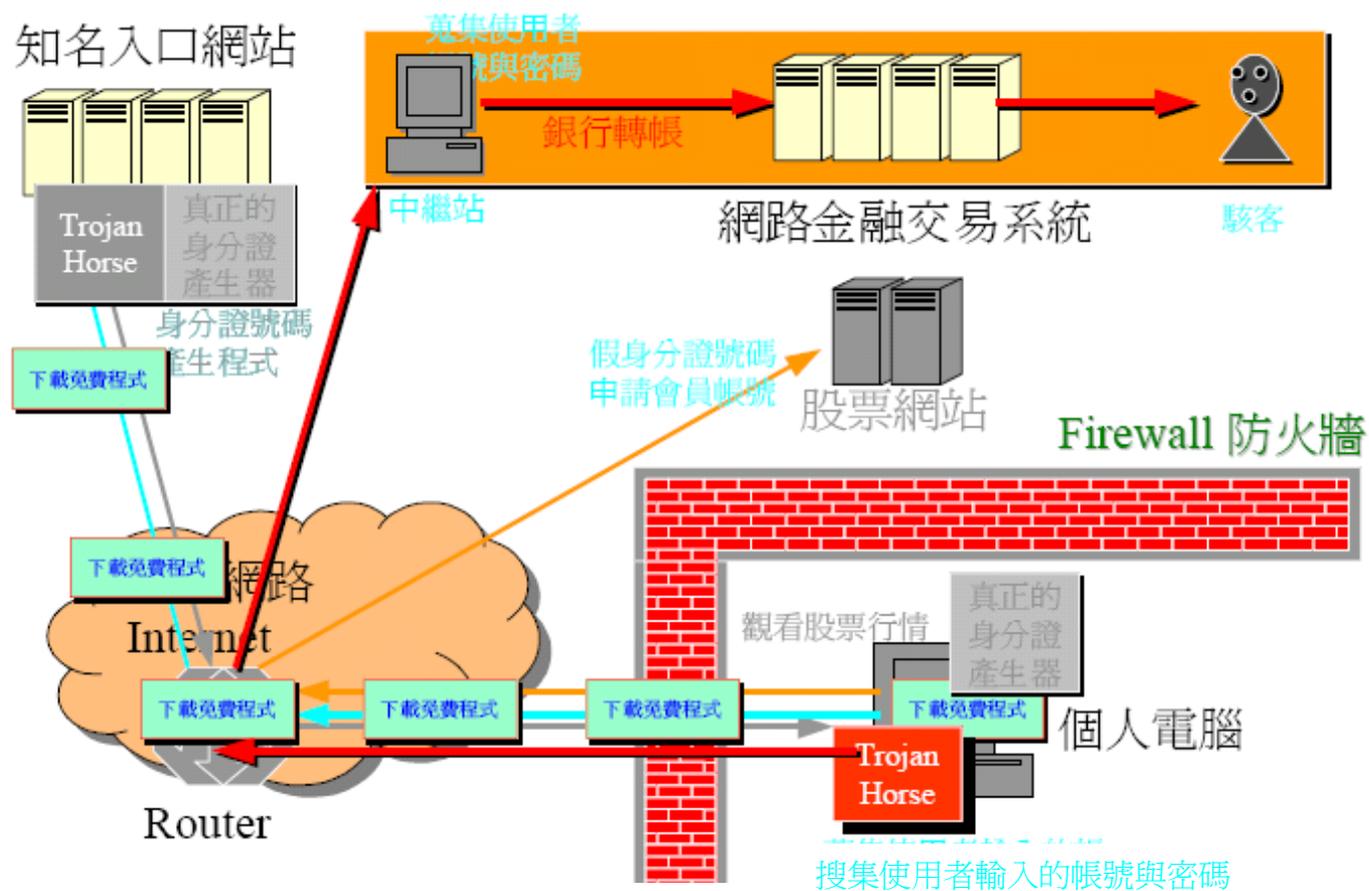
D:\>del autorun.inf
找不到 D:\autorun.inf

D:\>del ntdelect.com
找不到 D:\ntdelect.com

D:\>
```

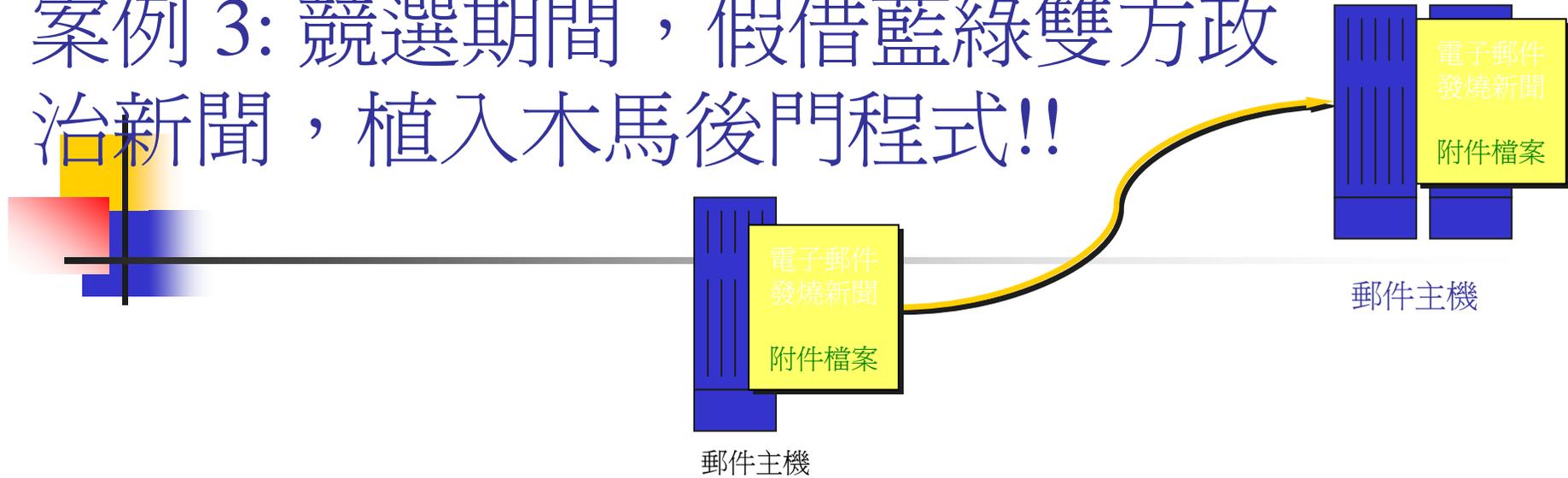


# 案例1：網路銀行盜領案件

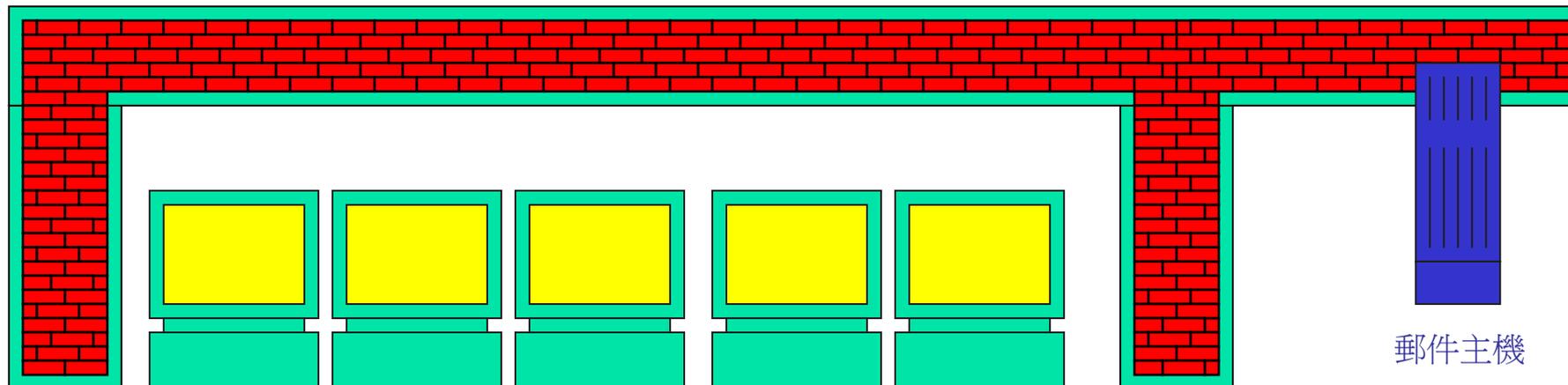




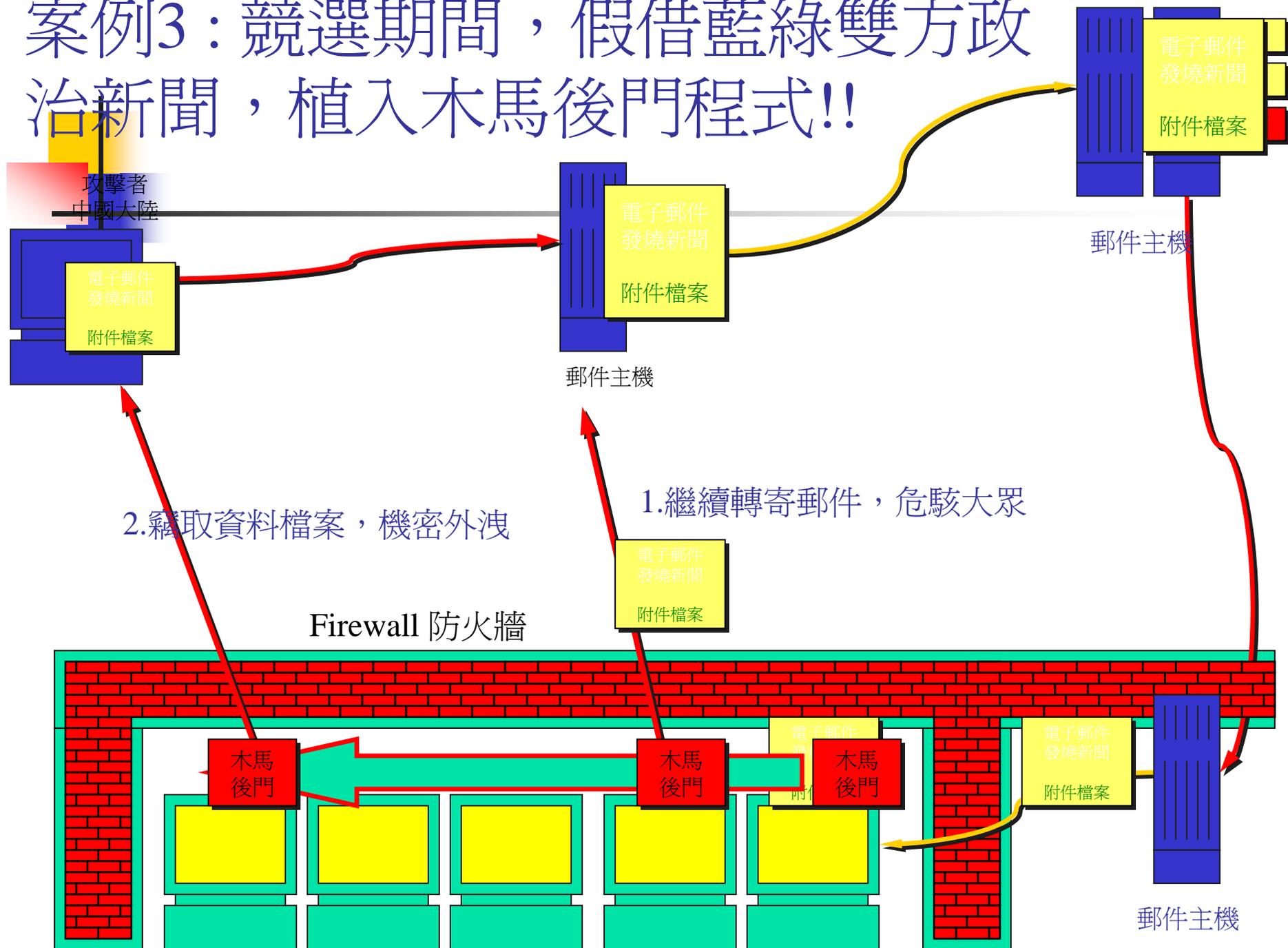
# 案例 3: 競選期間，假借藍綠雙方政治新聞，植入木馬後門程式!!



Firewall 防火牆



# 案例3：競選期間，假借藍綠雙方政治新聞，植入木馬後門程式!!



# 原作者應為中國大陸

假發票圖片.ppt  
Microsoft PowerPoint 簡報  
117 KB

國務機要費.eml  
Outlook Express 郵件訊息  
277 KB

總統府國務機要費.rar  
WinRAR 壓縮檔  
83 KB

假發票圖片.ppt 內容

一般 自訂 摘要

屬性	值
<input type="checkbox"/> 多媒體資料	0
<input type="checkbox"/> 比例	否
<input type="checkbox"/> 非資訊連結?	0
<input checked="" type="checkbox"/> 註解	
<b>原始檔案</b>	
<input checked="" type="checkbox"/> 作者	
<input type="checkbox"/> 上次存檔者	MC SYSTEM
<input checked="" type="checkbox"/> 修訂版編號	12
<input checked="" type="checkbox"/> 應用程式名稱	Microsoft PowerPoint
<input checked="" type="checkbox"/> 簡報格式	在螢幕上顯示
<input type="checkbox"/> 公司	
<input type="checkbox"/> 建立日期	
<input checked="" type="checkbox"/> 上次儲存日期	2006/6/29 下午 08:10
<input type="checkbox"/> 前次列印時間	
<input type="checkbox"/> 編輯時間	1601/1/1 上午 08:26

<< 簡易(M)

確定 取消 套用(A)

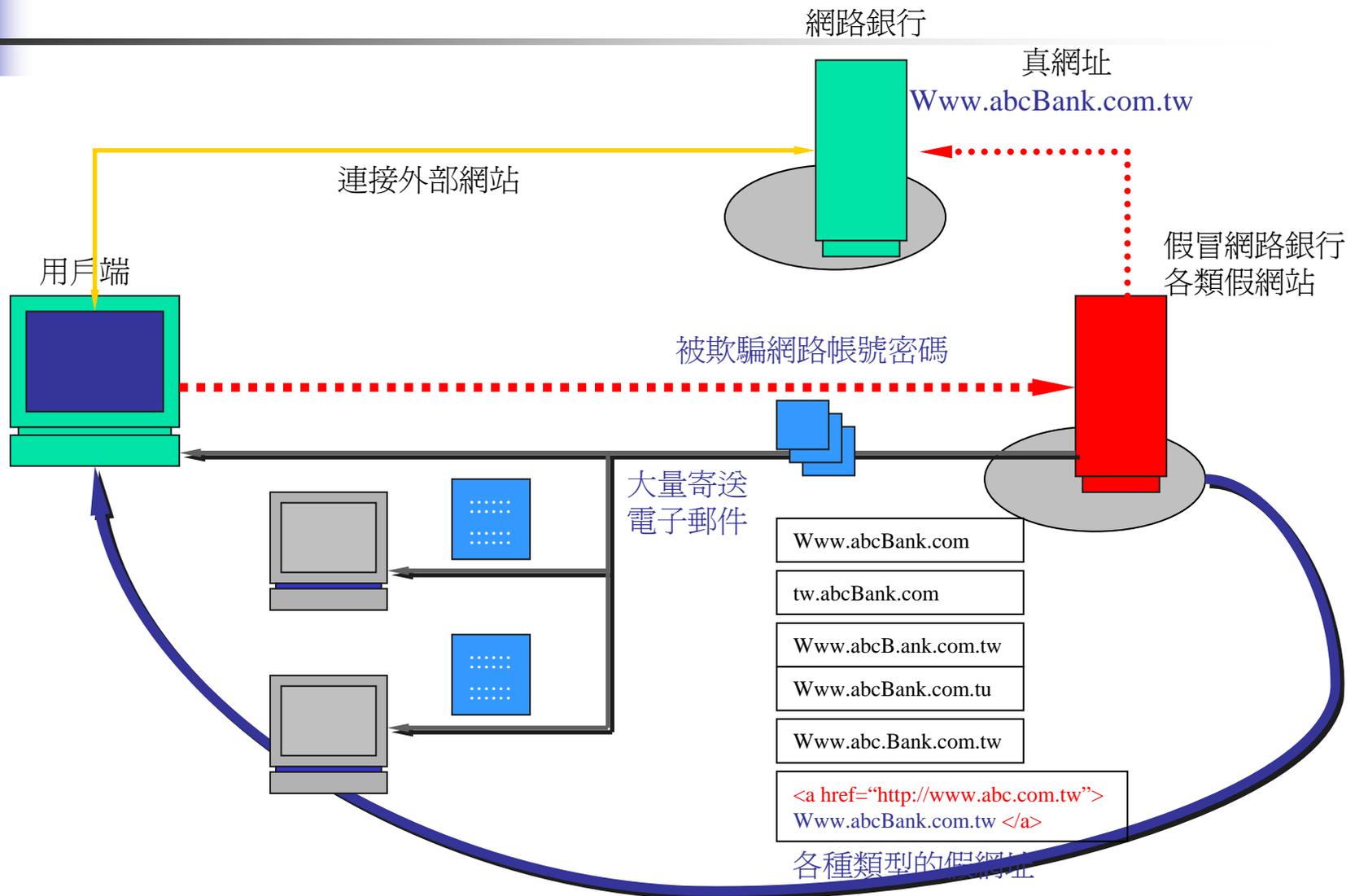
類型: Microsoft PowerPoint 簡報 標題: PowerPoint Presentation 修改日期: 2006/11/3 下午 10:24 大小: 116 KB

Windows Live Messen... Microsoft PowerPoint ... D:\案件調查資料\200...

上午 10:43



# 案例4：假網頁資料 (Web Middle Attack 又稱釣魚網站)



真網頁的網址連接

Yahoo!奇摩 會員登入

YAHOO! 奇摩 搜尋 網頁 知識+ 圖片 影片 部落格 商家 新聞 商品 更多

土地銀行 搜尋

台灣網頁優先 全球網頁

網頁搜尋 土地銀行 搜尋結果約12,959,999個，以下為1 - 10個，共花0.03秒

相關詞：台灣土地銀行, 土地銀行法拍屋, 土地銀行信用貸款, 台灣土地銀行總行, 土地銀行貸款 更多...

- 快速捷國際 - 全方位貸款專家  
首創網路指定專人服務，代辦土地銀行信貸、信用卡業務，整合您的負債！ www.aibank.com.tw
- Quick簡單貸 - 汽車貸款  
有車貸款真輕鬆，土地銀行汽車貸款，額度高，利率低，理財輕鬆真簡單。 www.quickloan.com.tw
- Money易貸網 - 免諮詢費  
提供土地銀行貸款產品免費諮詢，實際貸款請以銀行官方網站為準，或到銀行辦理。 www.1bank.com.tw

- 贊助網站
- 汽車貸款  
土地銀行優惠汽車貸款，額度高、利率低、手續簡便，省時、方便又安全。  
www.autoloan.com.tw
  - 免費諮詢 - 信貸1.88%起  
提供匯豐銀行貸款諮詢，優質信貸、快速2天撥款，55家銀行為您服務。  
www.sped.com.tw
  - 全程免收費 - 銀行貸款  
免費提供多家銀行各類貸款、信貸、整合負債、房屋、企業貸款諮詢，省息專案實施。  
www.wk168.com.tw
  - 免費負債諮詢 - 快速貸款專家  
免費提供土地銀行貸款、整合負債、房屋、企業貸款諮詢，額度高，利率低。  
www.topyybank.com.tw
  - 給您低利 - 銀行高額貸款規劃  
提供土地銀行線上貸款諮詢，3分鐘讓您知道，銀行給你的定位左眼裡。

- 土地銀行  
土銀簡介、網路銀行、業務簡介、便民資訊、理財天地、帳務資料等服務。... (C) 2006 COPYRIGHT LANDBANK 版權所有:土地銀行 最佳瀏覽效果請使用 Internet Explorer 5.0 以上 1024x768 解析度 ...  
www.landbank.com.tw 51k - 2007/08/28 - 庫存頁面 - 更多此站結果
- 土地銀行 - 歡迎蒞臨土地銀行  
... 土地銀行網路銀行憑證可運用於網路報稅(95.02.15) (C) 2006 COPYRIGHT LANDBANK 版權所有:土地銀行 最佳瀏覽效果請使用 Internet Explorer 5.0 以上 1024x768 解析度 ...  
www.landbank.com.tw/ebank/index.htm - 34k - 2007/08/25 - 庫存頁面 - 更多此站結果
- 土地銀行  
各銀行晶片金融卡及 COMBO 卡均可使用,晶片讀卡機不限土地銀行所發 網路ATM交易安全公告事項  
ebank.landbank.com.tw/eatm - 21k - 2007/08/08 - 庫存頁面 - 更多此站結果

# 假網頁的網址連接



網頁 知識+ 分類 商家 圖片 部落格 新聞 商品 學術

土地銀行

搜尋

台灣網頁優先 全球網頁

分享書籤 BETA 進階搜尋 使用偏好 工具下載 網頁翻譯

## 網頁搜尋

土地銀行 搜尋結果約 10,103,999 個, 以下為 1 - 10 個, 共花 0.01 秒

相關詞: [台灣土地銀行](#), [土地銀行信用貸款](#), [台灣土地銀行總行](#), [土地銀行法拍屋](#), [土地銀行貸款](#) 更多...

贊助網站

### 土地銀行 landbank

提供基金、信用卡、金融資訊相關連結服務。 [www.landbank.com.tw](http://www.landbank.com.tw)

刊登贊助網站

### 快速捷國際 - 全方位貸款專家

提供土地銀行代辦信貸、信用卡業務, 整合您的負債, 首創網路指定專人服務。 [www.aibank.com.tw](http://www.aibank.com.tw)

### Easyloan - 汽車貸款

土地銀行汽車貸款, 專業熱誠的服務, 利率低, 額度高, 輕鬆貸, 簡單償。 [www.easyloan.tw](http://www.easyloan.tw)

### 汽車貸款

土地銀行汽車貸款, 提供您資金週轉及購車需求, 額度高、利率低、貸款真容易。 [www.carloan.com.tw](http://www.carloan.com.tw)

### AutoLoan - 汽車貸款

有車讓您貸款更容易, 土地銀行汽車貸款, 額度高、利率低、省時方便又安全。

[www.autoloan.com.tw](http://www.autoloan.com.tw)

### My Bank 線上諮詢網

提供土地銀行貸款諮詢服務, 0%免諮詢費!

[www.lbank.com.tw](http://www.lbank.com.tw)

### 免費諮詢 - 信貸 1.88 起

提供土地銀行諮詢, 優質信貸、快速 2 天撥款, 55 家銀行為您服務。

[www.sped.com.tw](http://www.sped.com.tw)

### 全程免收費 - 銀行貸款

免費提供多家銀行各類貸款、信貸、整合負債、房屋、企業貸款諮詢, 省息專案實施。

## 在 Yahoo! 奇摩生活+ 查土地銀行的電話地址和評價

Yahoo! 奇摩捷徑 - 說明

### 1. 土地銀行

土銀簡介、網路銀行、業務簡介、便民資訊、理財天地、帳務資料等服務。 ... 臺灣土地銀行標售本行所有臺中市區仁愛段六小段 8-3、9-14 地號等 2 筆土地及地上 1 棟房屋。 ... 臺灣土地銀行標售行有嘉義市東區北門段二小段 44-1 及 44-2 地號土地。 ...

分類: 銀行

[www.landbank.com.tw](http://www.landbank.com.tw) - 52k - 2006/12/25 - 庫存頁面 - 更多此站結果 - 儲存 - 封鎖

# 真網頁的網址連接

Yahoo!奇摩 會員登入



網頁 知識+ 圖片 影片 部落格 商家 新聞 商品 更多

中華航空 搜尋

台灣網頁優先 全球網頁

網頁搜尋 中華航空 搜尋結果約6,470,000個，以下為1 - 10個，共花0.02秒

相關詞：[中華航空公司](#)、[中華航空班機時刻表](#)、[中華航空國際班機時刻表](#)、[中華航空訂位](#)、[中華航空精緻旅遊](#) 更多...

- [ZUJI足跡 - 提供特惠機票](#) 刊登贊助網站  
 新春航點降價優惠，各家航空公司促銷票、團體機票、來回機票，早去晚回超值滿點！ [www.zuji.com.tw](http://www.zuji.com.tw)
- [廣德旅行社 - 航空自由行](#)  
 日本個人旅行，多家航空公司加飯店或溫泉旅館自選任意組合搭配，讓您省時省力又安全。 [www.ctcn.com.tw](http://www.ctcn.com.tw)
- [可樂旅遊 - 國內外旅遊服務](#)  
 優質旅遊品牌，精選國內外旅遊、航空自由行、飯店住宿、機票等服務。 [www.colatour.com.tw](http://www.colatour.com.tw)

- 贊助網站
- [Ggogo台航吉帝航空自由行](#)  
 全日空自由行及華航假期等，各景點贈好康，酒店選擇搭配多，旅費成本自己決定！  
[www.ggogo.com](http://www.ggogo.com)
  - [101旅行社](#)  
 提供中華航空旅遊服務、世界各大城機票、訂房、自助旅行、航空套裝行程等。  
[www.101vision.com](http://www.101vision.com)
  - [巴里島五日加3千升來回商務艙](#)  
 雙向旅遊網，中華航空直飛巴里島，只要3千元，立即享受來回商務艙的尊榮禮遇。  
 202.168.193.28
  - [彩虹旅遊網 - 國際機票資訊](#)  
 桃園地區旅行社提供大陸機票、香港機票、長榮航空、中華航空、國泰航空等機票。  
[www.rainbow-traveling.com](http://www.rainbow-traveling.com)

- [中華航空公司](#)  
 中華航簡介、班機時刻、旅遊資訊、精緻旅遊、線上訂位購票、班機動態查詢。... 飛常好康團體行程 飛常好康團體行程 出發地點: 台北出發(直飛) 高雄出發(直飛) ... 德國 荷蘭 奧地利 超值的國際機票與航空公司自由行-中華航空讓您的旅途從登機開始就有好心情 ...  
[www.china-airlines.com](http://www.china-airlines.com) - 40k - 2007/08/27 - 庫存頁面 - 更多此站結果
- [中華航空公司](#)  
 提供公司簡介、機票預訂服務及價目、航班時間及航線資料。... 班機班號: CI 當地起飛日 啟程地點 到達地點 單程 來回 中停 直飛 啟程日 返程日 大人 小孩 艙等 啟程地點 到達地點 單程 來回 啟程日 返程日 常見問題 網站導覽 華信航空 ...  
[www.china-airlines.com/hk](http://www.china-airlines.com/hk) - 64k - 2007/08/21 - 庫存頁面 - 更多此站結果
- [中華航空氣象協會](#)  
 從事航空氣象之研究發展及國內外學術經驗交換,以利航空氣象事業之發展並進一步促進國民外交。... 歡迎光

# 假網頁的網址連接

china-airlines - Google 搜尋 - Mozilla Firefox

檔案 (F) 編輯 (E) 檢視 (V) 瀏覽 (G) 書籤 (B) Yahoo! 工具 (T)

http://www.google.com.t

Google china-airlines

搜尋 檢查 訂閱 選項 china-airlines

登入

Google

所有網頁 圖片 新聞 網上論壇 更多 »

china-airlines

搜尋

進階搜尋  
使用偏好

搜尋： 所有網站  所有中文網頁  繁體中文網頁  台灣的網頁

所有網頁

約有476項符合 china-airlines 的查詢結果，以下是第 1-10 項。共費 0.18 秒。

搜尋結果頁

www.china-airlines.com.tw ... 長榮航空- 旅遊... 機票訂購、國際旅行、旅遊諮詢、歡迎來找長榮航空！ www.evaavr.com ... 相約香港繽紛冬日節暢遊品美食... 試試你的好手氣，折扣券、旅遊行程線上即時抽！香港繽紛冬日節等你來玩！ ...

fe3.udn.com/search/udnsearch.jsp?Keywords=%AE%C8%B9C - 55k - 頁庫存檔 - 類似網頁

Yahoo! 奇摩 > 休閒天地 > 旅遊

NRT-東京, YVR-溫哥華, VIE-維也納, SHA-上海, 提供網上定位。

www.china-airlines.com.tw. 韓國 樂娛樂場 旅遊韓國, 一定要造訪7Luck豪華娛樂場, 享受七采帶給你的樂趣! www.7luck.com. 繁體中文: . seewa喜娃原住民旅遊網站: [\*] ...

tw.dir.yahoo.com/recreation/Travel/ - 22k - 頁庫存檔 - 類似網頁

Yahoo! 奇摩 > 休閒天地 > 旅遊

NRT-東京, YVR-溫哥華, VIE-維也納, SHA-上海, 提供網上定位。

www.china-airlines.com.tw. 相約香港繽紛冬日節暢遊品美食 試試你的好手氣, 折扣券、旅遊行程線上即時抽! 香港繽紛冬日節等你來玩! hkwf.chinatimes.com. o. b. 讓你那個來也不會輸 ...

tw.dir.yahoo.com/Recreation/Travel/ - 22k - 頁庫存檔 - 類似網頁

Yahoo! 奇摩 > 商業金融 > 公司行號 > 旅遊

NRT-東京, YVR-溫哥華, VIE-維也納, SHA-上海, 提供網上定位。

www.china-airlines.com.tw. 刷MasterCard免費出國 週週抽, 免費新加坡時尚節雙人行及五萬刷卡金。 www.mastercard.com. 昭盛52行館 台中全新125間客房商務旅館, 位中港SOGO精明

尋找: li 往後尋找 (N) 往前尋找 (P) 高亮度變色標記 (A) 符合大小寫 (C) 找不到指定文字

http://tw.dir.yahoo.com/recreation/Travel/

# 假網頁的網址連接

搜尋結果頁 - Mozilla Firefox

檔案 (F) 編輯 (E) 檢視 (V) 瀏覽 (G) 書籤 (B) Yahoo! 工具 (T)

http://72.14.235.104/search

Google china-airlines

聯合新聞網 udn.com

網站總覽 | 會員 | 繁 ↔ 簡 | RSS

旅遊 udn web GO YAHOO! 搜尋

UDN / 搜尋結果

### 旅遊 的相關網頁

- 搜尋贊助網站 讓您的網站高人一等，增加曝光率，說明！
- 中華航空公司...  
NRT-東京, YVR-溫哥華, VIE 維也納, SHA-上海, 提供網上定位。  
[www.china-airlines.com.tw](http://www.china-airlines.com.tw)
- 長榮航空 - 旅遊...  
機票訂購、國際旅行、旅遊諮詢、歡迎來找長榮航空！  
[www.evaavr.com](http://www.evaavr.com)
- 相約香港繽紛冬日節暢遊品美食...  
試試你的好手氣，折扣券、旅遊行程線上即時抽！香港繽紛冬日節等你來玩！  
[hkwf.chinatimes.com](http://hkwf.chinatimes.com)

搜尋結果 共找到約 364 個 查詢時間 0.577 秒。 [查詢小技巧]

- 進階查尋請至 [UDN大搜查](#) - 更多新聞搜尋請至 [聯合知識庫](#)

- 新聞：穆罕默德親王 打造杜拜奇蹟...  
杜拜領袖穆罕默德親王 (SHEIK MO-HAMMED BIN RASHID AL-MAKTOUM) 2003年宣布「杜拜公...

搜尋贊助網站

- O.B. 讓妳那個來也不會輸  
免費索取OB棉條、搶登PARTY QUEEN頭銜，藏愛婚紗彩妝造型送給妳。  
[www.obcity.com.tw](http://www.obcity.com.tw)
- 驛站精緻中國旅遊  
大陸旅遊領導品牌，提供詳實完整的中國旅遊資訊，以及豐富精采的實地照片與介紹。  
[www.travelstation.com.tw](http://www.travelstation.com.tw)
- 廣德旅行社 - 日本旅遊達人  
線上即時Q&A，自由行、團體行、機票、溫泉飯店、交通周遊？，帶您玩遍日本。  
[www.ctcn.com.tw](http://www.ctcn.com.tw)

旅遊 相關資訊

- 旅遊頻道  
提供聯合報系旅遊新聞，每日更新國民旅遊、海外旅遊、自然關懷、旅人手札、戶外休閒、旅遊資訊等相關報導。
- 旅遊夢享家  
旅遊夢享家提供嚴謹的旅遊情報，供傑出

尋找: li 往後尋找 (N) 往前尋找 (P) 高亮度變色標記 (A) 符合大小寫 (C) 找不到指定文字

完成

# 假網頁的網址連接

Yahoo! 奇摩 > 休閒天地 > 旅遊 - Mozilla Firefox

檔案 (F) 編輯 (E) 檢視 (V) 瀏覽 (G) 書籤 (B) Yahoo! 工具 (T)

http://72.14.235.104/sea

Google china-airlines

搜尋 檢查 訂閱 選項 china-airlines

YAHOO! 分類

搜尋排行榜 | 服務說明 | Yahoo! 奇摩

分類首頁 > 休閒天地 > 旅遊

[網站登錄]

搜尋 說明

台灣網頁  全球網頁  此分類下

- 公司行號@
- 主題樂園@
- 各縣市旅遊(33)
- 住宿@
- 風景遊樂區@
- 旅遊安全(1)
- 旅遊資源(174)
- 旅遊雜誌@
- 海外旅遊(23)
- 國家公園(21)
- 組織團體(24)
- 遊記(272)
- 護照與簽證@

- 刷MasterCard免費出國  
週週抽，免費新加坡時尚節雙人行及50,000刷卡金。 [www.mastercard.com](http://www.mastercard.com)
- 中華航空公司  
NRT-東京，YVR-溫哥華，VIE-維也納，SHA-上海，提供網上定位。 [www.china-airlines.com.tw](http://www.china-airlines.com.tw)
- 韓國7樂娛樂場  
旅遊韓國，一定要試試7樂豪華賭場，享受上級帶給你的樂趣！ [www.7luck.com](http://www.7luck.com)

刊登贊助網站

尋找: li 往後尋找 (N) 往前尋找 (P) 高亮度變色標記 (A) 符合大小寫 (C) 找不到指定文字

完成

# 假網頁的網址連接

國際機票 休閒旅遊票券 旅遊住宿 比價購物最便宜,種類多元,優質商

檔案(F) 編輯(E) 檢視(V) 瀏覽(G) 書籤(B) Yahoo! 工具(T)

http://72.14.235.104/sea

Google china-airlines

YAHOO! 購物通 會員登入 新使用者? 立即註冊

服務首頁 | 服務說明 | Yahoo! 奇摩

手機 相機 筆電 年終慶 資訊月 保養 名牌包 女鞋 彩妝 飾品 手錶 牛爾 Kevin 聖誕假期 特賣會

電腦資訊 數位影像 旅遊住宿 視聽娛樂 時尚精品 男女服飾 圖書雜誌 居家生活 折價券 新貨到 全部分類

全部分類 搜尋 進階搜尋 我的購物

熱門搜尋: 澳洲紐西蘭 青藏鐵路之旅 泡湯賞楓 住宿券 迪士尼 宜蘭賞鯨 離島風光 悠閒峇里 清境雙人 法國普羅旺斯

八大館聯合跨年慶★免消費送FANCL!

購物通首頁 > 旅遊住宿 > 休閒旅遊票券 > 國際機票

精準搜尋 搜尋結果: 共有9項商品, 顯示1-9項

檢視方式: 清單瀏覽 | 圖片瀏覽

排序方式: 依相關度 | 依價格

比較商品 加入追蹤清單

相關分類

- 行李箱拉桿包
- 旅遊觀光書籍
- 數位相機
- 旅行背包背袋
- 其他戶外休閒用品

縮小金額從

元至 元

搜尋商品 重設

上海計劃旅遊票5日(兩人成行、保證出團)NX

搭乘航班: NX+NX兩地機場稅+兵險安檢燃油費外加4000元

NT 8,999 起

商店名稱: 發現之旅 商店評比: ★★★★★

ezfly 易飛網香港機票優惠

●ezfly易飛網特別推薦●◎聖誕、元旦、春節熱門推薦◎港龍香港優惠票 讓您輕鬆飛往香港 免擔心價錢

贊助網站

中華航空公司  
NRT-東京, YVR-溫哥華, VIE-維也納, SHA-上海, 提供網上定位。  
www.china-airlines.com.tw

升達旅遊美加專業機票行程規劃  
專營洛杉磯、舊金山、紐約、溫哥華國際機票及美國加拿大各城市之國內機票及飯店。  
www.gogousa.com.tw

ZUJI足跡 - 提供特惠機票  
國際機票促銷熱賣中, 各大

尋找: li 往後尋找(N) 往前尋找(P) 高亮度變色標記(A) 符合大小寫(C) 找不到指定文字

完成

# 案例5：女行員盜銀行鉅款2千萬，同事還代開車門

- 復華銀行高雄市三民分行一名女會計行員，疑因負債四、五百萬元，利用職務之便竄改電腦紀錄，共詐領二千零九十二萬五千元銀行帳款，得手後於昨早搭澳門航空班機赴澳離台。銀行稍早發現該行員未到班、清查發現遭詐領後報案。警方調查發現因該分行便宜行事、未落實內部安全管控，才會讓行員輕鬆詐領二千多萬元逃逸。陳女依涉嫌詐欺、背信、《洗錢防制法》等罪嫌起訴

## 詐領手法與銀行疏失

陳女詐領手法	復華銀行疏失
● 虛設1640萬1800元的銀行調度資金，轉入蕭姓同學帳戶。	● 分行未落實查驗。
● 持蕭姓同學存摺與印章領1630萬元。	● 警方待查。
● 虛設一名蘇姓女子帳戶，存44萬3200元。	● 警戒心差。
● 匯款310萬元到自己的戶頭。	
● 拿走銀行代收的稅款98萬元。	

資料來源：高雄市警方

## 資安觀點：

1. 虛設幽靈數位帳號很容易。
2. 轉帳授權密碼隨意借。
3. 員工對系統與流程安全無意識。
4. 危機處理未及時。
5. 深知系統漏洞的最大駭客，常是內部不肖人員。

# 案例6：臍帶血業者競爭報告書 變對手文宣

- 民眾儲存臍帶血，資料卻遭外洩，淪為業者競爭下的犧牲者！有消費者到訊聯生物科技儲存臍帶血，但相關報告書卻被訊聯對手生寶生物科技刊登在廣告文宣上，還被批評這份報告書不夠專業，兩家業者卻不願道歉，讓消費者氣炸。訊聯說，資料不可能外漏，生寶則不願回應。律師表示，兩家業者的做法已侵害個人隱私，消費者可向業者提告求償。

## 民眾保護個人資料應注意事項：

1. 簽約內容應有保密條款，明定保密內容，如：個人資料等。
2. 民眾可自行訂定違約條款。
3. 發生個人資料遭盜用時，須保留證據，如：廣告單及契約正本等。

## 資安觀點：

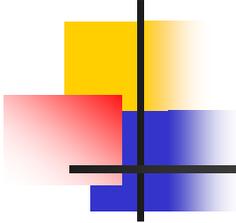
1. 客戶資訊保護不周毀了商譽(訊聯)。

# 案例7：台彩大烏龍當機兼派錯獎金

- 由中國信託商業銀行接手的公益彩券昨天開賣，但狀況百出，各地投注站電腦大當機、久久無法連線，有民眾排了三小時還買不到彩券，有經銷商因此整個上午一張都沒賣出去，民眾與經銷商昨罵聲不斷。負責中信銀彩券業務的台灣彩券表示，無法連線與當機問題應是網路塞車造成。
- 台灣彩券公司再度擺烏龍，昨晚開獎的樂透彩，本期各獎項獎金總額原本為五千三百十萬餘元，卻誤植為七千五百卅七萬餘元，台彩公司在深夜十一時四十分緊急通知更正。

## 資安觀點：

1. 資安的範圍，除了資訊的機密性外，亦涵蓋了可用性與完整性。即使重要資料沒有洩漏，但**系統無法提供服務**，或**未達預期服務水準**，以及**資料錯誤或誤用**，都必須視為**資訊使用的風險**，亦需提出矯正預防措施來改善。
2. 除了健全的資訊系統外，**系統的維護人員及使用人員的訓練**，也是降低資訊風險不可或缺的一環。



## 案例8：盜用他人帳號遭函送

- 某科技大學助理教授，遭檢舉涉嫌盜用校內教授帳號及密碼，在網路上行使國科會產學計劃共同主持人的同意權，企圖讓自己成為計劃共同主持人，經學校舉報檢調依違反「電腦處理個人資料保護法」函送法辦。

**妨害電腦使用罪 刑法第358條：**

「無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。」

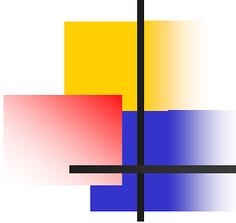
**資安觀點：**

1. 密碼除了保障資訊的“機密性”與“完整性”外，對於資訊作業的“可歸責性”維持亦是相當的重要。
2. 使用他人的帳號密碼非但違反個資法，若情節重大，還有可能



休息一下

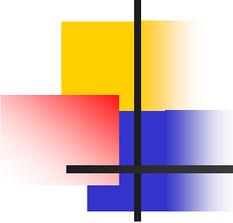
---



# 資通安全相關法令

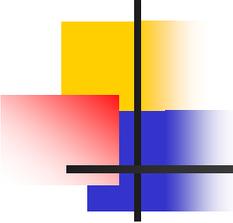
---

- 國家機密保護法
- 電子簽章法
- 刑法(防駭條款)
- 電腦處理個人資料保護法
- 檔案法
- 著作權法
- 行政院及所屬各機關資訊安全管理要點
- 機關公文電子交換作業辦法
- 智慧財產權Intellectual Property Rights (IPR)



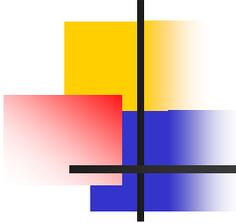
# 妨害電腦使用罪簡介

- 隨著資訊科技快速發展，網際網路應用日益普及與多元，除了帶給我們許多生活上的便利，但也衍生一些資通安全問題，特別是網路犯罪行為已有增多趨勢。
- 網路犯罪行為大約可歸類下列三種
  - 1、以網路作為犯罪工具—網路詐欺、網路恐嚇等
  - 2、以網路作為攻擊標的—竄改檔案、阻斷式服務攻擊、駭客入侵、電腦病毒等。
  - 3、以網路作為犯罪場所—如色情、誹謗、賭博等
- 為避免電腦犯罪與維護網路秩序，特於刑法中設立相關法令條文以為管理-刑法第**36**章「妨害電腦使用罪」章。



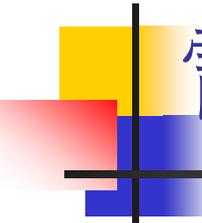
# 妨害電腦使用罪主要內容---1

- **第358條無故入侵電腦罪**
  - 無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。— 本條主要目的為遏止駭客入侵行爲。
- **• 第359條無故取得、刪除或變更他人電磁紀錄罪**
  - 無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。— 本條主要目的為確保電腦內部電磁紀錄安全。
- **第360條無故干擾電腦系統罪**
  - 無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。— 本條主要目的為維護電腦及網路運作正常。



## 妨害電腦使用罪主要內容---2

- **第361條對公務機關犯罪之加重**
  - 對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一。- 本條主要目的為確保國家安全。
- **第362條製作供犯罪程式罪**
  - 製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。- 本條主要目的為防止犯罪工具之利用與擴散。
- **第363條告訴乃論**
  - 第三百五十八條至第三百六十條之罪，須告訴乃論。- 本條主要目的為集中司法資源對抗重大犯罪。



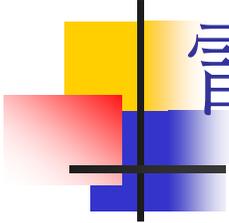
# 電腦處理個人資料保護法說明-1

- **立法目的**

- 對公務與非公務機關蒐集、處理、與利用個人資料的情形，加以明文規範。
- 避免個人**人格權**（**隱私權**）遭受侵害，促進個人資料之合理利用，特此制定電腦處理個人資料保護法。

- **保護客體**

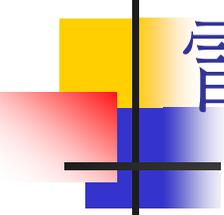
- 本法保護客體限於**經電腦處理的個人資料**。
- 受本法保護之個人資料以**現仍生存之自然人為限**，已死亡之自然人與法人，不受本法之規範。
- 個人資料包含：自然人之姓名、出生年月日、身分證統一編號、特徵、指紋、婚姻、家庭、教育、職業、健康、病歷、財務情況、社交活動、及其他**足以識別該個人之資料**。



# 電腦處理個人資料保護法說明-2

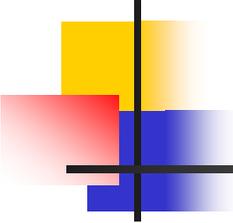
## • 適用主體

- 本法規範的對象有公務機關及非公務機關。
- 公務機關係指依法行使公權力之中央或地方機關。
- 非公務機關係指以下所列之事業、團體或個人。
  - 徵信業、以蒐集或電腦處理個人資料為主要業務之團體或個人
  - 醫院、學校、電信業、金融業、證券業、保險業、大眾傳播業
  - 其他經法務部會同中央目的事業主管機關指定之事業、團體或個人
- 受公務機關或非公務機關委託處理資料之團體或個人，於本法適用範圍內，其處理資料之人，視同委託機關之人。



# 電腦處理個人資料保護法說明-3

- **機關對個人資料之蒐集或利用的原則**
  - 應尊重當事人之權益，依誠實及信用方法為之。
  - **不得逾越特定目的之必要範圍**，以確保當事人權益，避免人格權受到侵害。
- **揭露個人資料，當事人是主要關鍵人物，當事人本身需審慎決定何者為提供給公務與非公務機關的必要個人資料。**



# 電腦處理個人資料保護法修訂 草案

- 修法背景
  - 法務部為因應急速變遷之社會環境，特別彙整國內學界與實務界的相關修法建議，並參考其他國家之個人資料保護相關法令來針對本法進行修訂。
- 修訂草案共有**55**條，並將本法名稱修訂為「個人資料保護法」。
- 草案修正方向
  - 擴大保護客體
  - 普遍適用主體
  - 增修行為規範
  - 強化行政監督
  - 妥適調整罰則
  - 促進民眾參與

# 電腦處理個人資料保護法修訂 草案

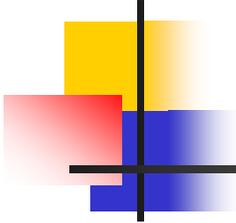
- 修法重點說明

將買賣個人資料行為從告訴乃論罪修改為公訴罪，並提高刑責，最高為五年有期徒刑。

1、寄廣告信、垃圾郵件將觸法，未經個人同意，網路公司或個體戶大舉販賣蒐集的大筆電子郵件信箱供寄發垃圾郵件等行為，均將觸犯本法，檢警接獲檢舉後必須主動追查。

2、若是公務員涉案，依法得加重其刑二分之一，最重可處七年半徒刑，與刑責已接近涉及貪瀆案。

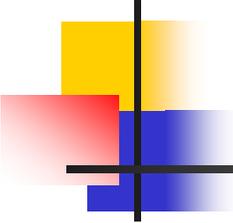
- 重罰意圖營利而違法的行為，修訂草案大幅加重「意圖營利而違法蒐集、利用或盜賣個人資料者」的刑責，由原本二年以下徒刑，提高為五年以下徒刑，且併科由原先四萬元大幅提高為五百萬元罰金。



# 個人資安守則--- 使用者責任

---

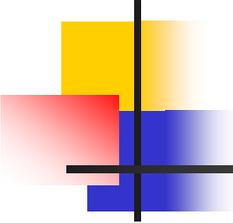
- 使用者的態度，對於有效防止非法的使用者存取，以保障安全的工作非常重要。
- 目標：防止未經授權的使用者存取資訊與資訊處理設施，以及使其避免遭受破壞或竊盜。
  - 1、通行碼的使用。
  - 2、無人看管的使用者設備。
  - 3、桌面淨空與螢幕淨空政策。



# 通行碼的使用—密碼管理

---

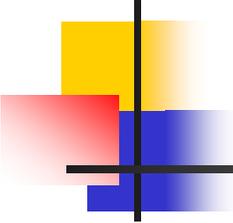
- 定期更新密碼
- 定期檢查密碼
- 設定優質密碼
  - 1、避免使用重複數字、單位簡稱、詞語、生日
  - 2、數字字母符號穿插且不過於複雜。
  - 3、避免重複使用密碼。
- 不告訴他人密碼或寫下密碼
- 懷疑密碼外洩立即更新



# 無人看管的使用者設備

---

- 使用者應確保無人看守的設備獲得適當保護
  - 安裝在公共區域的設備（如公用主機、印表機
  - 或伺服器），應有具體的保護
- 1、在活動完成時應終止對話，結束畫面。
  - 2、螢幕保護程式需設定密碼保護。
  - 3、活動結束時登出系統或主機，再關閉電腦。
  - 4、PC或設備不用時，應使用密鑰鎖或其他安全控制措施，以防止他人非法使用。



# 桌面淨空與螢幕淨空政策

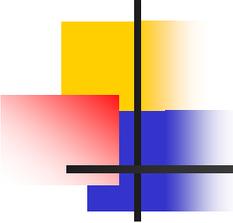
---

- 桌面淨空

- 1、重要、機密文件不置於桌上。
- 2、重要、機密文件下班或離開辦公室前應鎖入安全空間。

- 螢幕淨空

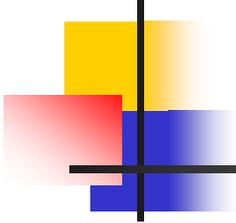
- 1、設定螢幕保護程式。
- 2、設定保護密碼。
- 3、離開座位或暫時不使用時鎖定螢幕。



# 個人資安守則--- 處理公務時的安全防護

---

- 勿從網路下載與公務無關之不明程式。
- 不得將與公務有關之內容上傳至網際網路個人儲存空間。



# 個人資安守則--- 網路使用安全

---

- 確保網頁瀏覽器使用安全
  - 1、設定網頁瀏覽器安全性、隱私權。
  - 2、設定信任的網站。
- 遠離網路釣魚犯罪陷阱與騙局
  - 1、不回應不明公司、技術部門要求提供個人隱私或安全資訊。
  - 2、不點選來路不明郵件的網頁連結。
  - 3、不利用企業網路轉寄垃圾郵件。

# 惡意程式網站

每十個網站就有一個是惡意網站

APWG: 全球藏有惡意程式網站的前三名國家

2006年11月：美國、中國大陸、韓國，委內瑞拉首次入榜

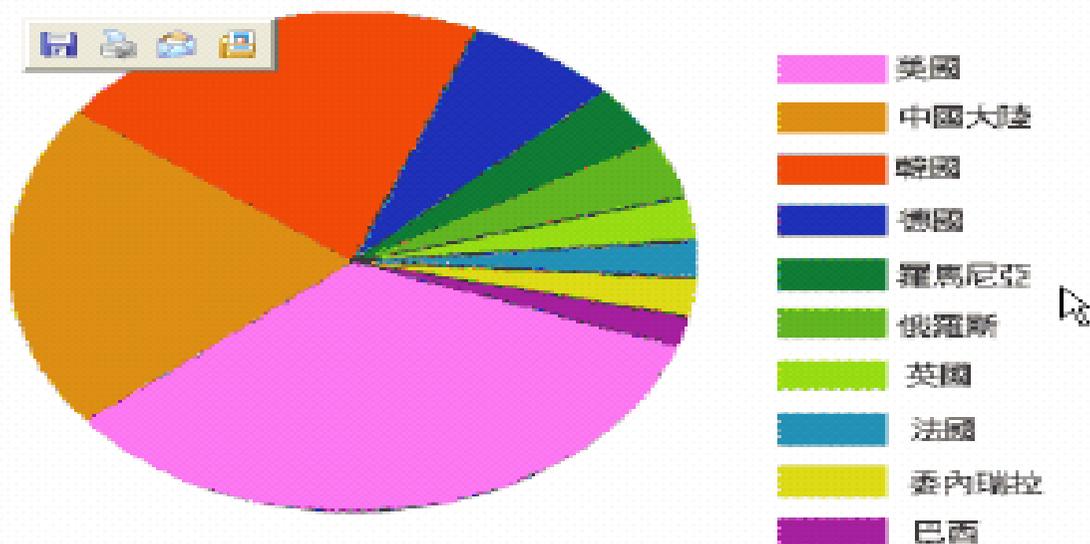
資料來源：反網路釣魚工作小組(APWG)

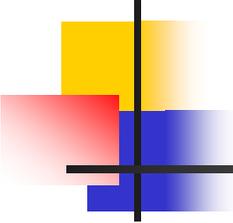
公布日期：2007年1月

反網路釣魚工作小組 (Anti-Phishing Working Group) 2006年11月全球網路釣魚調查報告：

全球藏有惡意程式的網站前十名分別在美國(24.2%),中國大陸(15.42%),韓國(14.88%),德國(5.27%),羅馬尼亞(2.84%),俄羅斯(2.64%),英國(2.04%),法國(1.83%),委內瑞拉(1.81%),巴西(1.43%)。

全球10大藏有惡意程式網站所在地

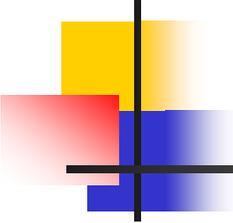




# 網路釣魚攻擊

---

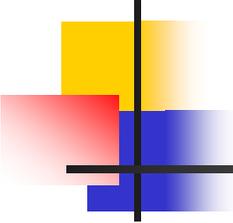
- 全球120個企業品牌被駭客用來透過電子郵件進行網路釣魚詐騙活動。
- 英國2006年約350萬人遭網路詐騙。



# 電子郵件風險

---

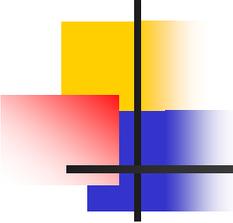
- 國內30.7%網路人口一天收到10封垃圾郵件。
- 垃圾郵件讓美國企業一年損失達700億美金。
- 個人的電子郵件信箱中近8成含有惡意程式或垃圾郵件。



# 個人資安守則--- 即時通訊軟體

---

- 存在的風險
  - 1、病毒威脅。
  - 2、垃圾訊息。
  - 3、檔案交換。
  - 4、洩密。
  - 5、工作效率的影響。
- 常犯之錯誤
  - 1、盲目的檔案分享。
  - 2、花費過多時間於私人聊天。
  - 3、將個人帳號資訊以儲存密碼方式設定儲存。
  - 4、任意將個人之連絡者清單給他人。

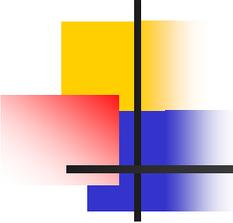


# 個人資安守則---

## 即時通訊軟體使用安全

---

- 登入密碼最好不要用「儲存密碼」記錄於系統內。
- 不任意傳遞與分享公司重要資訊或檔案。
- 不任意接收來路不明之分享檔案。
- 使用者必須秉持以公事使用之目的使用企業即時訊息。
- 隨時更新使用端程式。

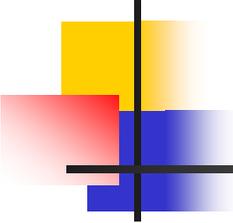


# 個人資安守則--- 電腦病毒

---

## ■ 電腦中毒徵兆

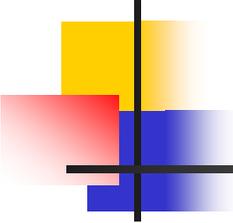
- 1、電腦系統運行速度異常緩慢。
- 2、上網速度越來越遲緩。
- 3、異常的系統訊息通知。
- 4、螢幕顯示異常，例如畫面突然一片空白。
- 5、來自防毒軟體的警告訊息。
- 6、電腦無故自動關機或不斷重新開機。
- 7、瀏覽器自動出現產品廣告或色情網頁。
- 8、網路流量異常，例如沒有使用網路服務或收發電子郵件，但網路的連線燈號卻一直閃爍。



# 電腦病毒的防範

---

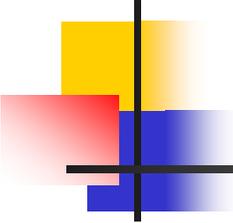
- 確認防毒軟體隨時運作。
- 勿隨意安裝未經許可的電腦軟體。
- 確保軟體在最新更新狀態。
- 使用有問題立即反應。



# 個人資安守則--- 廣告、間諜軟體

---

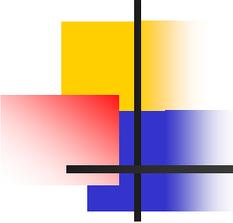
- 廣告或間諜軟體的症狀
  - 1、沒有上網卻還是一直看見廣告視窗。
  - 2、網路速度時快時慢。
  - 3、首頁被更改成奇怪的網站。
  - 4、視窗下方的工具列出現許多原本沒有的工具
  - 5、瀏覽器多出沒有安裝過的工具列、搜尋工具，而且無法移除。
  - 6、電腦處理速度變慢或當機頻率增加。



# 個人資安守則--- 廣告或間諜軟體的防範

---

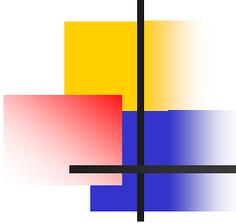
- 使用防火牆阻擋。
- 關閉網路瀏覽器的ActiveX 功能。
- 安裝封鎖彈跳視窗功能的工具。
- 下載免費軟體前仔細閱讀所有相關訊。
- 學習資料備份基本技巧。



# 個人資安守則--- 駭客入侵

---

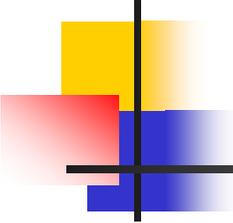
- 駭客入侵的徵兆
  - 1、檔案及資料庫內容遭到竊取或篡改。
  - 2、不知名的IP來源與電腦連線。
  - 3、系統中異常的服務程式。
  - 4、異常通訊埠開啓。
  - 5、稽核紀錄及檔案中的異常事件。
  - 6、系統帳號的異常增加。
  - 7、系統異常的訊息或行爲。



# 個人資安守則--- 駭客入侵的簡易處理

---

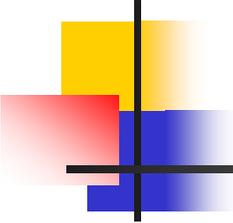
- 定期系統備份。
- 針對可能入侵途徑系統作隔離。
- 蒐集入侵紀錄、檔案等軌跡。
- 追查駭客IP來源。
- 分析資料找出入侵方式並改善。
- 報告相關單位。
- 適時尋求協助。



# 個人資安守則--- 駭客入侵的防範

---

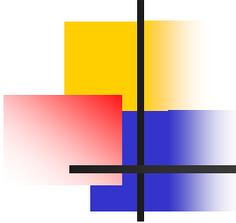
- 即時更新修正檔。
- 檢視權限設定。
- 日常備份作業。
- 紀錄及檢視稽核軌跡。
- 設定自動時間校正作業。



# 個人資安守則--- 資料備份

---

- 不論是紙本或電子檔的重要資料，皆應：
  - 1、定期備份。
  - 2、存放在不同地方(異地備份)。
- 資料備份原則
  - 1、資料價值較高時應優先備份。
  - 2、擇適合之儲存媒介進行資料備份工作。
  - 3、按所欲備份的資料型態，選擇方法進行備份(如：完全備份、選擇性備份、漸進式(增量)備份)。
  - 4、備份的資料需定期做資料回復測試，以確認備份資料的可用性。



# 個人資安守則--- 用戶端網路安全的三不政策

- **不自行下載軟體程式(政府網站除外)**  
如果要下載程式，請至官方網站。  
不要相信入口網站的下載資料。  
不要聽從網頁下載元件的指令。
- **不執行外部來源程式(網管人員寄送除外)**  
不要執行(開啓)電子郵件的附件檔案(exe,pif)。  
不要互相傳送電子郵件的可愛檔案(doc,xls,pps)。  
不要自行安裝自己私帶的程式。
- **不攜帶私人電腦設備**  
不要允許廠商私帶電腦連接網路  
不要允許下屬(同僚)私帶筆記本電腦與掌上電腦Palm。

