

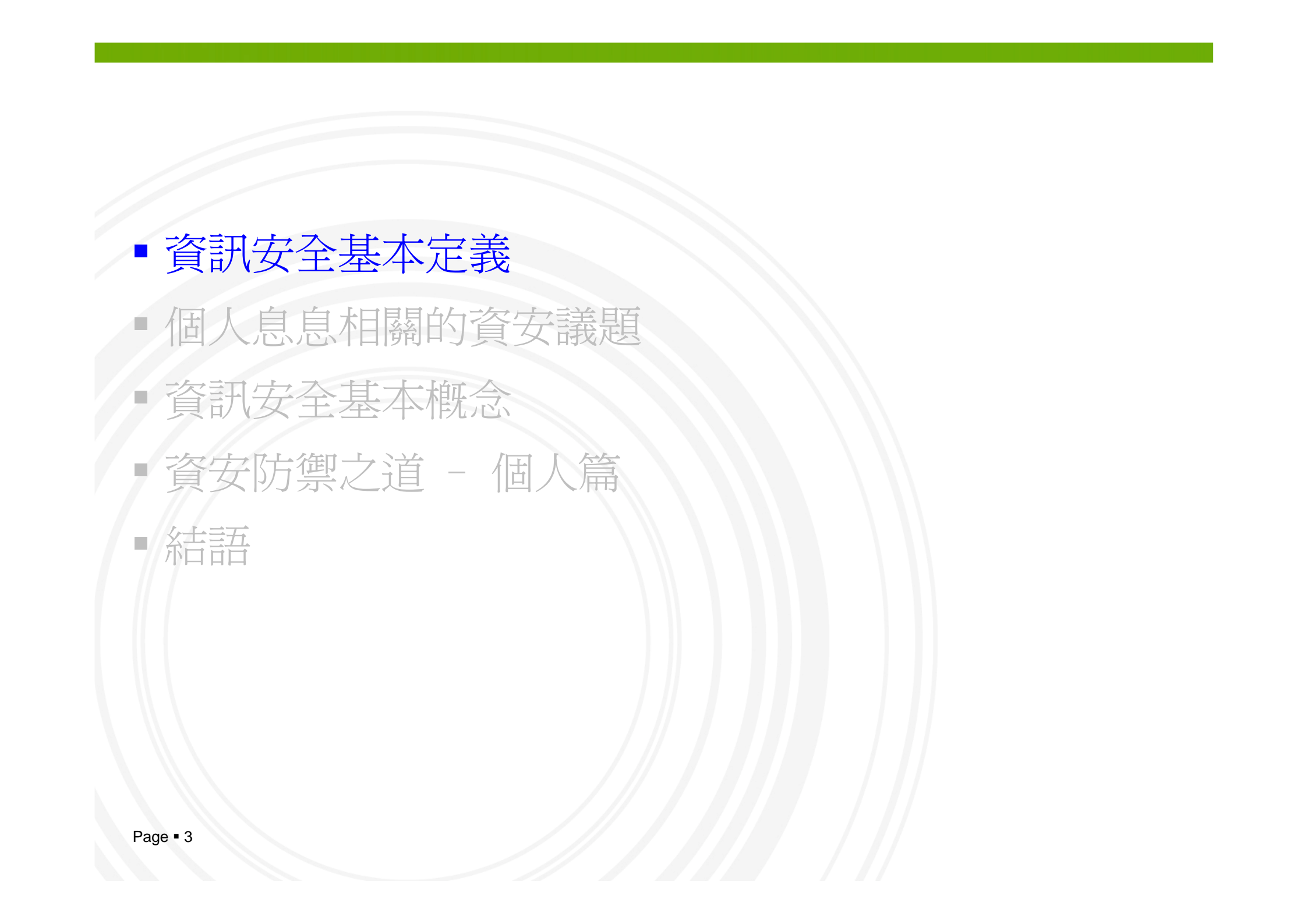
# 資訊安全與維護

講師：NII產業發展協進會 邱瑩青

日期：2010/2/23

# 大綱

- 資訊安全基本定義
- 個人息息相關的資安議題
- 資訊安全基本概念
- 資安防禦之道 - 個人篇
- 結語

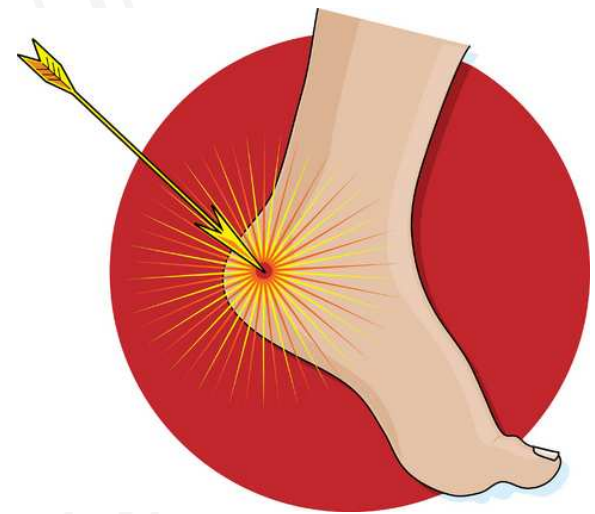
- 
- 資訊安全基本定義
  - 個人息息相關的資安議題
  - 資訊安全基本概念
  - 資安防禦之道 - 個人篇
  - 結語



(圖片來源)

- 2004年5月，電影「特洛依：木馬屠城」
- 電影主角阿基里斯在希臘神話中是刀槍不入的勇猛戰士，堪稱無敵！

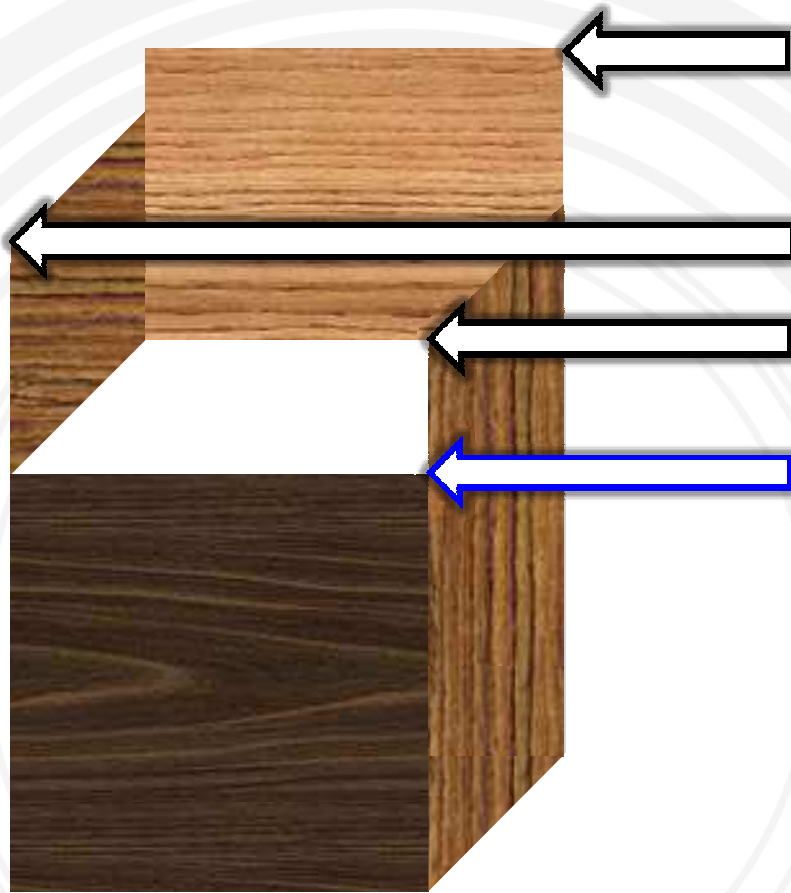
- 阿基里斯刀槍不入的全身，源於嬰兒時由母親倒抓其右腳踝浸泡冥河，所以只有沒浸泡到的右腳踝是其唯一弱點
- 所以縱使阿基里斯神勇無敵，在敵人一箭射中其右腳踝後，無敵神話仍舊破碎！



(圖片來源)

在資訊安全裡，我們說：  
**Security is a chain.**  
**It's only as secure as the weakest link.**

# 資訊安全的「木桶理論」



- 四塊長短不一的木板組成木桶，所能承盛的水量高度取決於最短的那塊木板
- 一個團體的整體素質水準不取決於最好的一位，而是取決於最差的那一名



- 組織建構了護城河 → 內部網路保護  
建起了高昂的城牆 → 各項安全防護  
建造了堅固的城門 → 防火牆
- 而您，士兵準備好了嗎…  
您的輕忽，可能開啓防護漏洞…

(圖片來源)



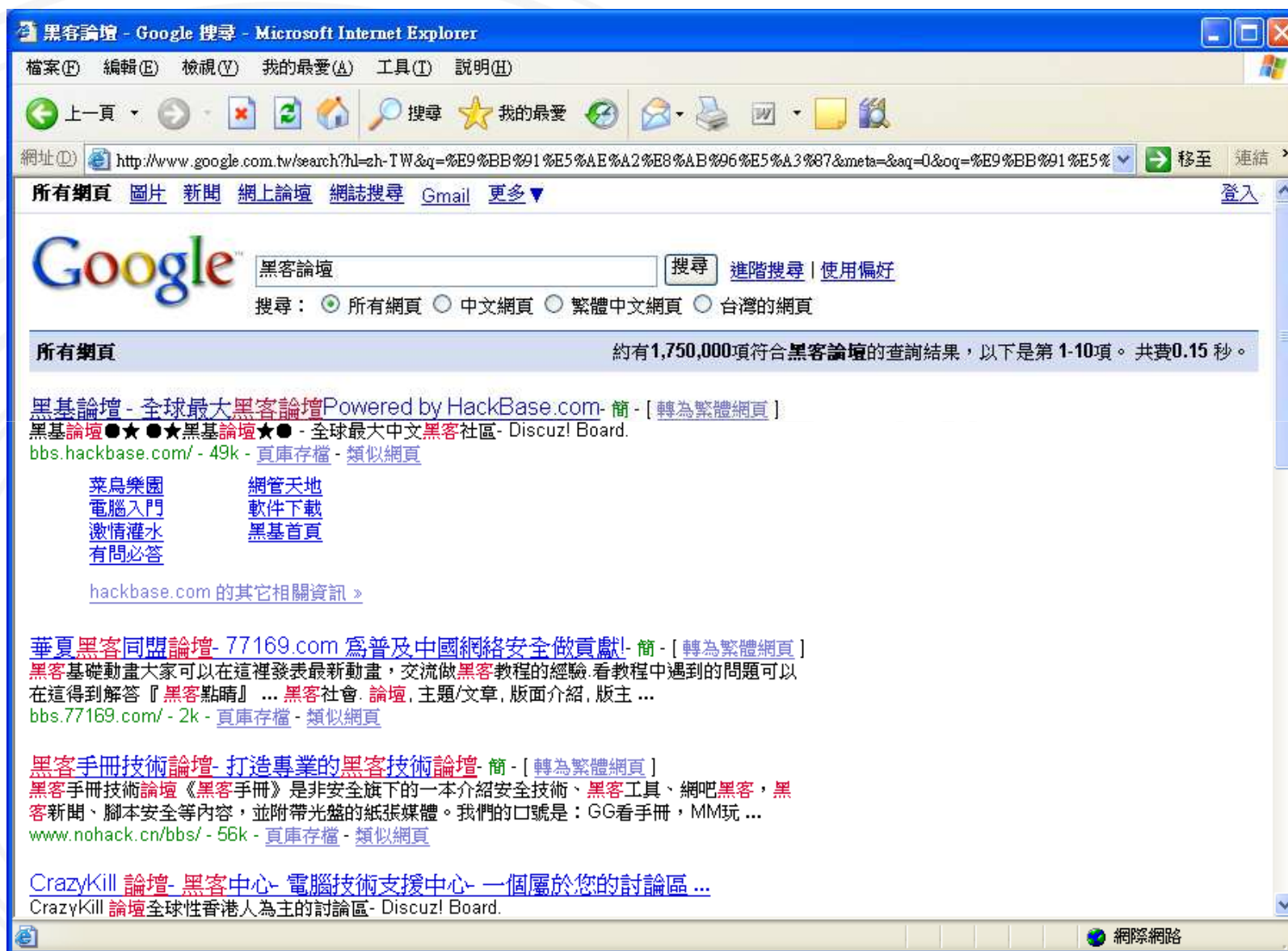


專業駭客  
特定目標



玩家  
亂槍打鳥

# 透過網路駭客論壇就可以找到駭客工具和教學



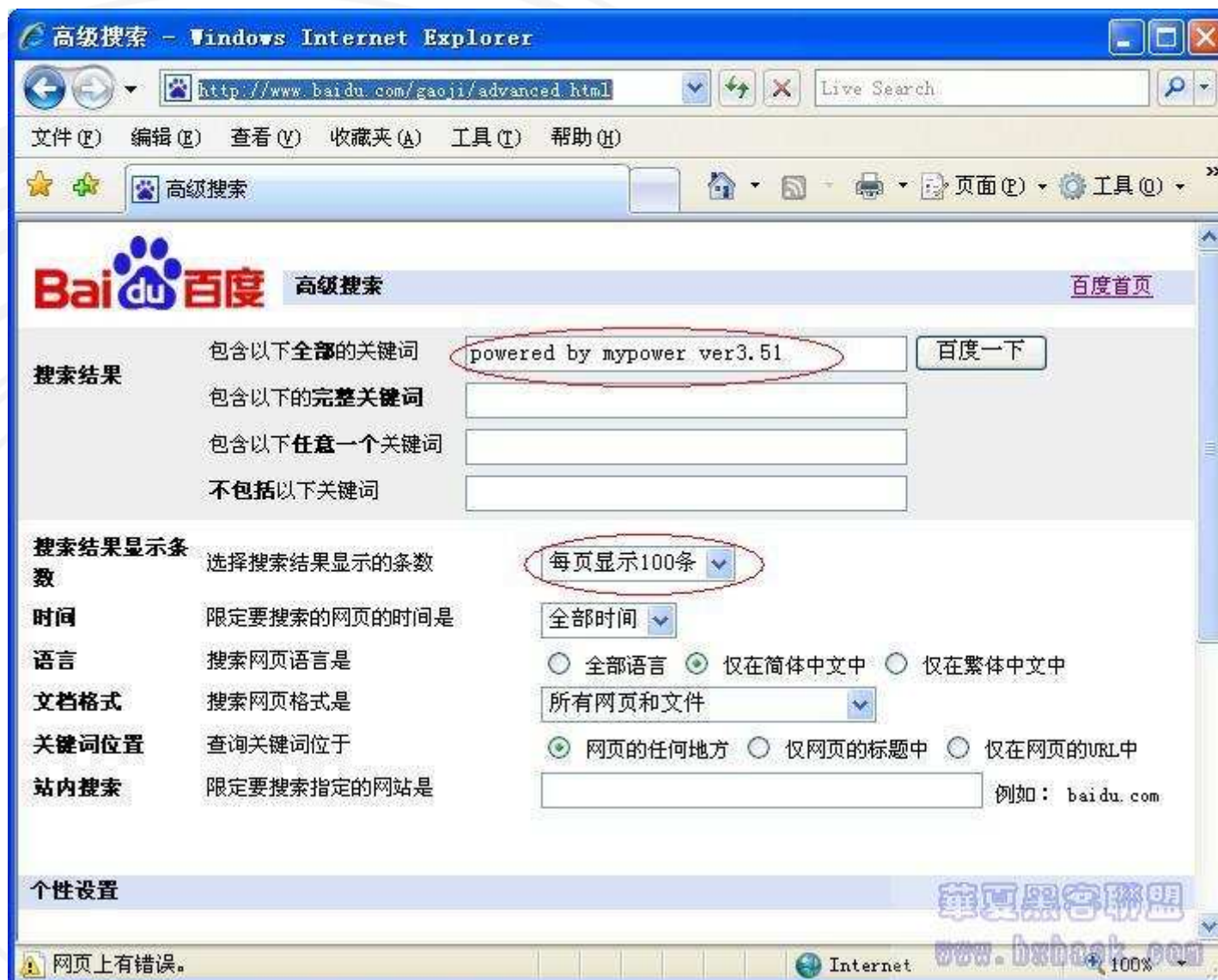
# 各種詳細的駭客入門教學

The screenshot shows a forum page with the following threads and annotations:

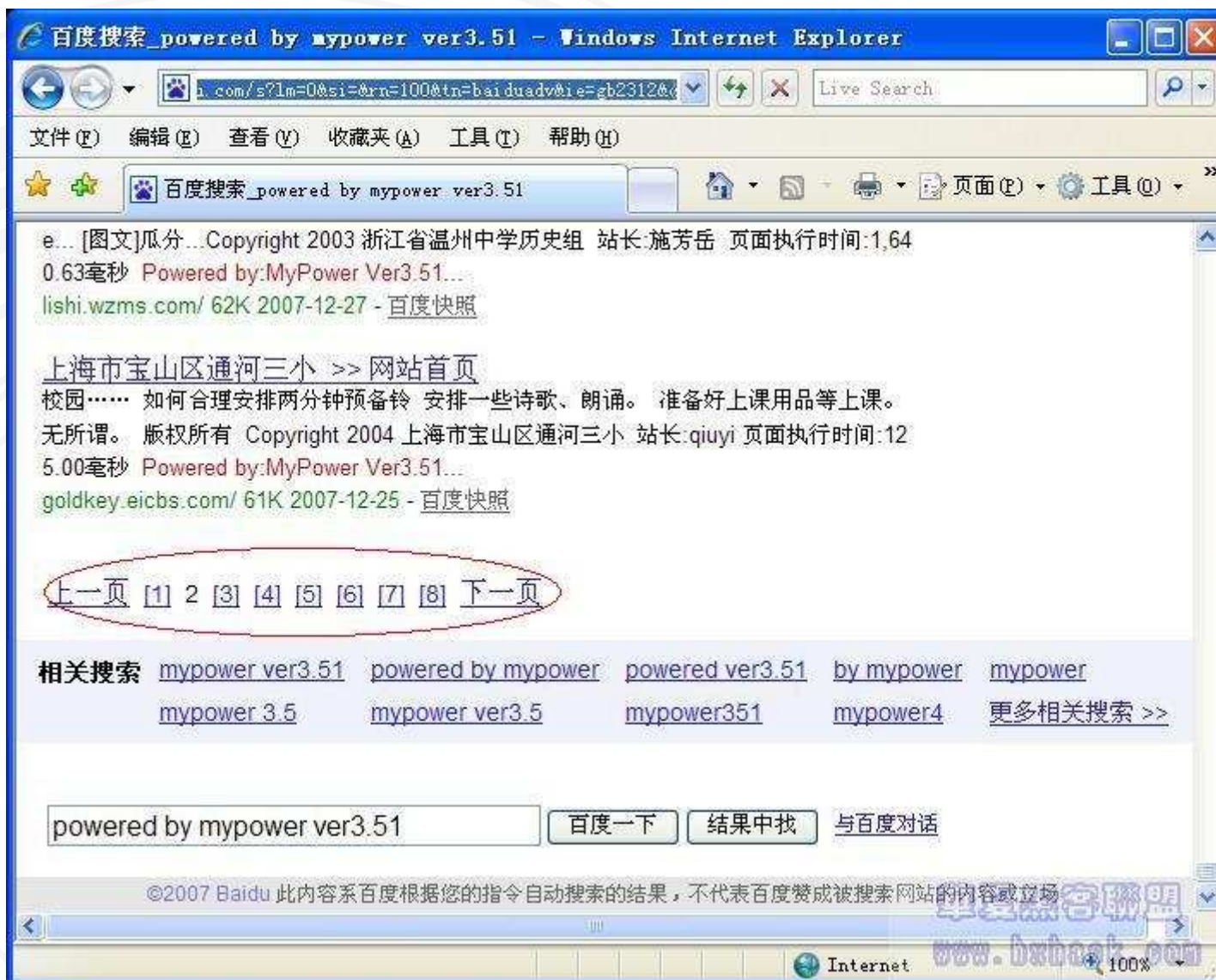
Thread Title	Author	Replies / Views	Date	Annotation
[求助] ASP網站出現這個代碼，可以入侵嗎???	風依然二	23 / 747	2008-3-17 05:08	➤ ASP網站出現這個代碼，可以入侵嗎？
[原創] 什麼都不會的菜鳥入門篇	2008-3-7			
[求助] 請問ASP的網站隱藏了真實下載路徑怎麼找的到??	ririio	2 / 65	2008-3-16 21:00	
[求助] 有些網站限制登陸要密碼怎麼辦啊??	ririio	0 / 43	2008-3-16 18:53	
網速度變快???	a529823793	12 / 246	2008-3-16 17:08	
[求助] 木馬是不是這樣生成的，怎麼掛馬，空間收信	2008-3-11			➤ 木馬是不是這樣生成的...
[求助] 什麼盜QQ好	tianwaiqlixing	4 / 226	2008-3-16 14:24	
討論] 主題: 教菜鳥怎樣抓肉雞成群	danjan	0 / 67	2008-3-16 08:39	
討論] 一秒鐘破解網頁鎖定! 不頂勿進	2008-3-16			➤ 一秒鐘破解網頁鎖定...
[求助] 高手來下	tianwaiqlixing	0 / 49	2008-3-15 18:22	
討論] XP有一個很無敵的命令----很有用	lovechina	28 / 1993	2008-3-15 16:46	
[求助] 求助!木馬高手黑客進	lujie	2 / 124	2008-3-15 16:41	
討論] 本網吧攻擊				➤ 本網吧攻擊...

某網頁撰寫工具被發現有一個系統漏洞，  
有駭客撰寫了一個工具  
可以透過這個系統漏洞進行入侵，  
並將工具放在網路上...

# 入侵網站後端範例



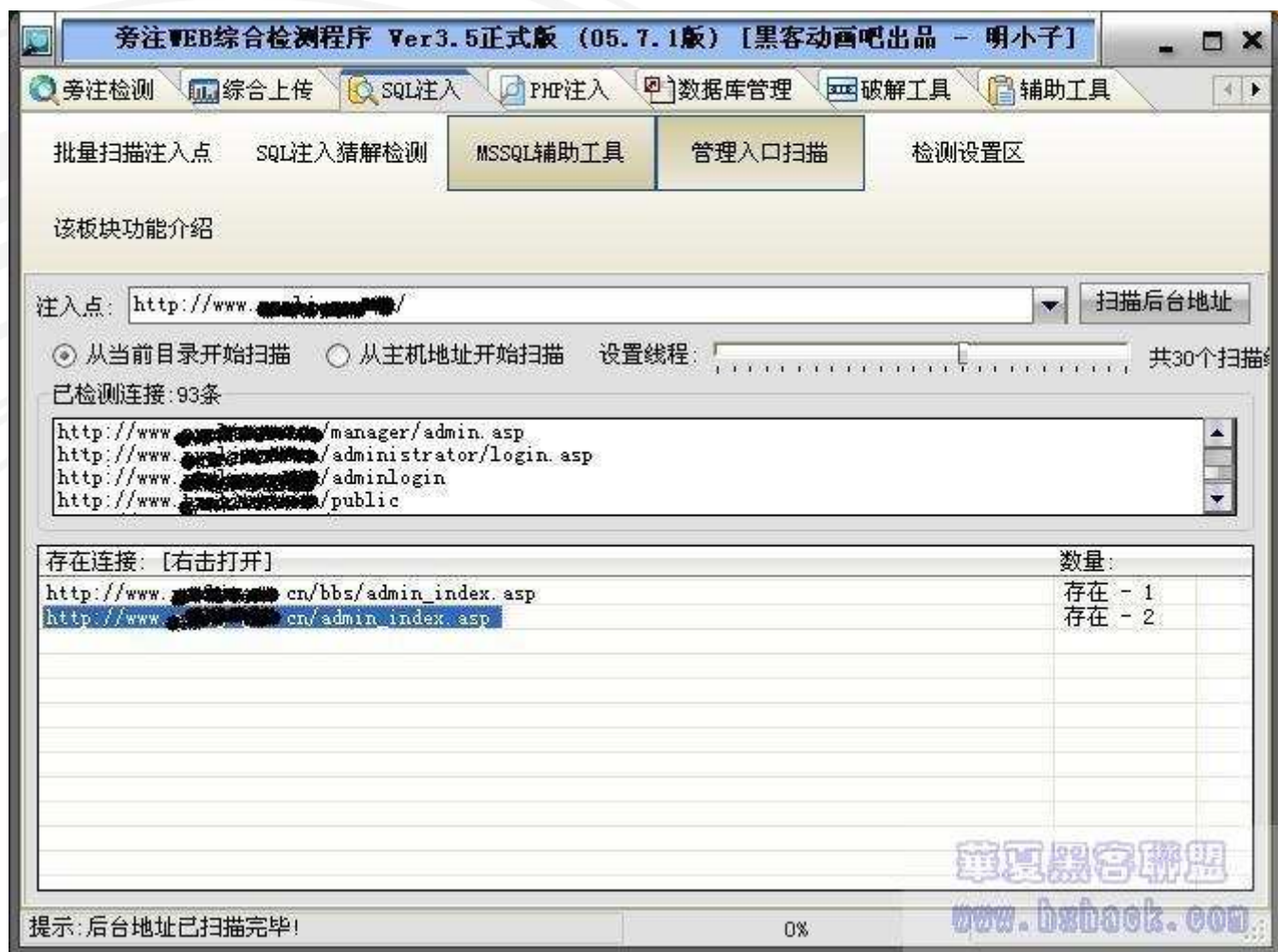
# 選擇目標



# 使用駭客工具破解得到帳號密碼...



# 用駭客工具猜測網站後端網址





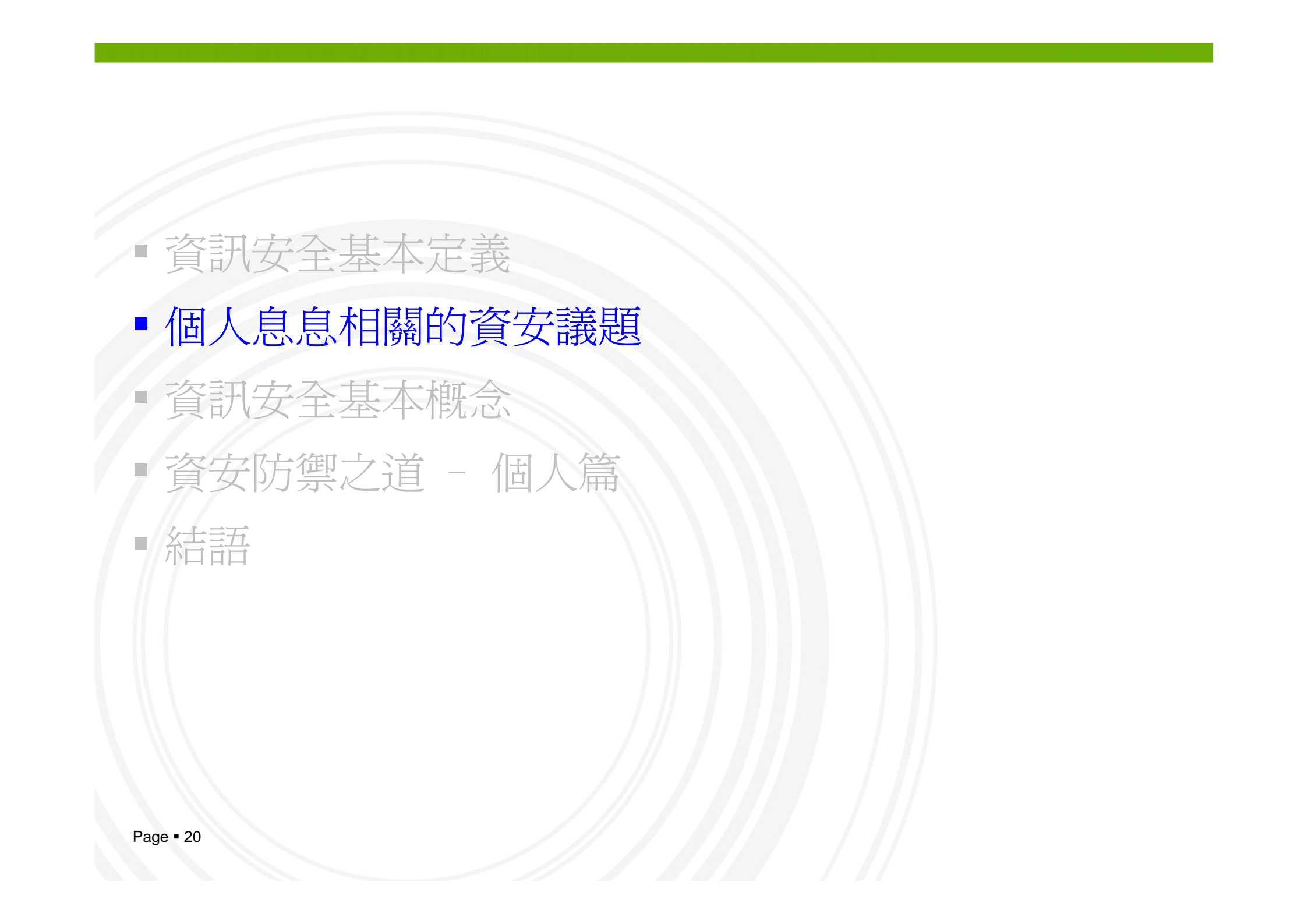
# 得到網站後端網址



# 輸入帳號密碼，進入了網站後端系統~



所以，不要覺得您不會是駭客的目標~  
這些玩家駭客並沒有特定目標，  
只要是系統有漏洞、疏於防護的，  
可能就是他的目標！！

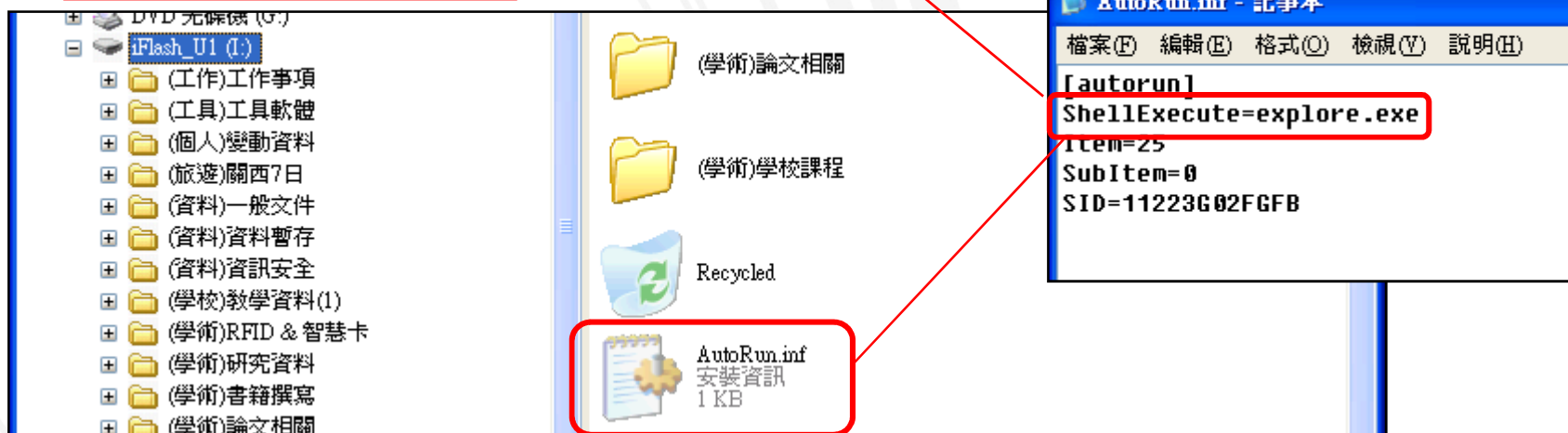
- 
- 資訊安全基本定義
  - 個人息息相關的資安議題
  - 資訊安全基本概念
  - 資安防禦之道 - 個人篇
  - 結語

# USB病毒

您可能不曉得...

您的電腦病毒是您自己帶回家的！

在隨身碟寫入自動  
執行電腦病毒

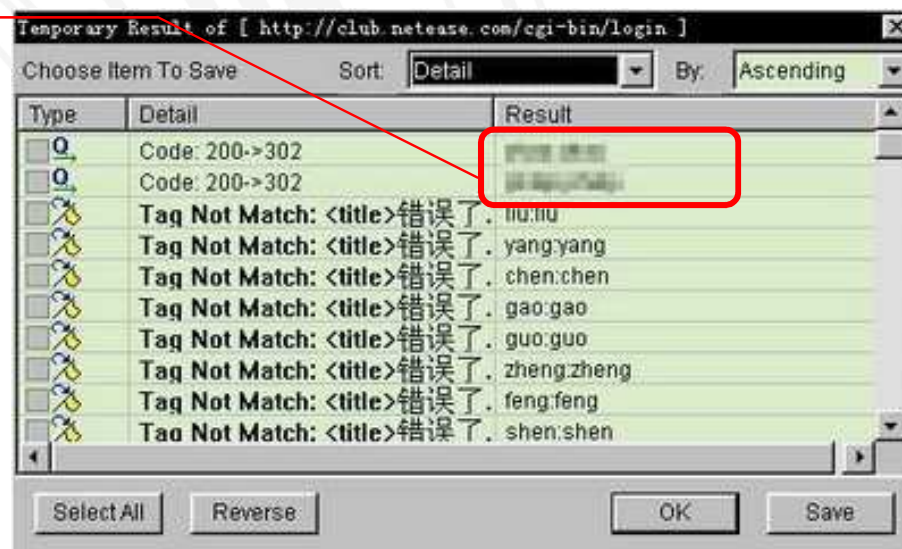


# 密碼安全

您可能不曉得...

您的懶人密碼讓駭客輕易破解您的密碼！

使用暴力破解軟體  
破解網路相簿密碼

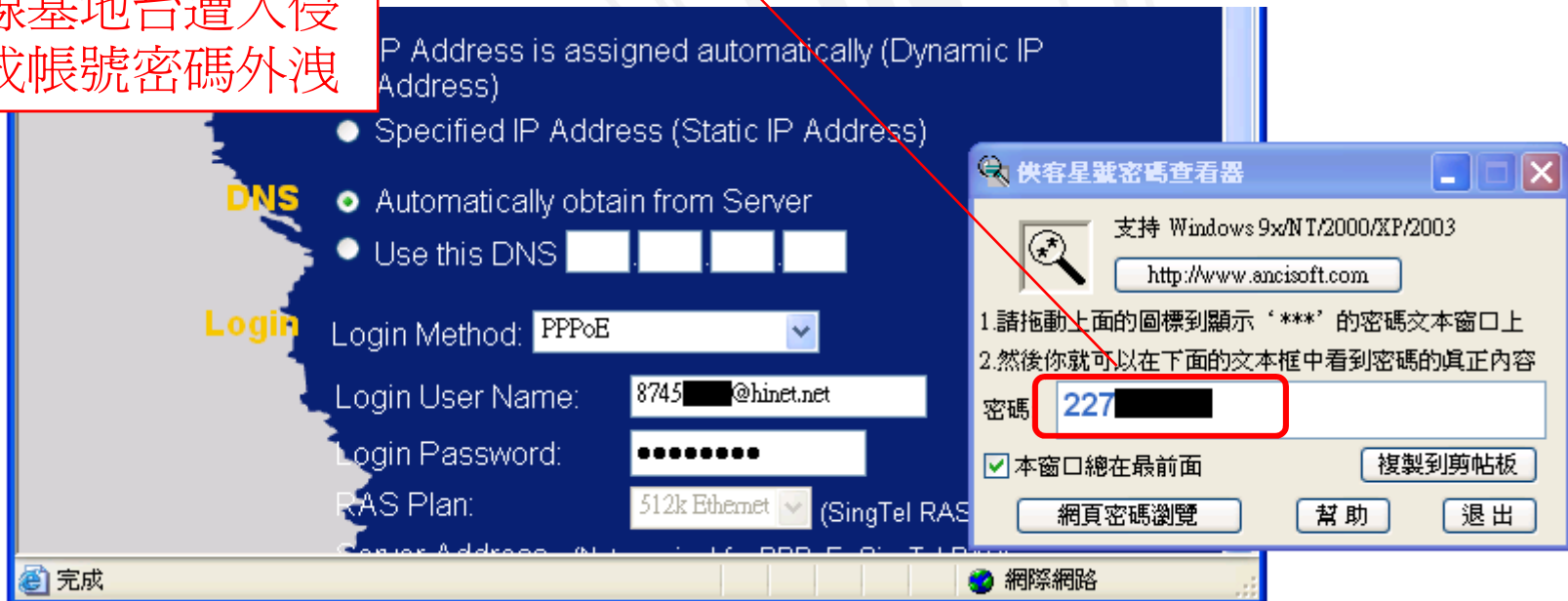


# 無線網路威脅

您可能不曉得...

您輕忽無線網路安全所造成  
資安嚴重威脅！

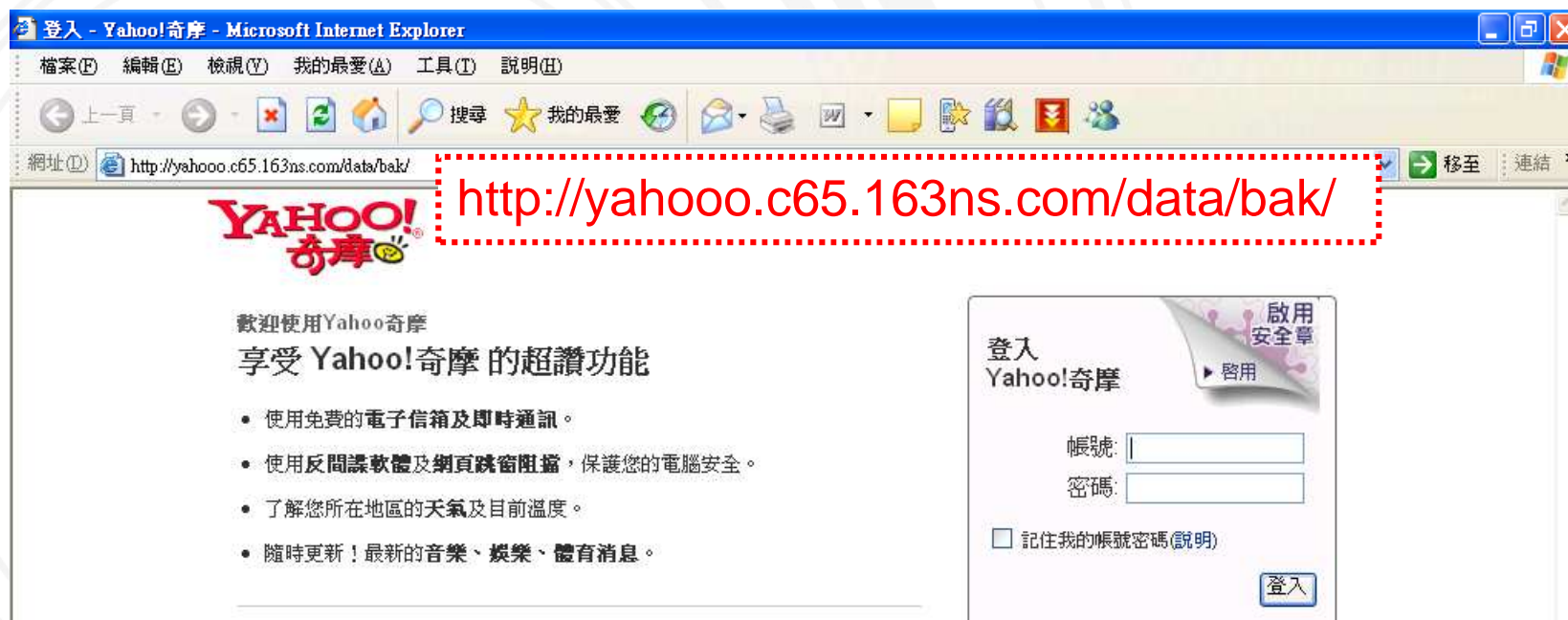
無線基地台遭入侵  
造成帳號密碼外洩



# 釣魚網頁

您可能不曉得...

您接到詐騙電話是因為您自己在釣魚網站  
洩露了帳號密碼！

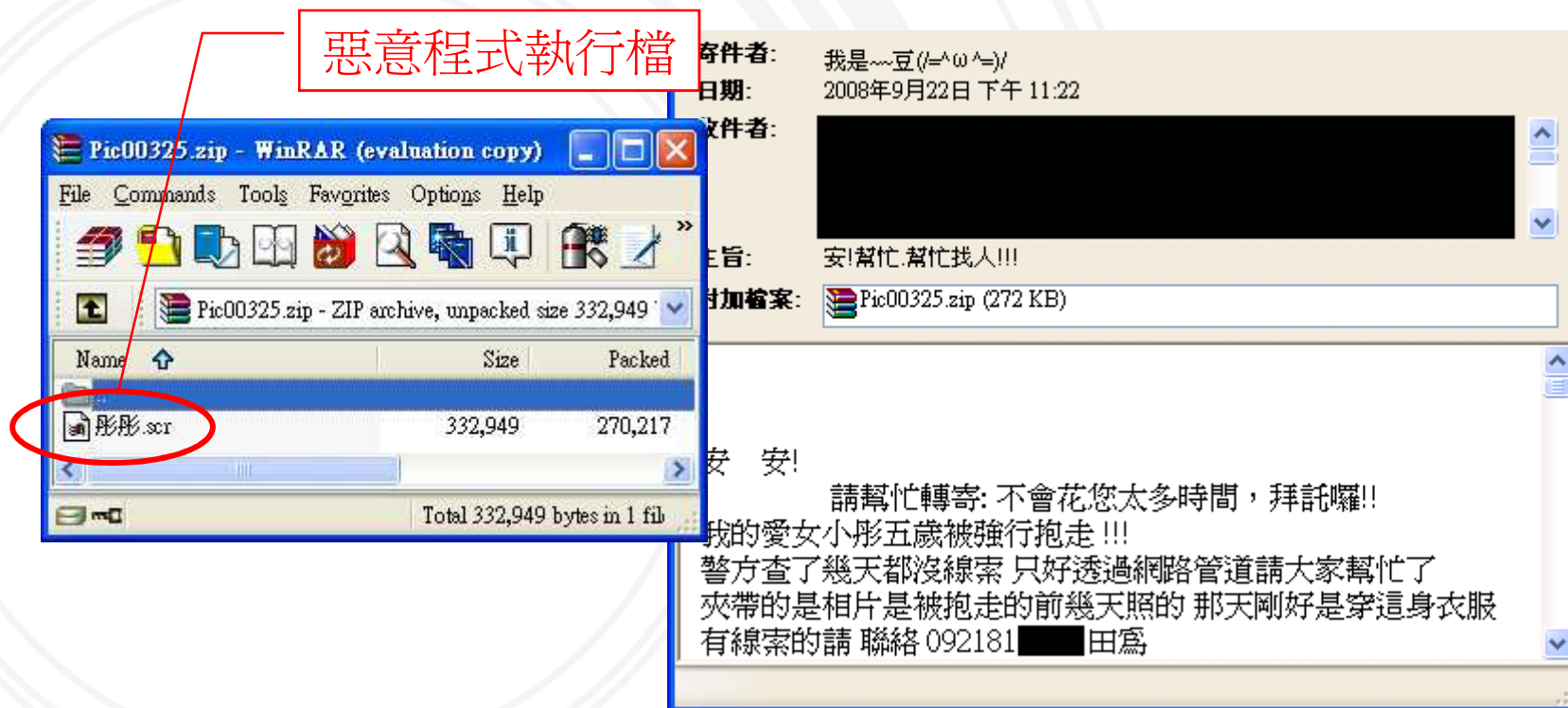




# 社交工程攻擊

您可能不曉得...

您早就淪為社交工程攻擊受害者！



# 駭客如何入侵您的電腦？！

## 誘騙您上當植入木馬程式

- 主動式的攻擊
  - 電子郵件
  - 即時通
- 上勾式的攻擊
  - 釣魚網站
  - 工具軟體嵌入惡意程式

## 利用漏洞進行入侵

- 未更新修補程式
- 安全防護不足
  - 例如未啓用防火牆功能

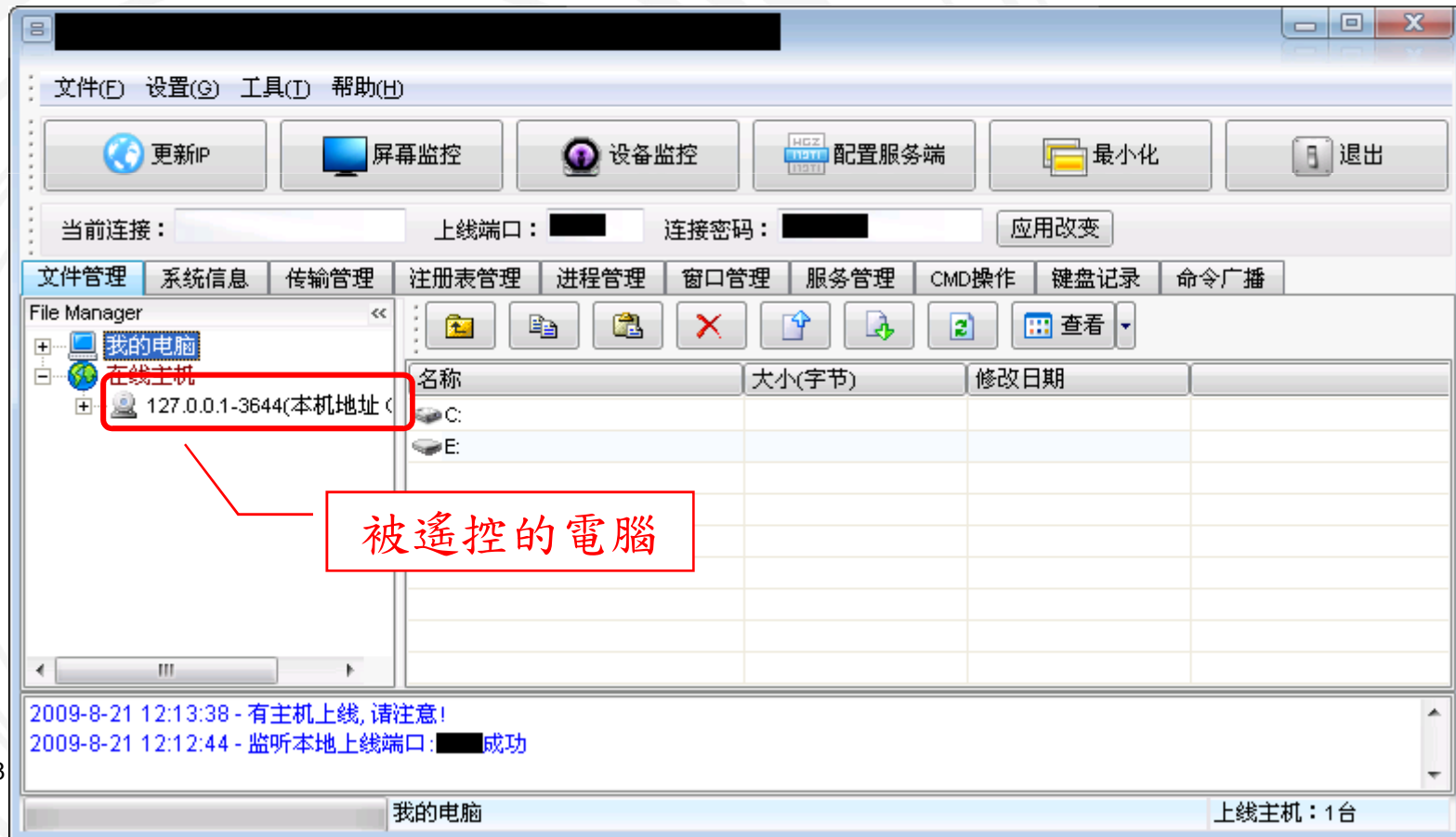
# 媒體報導「駭客侵視訊 偷拍出浴女」

- 駭客以木馬程式植入他人電腦，再遠端開啓女子電腦上的攝影機…

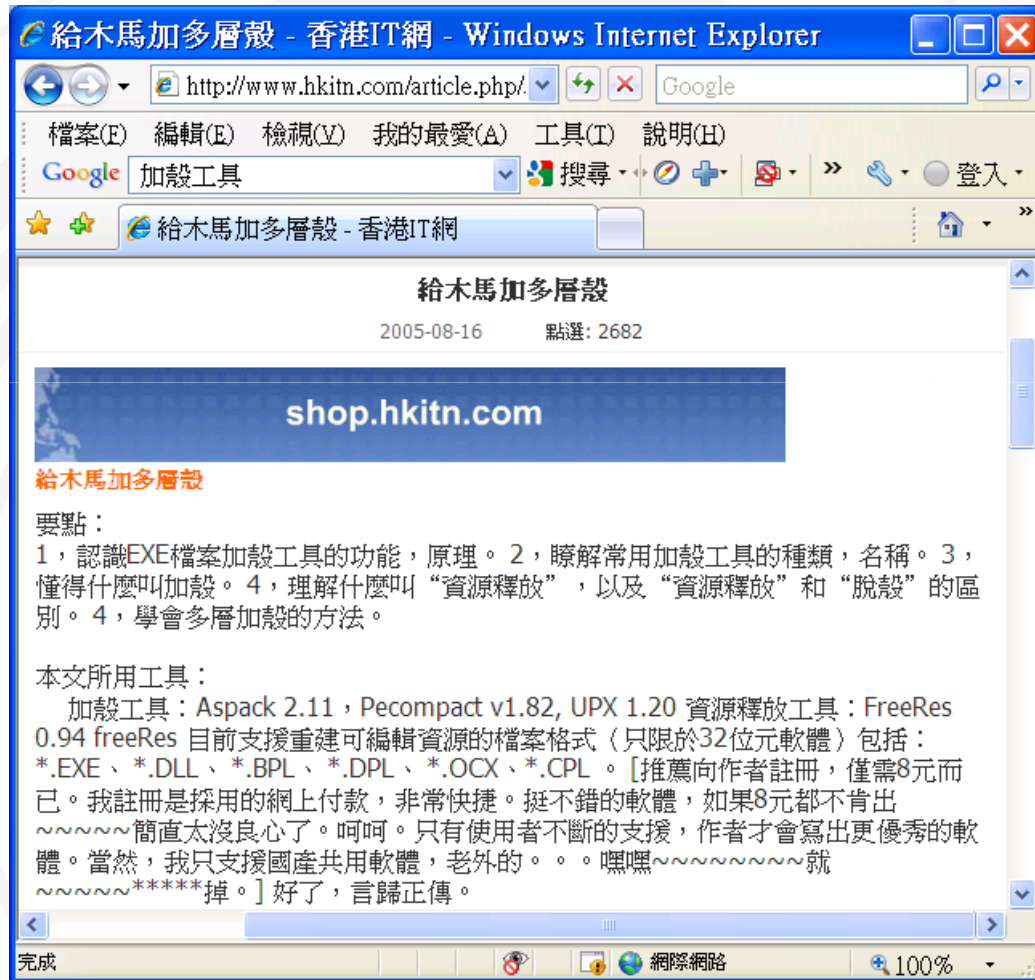


# 木馬程式

所以您要曉得，  
這些木馬程式威力強大，一旦中招，可能就任由宰割了！



# 木馬程式的威脅



- 您不能依賴防毒軟體能幫您阻擋掉所有的木馬程式，因為這些惡意程式可能利用「加殼免殺」技術避過防毒軟體的偵測！

# 木馬程式的技倆

所以只要想辦法讓您去執行它…

您就被植入木馬程式了！！

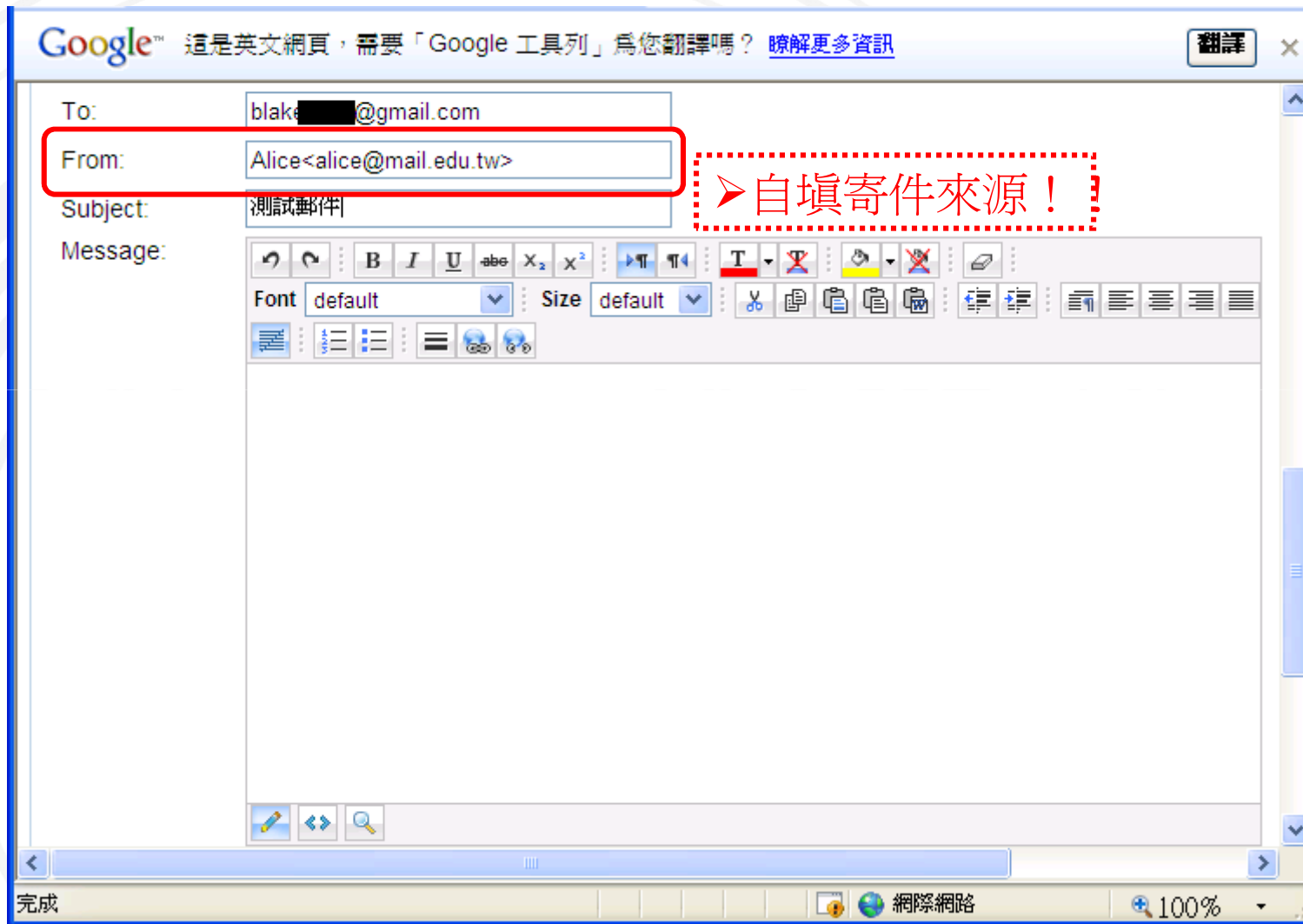


所謂「社交工程」，就是詐騙！

透過電子郵件等方式偽裝身份  
誘騙您上勾受騙...

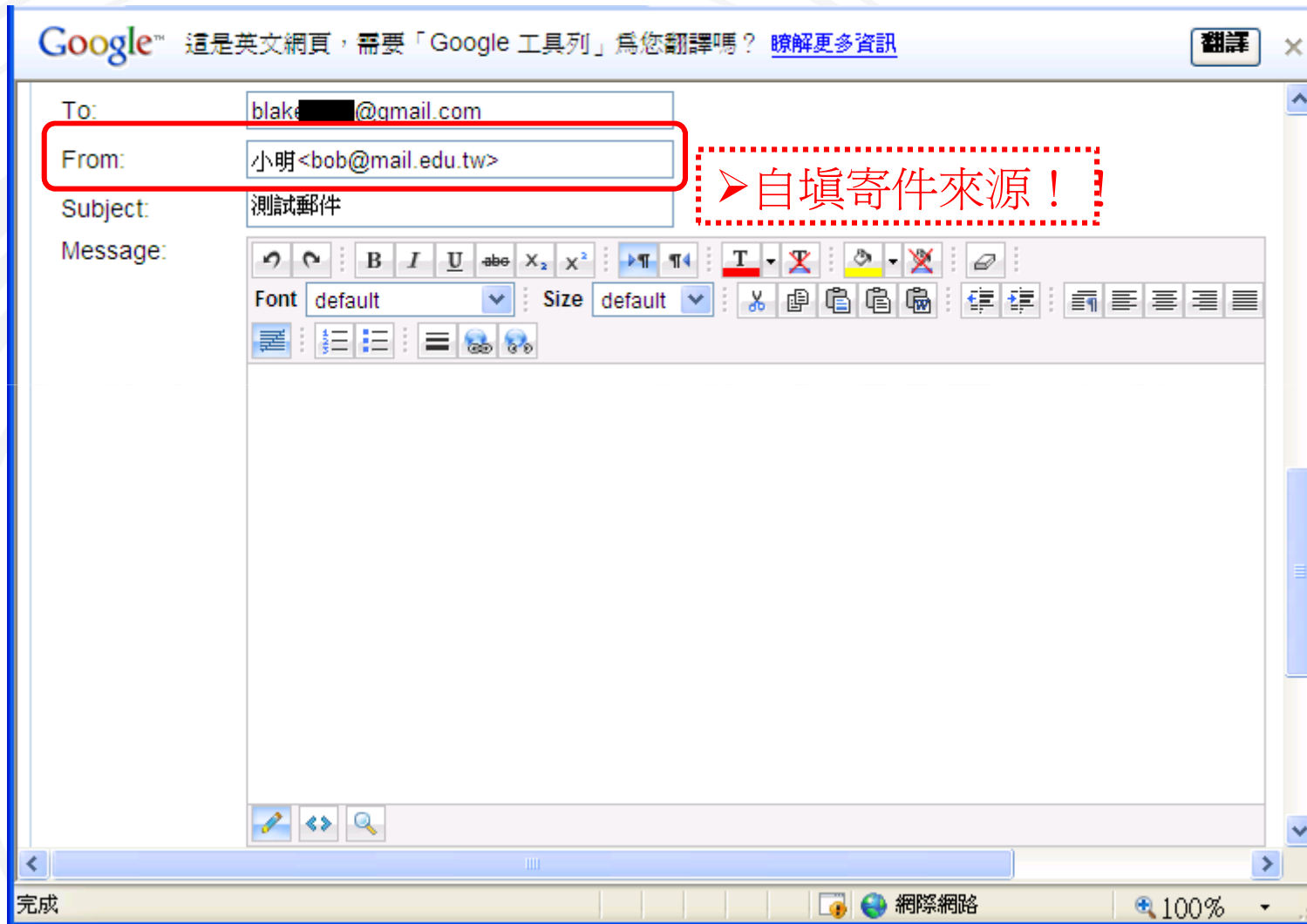
假冒的身份；友善、誘惑的內容...

# 偽冒身份的電子郵件(1)





## 偽冒身份的電子郵件(2)





# 電子郵件攻擊的陷阱

夾帶惡意程式執行檔

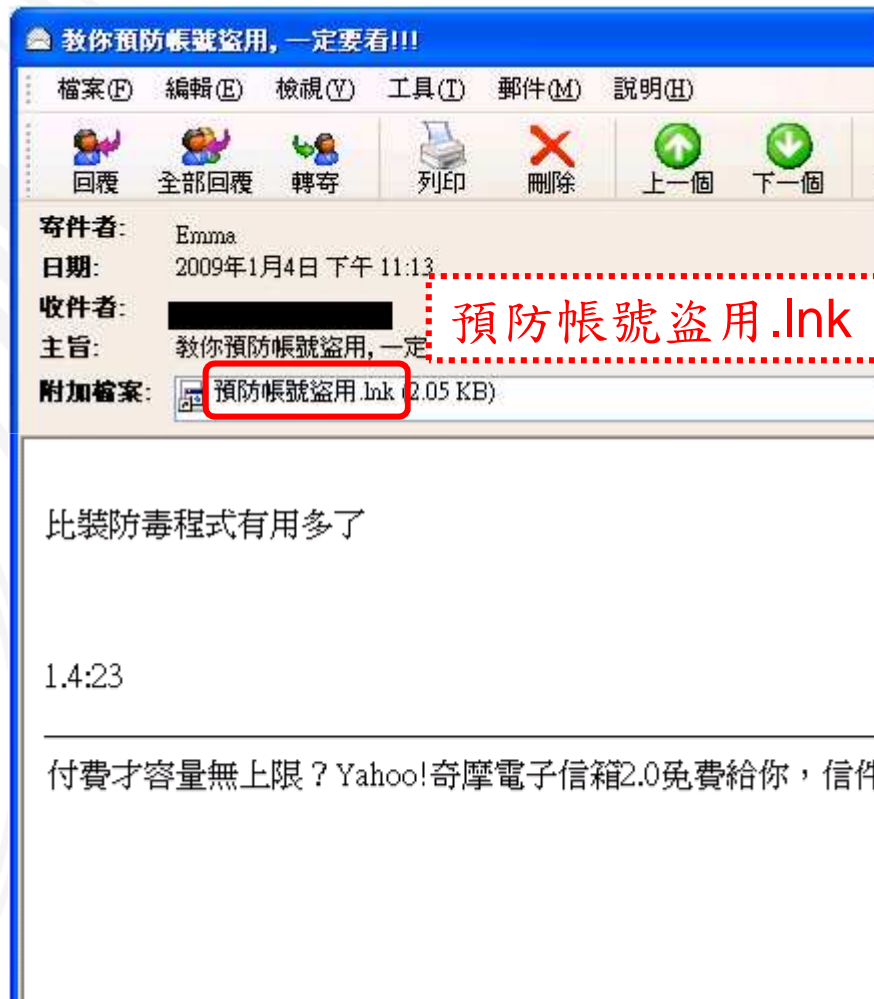
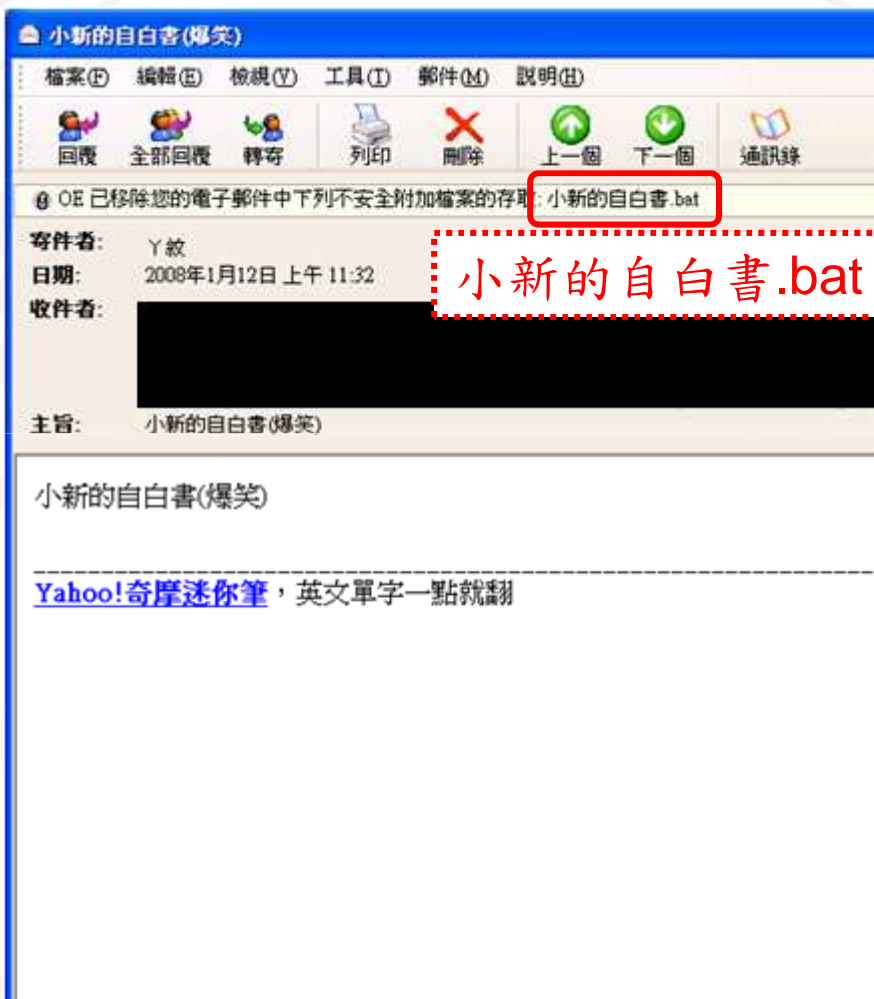
內文中的惡意網頁超連結

Html郵件隱藏遠端下載

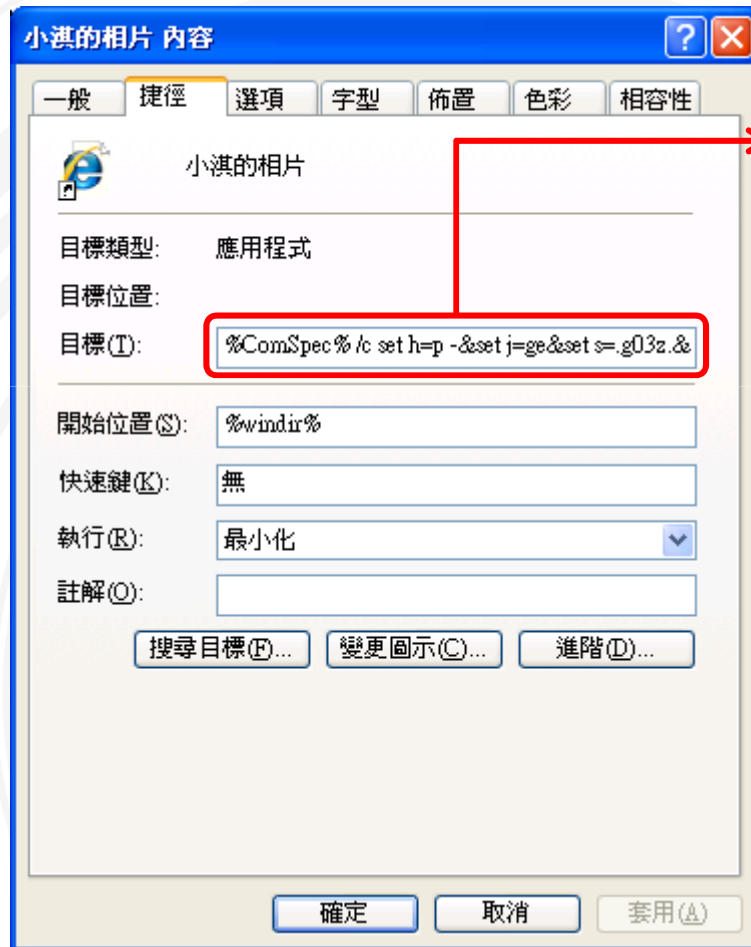
# 夾帶惡意程式執行檔

- 常見的惡意程式執行檔類型
- 「捷徑」亦是下載與執行惡意程式的方法



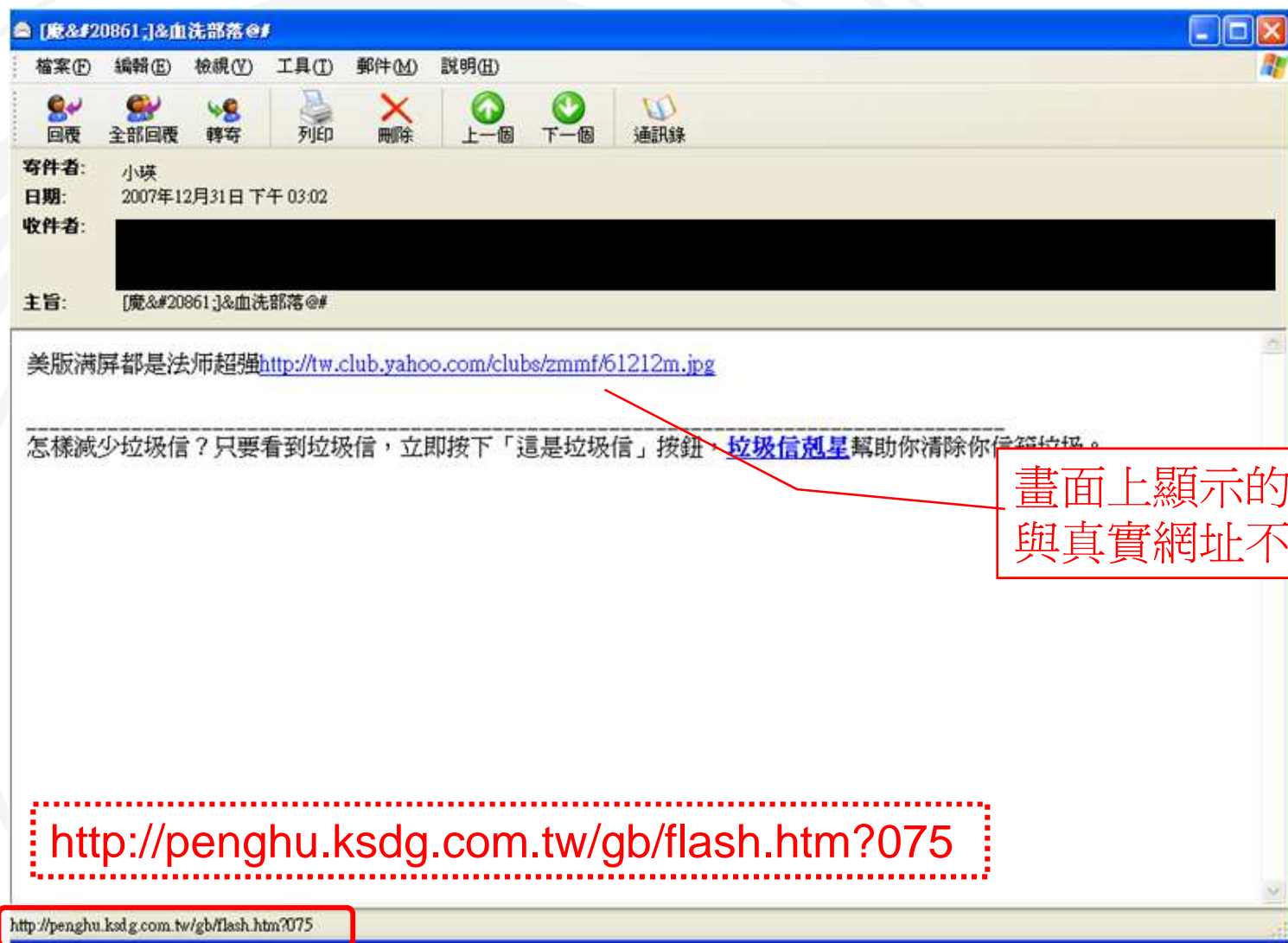


# 「捷徑」攻擊技倆解析

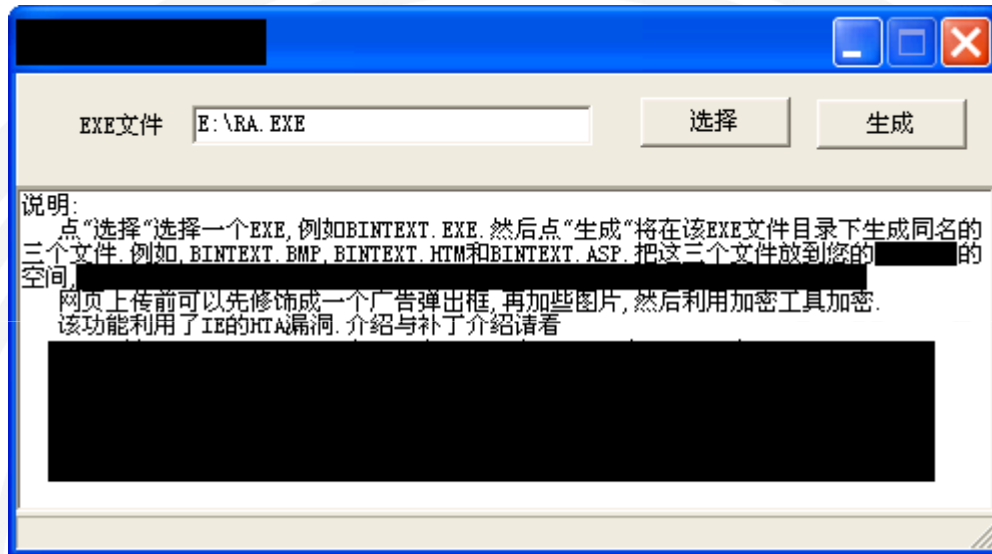


- 捷徑是一串DOS指令的集合
- 此例中，這串指令執行了
  - 連接一個伺服器
  - 下載惡意程式(木馬程式)
  - 執行它！

# 內文中的惡意網頁超連結



# 惡意網頁技倆解析



- 利用工具將惡意程式執行檔(.exe)轉檔為.bmp、.htm和.asp三個檔案，放上網頁
- 當您受騙連上這個鏈結網址(.htm)，即下載安裝了這個惡意程式！

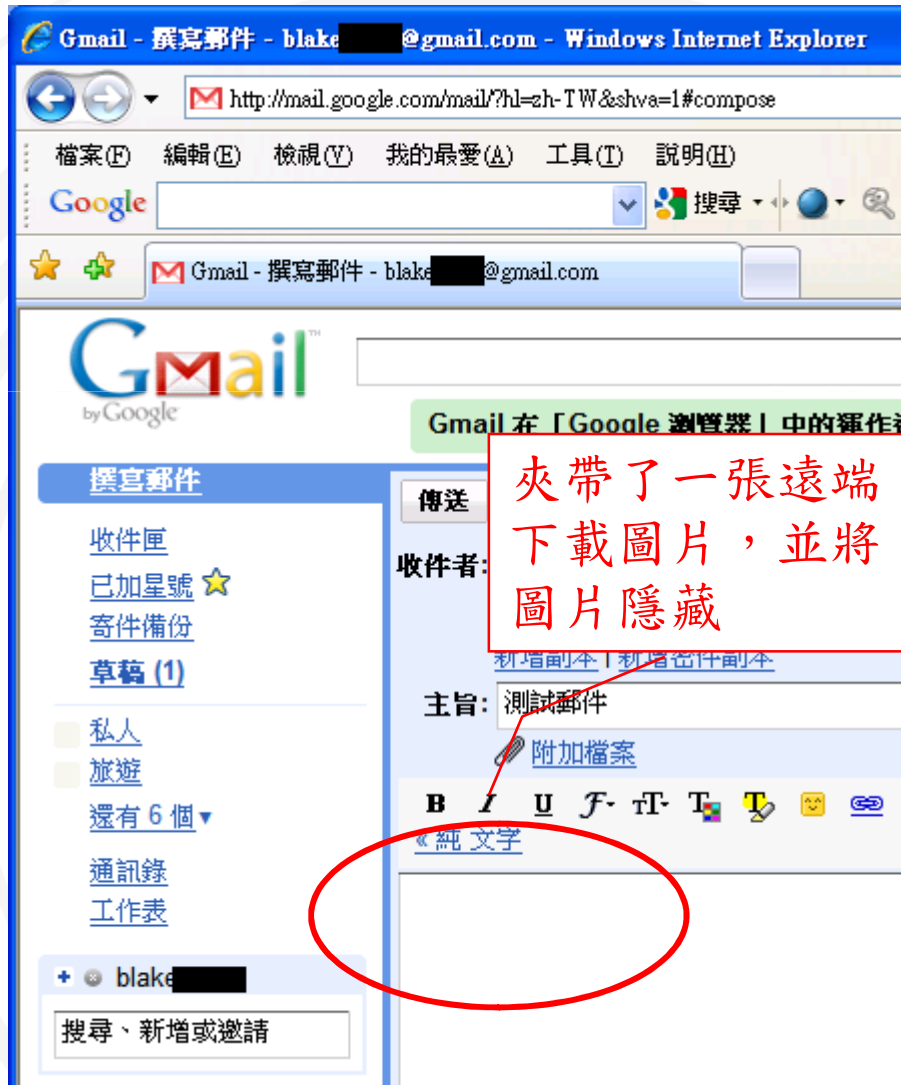


# Html郵件隱藏遠端下載

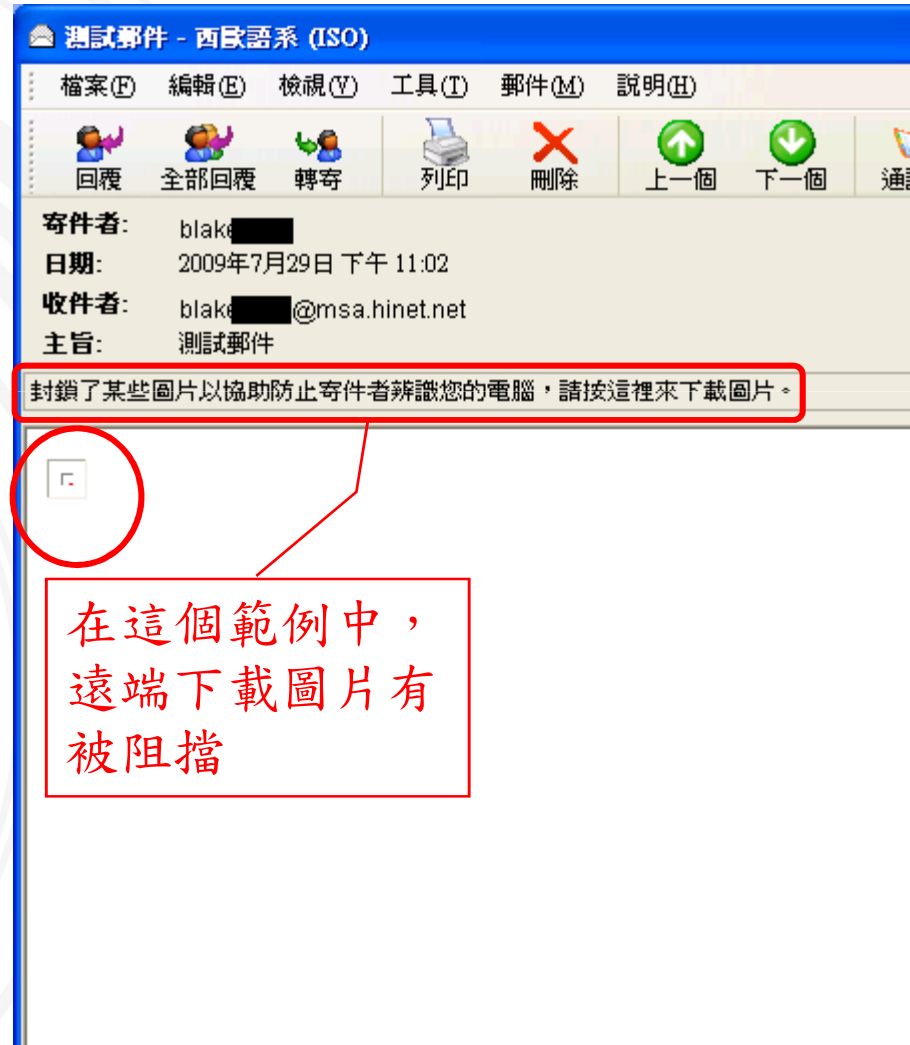
- Html電子郵件可以在Html中撰寫程式語法，所以您**只要瀏覽電子郵件，就觸發該程式執行**
- **利用IE漏洞，不開啓附檔也會中毒！**
  - 2004年3月，Beagle.O電腦病毒使用IE漏洞攻擊，使用者在Outlook / Outlook Express環境下啓用信件預覽功能，信件中的script就會啓動，連結到惡意程式網站下載病毒程式

# Html郵件遠端下載範例

## 發信端



## 收信端



# Html郵件遠端下載範例 (續)

Google™ 這是英文網頁，需要「Google 工具列」為您翻譯嗎？ [瞭解更多資訊](#)

Hello [blake \[REDACTED\]@gmail.com](#).

**Your email has been read.**

**Email Title:** Read Mail

**Sent by You:** Wednesday, July 29, 2009, 10:59:04 PM (GMT +8:00)  
5 minutes 9 seconds ago

**Opened by Recipient:** Wednesday, July 29, 2009, 11:04:43 PM (GMT +8:00)  
(This email has been opened **1** time)  
Up to 5 openings are tracked as per your selection

**Recipient Location:** Taipei, Tai-pei, Taiwan  
(May be inaccurate)

**Recipient IP:** 61.219.37.12  
([61-219-37-12.HINET-IP.hinet.net](#))

**Recipient Browser:** Internet Explorer 7.0 - possibly used within another application such as Outlook (Windows)  
(Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; GTB6; .NET CLR 2.0.50727; .NET CLR 1.1.4322; InfoPath.2))  
URL: [Information not available]

- 如果收信端下載了這張圖片，即沒有設定阻擋
- 籍這張圖片下載，發信端獲取了牠的電腦環境資料...

# 關閉自動下載圖片

## 以 Microsoft Outlook 2007 為例

The screenshot shows the Microsoft Outlook 2007 interface. The 'Tools' menu is open, and the 'Trust Center' option is highlighted. The Trust Center dialog box is displayed, showing the 'Automatic Download' section. The checkbox for 'Do not automatically download pictures in HTML e-mail messages or RSS items' is checked.

**信任中心**

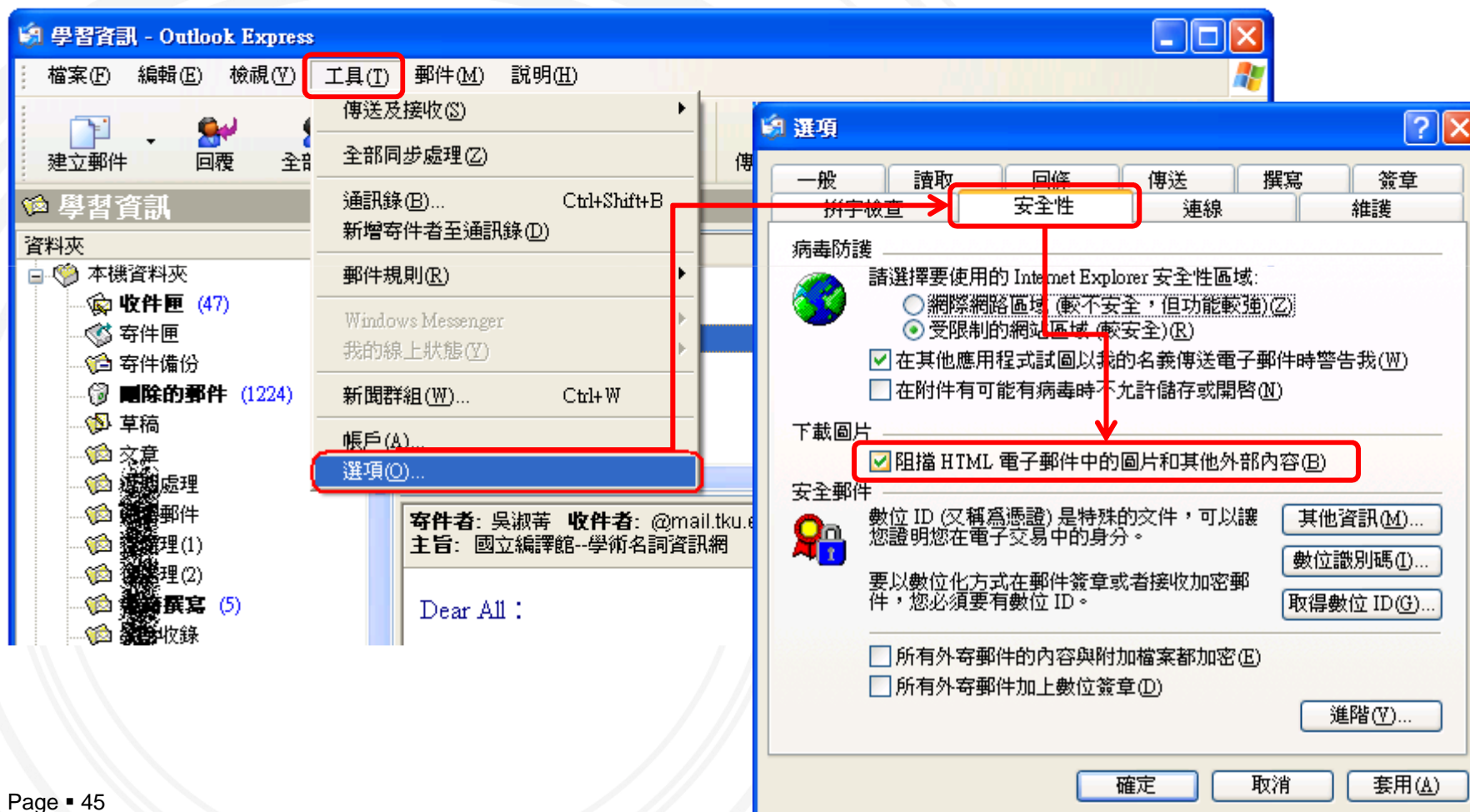
受信任的發行者  
增益集  
隱私選項  
電子郵件安全性  
附件處理  
自動下載  
巨集安全性  
以程式設計方式存取

當開啟 HTML 電子郵件訊息時，您可以控制 Outlook 是否自動下載封鎖電子郵件訊息中的圖片，可協助保護您的隱私。HTML 電子郵件用此種方式與外部伺服器通訊，可讓寄件者驗證您的電子郵件地址。

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

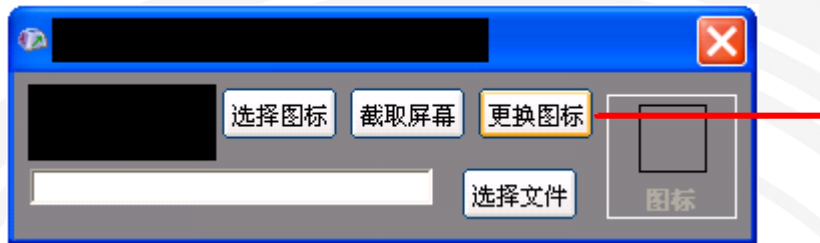
# 關閉自動下載圖片

## 以 Outlook Express 為例



# 工具軟體嵌入惡意程式

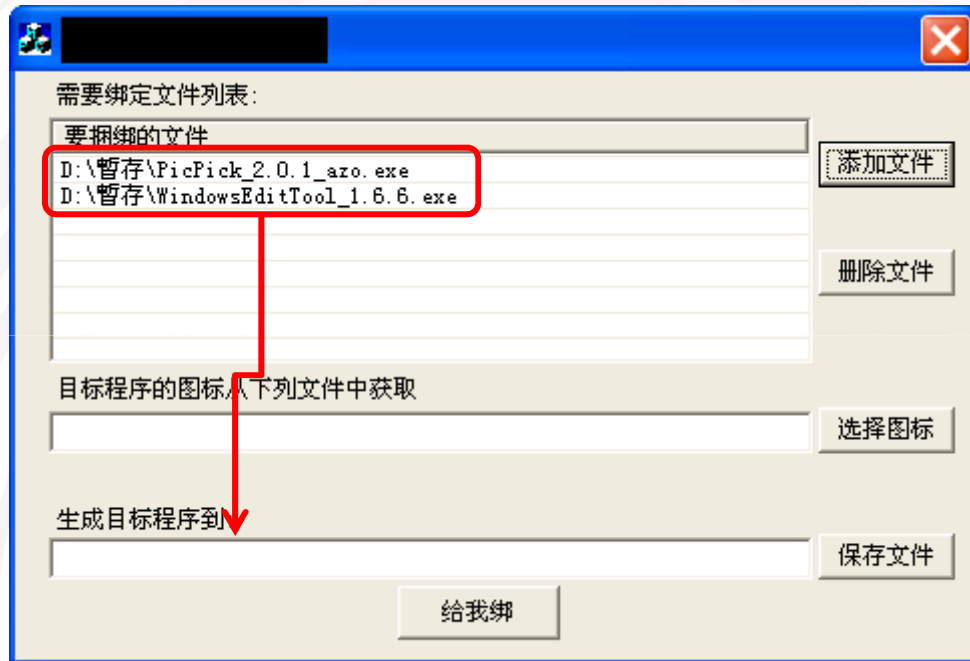
## 惡意程式偽裝技倆解析 - 變更檔案圖示



- 例如將惡意程式執行檔偽裝成一個自解壓縮檔
- 所以您以為您下載了一個某壓縮檔，但其實您一點擊(您以為是解壓縮)，惡意程式就執行與植入了！

# 工具軟體嵌入惡意程式

## 惡意程式偽裝技倆解析 - 合併檔案



- 將A(您想下載的檔案)、B(惡意程式)兩個檔案合併成一個新檔案，並命名為A
- 執行這個新檔案時，A、B兩個檔案都會執行
- 您會看到A檔案正常執行，但您大概不曉得B檔案也已同時安裝進您的電腦！

# 利用漏洞進行入侵

## 利用尚未更新修補程式的漏洞

软件名称	更新时间	软件大小	下载人气	软件评价
 Oday 网马生成器 更新版	2009-08-03	190KB	5	★★★★★
本软件利用Flash的Oday漏洞进行挂马 1 用 pack.exe编码.exe文件(即: The URL of exe中填写的这个exe文件)。2 需要注意的是Flash.exe最后生成的index.html只是一个建议文件,可以根据用户自己的情况再做修改,...				
语言界面: 简体中文 授权方式: 共享软件运行平台: win98/winxp/win2000				
 最新Office Oday网马生成器	2009-07-22	14KB	18	★★★★★
一个体积比较小的Office网络组件远程控制漏洞代				
码,免杀测试通过常用杀毒软件				
语言界面: 简体中文 授权方式: 共享软件运行平台: win98/winxp/win2000				
 ODAY网马生成器 Ms09-014	2009-05-19	1.1MB	131	★★★★★
MS09-014 - 严重Internet Explorer 的一个漏洞,				
详细资料可以参详微软官方网站				
语言界面: 简体中文 授权方式: 共享软件运行平台: win98/winxp/win2000				
 影音Oday网马生成器	2009-05-08	1.0MB	57	★★★★★
暴风影音Oday网马生成器(亲测可用) 叫什么神斧				
网马的,头一次听,不过网马是可以用的				
语言界面: 简体中文 授权方式: 共享软件运行平台: win98/winxp/win2000				

搜索"Oday"共找到 4条记录 当前页: 1 总页数: 1 只有一页

- 網路上有各種利用系統漏洞 / 軟體漏洞進行攻擊的惡意程式
- 若您沒有即時更新修補程式，您可能成為這些惡意程式的受害者



# 利用漏洞進行入侵

## 利用安全防護不足的漏洞

- 很多攻擊手法都是利用您電腦的安全防護不足才能成功入侵
- 例如如果您啓用了防火牆
  - 那麼利用網路掃瞄來試圖入侵，大概就無效！
- 如果您更新了最新的病毒碼
  - 那麼試圖置入特定程式的入侵方法，也會無效！

# 政府社交工程演練電子郵件範例(一)

- 郵件主題

- 政治新聞
- 影劇新聞
- 情色主旨
- 休閒娛樂

- 郵件類型

- 惡意網頁連結
- 惡意Word檔

# 演練電子郵件(政治新聞)

中共十七大即將召開，民主開放將成為共產黨存亡的大難題... - 郵件 (HTML)

檔案(F) 編輯(E) 檢視(V) 插入(I) 格式(O) 工具(T) 執行(A) 說明(H)

回覆(R) | 全部回覆(L) | 轉寄(W) | [Icons]

寄件者: 兩岸觀察站 [Montague@applepie.serveblog.net] 寄件日期: 2007  
收件者: [Redacted]  
副本:  
主旨: 中共十七大即將召開，民主開放將成為共產黨存亡的大難題...



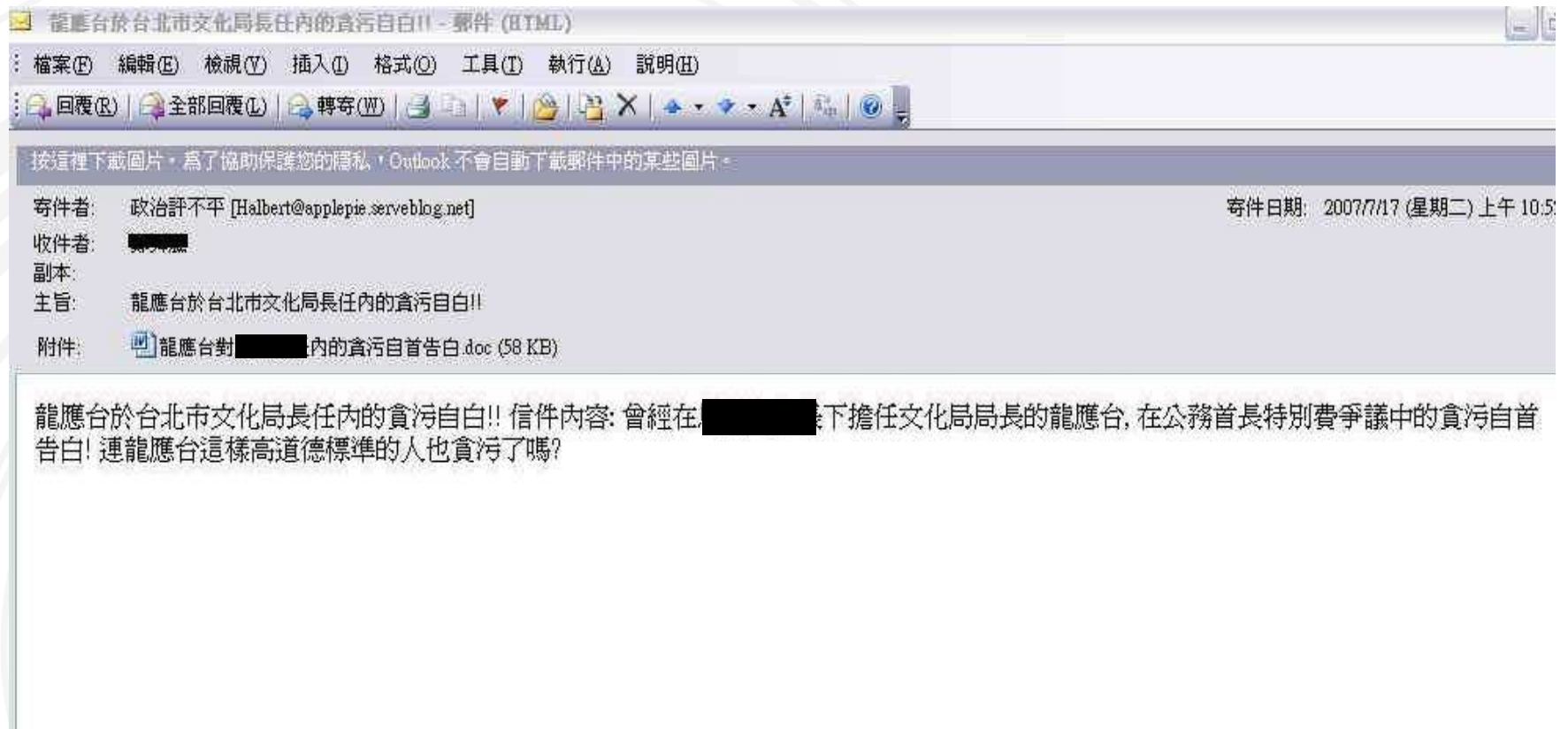
### 中共十七大前民主開放暗潮洶湧

共十七大代表大會將在年底召開...  
而在此時民主開放的思潮已經漫天蓋地的展開...

“改革了，亡黨；不改革，亡國。”

民主開放會在這次十七大投下怎樣的震撼彈... [\[觀看全文\]](#)

# 演練電子郵件(政治新聞)



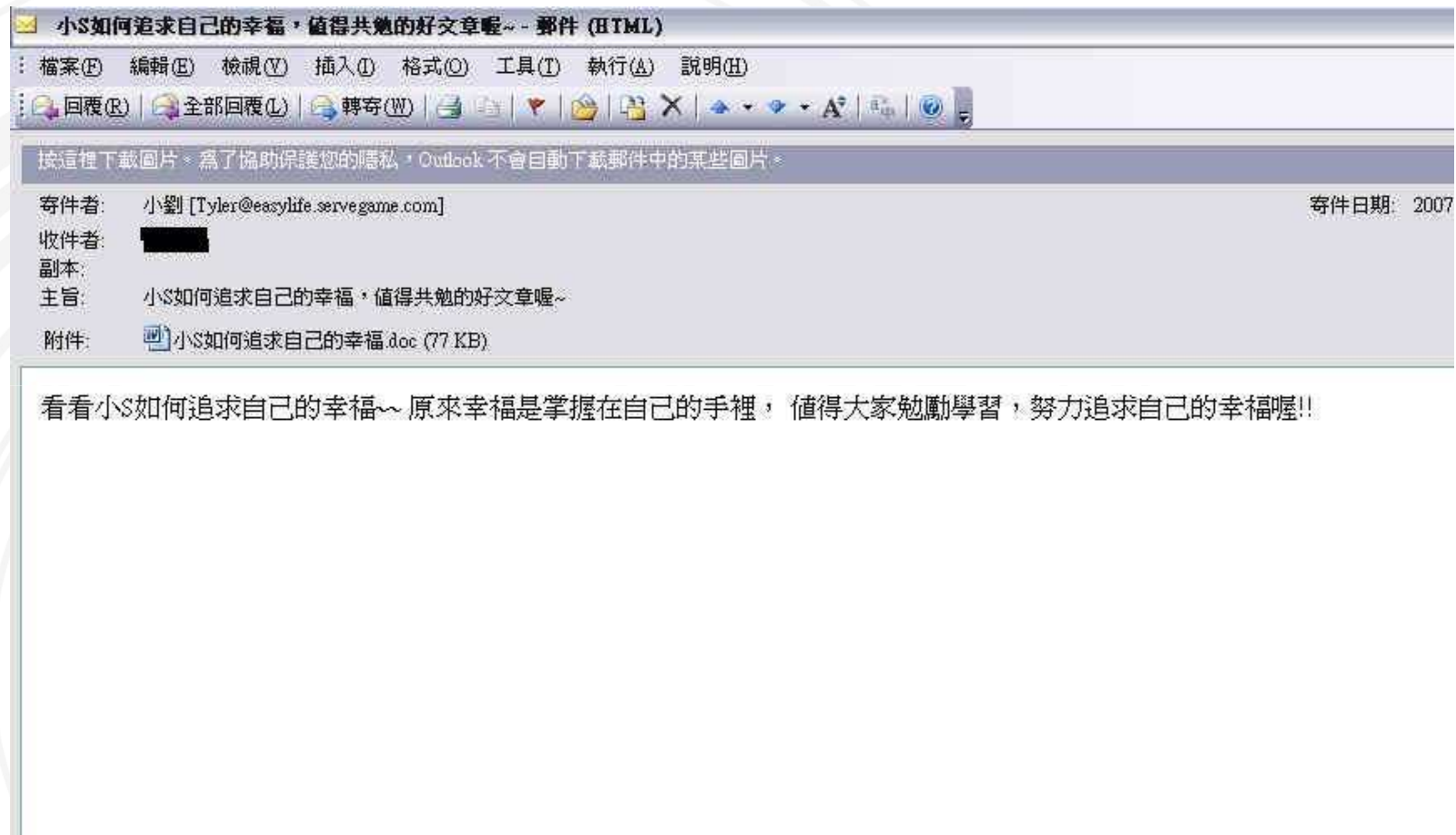
# 演練電子郵件(影劇新聞)



## 周潤發表示力挺 [REDACTED] 參選總統

迪士尼強檔新片「神鬼奇航3：世界的盡頭」中扮演新加坡海盜頭子嘯風船長的周潤發，日前在東京出席宣傳活動時，親口表示：「戲里壞人好演、好做，..... [REDACTED] .....，如果他選總統，我一定投他一票！」...

# 演練電子郵件(影劇新聞)



# 演練電子郵件(情色主旨)



# 演練電子郵件(休閒娛樂)

2007宜蘭童玩節來了!! - 郵件 (HTML)

檔案(F) 編輯(E) 檢視(V) 插入(I) 格式(O) 工具(T) 執行(A) 說明(H)

回覆(R) 全部回覆(L) 轉寄(W)

寄件者: 童玩大使 [Felix@extremefun.servebeer.com] 寄件日期: 2007/7/17 (星期)

收件者: [REDACTED]

副本:

主旨: 2007宜蘭童玩節來了!!



童玩節 12 歲囉！  
讓我們大手牽小手 邁開腳步  
1 2 1 2 齊步走 ~ 一起向充滿歡笑希望的兒童夢土出發！

今年在冬山河畔，用最快樂的節奏 最熱情的步伐，享受夏日水舞的沁涼，隨著海洋之歌的音符起舞，7月7日 讓我們跟著小雨和童玩娃娃兵團，展開童玩國度51天的夏日冒險！

[\[更多活動資訊\]](#)

演出	<ul style="list-style-type: none"> <li>【野外劇場】來自全世界五大洲民俗音樂舞蹈團隊的精采演出</li> <li>【蔚藍舞台】海洋之歌的曼妙樂符 悠揚於冬山河畔！</li> </ul>
展覽	<ul style="list-style-type: none"> <li>【七彩陀螺館】感受陀螺七彩旋風的魅力！</li> <li>【童玩童食回味屋】回味兒時童玩童食的時光之旅！</li> <li>【飛行船劇場】全國首座的球體型可移動式3D立體劇場</li> </ul>

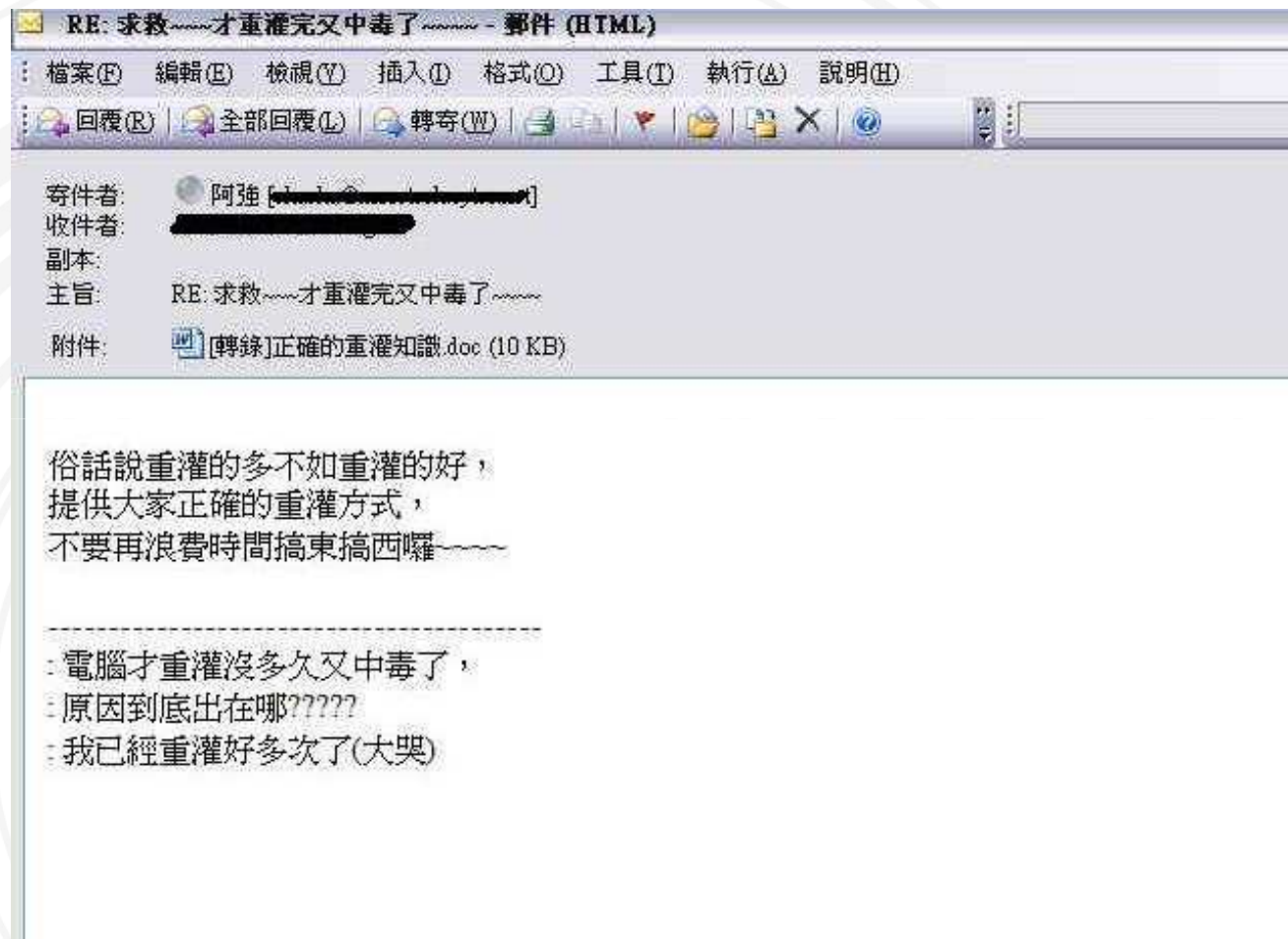
飄浮在半空中的【水母瀑布】，突如其來的多樣水幕瀑布，傾瀉而出，彷彿水母的觸足沖及全身，讓你感受浪花濺起、七彩旋轉的聲光刺激，還有不時噴出湯工七雲與多變噴射七



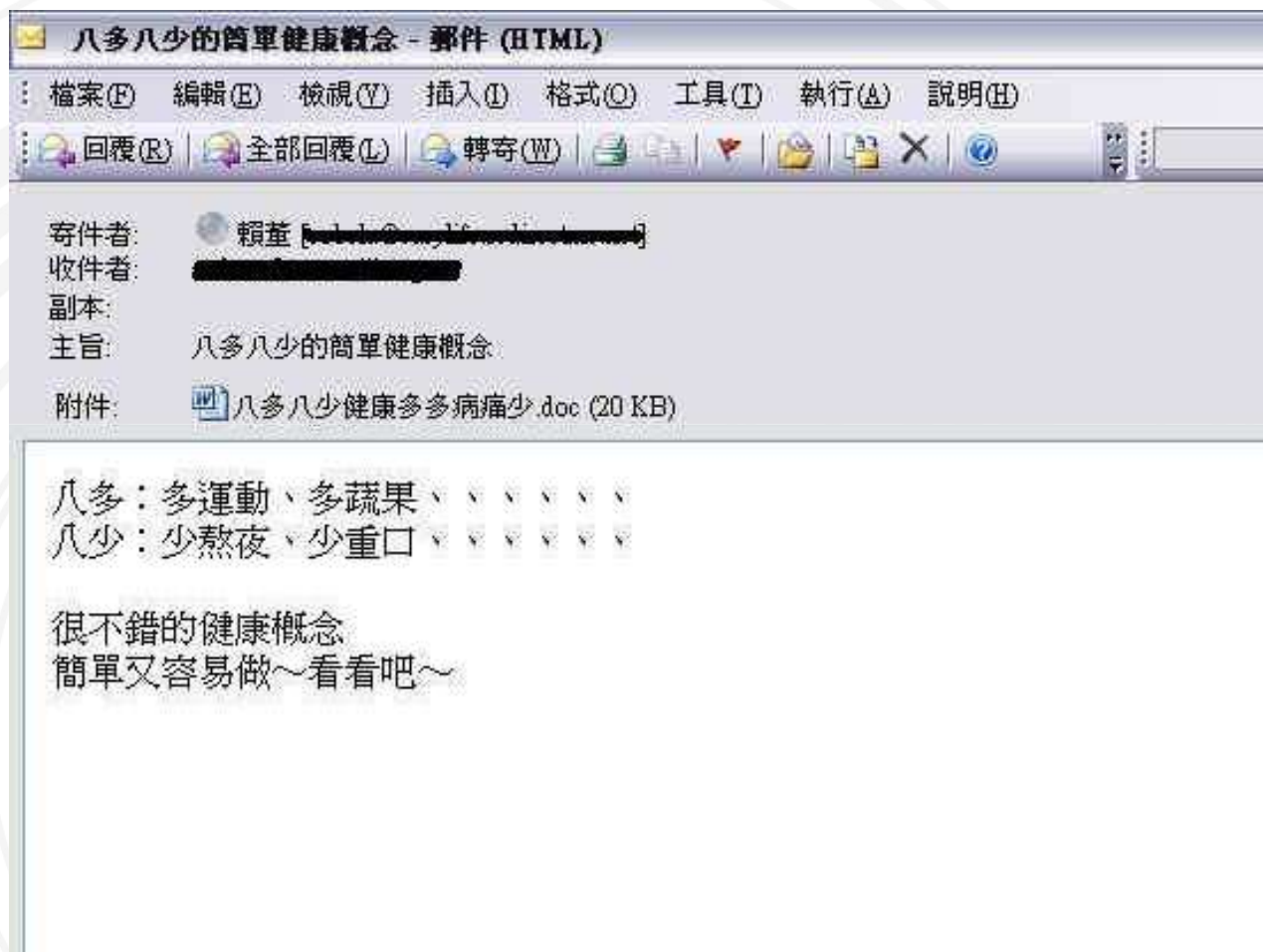
# 政府社交工程演練電子郵件範例(二)

- 郵件主題
  - 科技新知
  - 保健養生
  - 休閒娛樂
  - 影視八卦
  - 體育新聞
  - 情色內容

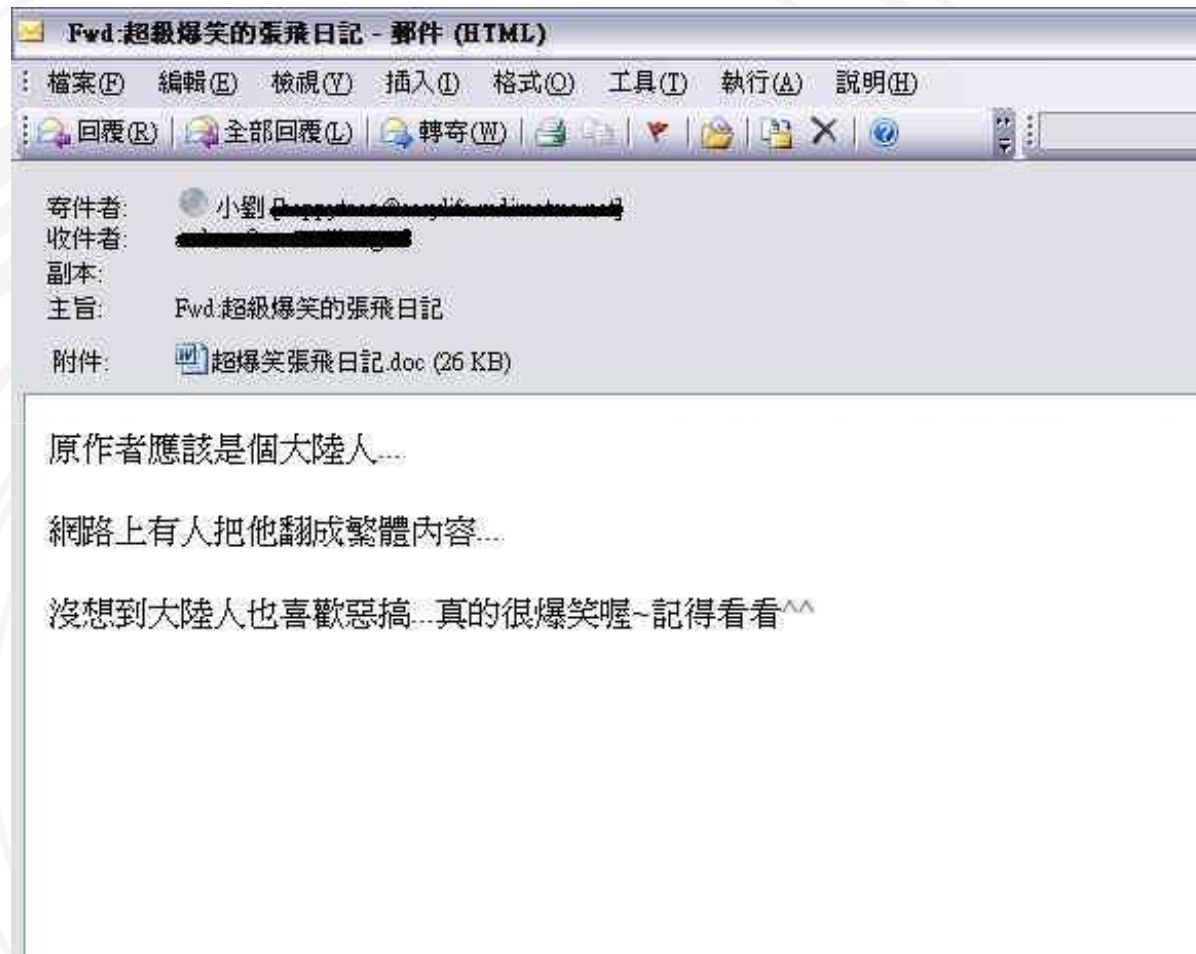
# 演練電子郵件(科技新知)



# 演練電子郵件(保健養生)



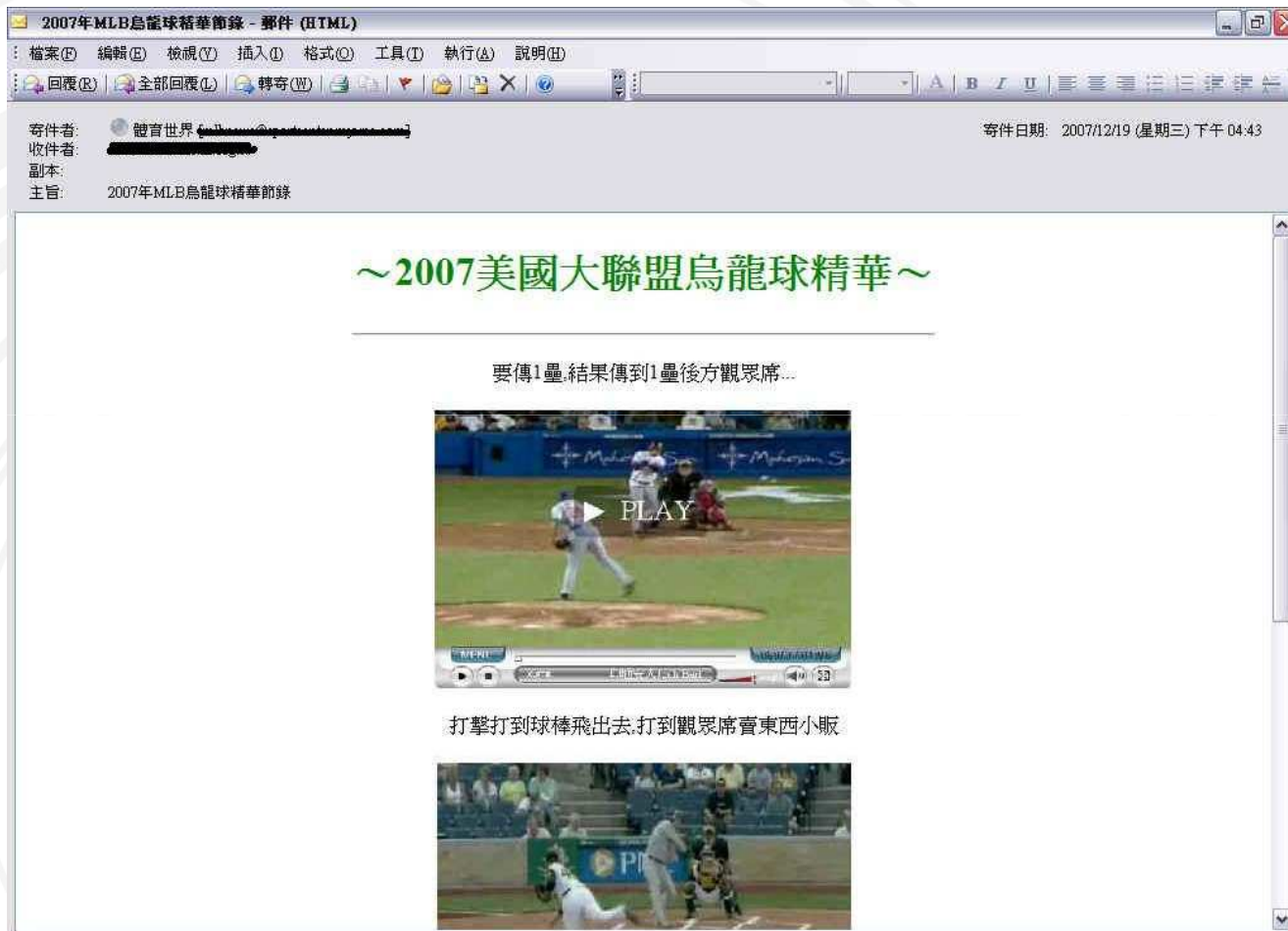
# 演練電子郵件(休閒娛樂)



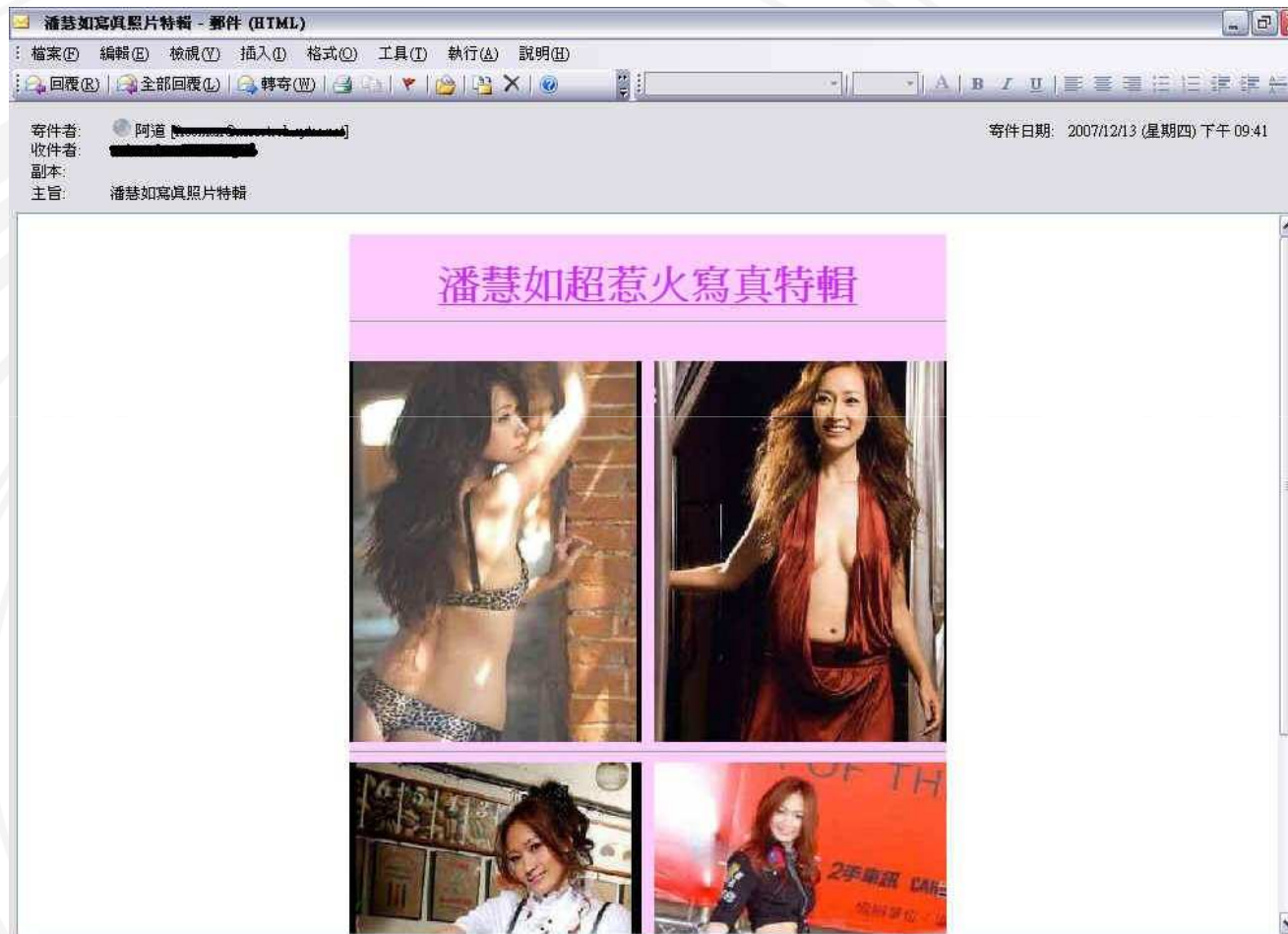
# 演練電子郵件(影視八卦)

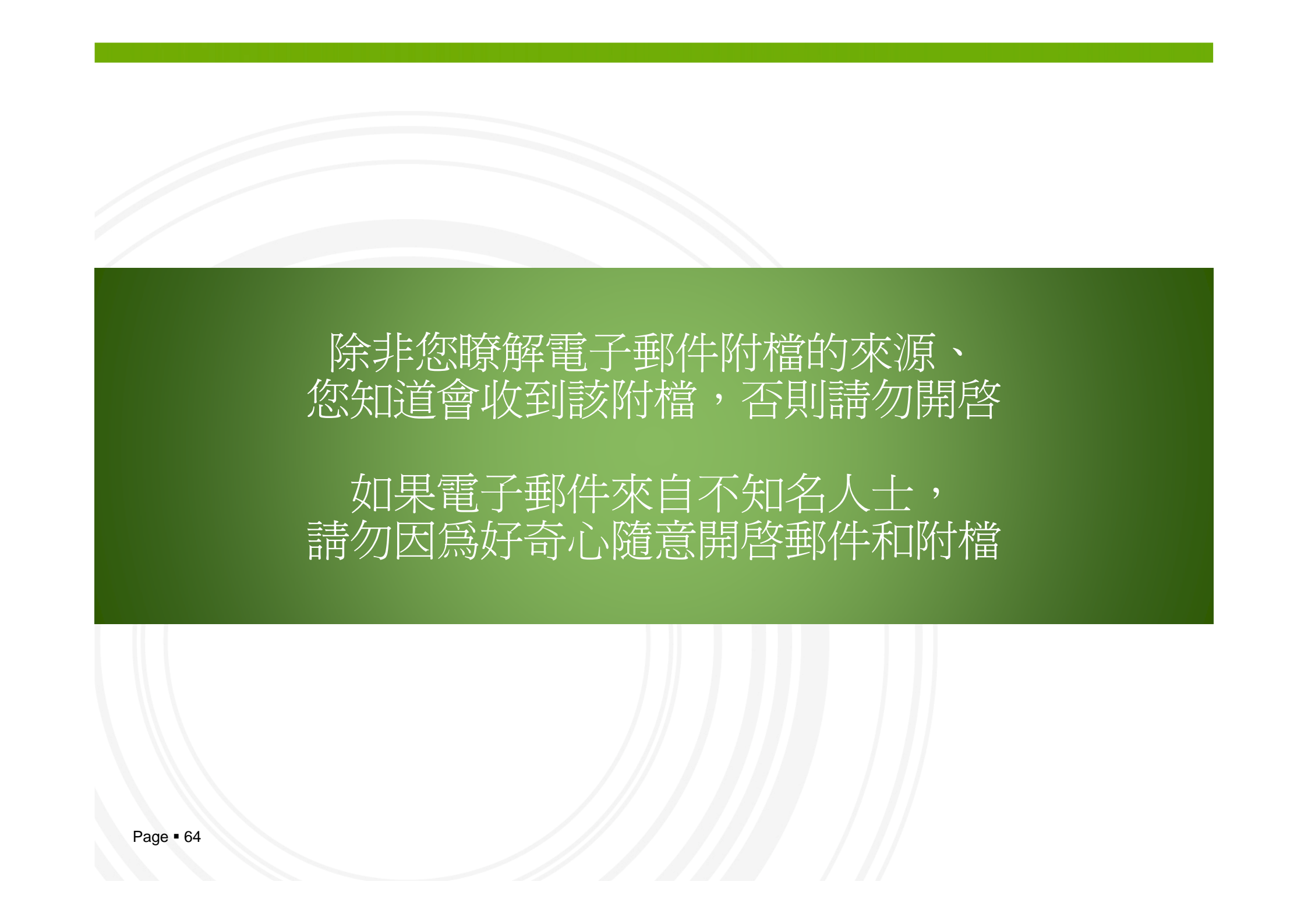


# 演練電子郵件(體育新聞)



# 演練電子郵件(情色內容)

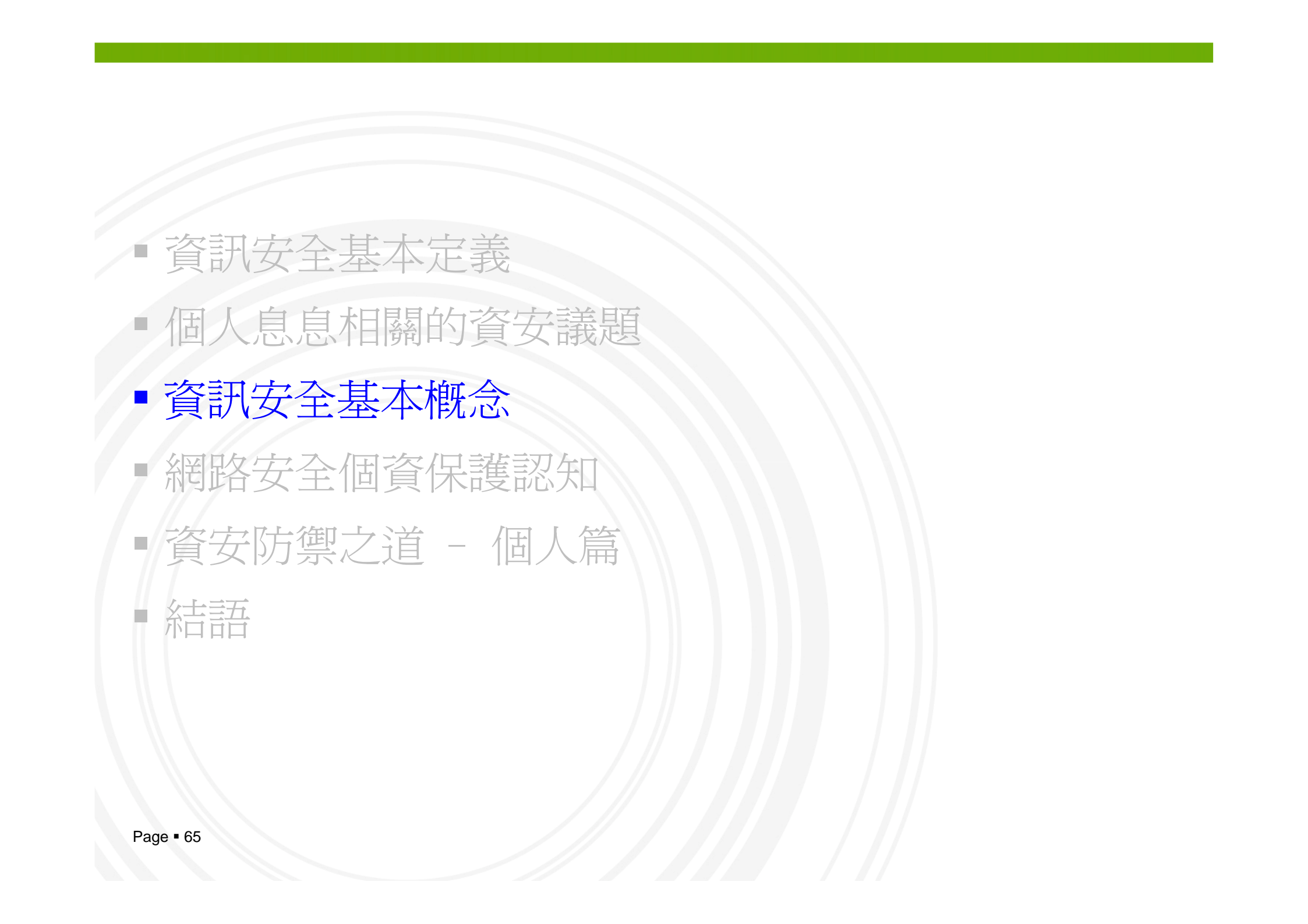




除非您瞭解電子郵件附檔的來源、  
您知道會收到該附檔，否則請勿開啓

如果電子郵件來自不知名人士，  
請勿因為好奇心隨意開啓郵件和附檔



- 
- 資訊安全基本定義
  - 個人息息相關的資安議題
  - 資訊安全基本概念
  - 網路安全個資保護認知
  - 資安防禦之道 - 個人篇
  - 結語

您可能沒有注意到，  
其實您不經意的電腦使用習慣，散播了他人的個資…

# 郵件轉寄

## 轉寄網路郵件

可能沒注意到要保護他人個資，而外洩了他人的個人資料…

寄件者: charels  
日期: 2008年2月19日 下午 09:51  
收件者: charels  
主旨: FW: Fwd: 面對它---(看看這文章)

- ◆ 避開吵雜→感到四周聲音過於嘈雜時，可戴上耳塞。
- ◆ 洗個熱水澡鬆弛情緒 → 夏季可改採冷水浴。
- ◆ 就寢前，先將第二天的生活做一計劃→包括進餐、衣著。
- ◆ 睡眠要充足→缺乏睡眠會使人變得焦慮、易怒。

刪除 導遊

文字工作者

陽光房出版社

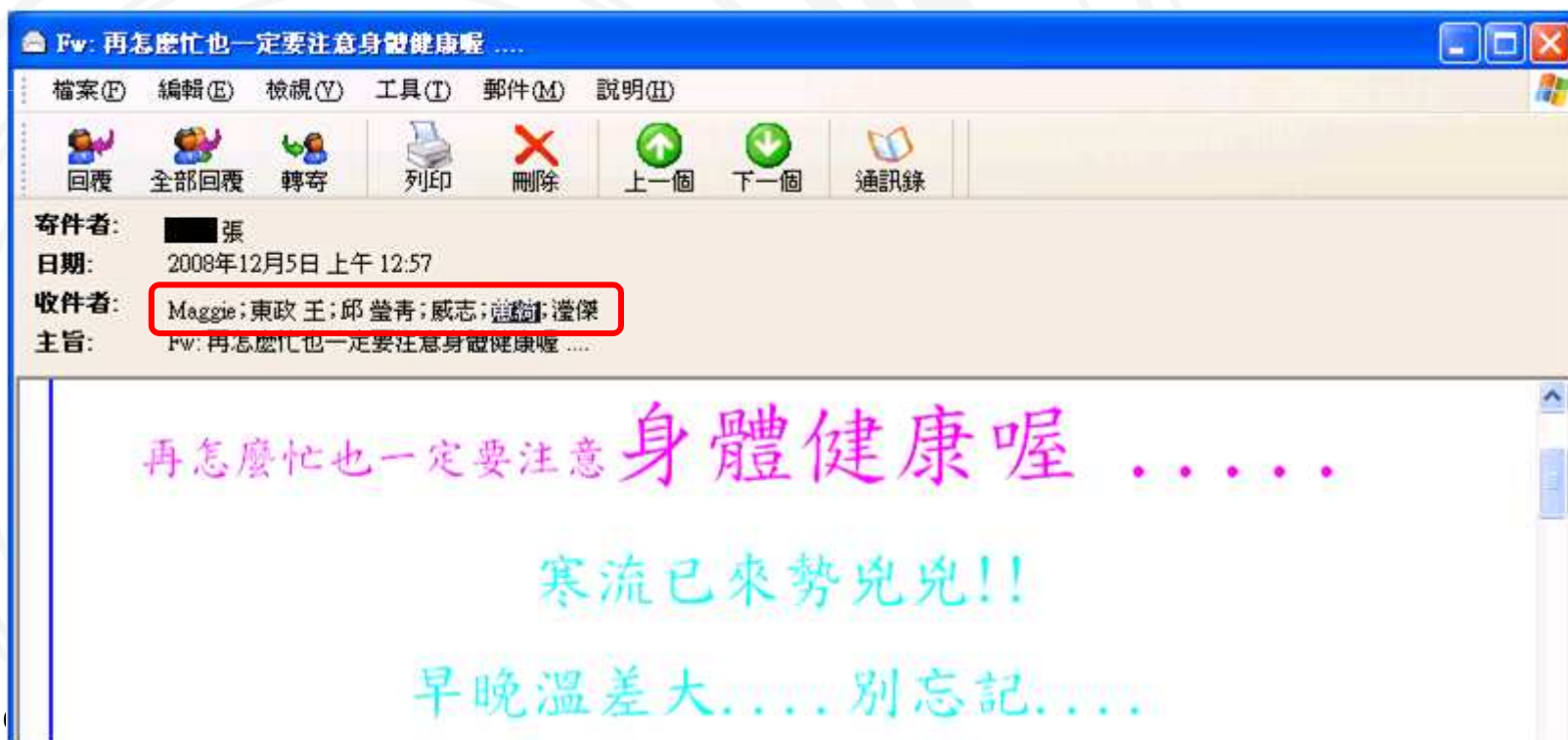
許永生 Commis Hsu

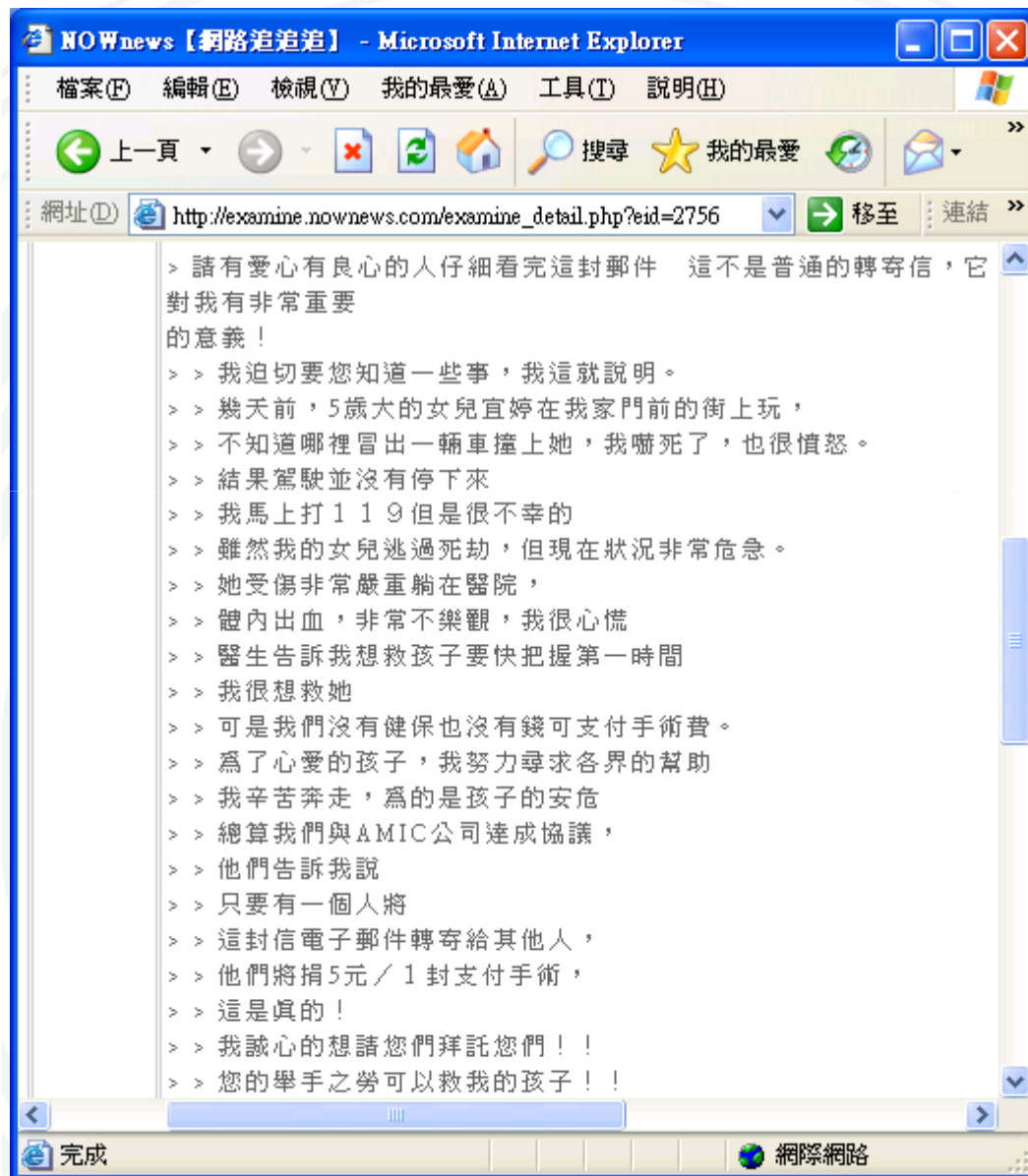
0936-23[REDACTED]

# 郵件轉寄

## 轉寄網路郵件

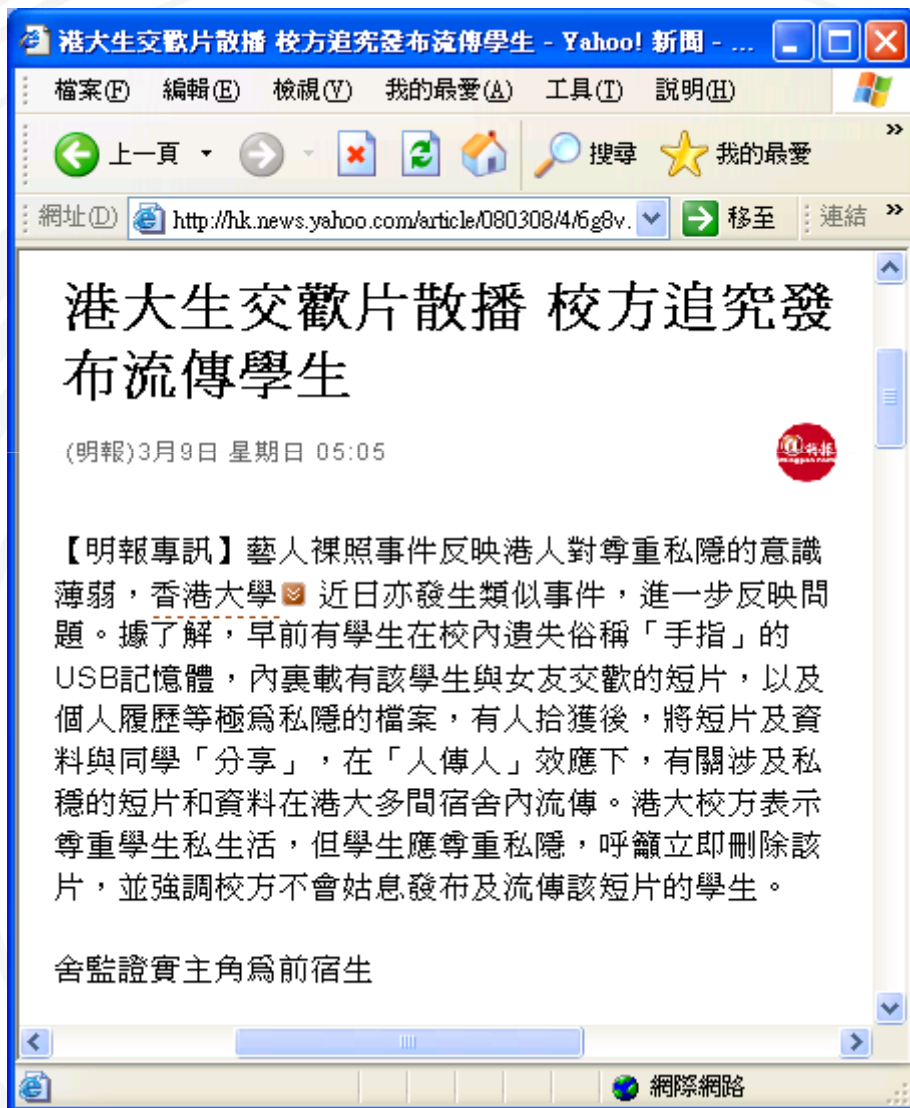
可能沒注意到要保護他人隱私，而外洩了他人的郵件信箱…



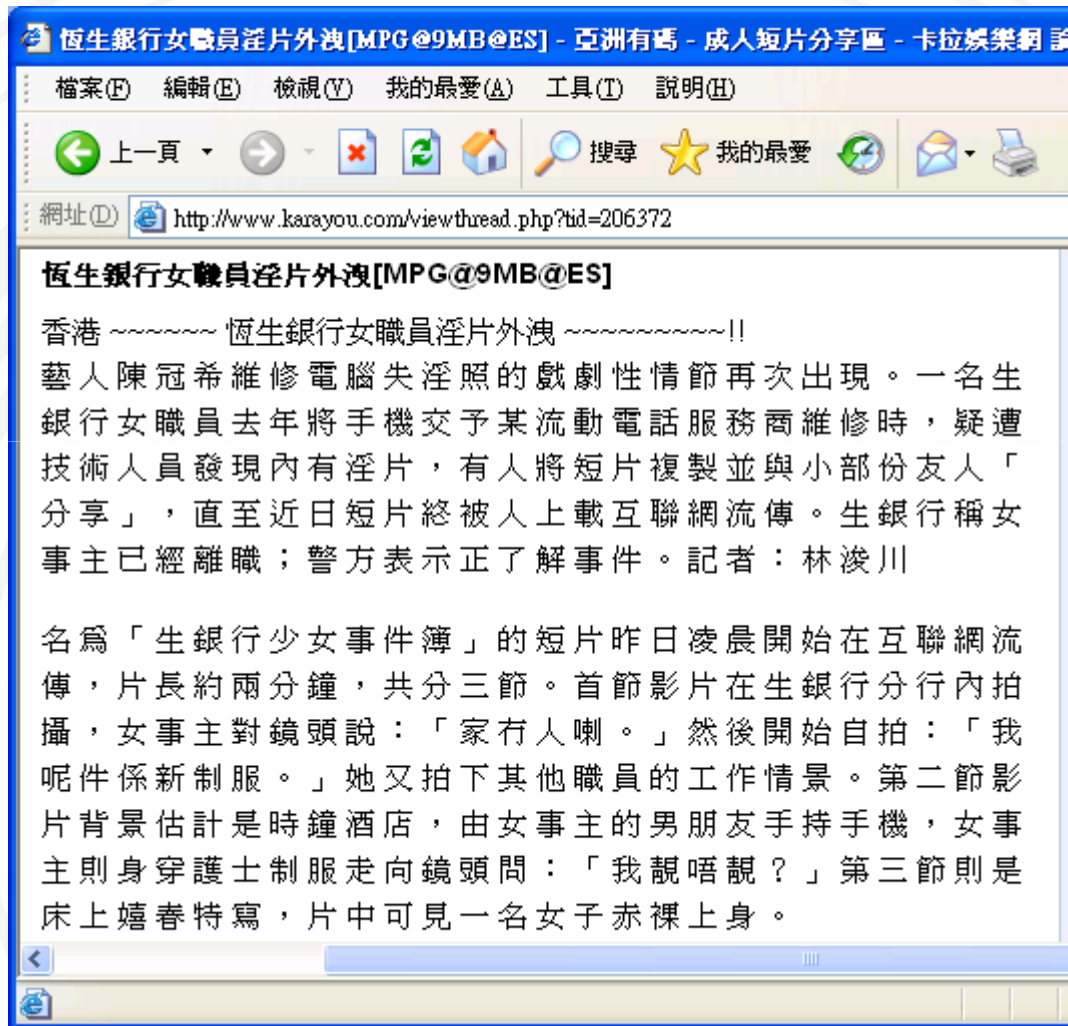


- 號稱您的轉寄贊助捐款，是垃圾郵件業者收集郵件信箱的伎倆
- 您轉寄這些郵件亦只是外流您朋友的郵件信箱

您可能沒有也不曉得，  
下列這些都是您沒有適當保護自己個資與隱私  
的外洩風險…



- 學生在校內遺失USB記憶卡，內載有該學生與女友交歡的短片



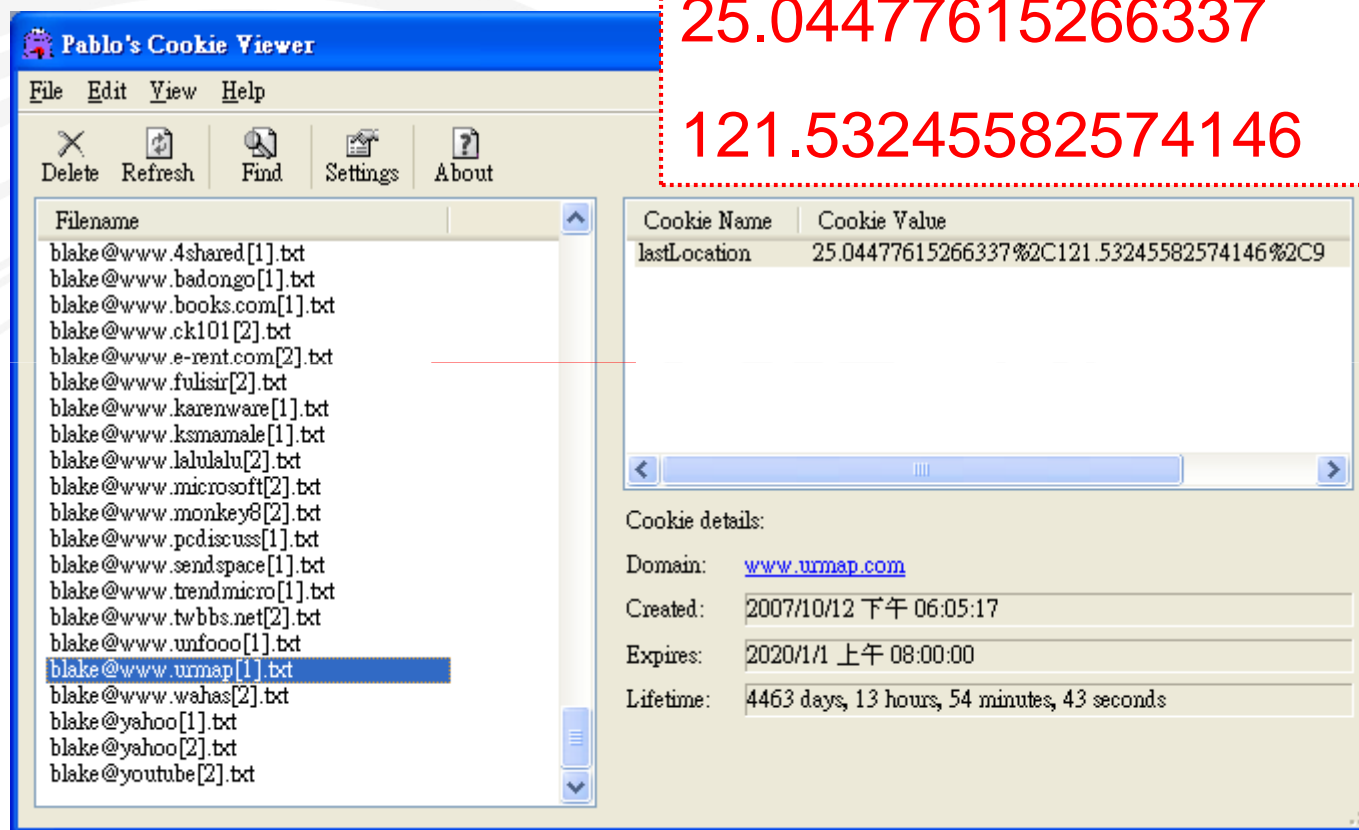
- 將手機交予電話服務商維修，遭技術人員發現內有淫片，將短片複製與友人分享，終被人上載網路流傳



## cookie說明

- Cookie是存在瀏覽器中的小型文字檔，記錄使用者瀏覽網頁的資訊，例如網站網址、使用者曾經輸入的資訊等

# 查詢cookie



The screenshot shows the 'Pablo's Cookie Viewer' application. The main window displays a list of cookies with the filename 'blake@www.urmap[1].txt' selected. To the right, the 'Cookie Name' and 'Cookie Value' are shown as 'lastLocation' and '25.04477615266337%2C121.53245582574146%2C9' respectively. A red dashed box highlights the IP address components '25.04477615266337' and '121.53245582574146' from the cookie value. Below the cookie list, the 'Cookie details' section provides information for the selected cookie.

Cookie Name	Cookie Value
lastLocation	25.04477615266337%2C121.53245582574146%2C9

Cookie details:

Domain: [www.urmap.com](http://www.urmap.com)

Created: 2007/10/12 下午 06:05:17

Expires: 2020/1/1 上午 08:00:00

Lifetime: 4463 days, 13 hours, 54 minutes, 43 seconds

# UrMap是一個電子地圖瀏覽網站

UrMap你的地圖網 - Microsoft Internet Explorer

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

上一步 一步 搜尋 我的最愛

網址(D) http://www.umap.com/ 移至 連結 >>

UrMap 你的地圖 縮空機車 搜尋

全部搜尋 僅道路 僅交叉路口 僅地標 Beta版新首頁

開/關搜尋列 列印 郵寄 網頁連結 回到原查詢點 測量距離 地址回報(新增地址) NEW UrMap Blog 開/關搜尋列

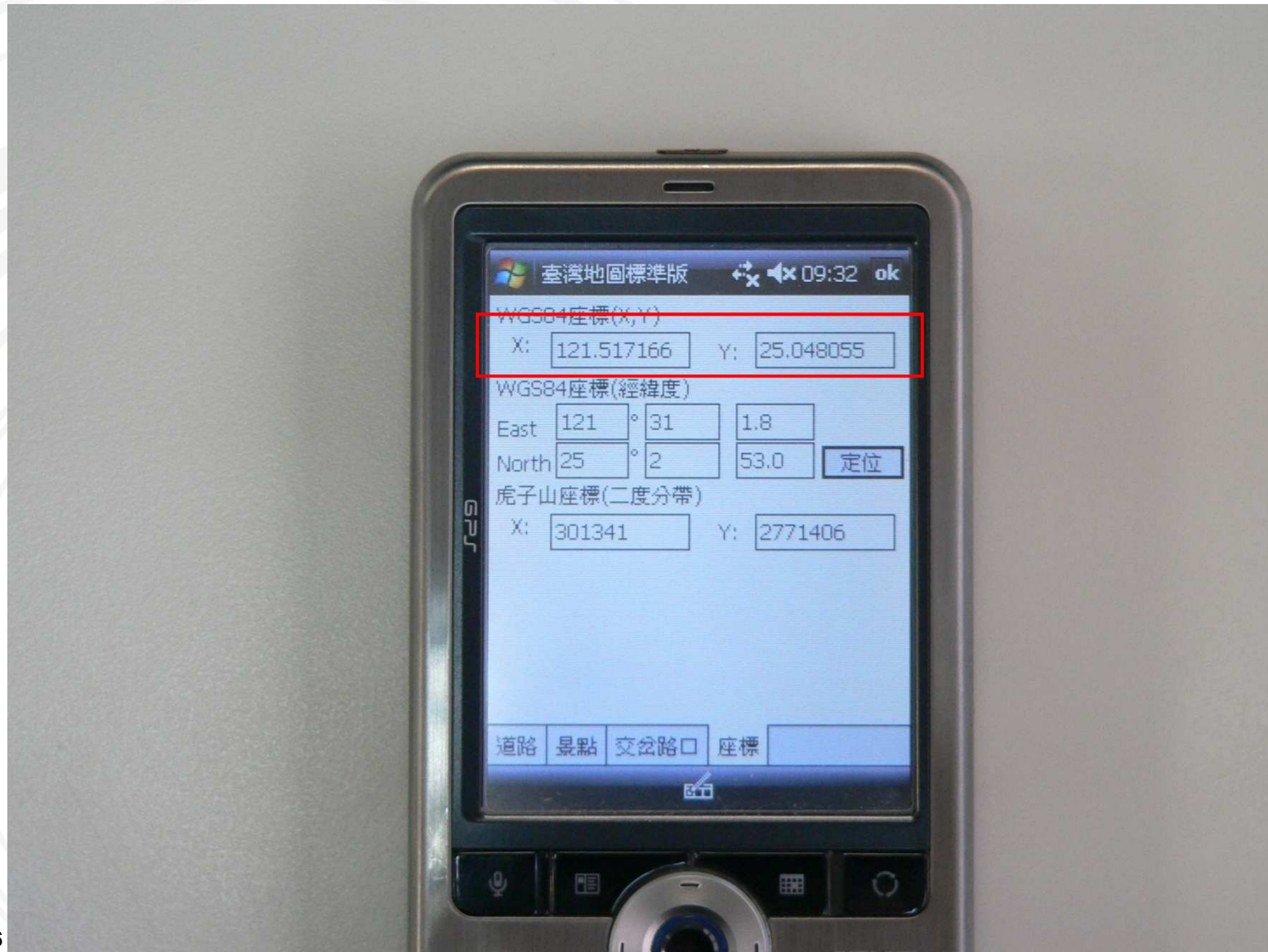
地標 搜尋結果 精彩內容 導航

地標(7)

本站內容版權所有，轉載請與 友通科技 聯絡 福衛二號影像由 國家太空中心 與 台灣師範大學 授權，向量圖資由 九福科技 提供 Copyright©2005 OleMap Inc. 2

網際網路

# 輸入cookie的資訊作查詢



# 表單資料與密碼

- Internet Explorer提供了功能，記住曾經在瀏覽器中輸入的表單及密碼等資料

# 自動記錄登入資料的風險

Windows Internet Explorer  
http://forum.ruten.com.tw/replylist.php?article=2169289

隱藏

請露天拍賣停掉我的帳號~  
帳號1:annac [redacted] 帳號2:pinkbea [redacted]

因為家中電腦壞掉,所以我現在都到外面的公用電腦上網~但是貴站的系統卻會記錄帳號與密碼,也就是我現在已經處在危險之中~我的帳號很容易被有心人士所利用,但~貴站卻沒有電話可供連繫~無法在第一時間做最快速的處理~所以~我只好在此留言~

【討論】 RE:請露天拍賣停掉我的帳號~  
帳號: ~ω~焦糖小兔~ω~ 張貼時間: 2008/04/02 10:30:41 我要回應

哈囉《貓貓》~

小兔已請相關處理人員協助將您的帳號進行停權動作,請您確認看看喔~

~ω~焦糖小兔~ω~

△TOP | 回話題列表

完成 網際網路 100%

因為家中電腦壞掉，所以我現在都到外面的公用電腦上網..

## 暫存檔案說明

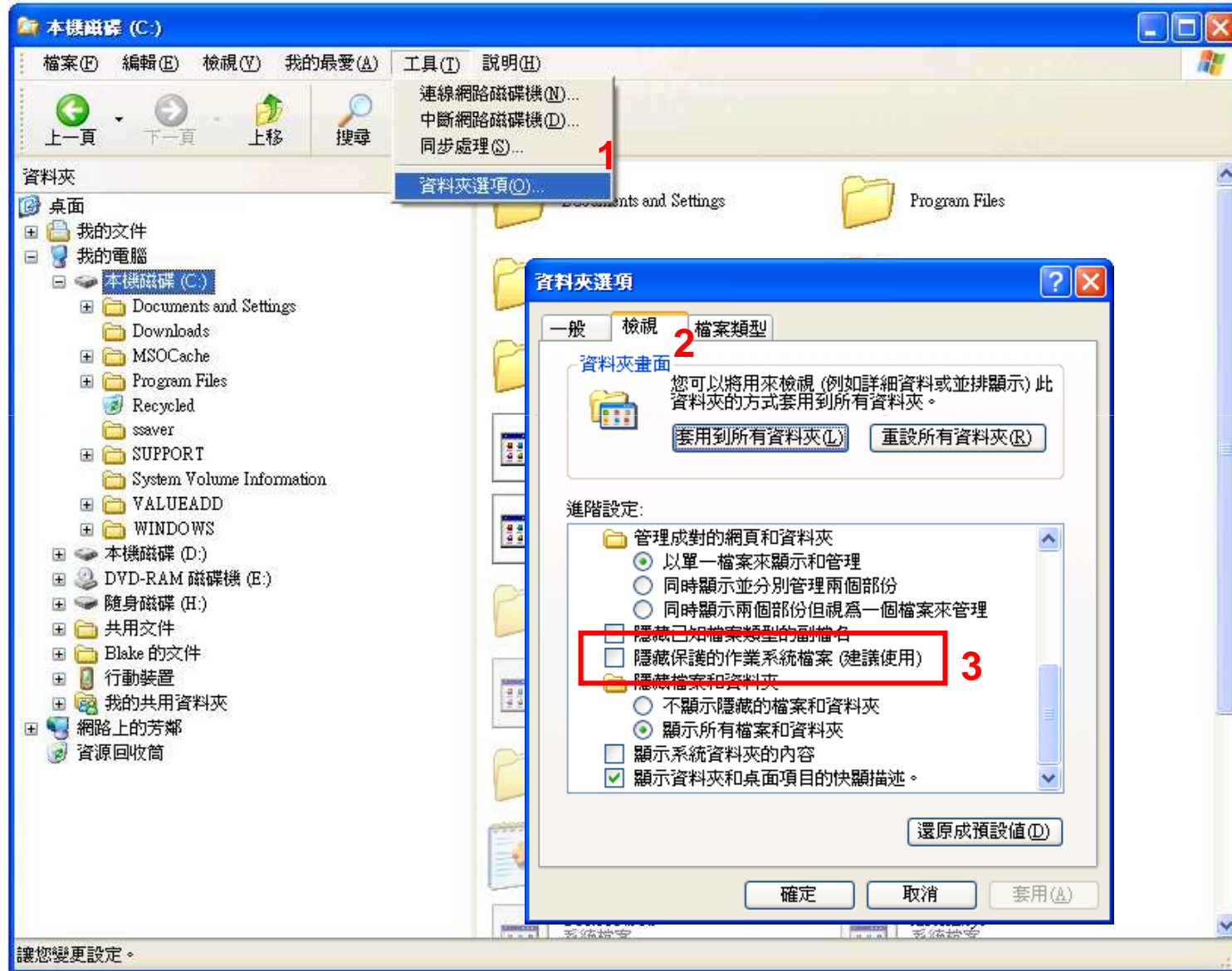
- 爲了更快速地檢視而儲存的網頁、影像和媒體複本

# 參訪網站 (1/3)

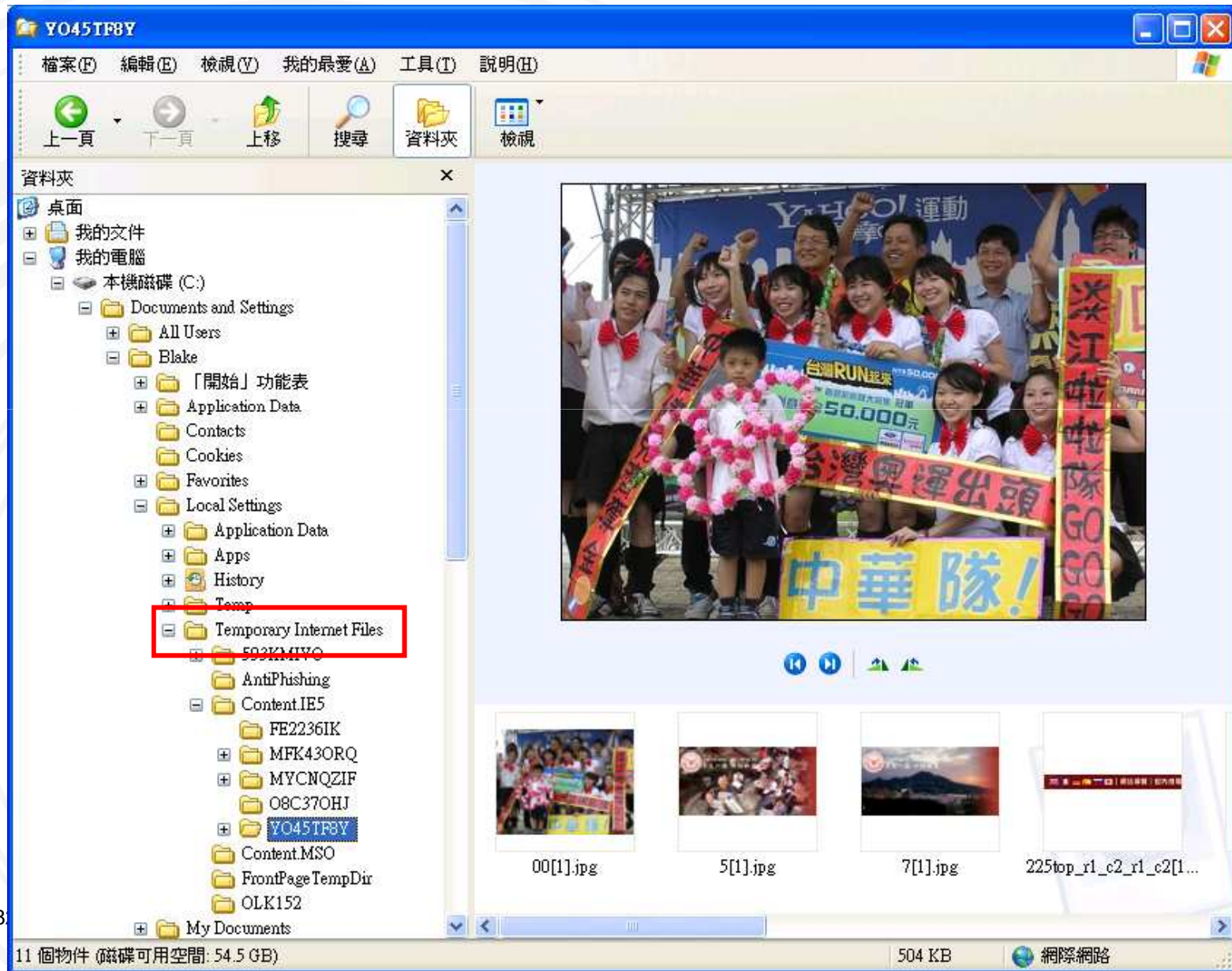




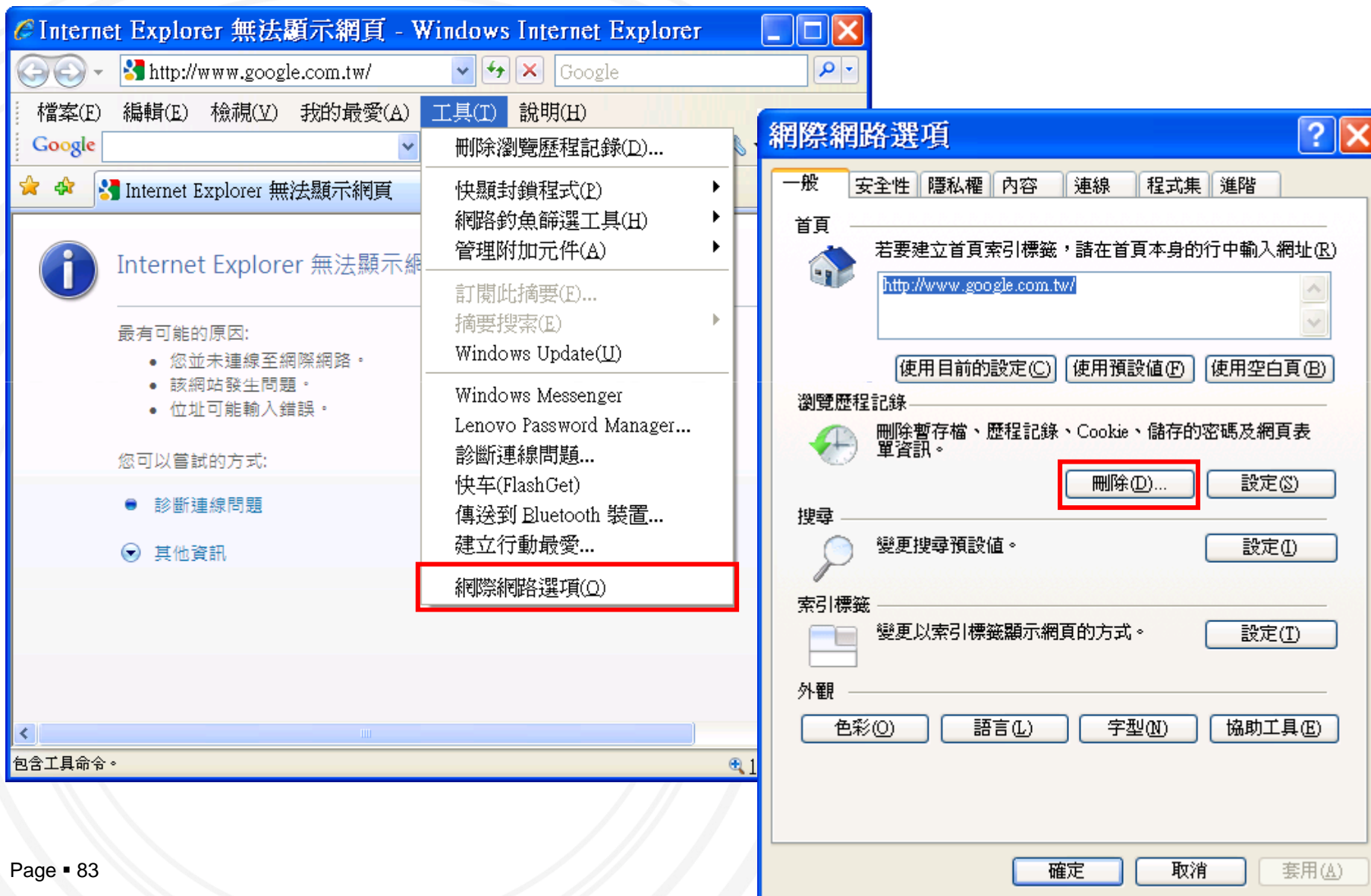
# 將隱藏的系統檔案設定顯示 (2/3)



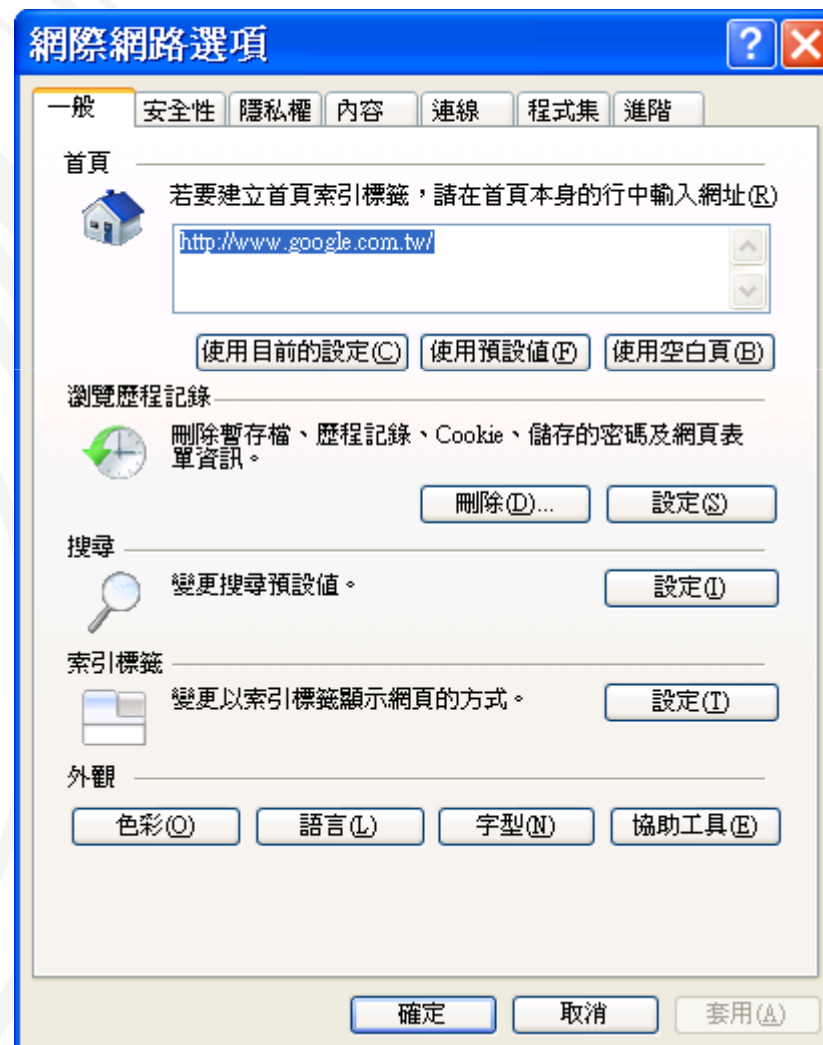
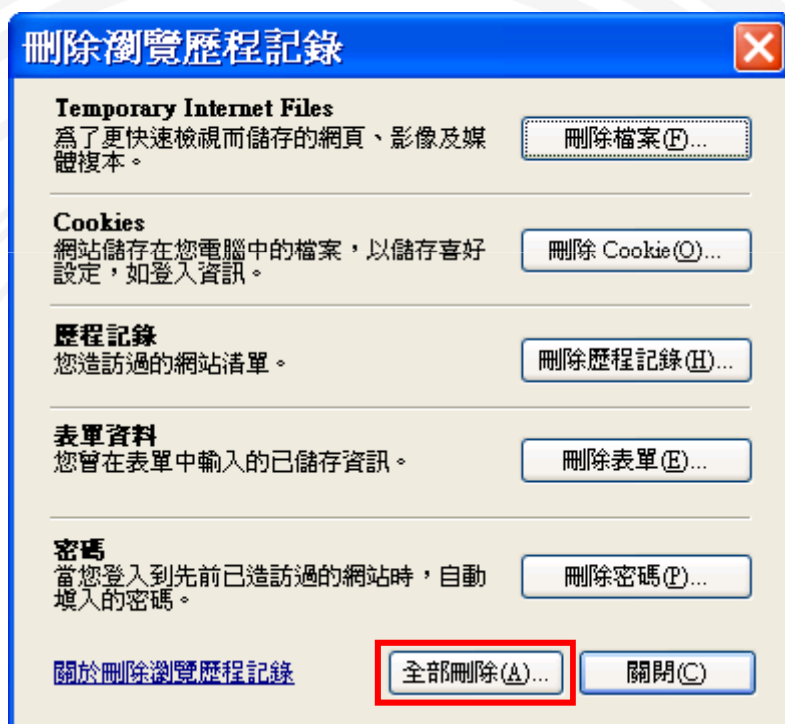
# 電腦上的暫存檔 (3/3)



# 清除檔案



# 清除檔案






# 啓用快顯封鎖

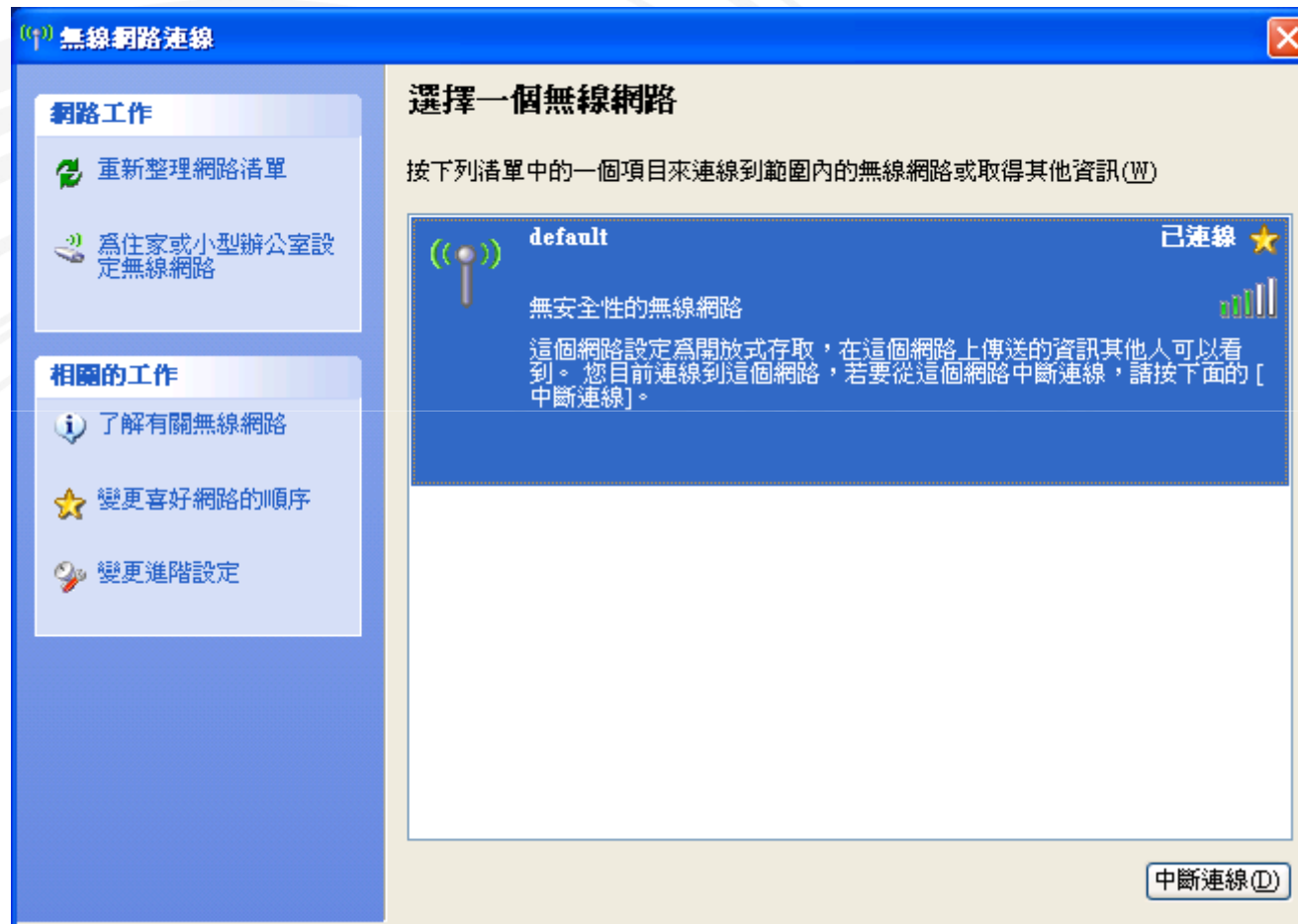
The image shows a Windows Internet Explorer browser window with the address bar set to <http://www.google.com.tw/>. The 'Tools' menu is open, and 'Internet Options' is highlighted with a red box. The 'Internet Options' dialog box is also open, with the 'Privacy' tab selected. The 'Privacy' slider is set to '中' (Medium). Below the slider, the following text is displayed:

- 封鎖缺乏簡潔隱私權政策的第三方 Cookie
- 封鎖那些沒有明確許可就儲存您的連絡資訊的第三方 Cookie
- 限制那些沒有明確許可就儲存您的連絡資訊的第一方 Cookie

At the bottom of the dialog box, the '快顯封鎖程式' (Pop-up Blocker) section is visible. The checkbox '開啓快顯封鎖程式(B)' (Enable pop-up blockers) is checked and highlighted with a red box. Other buttons like '確定' (OK), '取消' (Cancel), and '套用(A)' (Apply) are also visible.

點選彈跳廣告視窗內的超連結與按鍵，  
使用視窗右上角的    關閉視窗

# 沒有加密無線網路...



# 嘗試連線基地台...

Setup - Microsoft Internet Explorer

OFF RETURNIL

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

← 上一頁 → 搜尋 我的最愛

網址(D) http://192.168.0.1/home.htm 移至 連結 >>

level one

## Wireless BroadBand Router

**WAN Wizard**

- [LAN](#)
- [Wireless](#)
- [Password](#)
- [Status](#)
- [Advanced](#)

**Help**

Log Out

**SCFF44DC**

<b>Internet:</b>	IP Address:	61.229.64.248
	Connection:	PPPoE

---

<b>Wireless:</b>	SSID	default
	WEP:	Off

---

<b>LAN:</b>	IP Address:	192.168.0.1
	DHCP Server:	ON



# 沒有設定基地台密碼...



# Configuration 頁面

**WAN Port Configuration**

**Identification**

Hostname: SCFF44DC

Domain Name: [Redacted]

WAN Port MAC Address: 00c002ff44dd

Default Copy from PC

**IP Address**

- IP Address is assigned automatically (Dynamic IP Address)
- Specified IP Address (Static IP Address)

**DNS**

- Automatically obtain from Server
- Use this DNS [Redacted]. [Redacted]. [Redacted]. [Redacted]

**Login**

Login Method: PPPoE

Login User Name: [Redacted]@hinet.net

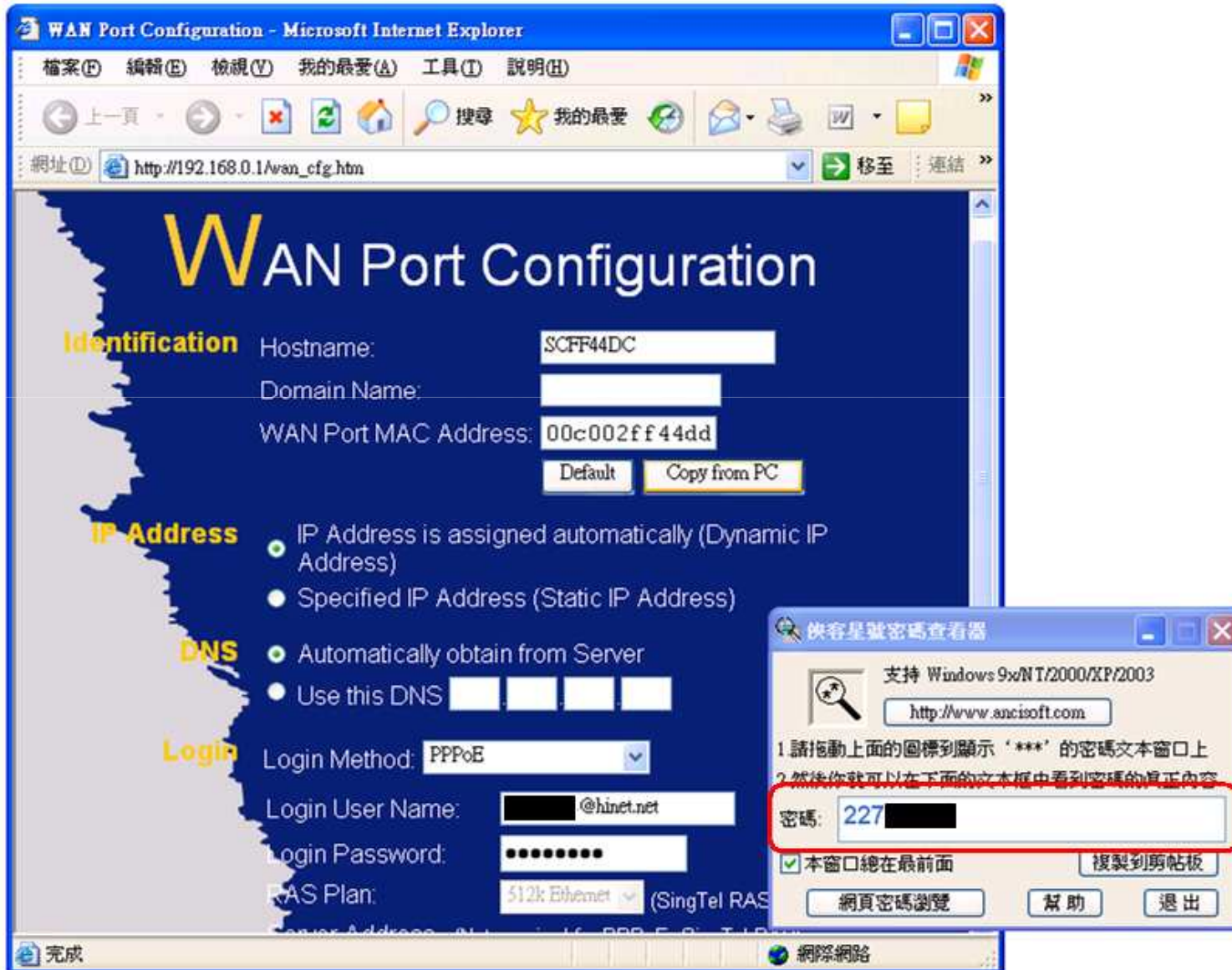
Login Password: [Masked]

RAS Plan: 512k Ethernet (SingTel RAS only)

Server Address: [Redacted]

完成 網際網路

# 破解得到連線密碼...



# 駭客入侵無線網路的問題

- 內部網路安全問題

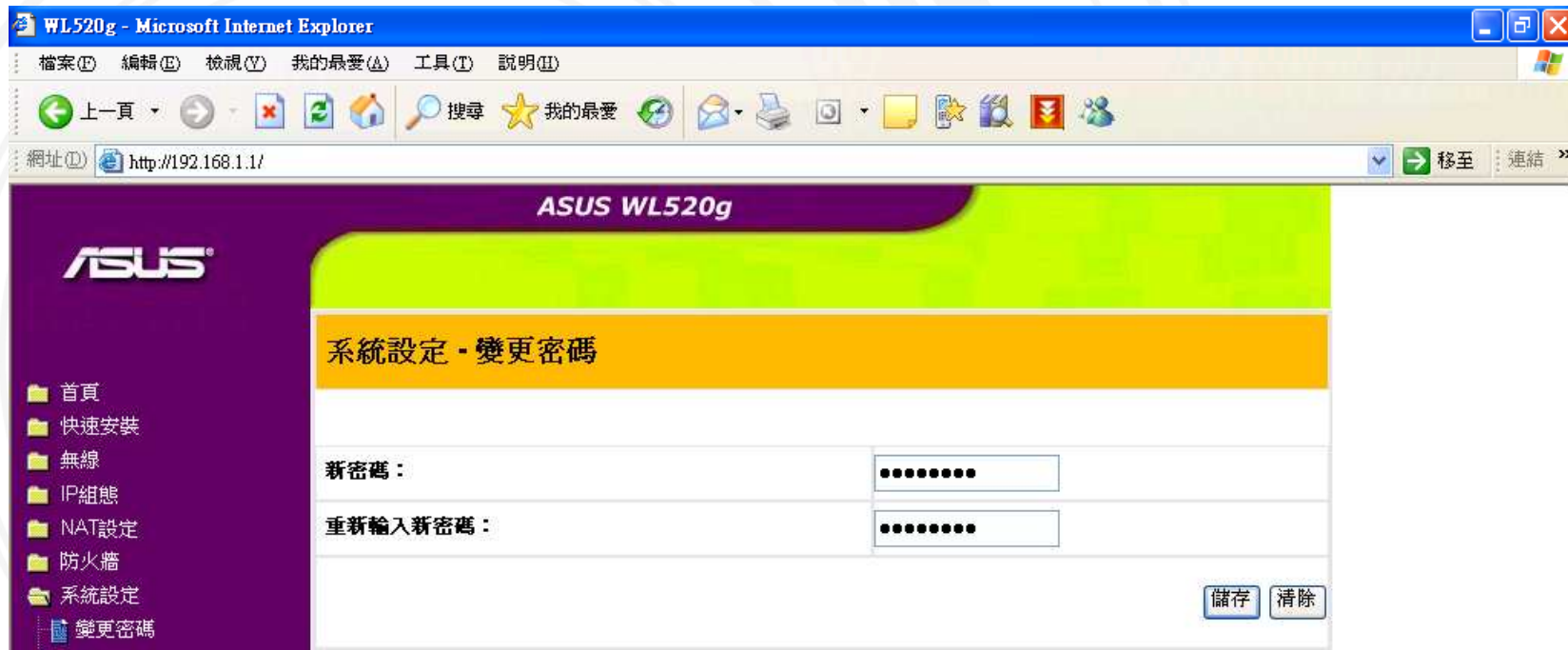
- 駭客與您的電腦處於同一區域網路，可能利用資源共享進行攻擊

- 外部網路安全問題

- 駭客進行犯罪，基地台擁有者成了代罪羔羊

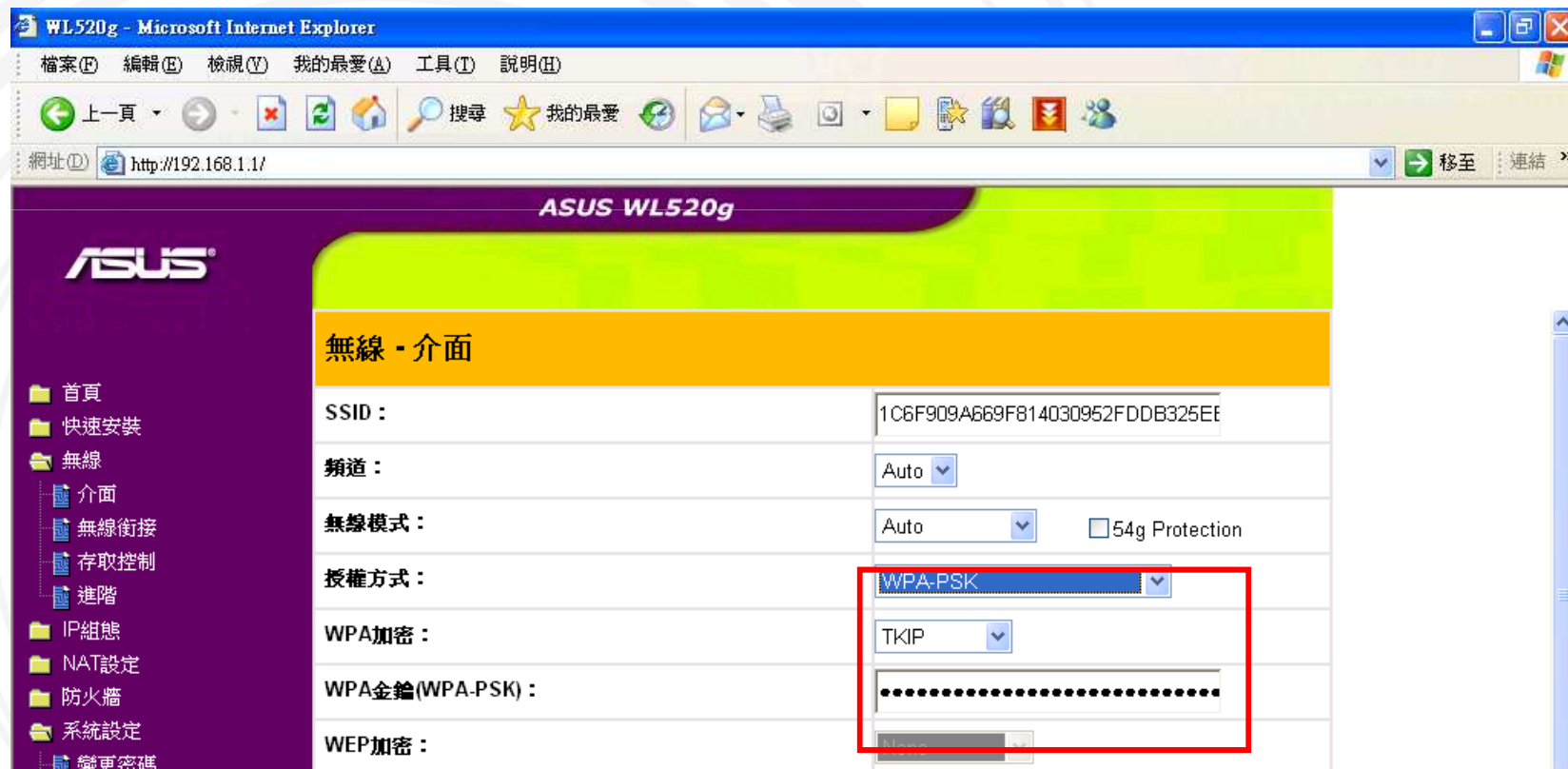
# 無線網路防護(一)

- 設定基地台管理密碼
  - 預設值常是admin/1234
  - 修改無線基地台的預設登入帳號密碼



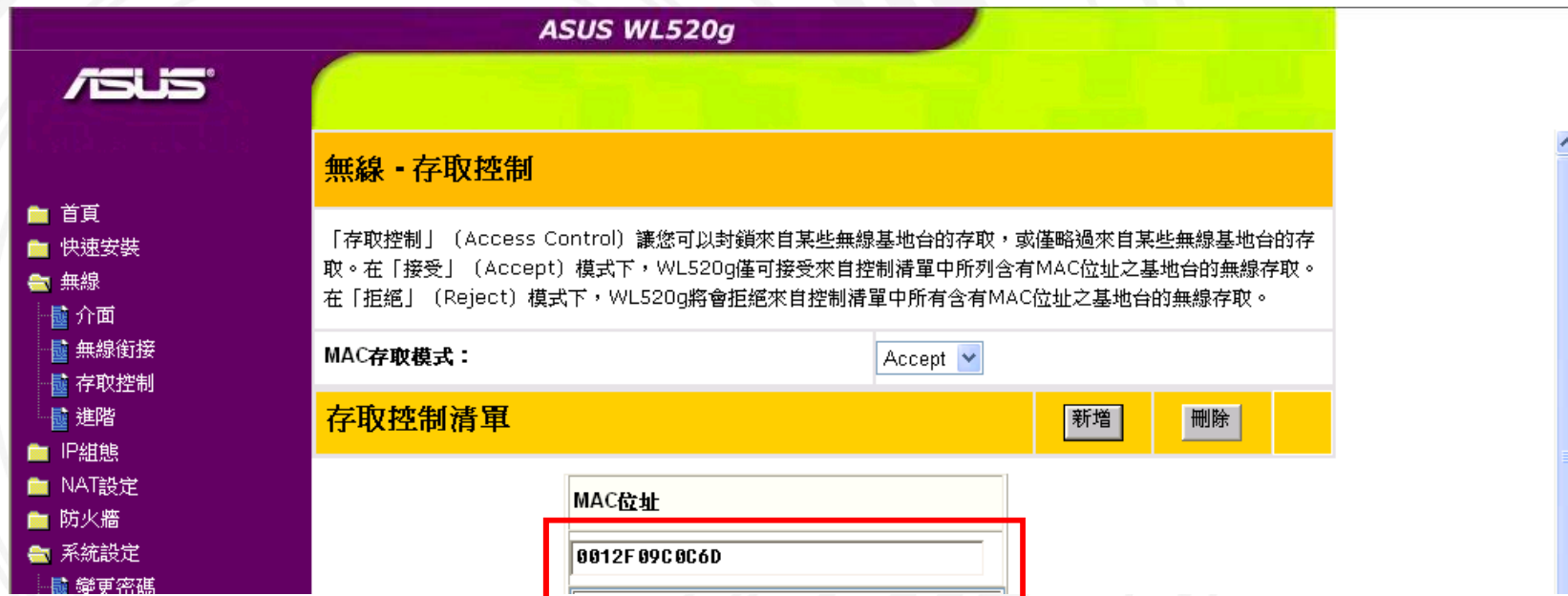
# 無線網路防護(二)

- 設定WPA2加密傳輸



# 無線網路防護(三)

- 鎖定網路卡MAC位址
  - 所有網路卡都有唯一ID，稱為MAC
  - 設定允許連線的MAC位址



# 查詢網路卡MAC...

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Blake>IPCONFIG /ALL

Windows IP Configuration

    Host Name . . . . . : NB
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Mixed
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Ethernet adapter 區域連線:

    Media State . . . . . : Media disconnected
    Description . . . . . : Realtek RTL8139/810x Family Fast Eth
ernet NIC
    Physical Address. . . . . : 00-13-D4-67-A3-B6

Ethernet adapter 無線網路連線:

    Connection-specific DNS Suffix . :
    Description . . . . . : Intel(R) PRO/Wireless 2200BG Network
Connection
    Physical Address. . . . . : 00-12-F0-9C-0C-6D
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address. . . . . : 192.168.1.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1
    DHCP Server . . . . . : 192.168.1.1
    DNS Servers . . . . . : 192.168.1.1
    Lease Obtained. . . . . : 2007年10月23日 上午 10:06:44
    Lease Expires . . . . . : 2007年10月24日 上午 10:06:44

C:\Documents and Settings\Blake>
```



# 無線網路安全注意事項

- 修改無線基地台的預設帳號密碼
- 使用WPA2 連線加密或是啓用MAC控管
  - 多一層防護多一層入侵的障礙
- 啓用日誌 (Log) ，定期查看
- 良好的使用習慣
  - 沒加密的無線網路環境，避免使用登入帳號密碼的服務

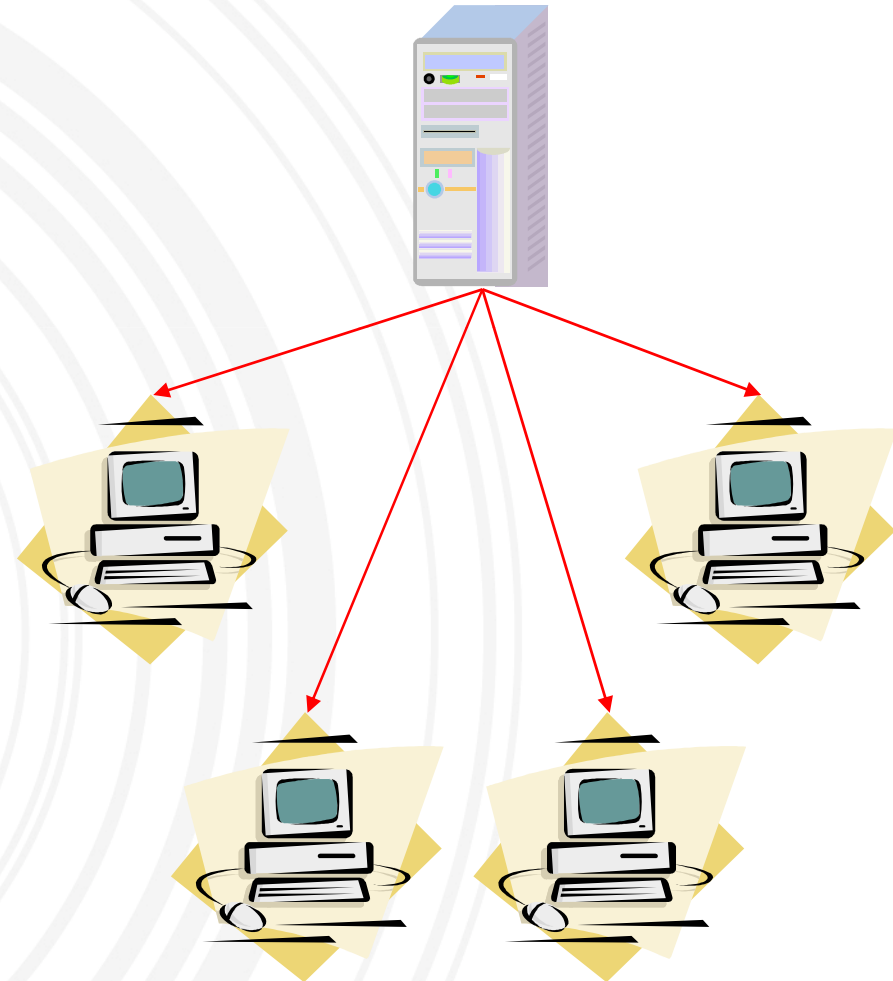
# 常見的P2P程式

- 即時通訊軟體
- eDonkey
- eMule
- Foxy
- BitTorrent / BitComet
- Clubbox / GOGOBOX
- Kuro / ezPeer

分享加速式檔案下載

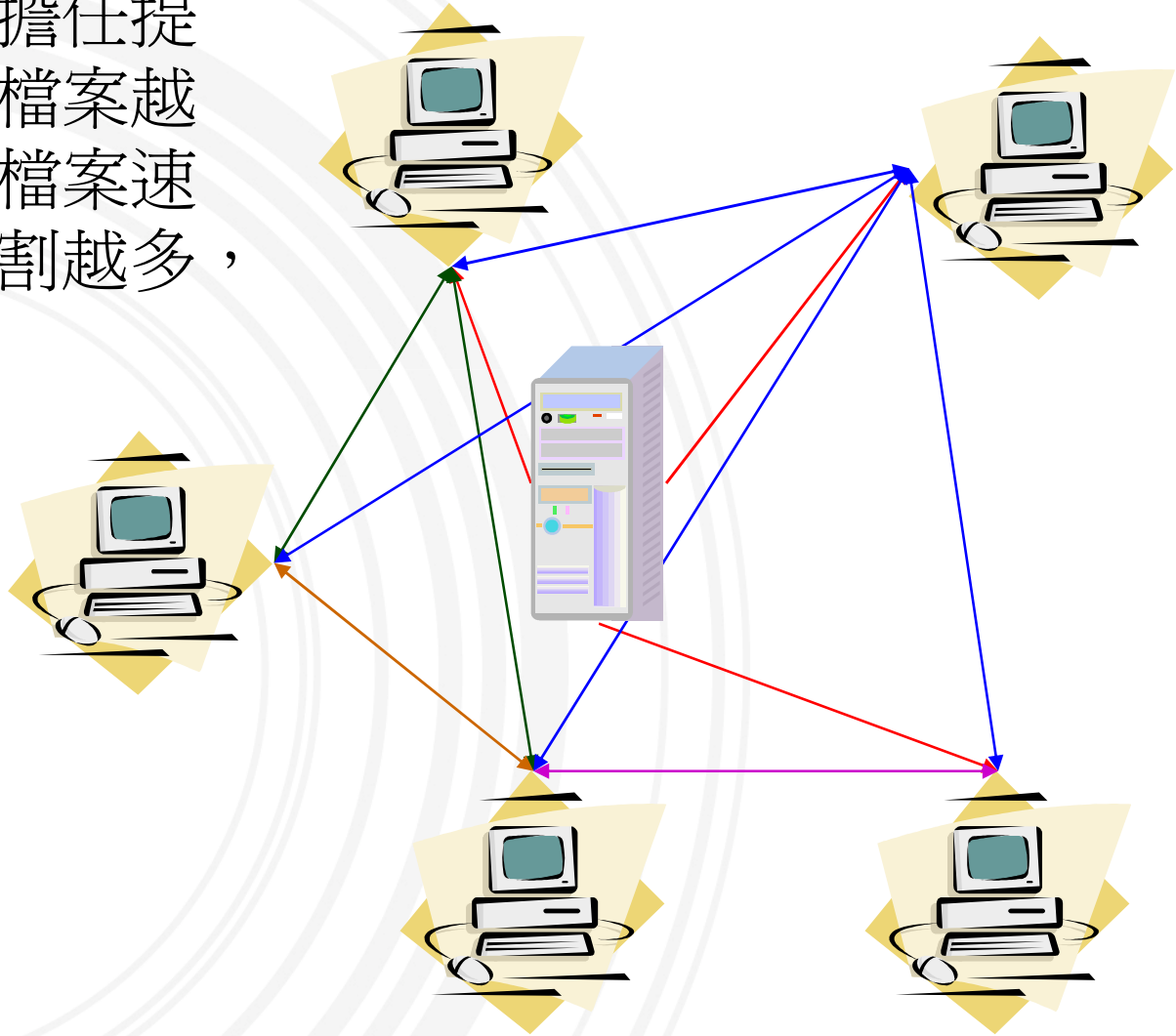
# 傳統伺服器下載

- 使用者由伺服器下載檔案，多使用者同時下載檔案時會因頻寬分用，下載檔案速度會變慢



# P2P網路下載

- 每一個使用者同時擔任提供檔案角色，某一檔案越多人下載時，下載檔案速度會因檔案分段切割越多，速度越快



# 使用P2P軟體可能衍生的問題

- 任意使用各種P2P軟體下載盜版軟體、電影與音樂等
- 使用不當造成電腦內資料外洩
- P2P網路上散播的惡意程式造成電腦中毒
- 佔用區域網路連外頻寬

## 關於Foxy

- 該軟體在分享資料夾的設定上容易讓使用者誤設為整台電腦全部分享
- 該軟體亦容易被植入木馬，資料外洩情況最嚴重



## Foxy資料外洩事件

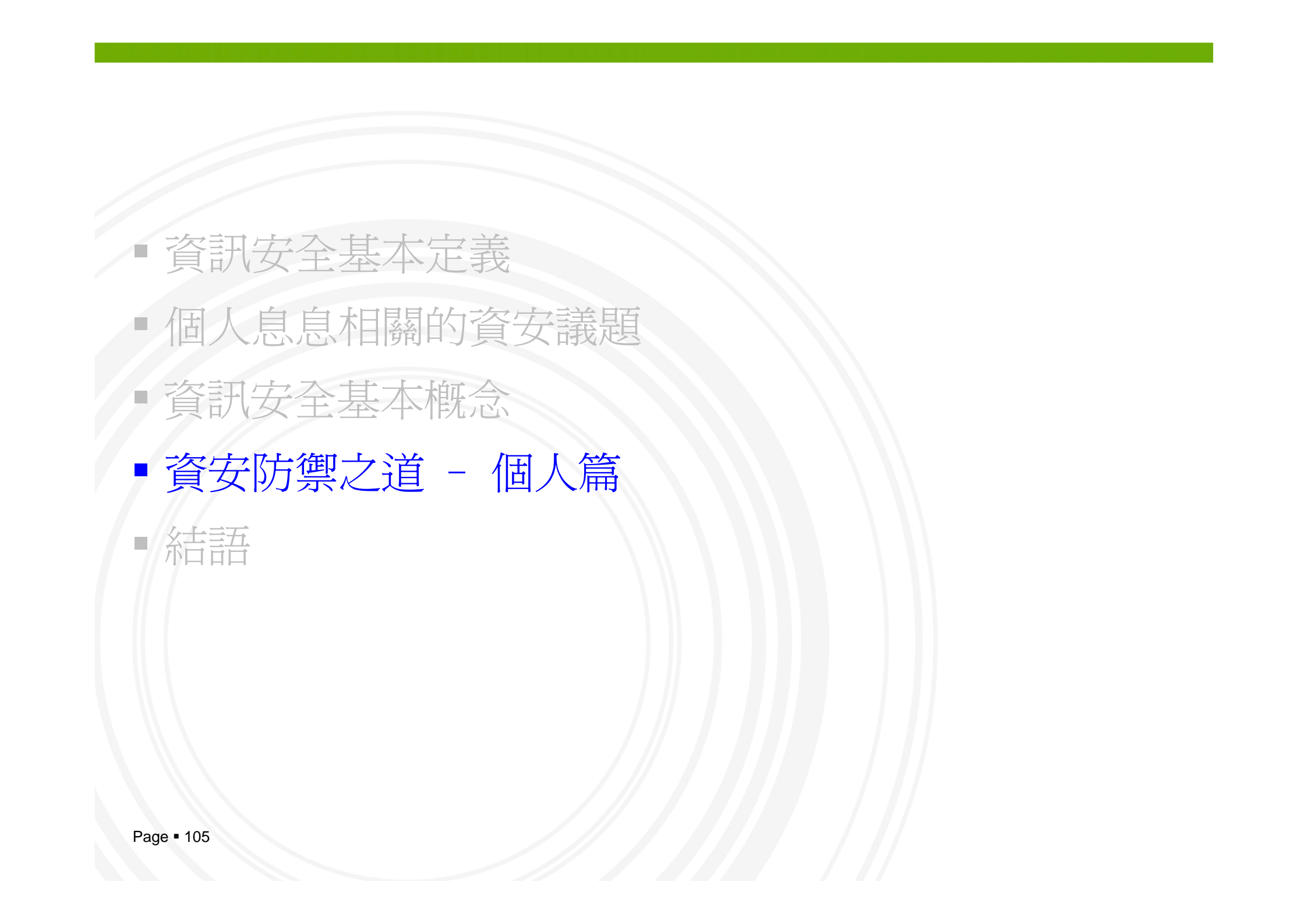
- 2007年4月，警察機關因員警違規使用P2P分享軟體，導致內部筆錄外洩
  - 在新聞熱潮下，部分以「刑案筆錄」等文字為檔名的假檔案藉機散播
- 檔名與實際內容不符的假檔案在P2P網路上相當常見

# Skype的資安威脅



- 竊聽木馬，針對Skype竊聽。
- 電腦被植入這個木馬，任何通話內容會以MP3檔的形式存於電腦，再傳送給駭客



- 
- 資訊安全基本定義
  - 個人息息相關的資安議題
  - 資訊安全基本概念
  - 資安防禦之道 - 個人篇
  - 結語

# 員工的資料保護安全認知 (1/5)

## 重視個人帳號的密碼安全

- 帳號密碼為身份驗證的基本防護，務必重視密碼保護並設定強度足夠的安全密碼
- 在工作場所之外的電腦登入使用系統，須留意是否為安全的使用環境並確認密碼無外洩之虞

## 員工的資料保護安全認知 (2/5)

### 注意敏感資料的保護

- 適當保護敏感資料，例如將文件加密或設定開啓密碼
- 遵守組織的保密規定及遵行各項使用規範
- 提供資料供公開查閱，須確認是否有民眾敏感資料（例如身份證字號、通訊資料等）被不當暴露

## 員工的資料保護安全認知 (3/5)

### 遵循公司的電腦使用規定

- 工作電腦的使用，應遵循組織的電腦使用規定
- 即使工作電腦的使用權限允許安裝軟體，亦必須合乎組織資訊安全規定、軟體使用規範與法令

# 員工的資料保護安全認知 (4/5)

## 防範網路詐騙攻擊

- 仔細辨視網址列上的網址，詐騙網頁常使用一些易混淆的字母來偽裝誘騙
- 當點擊的網址為原網站的外部連結時，應格外提高警覺
- 不要因為好奇心任意點擊情色、聳動等標題的網址連結
- 網頁、電子郵件畫面上顯示的連結網址，可能造假。可將游標停留在該連結，左下方會出現真實的連結網址，可確認該連結是否為真
- 電子郵件夾帶副檔名.exe、.com、.bat等檔案，幾乎都是惡意程式，不要開啓

# 員工的資料保護安全認知 (5/5)

## 工作帶回家可能致生的資料外洩風險

- 除非組織規定允許，否則不應將公務資料帶回家
- 如果必須將公務資料帶回家處理，應確認家中電腦亦有適當的安全防護，例如啓用防火牆、安裝防毒軟體並更新最新病毒碼、更新系統修補程式等
- 若使用家中電腦處理公務資料，應儘量保持為較安全的使用環境，例如不要安裝P2P軟體，甚至離線作業
- 儲存重要資料的外接式儲存媒體應小心保管
- 個人慣用的筆記型電腦常存有個人、公務資料，應特別留意保管，勿讓宵小有機可乘

2010年，美國《紐約時報》一篇報導指出，  
網路安全公司Imperva公布了一份統計資料，  
分析了被駭客入侵竊取的某網站會員帳號密碼，  
在三千兩百萬個密碼中，

最多使用者使用的密碼是「123456」，  
有高達1%的會員使用！

• 第二至十名

2) 12345

3) 123456789

4) password

5) iloveyou

6) princess

7) rockyou

8) 1234567

9) 12345678

10) abc123

• 第十一至二十名

11) nicole

12) daniel

13) babygirl

14) monkey

15) jessica

16) lovely

17) michael

18) ashley

19) 654321

20) qwerty



這些容易記憶的簡單數字密碼，就是「**懶人密碼**」

雖然方便記憶，卻也容易遭駭客破解！

常見的懶人密碼除了簡單數字外，還包括：

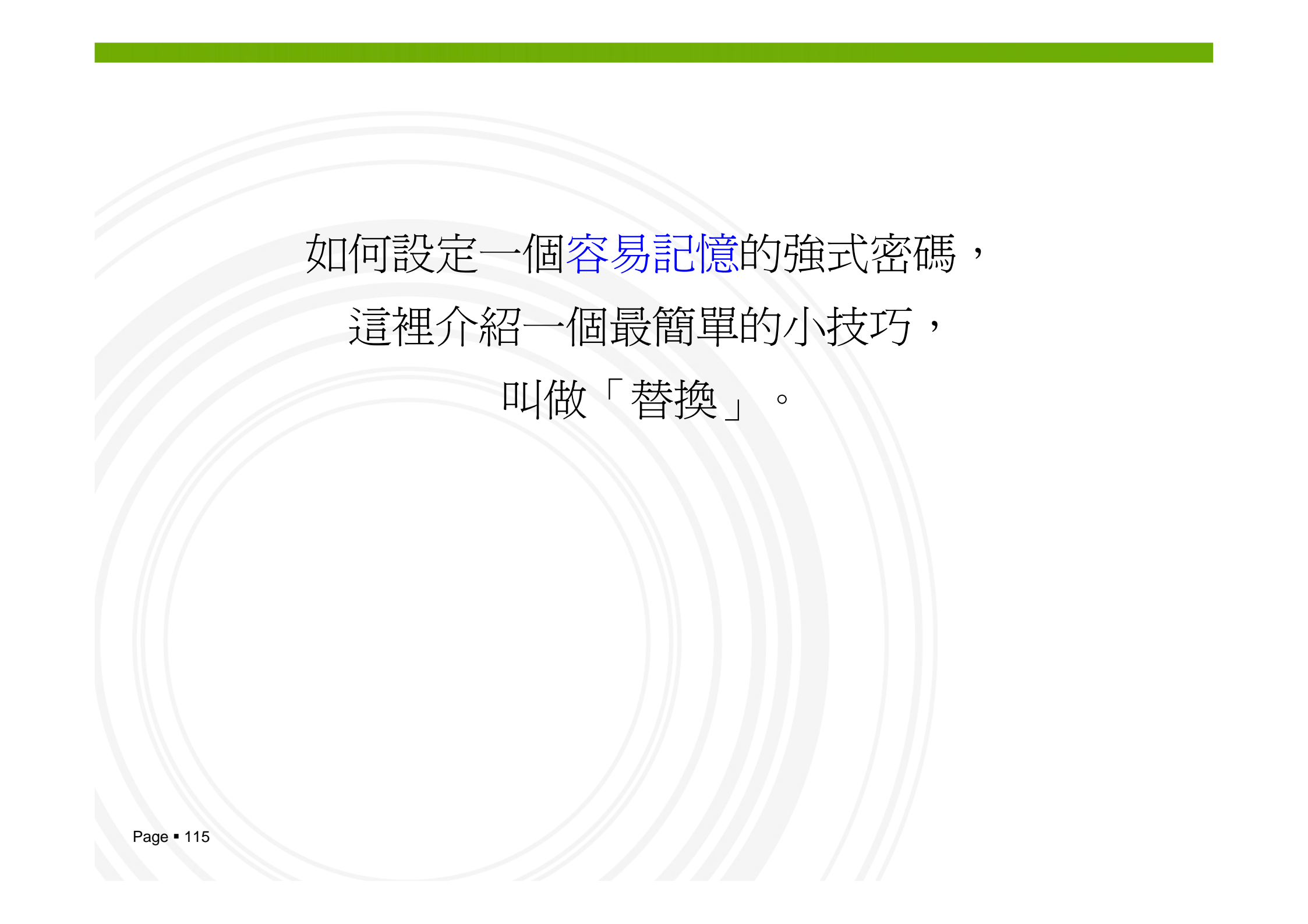
- 1) 自己的英文名、生日、電話等個人資料
- 2) 與帳號相同
- 3) 簡單的連續英文字元，例如aaaa
- 4) 簡單的英文字元加數字，例如abc123
- 5) 電腦鍵盤上的連續字元，例如asdf、qwerty
- 6) 單字或簡單詞語，例如上述的password與iloveyou

# 正確的密碼設定

- 1) 不使用個人資料
- 2) 不使用有意義的單字
- 3) 結合大小寫英文、數字和特殊符號

越長的密碼長度當然亦越難被破解，  
建議密碼最少為八個字元。

包括大小寫英文、數字和特殊符號的  
八個字元以上密碼，  
即稱為「強式密碼」



如何設定一個容易記憶的強式密碼，  
這裡介紹一個最簡單的小技巧，  
叫做「替換」。

# 替換(一)

- 1) 首先選擇一個容易記憶的單字，例如「powerpoint」
- 2) 設計您的替換原則，例如英文「o」替換為數字「0」、英文「i」替換為數字「1」
- 3) 這樣即產生出一個結合英文和數字的密碼  
「p0werp01nt」

## 替換(二)

- 1) 同樣選擇一個單字，例如「password」
- 2) 設計替換原則，例如英文「a」替換為符號「@」、英文「s」替換為符號「\$」
- 3) 產生出一個結合英文和符號的密碼「p@\$sword」

## 替換(三)

- 1) 選擇一個單字，例如「facebook」
- 2) 設計包括數字和符號的替換原則，例如英文「o」替換為數字「0」、英文「a」替換為符號「@」
- 3) 再將奇位數的小寫英文字元替換成大寫英文字元
- 4) 替換後的結果為「F@CeB00k」，即為一個包括大小寫英文、數字和特殊符號的強式密碼了

不要只用一組密碼，  
至少使用兩至三組密碼，

可設定不同重要群組的使用密碼，例如：

- 1) 低重要性群組的密碼：論壇、網站會員…
- 2) 中重要性群組的密碼：郵件、網路空間…
- 3) 高重要性群組的密碼：網路銀行…

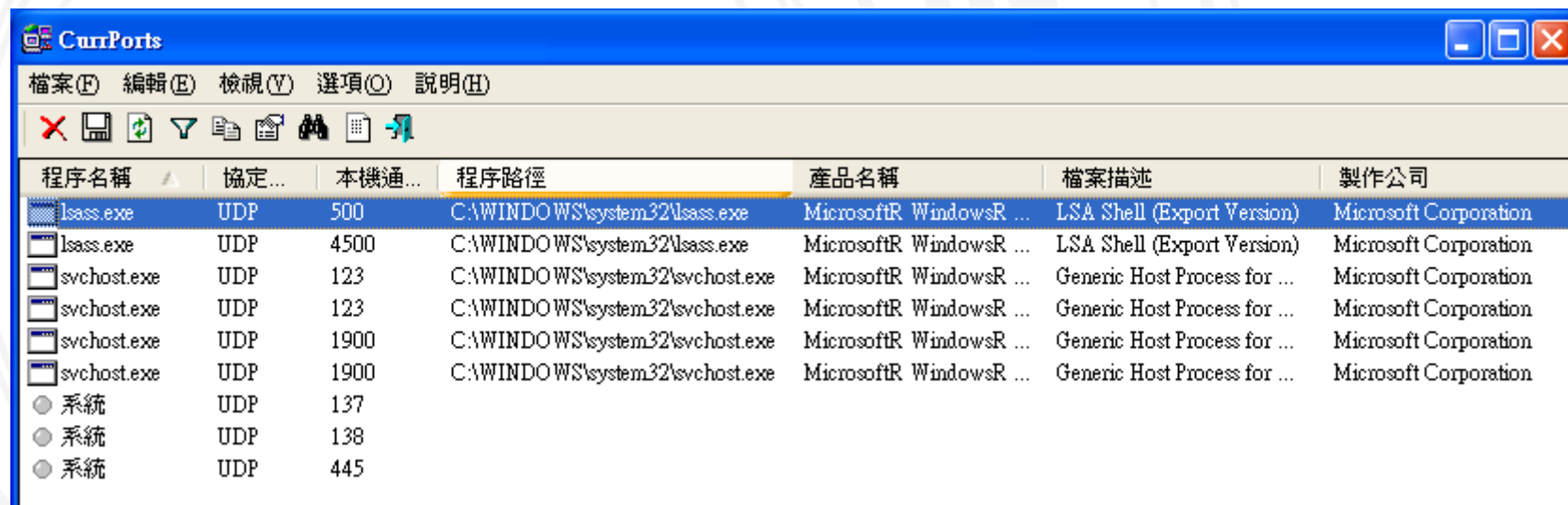
# 監控網路連線工具

## ■ CurrPorts

- 監控電腦上各個通訊埠連線情況

- 綠色軟體

- <http://azo-freeware.blogspot.com/2007/09/currports-130.html>



The screenshot shows the CurrPorts application window with a menu bar (檔案(F), 編輯(E), 檢視(V), 選項(O), 說明(H)) and a toolbar. The main area displays a table of active network connections.

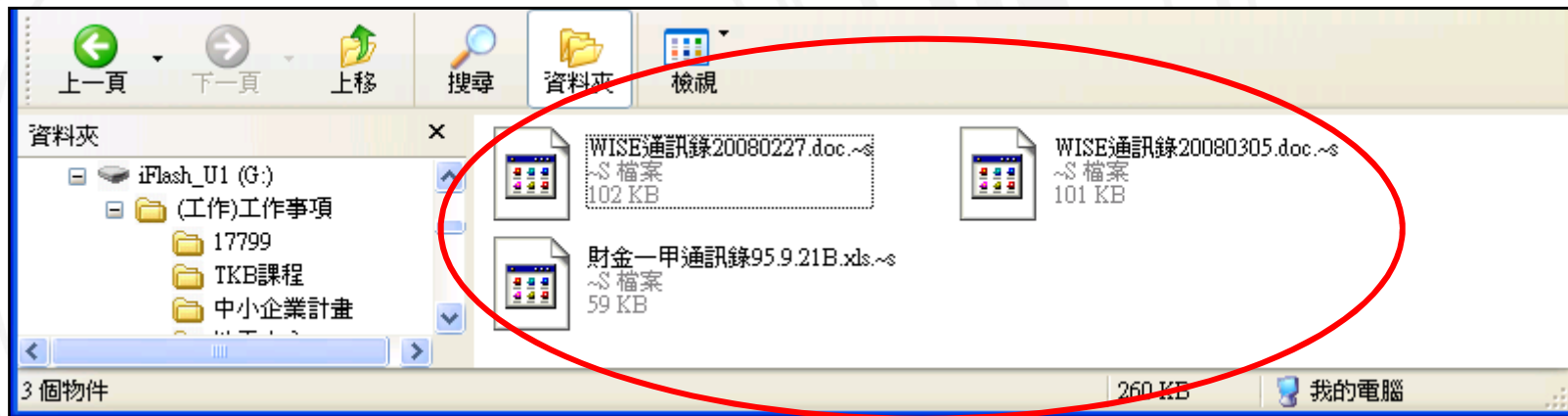
程序名稱	協定...	本機通...	程序路徑	產品名稱	檔案描述	製作公司
lsass.exe	UDP	500	C:\WINDOWS\system32\lsass.exe	Microsoft WindowsR ...	LSA Shell (Export Version)	Microsoft Corporation
lsass.exe	UDP	4500	C:\WINDOWS\system32\lsass.exe	Microsoft WindowsR ...	LSA Shell (Export Version)	Microsoft Corporation
svchost.exe	UDP	123	C:\WINDOWS\system32\svchost.exe	Microsoft WindowsR ...	Generic Host Process for ...	Microsoft Corporation
svchost.exe	UDP	123	C:\WINDOWS\system32\svchost.exe	Microsoft WindowsR ...	Generic Host Process for ...	Microsoft Corporation
svchost.exe	UDP	1900	C:\WINDOWS\system32\svchost.exe	Microsoft WindowsR ...	Generic Host Process for ...	Microsoft Corporation
svchost.exe	UDP	1900	C:\WINDOWS\system32\svchost.exe	Microsoft WindowsR ...	Generic Host Process for ...	Microsoft Corporation
系統	UDP	137				
系統	UDP	138				
系統	UDP	445				



# 打造隨身碟加密鑰匙

## ■ Remora行動碟終極保鑣

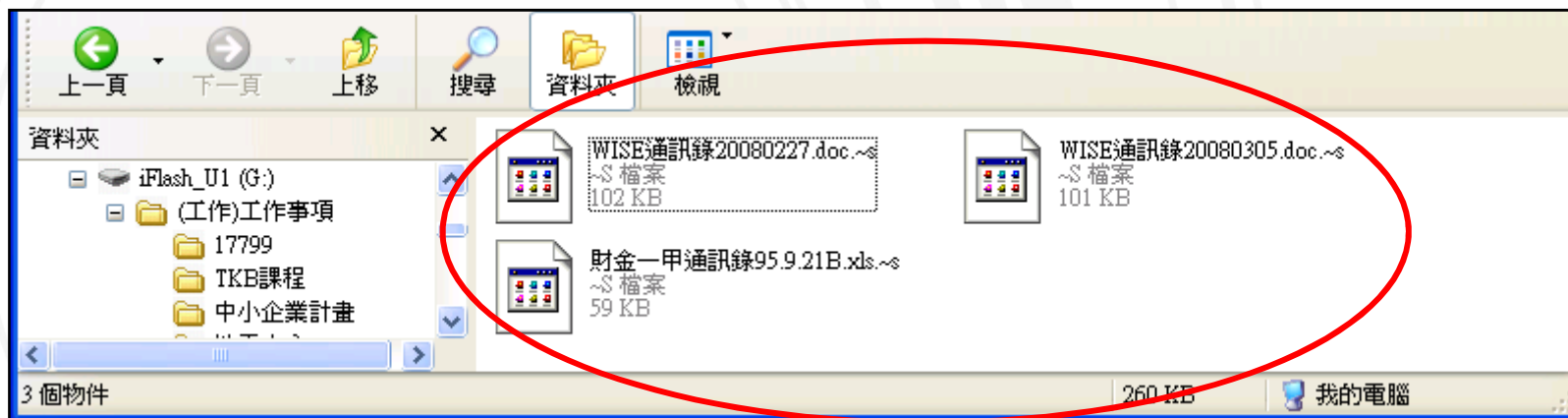
- 直接在隨身碟中執行加密，能加密整個資料夾
- 綠色軟體
- <http://www.richskills.com/taiwan/download>

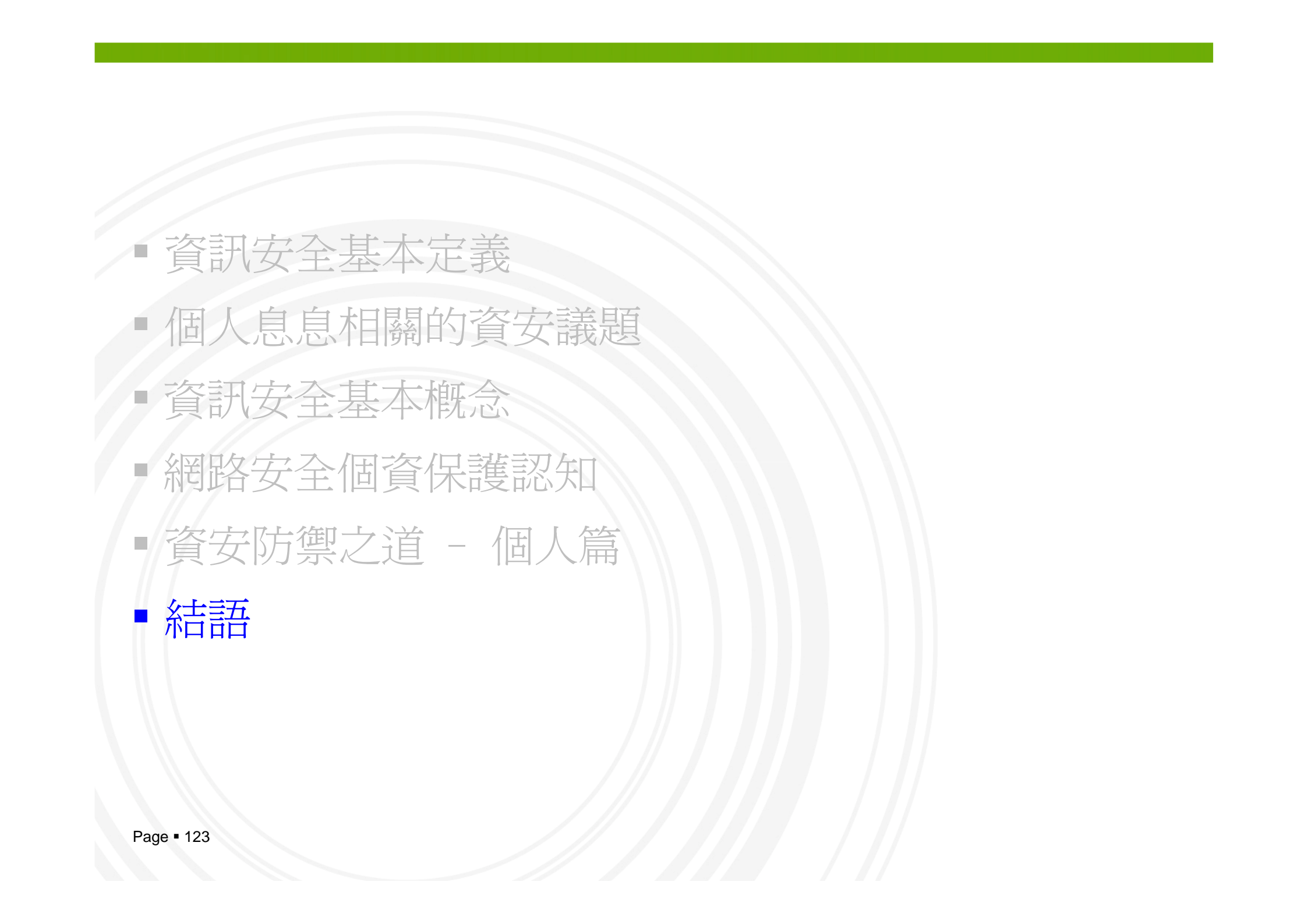


# 免費的磁碟 / 資料加密軟體

## ■ TrueCrypt

- 在硬碟上新增一個加密磁區，使用時只需將要加密的檔案移入
- 綠色軟體
- <http://www.truecrypt.org/downloads.php>



- 
- 資訊安全基本定義
  - 個人息息相關的資安議題
  - 資訊安全基本概念
  - 網路安全個資保護認知
  - 資安防禦之道 - 個人篇
  - 結語

資訊安全須融入日常生活方能久遠維護  
觀念認知 → 習慣養成

The background features several concentric, semi-transparent grey arcs that curve across the top half of the slide. Below these arcs is a solid green horizontal bar that spans the width of the slide. The bottom half of the slide is a lighter green gradient with faint, overlapping circular patterns.

簡報完畢，敬請指教