



資訊安全基本防護

南投區域網路中心
張瑛杰



Outline

資訊安全 ?



資訊安全

- 電腦資料
- 個人隱私
- 人身財產
- ... 等等



資訊安全

- 電腦資料
 - 被病毒破壞… 等
- 個人隱私
 - 密碼破解
 - 個人資料外洩、照片外流…

釣魚攻擊得逞 上萬筆Hotmail用戶密碼遭駭外洩



記者蘇湘雲／綜合報導

微軟5日封鎖數千個Hotmail帳號登入，發言人對外公開表示，部份Hotmail電子郵件使用者密碼在網路上外洩，但已移除。不過，微軟沒有說明受影響的帳號數目，但綜合各方報導，據相信已經超過1萬個帳號密碼遭到公開，多數來自歐洲。

微軟發言人表示，微軟已經得知一些Windows LiveHotmail使用者憑證遭網路釣魚非法取得，並公佈在網站上；網路罪犯顯然是利用「釣魚」手法，竊取微軟免費電子郵件服務使用者帳號及個資。

微軟說，外洩在違法網站上的密碼已移除，並封鎖所有受影響的帳號登入；而且將協助使用者收回Hotmail帳戶。不過，微軟也強調，密碼外洩跟微軟伺服器無關。

科技部落格neowin.net指出，超過1萬個Hotmail帳戶的資料在10月1日被人貼上pastebin.com這個常被用來分享密碼的網站。Neowin官方說，這些帳戶資料可能是作為網絡詐騙活動的一部分被駭，這些帳戶的名字都以a和b開頭，大部分帳戶都被確認屬實，大多來自歐洲。

英國警方也證實，受影響的包括電郵地址以hotmail.com、msn.com、live.com作結尾的用戶，駭客盜用用戶密碼後，極有可能登入帳戶盜取信用卡等個人資料。微軟也在部落格上建議，擔心受到釣魚詐騙影響的用戶，應該立即更換密碼。

2009/10/06



資訊安全

- 人身財產
 - 網路詐騙

*SPAM***** [wtuiqccqh] 最多最新超好盒即補給網站	● p2lzw59pxxup8p4...
*SPAM***** [ultteefyk] ■ ■ ■ 獨家超棒偷偷賣 ■ ■ ■	● ehmswls5h6h94wr...
*SPAM***** 你好! 要作 關b鍵◆◆做不到不用錢前所未...	● charlesdonvictoria...
*SPAM***** 你好! 要作 關b鍵◆◆做不到不用錢前所未...	● charlesdonvictoria...
*SPAM***** 專櫃真皮皮包 ~ 新款購物包 PHBDOTX	● 吳佳慧
*SPAM***** 余天 到帶女助理上旅館	● 蔡依琳^被強拍裸照
*SPAM***** 豬哥亮"開BMW夜店把妹	● 林志玲'被強拍裸照
你想要得軟體了麼	● 平嬌 沈
*SPAM***** [jbskpqkid] 超級片資源站.讓妳一次購足想要	● fg64pdi0n1nvr0rj4...
*SPAM***** [wtuiqccqh] ■ ■ ■ 此站將以最優質的服務來...	● p2lzw59pxxup8p4...



資訊安全

- USB 隨身碟病毒
- E-Mail 電子郵件
- 瀏覽網頁
- 其他
 - P2P
 - 相簿
 - 攝影機、讀卡機
- 良好習慣



USB 隨身碟病毒

- Windows 自動執行
- 透過 autorun.inf 執行病毒程式
- Kavo.exe, ntdelete.com, ubs.exe ...



autorun.inf
Setup Information
0 KB



USB 隨身碟病毒

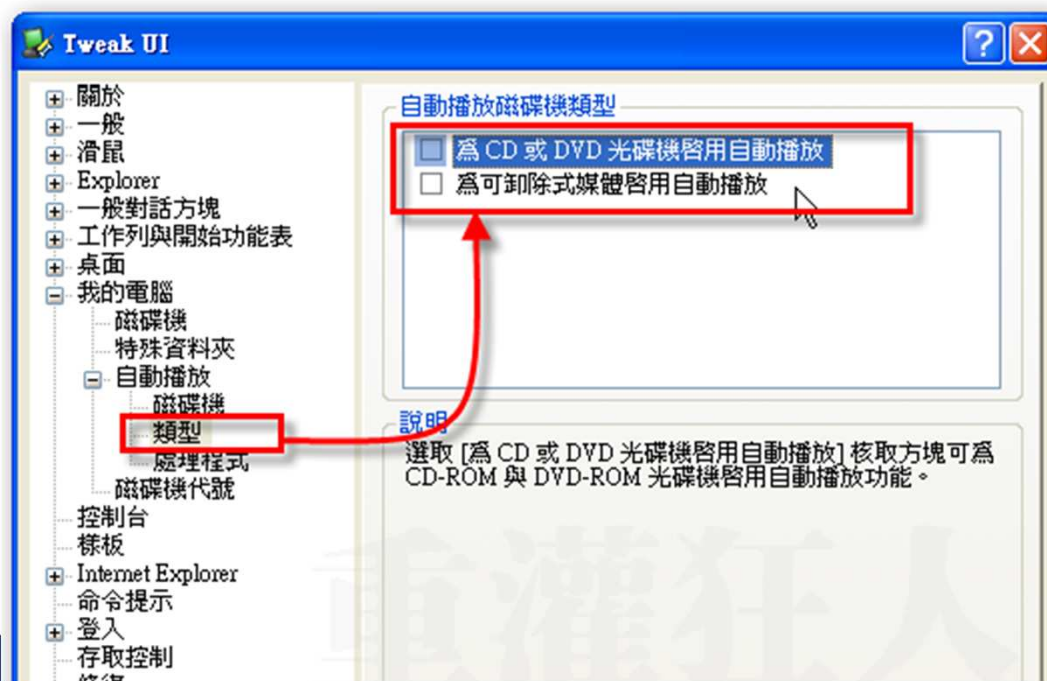
- 徵兆
 - 無法顯示隱藏檔
 - 我的電腦 C槽 D槽 開不了





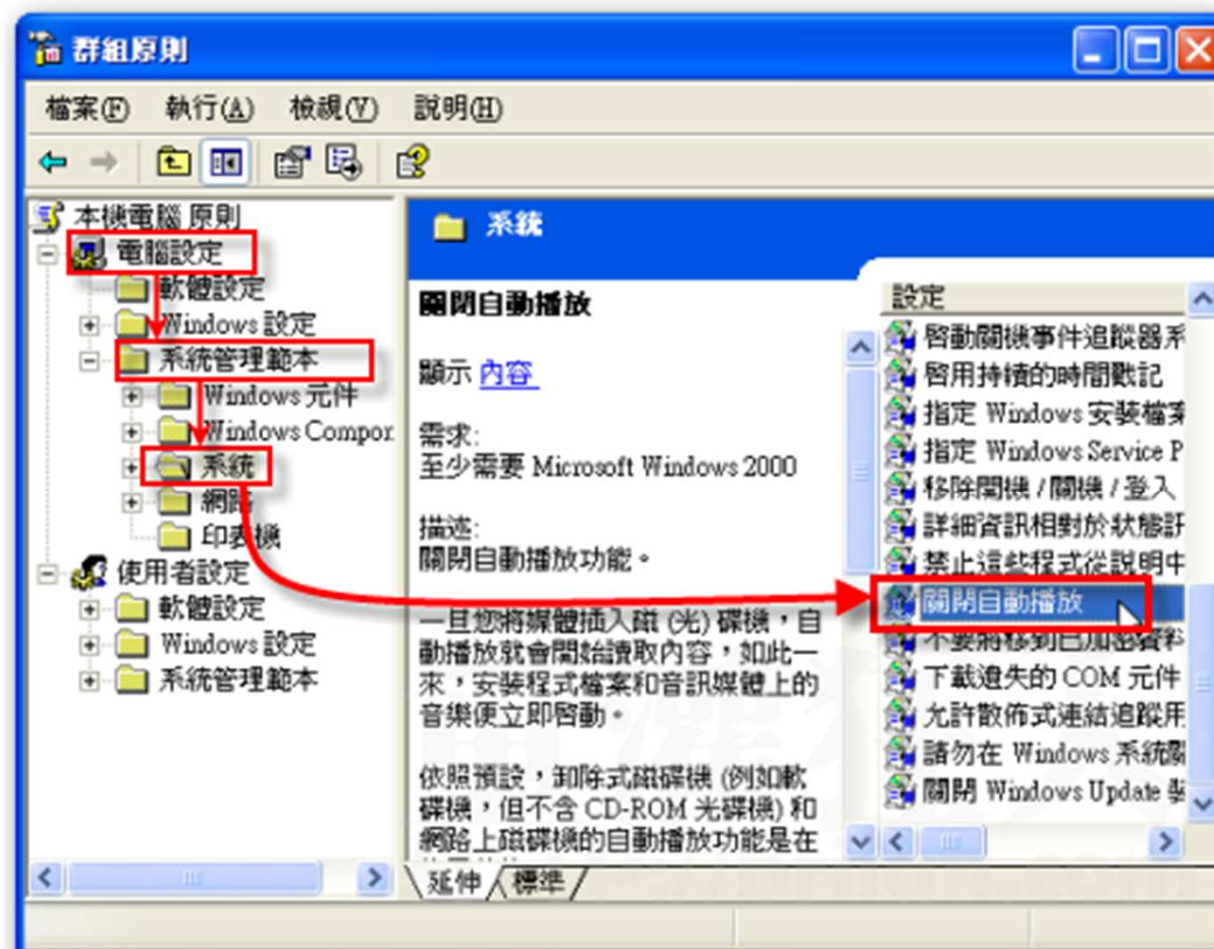
USB 隨身碟病毒

- 關閉Autorun(自動執行)功能
 - 使用TweakUI停用Autorun
 - gpedit.msc -> 群組原則 -> 電腦設定 -> 系統管理範本 -> 系統 -> 關閉自動播放





USB 隨身碟病毒





USB 隨身碟病毒

- 或是購買具防寫功能的隨身碟/記憶卡

有讀寫開關



+





E-Mail 電子郵件

- 木馬郵件
 - 帶有惡意程式的郵件，會引誘使用者開啟
- 社交工程
 - 帶有惡意連結的郵件，會引誘使用者到惡意的網站上
 - 騙取個人資料、信用卡卡號 等



E-Mail 電子郵件

- 木馬郵件

主旨: 最美好的祝福! ◇
寄件者: [ウン 玲奈 <taibijin@hotmail.com>](mailto:taibijin@hotmail.com)
日期: 2009/9/29 下午 04:05
收件者: s308tw@yahoo.com.tw

想成為你的專屬，守候在你身旁，看著你，喜怒悲傷
想成為你的天使，伴隨在你心裡，守護你，一路歸航
傳說看到仙女棒的祝福，會得到幸福唷！
請在看到信的一個鐘頭內轉寄給
10個人以上~妳會十分幸運唷~
20個人以上~妳會得到一段妳想要的戀愛唷~
30個人以上~妳會和戀人長相廝守一輩子唷~
夾帶裡是最美好的祝福！



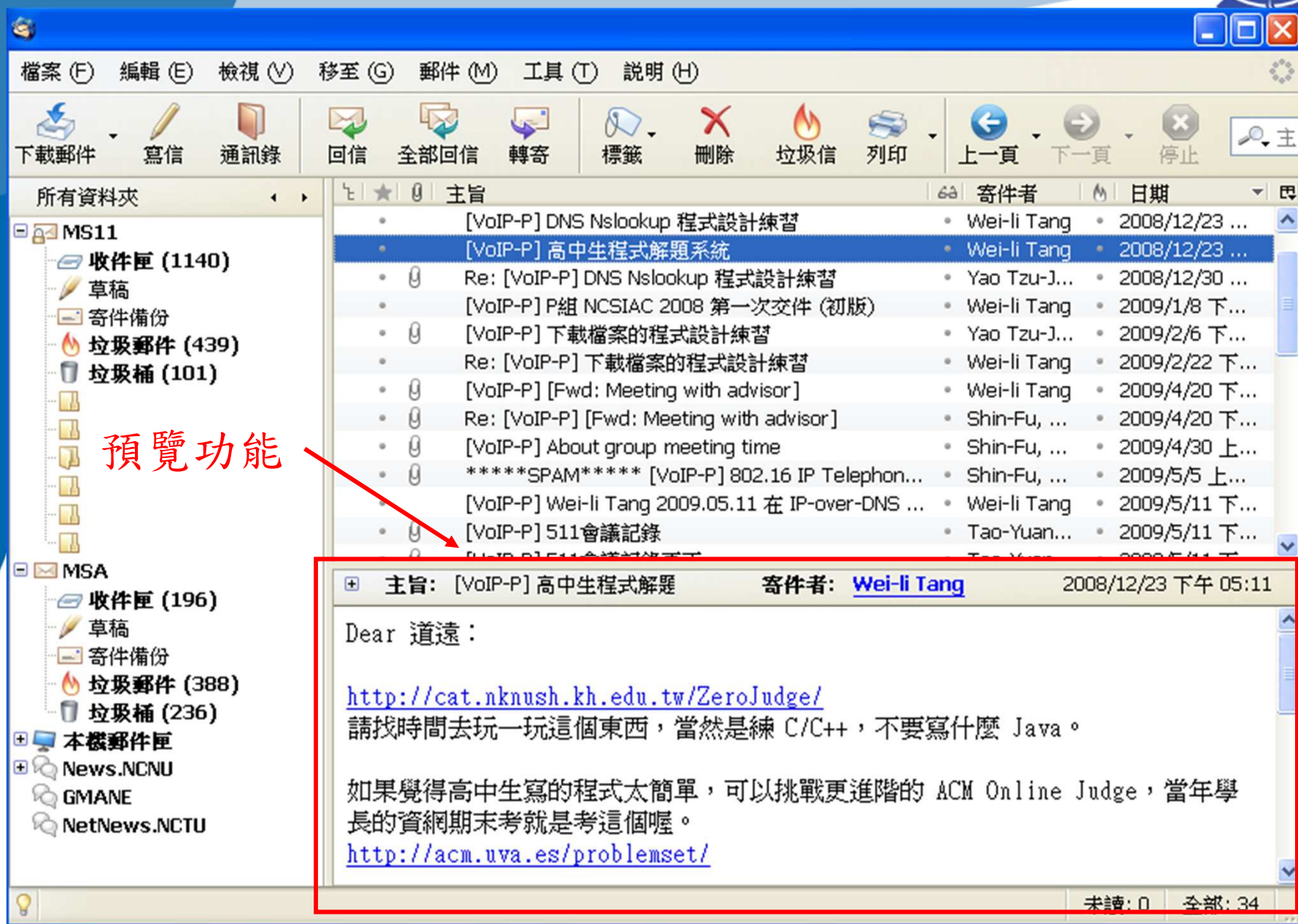
bestwish.zip

詭異的壓縮檔



E-Mail 電子郵件

- 防止社交工程詐騙
 - 不要亂點信件裡面的網址、連結
 - 常用「我的最愛」(書籤)到常去的網站
 - 不輕易開啟來路不明的附件檔案
 - 關閉郵件軟體的「預覽(Preview)」功能





檢視 (V) 移至 (G) 郵件 (M) 工具 (T) 說明 (H)

工具列 (T)

視窗配置方式 (L)

資料夾 (F)

排序 (S)

主題郵件串 (E)

郵件標頭 (H)

內文顯示方式 (B)

✓ 直接檢視附件 (A)

文字大小 (X)

語言及字元編碼 (C)

郵件原始內容 (O) Ctrl+U

郵件安全資訊 (I)

傳統檢視 (C)

水平檢視 (W)

垂直檢視 (V)

預覽面板 (M) F8

刪除 垃圾信 列印 上一頁 下一頁 停止

寄件者	日期
Wei-li Tang	2008/12/23 ...
Wei-li Tang	2008/12/23 ...
Yao Tzu-J...	2008/12/30 ...
Wei-li Tang	2009/1/8 下...
Yao Tzu-J...	2009/2/6 下...
Wei-li Tang	2009/2/22 下...
Wei-li Tang	2009/4/20 下...
Shin-Fu, ...	2009/4/20 下...
Shin-Fu, ...	2009/4/30 上...
Shin-Fu, ...	2009/5/5 上...
Wei-li Tang	2009/5/11 下...
Tao-Yuan...	2009/5/11 下...
Tao-Yuan...	2009/5/11 下...
吱吱茸茸	2009/5/25 下...
Shin-Fu, ...	2009/5/31 下...
Wei-li Tang	2009/5/31 下...
Tao-Yuan...	2009/5/31 下...
Shin-Fu, ...	2009/6/1 下...
Shin-Fu, ...	2009/6/2 下...
s95321040	2009/6/3 上...
Shin-Fu, ...	2009/6/3 上...
s95321040	2009/6/3 下...
Shin-Fu, ...	2009/6/3 下...
s95321040	2009/6/3 下...

未讀: 0 全部: 34



網頁瀏覽

- IE6的問題
 - 2001年發表
 - 安全漏洞
 - 修補緩慢
(微軟已停止維護)
 - KKMan
(BBS請用其他連線軟體如PCMan...)

Facebook | 首頁 - 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(D) http://www.facebook.com/home.php?

facebook 首頁 個人檔案 朋友 收件匣

你可能需要將你的瀏覽器升級。

你正在使用舊版的 Internet Explorer 瀏覽 Facebook。要順利使用 Facebook，請將你的瀏覽器升級或是改用另一種瀏覽器。

升級至 Internet Explorer 8
改用火狐 (Firefox)
改用 Safari
改用 Google Chrome

twitter

Home Pr

What are you doing?

Latest: 34 minutes ago

update

There's a better way to browse the web!

Twitter recommends that you upgrade to the latest version of Internet Explorer.

YouTube - Broadcast Yourself - 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(D) http://www.youtube.com/index?gl=US

You Tube

Broadcast Yourself™ 首頁 影片 頻道

Xuite.net - 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(D) http://www.xuite.net/

Firefox 3.5

請升級至最新的瀏覽器，體驗更多采多姿的線上瀏覽環境。
我們將在不久後停止支援 Internet Explorer 6，請立刻升級。

首頁 日誌 相簿 影音 旅遊 推薦服務

我們將逐步停止支援您的瀏覽器。
請升級至下列任何一種新版的瀏覽器。

目前使用者正在觀賞的影片 (檢視全部)

Leave me alone
God let me go
I'm blue and cold
Black sky will burn
Love pull me down
Hate lift me up
Just turn around
There's nothing left

4:18

Breaking Benjamin - Dear Agony

痞客邦 PIXNET - 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(D) http://www.pixnet.net/

痞客邦

服務 相簿 部落格 小圈圈 活動專
焦點 運動邦 化妝台 電影專區 娛樂大

搜尋:

熱門關鍵字: 上五樓的快活, 明日之星, 五月天, 姚香秀...

情報: 隨時隨地學英文! 回答問題

建議您將瀏覽器升級

系統偵測您目前使用舊版瀏覽器。
為了提昇網頁瀏覽品質與體驗全新痞客邦快捷發文功能。

中秋節(日誌) 928(日誌) 無車日(日誌) 美式餐廳(旅遊)

日誌 相簿 影音

相簿



網頁瀏覽

- 使用最新版的網頁瀏覽器
 - Internet Explorer 8 (IE8)
 - Mozilla Firefox 3 (火狐)
 - Google Chrome
- 安裝反間諜/反廣告軟體
 - Ad-aware
 - Adblock Plus



網頁瀏覽

來路不明
亂七八糟的站
不要上！

• • • • • • • • • •



看網頁，中木馬!!

Security Norton AntiVirus

新增檔案 精華區 編輯管理

類別 檔案名稱 檔案大小 推薦人 日期

女大學生的手淫自述，手淫時我喜歡自摸陰蒂	70 K	「*」-布 Y, :」 (j1394596)	2005/09/19 15:02:38
女大學生的手淫自述，手淫時我喜歡自摸陰蒂，那種感覺可真是			
我和我妹不下千次的性交	1 K	大野狼~~~ (lntzhung)	2005/08/24 20:12:57
美味一個勁兒地搖頭，馬華捏弄她的乳頭，使她既羞澀，又受			
用，當他把她的乳蒂輕搖起來時，			
媽媽真偉大	124 K	哇！白仔來惹♡ (bbb800720)	2005/08/17 01:32:09
九頭唐事件塵埃落定			
公車上有人摸你屁股怎麼辦	117 K	大野狼~~~ (lntzhung)	2005/08/05 18:23:04
給你防性侵害20招...			
女人被2.3個男生搞..	150 K	大野狼~~~ (lntzhung)	2005/07/31 11:37:33
翻牆模式..後來的女生皮膚真是棒.			
被盜賊後的慘痛經歷。。。.	68 K	風 (p1234567924)	2005/07/30 15:28:48
被盜賊後的慘痛經歷。。。.			
嚴淑明白色激凸性感裝	217 K	大野狼~~~ (lntzhung)	2005/07/21 12:13:46
得按漂白乳量秘絕(組圖)			
集体裸泳被偷拍	437 K	大野狼~~~ (lntzhung)	2005/07/12 18:56:46
台南交通大學全班偷照(圖)			
作業底圖	95 K	17 (supermilk_viva)	2004/04/13 13:05:49
教教我如何運用PHOTOSHOP製作成一景一模一樣的			

第 1-9 篇，共 9 篇

編輯管理

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

Yahool奇摩

木馬後門

http://tw.webfile.yahoo.com/file/1003/xxx.jpg.exe?cid=photoshoper&p=0&f=xxx.jpg.exe&r=357110

網際網路



網頁瀏覽

- 盡量使用「我的最愛」(書籤)上網
 - 或是背好網址、別打錯！
- 假網址範例
 - www.gamania.com (正牌網站)
 - www.gamannia.com (假網址)
 - www.ganannia.com (假網址)
 - ...等



偽官網！網域多個n 變成「假橘子」

【記者曹明正／報導】

繼6月底傳出旗下的「天堂」與「希望Online」有不法分子製造假官網竊取玩家的帳號密碼後，近日遊戲橘子又發現一大陸網站以「gamannia」的名字做為網域名稱，並放上遊戲橘子的識別Logo企圖瞞天過海，所幸發現得早、未接獲受騙案例。

遊戲橘子客服部經理宋時亮指出，該公司是在本月21日接到玩家以E-mail的方式提醒，有一網站註冊「gamannia」的網域名稱，左上角有遊戲橘子Lo-go，說明配合政府打擊詐騙，要求玩家輸入資料進行核對，不過事實上這個網站正是犯罪集團的幌子。

常上線的玩家可以發現，遊戲橘子的網域名稱是「gamania」，至於「假官網」則在字母中間多了1個n。宋時亮表示，第1時間接到玩家來信之後，隨即檢測發現該網站的主機位置架設在大陸，不明所以而登錄資料的玩家可能會被植入木馬程式。

另外，針對日前在電玩資訊站巴哈姆特上有玩家上傳「天堂2」官網已被植入木馬程式的圖片，宋時亮也澄清，真正官網上的公布欄寬度較小，疑為有心人士造假。面對層出不窮的詐騙事件，遊戲橘子則是提醒玩家留意官方真正的網路位址避免受騙。

【2004/09/24 星報】

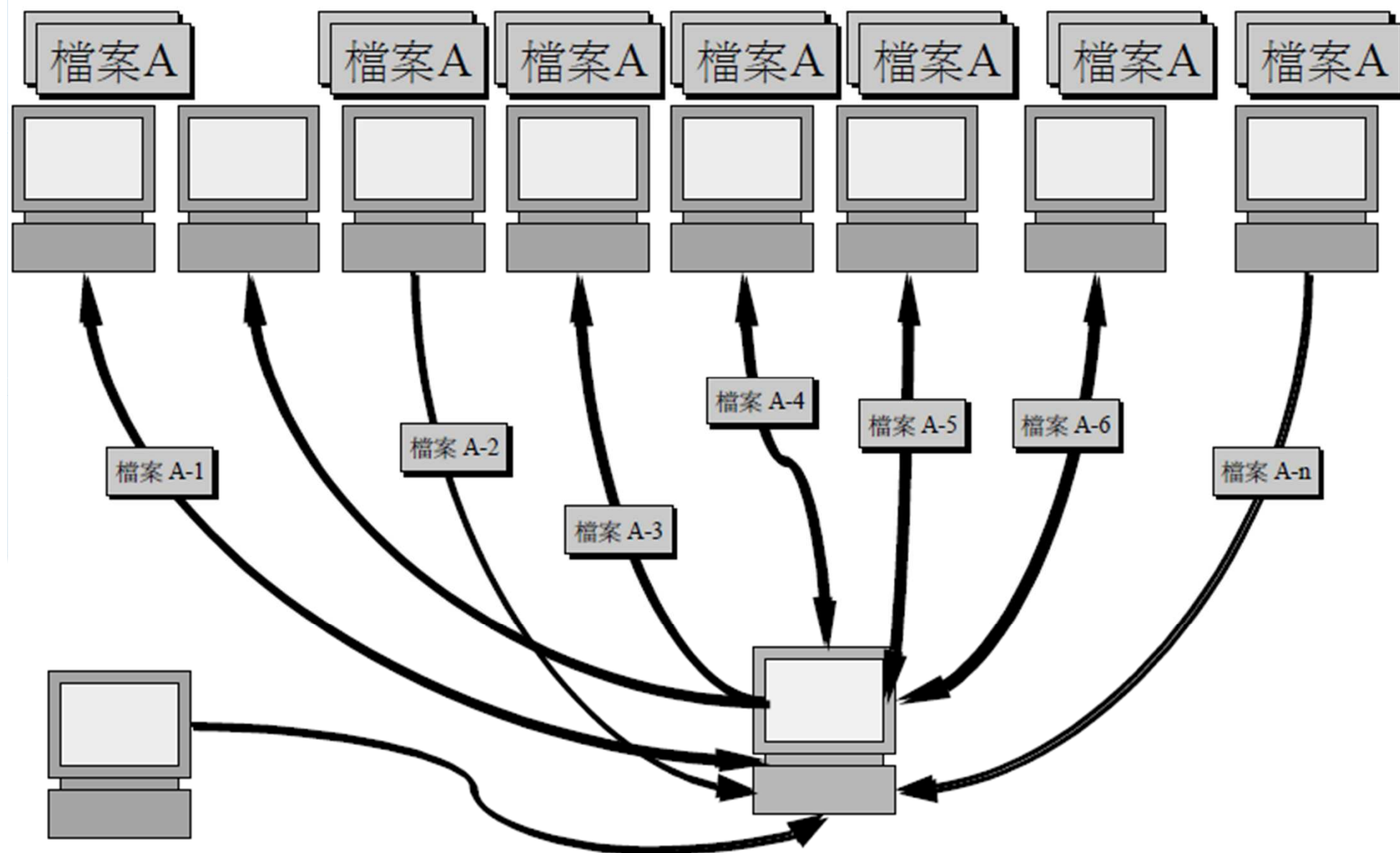


P2P

- 什麼是P2P軟體？
 - 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)
- P2P 採取用戶與用戶的通訊模式，可以同時連接多個下載點，分散式下載檔案
- P2P 通常擁有快速下載檔案的特徵
- Skype, PPStream 也是P2P的應用之一

• • • • • • • • • •

Peer to Peer, 點對點通訊傳輸工具





P2P 常見軟體

- eDonkey, eMule
- Foxy
- BitTorrent, BitComet, Azureus
- Gnutella, ezPeer, MXIE
- Fasttrack, KaZaR
- WinMX, Winny(NY), NapMX
- Share, Perfect Dark

• • • • • • • • • •



P2P

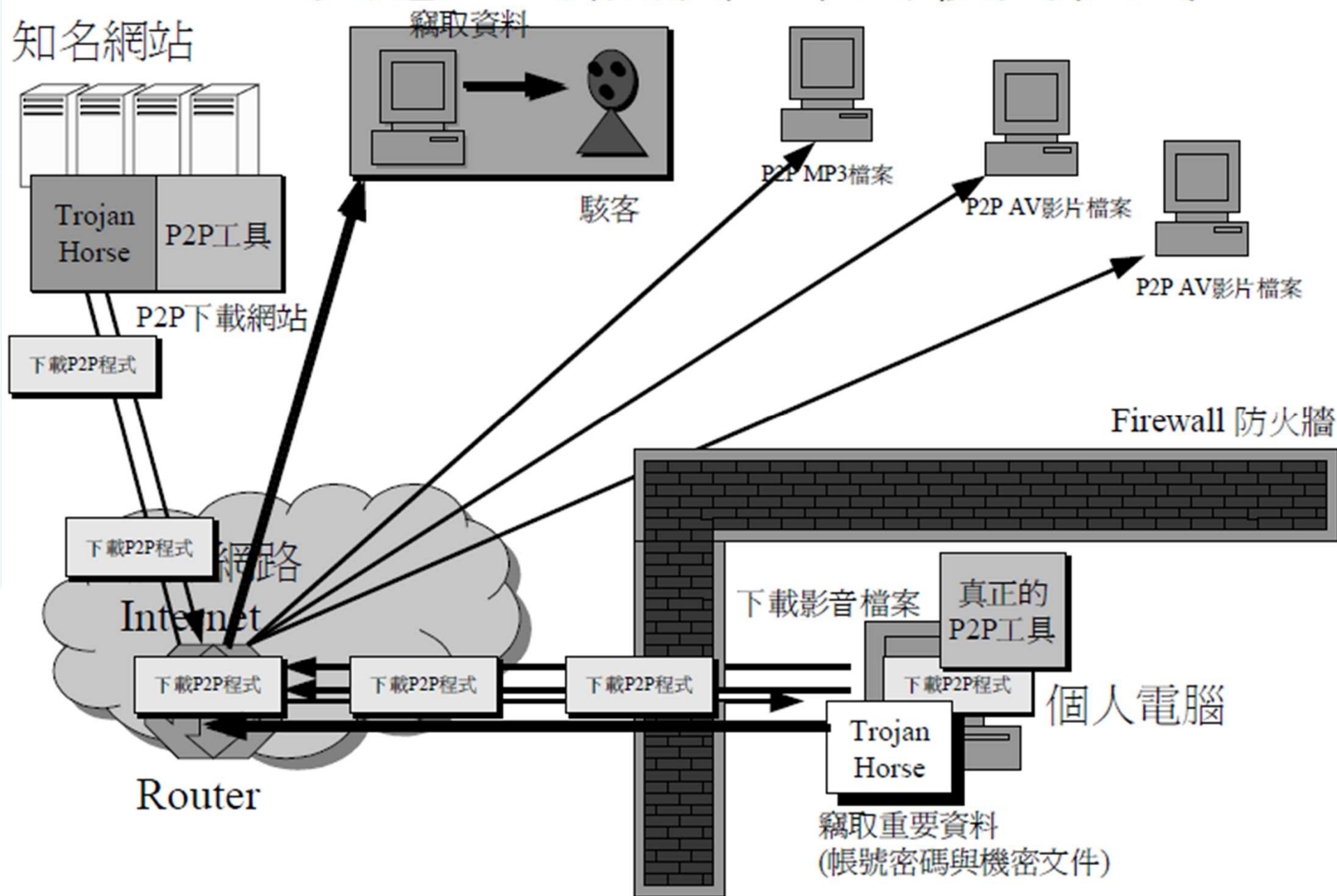
- eDonkey, eMule, Foxy, BitTorrent
等等...畜牧業 少用！
 - 即使要用，盡量與平時用的電腦區隔開
 - 動物機
- 潛藏危機
 - 病毒怎麼中的也不知道
 - 個人資料、機密外洩



P2P 可能的安全問題

- P2P軟體本身可能藏有病毒、木馬、後門
- P2P軟體本身漏洞、造成駭客入侵
- 誤將本機目錄開放分享
 - C槽、D槽
 - 我的文件夾
 - 郵件信箱...等
- 使用P2P下載影音檔案可能侵權
 - mp3, wmv, avi, mpg, mp4, rmvb...

P2P工具包，可能放置木馬後門程式





P2P 案例

- 台灣
 - 警局筆錄流出 (Foxy)
 - 成大MP3事件 (侵權)
- 日本
 - 自衛隊洩密 (Winny)



警局筆錄外洩 凸顯P2P軟體威脅

記者馬培治／台北報導

2007/04/13 20:51:02

警局傳出筆錄因P2P軟體使用不當而外洩的事件，凸顯了P2P軟體在方便之外的安全威脅問題。

據媒體報導，國內若干警分局因員警違反資安規範，私下在警局公用電腦上安裝「Foxy」等點對點(P2P)檔案分享軟體，意外將案情筆錄等機密資料一併「分享」出去，使得相同軟體使用者可以透過搜尋檔名的方式，找到並下載筆錄等資料，造成資料外洩。

P2P(Peer to Peer)軟體是一種藉由點對點連線來分享、交流檔案的軟體。使用者可以搜尋到其他使用者分享的檔案，並藉由該軟體建立的點對點連線上傳、下載檔案。早期P2P多半以分享影音類檔案，如mp3等為主，但近期流行的P2P軟體如eMule及Foxy、BT等，可分享或下載的檔案類型不再限於影音檔(例如文件、壓縮檔、執行檔等)，也因此較過去有更多安全疑慮。

「從個人履歷、企業資料，乃至此次發生的警方筆錄，都已在輕忽中外洩，」CA(組合國際)技術顧問林宏嘉便說，警方筆錄外洩僅是冰山一角，許多企業內或個人的機密資訊，都已藉由P2P軟體洩漏，「絕對不是只有警方受影響，」他說。

儘管刑事局不願說明此一事件詳情，但該局科技犯罪防治中心數位證據組組長蘇清偉表示，不當使用P2P軟體，的確會造成資料外洩，甚至招致惡意程式進門。他解釋道，一般P2P軟體如Foxy、eMule等，都有提供分享資料夾設定的功能，使用者應該把不願分享的檔案移出分享資料夾；此外，對於下載所得的軟體也要留意是否為偽裝的假檔案，搭配防毒軟體掃描，以避免感染惡意程式，他說。

網路洩密：美軍曾訓練日本軍隊鎮壓暴動

✉ 寄給朋友

🖨 友善列印



【法新社 彭木芳】

（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軍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。

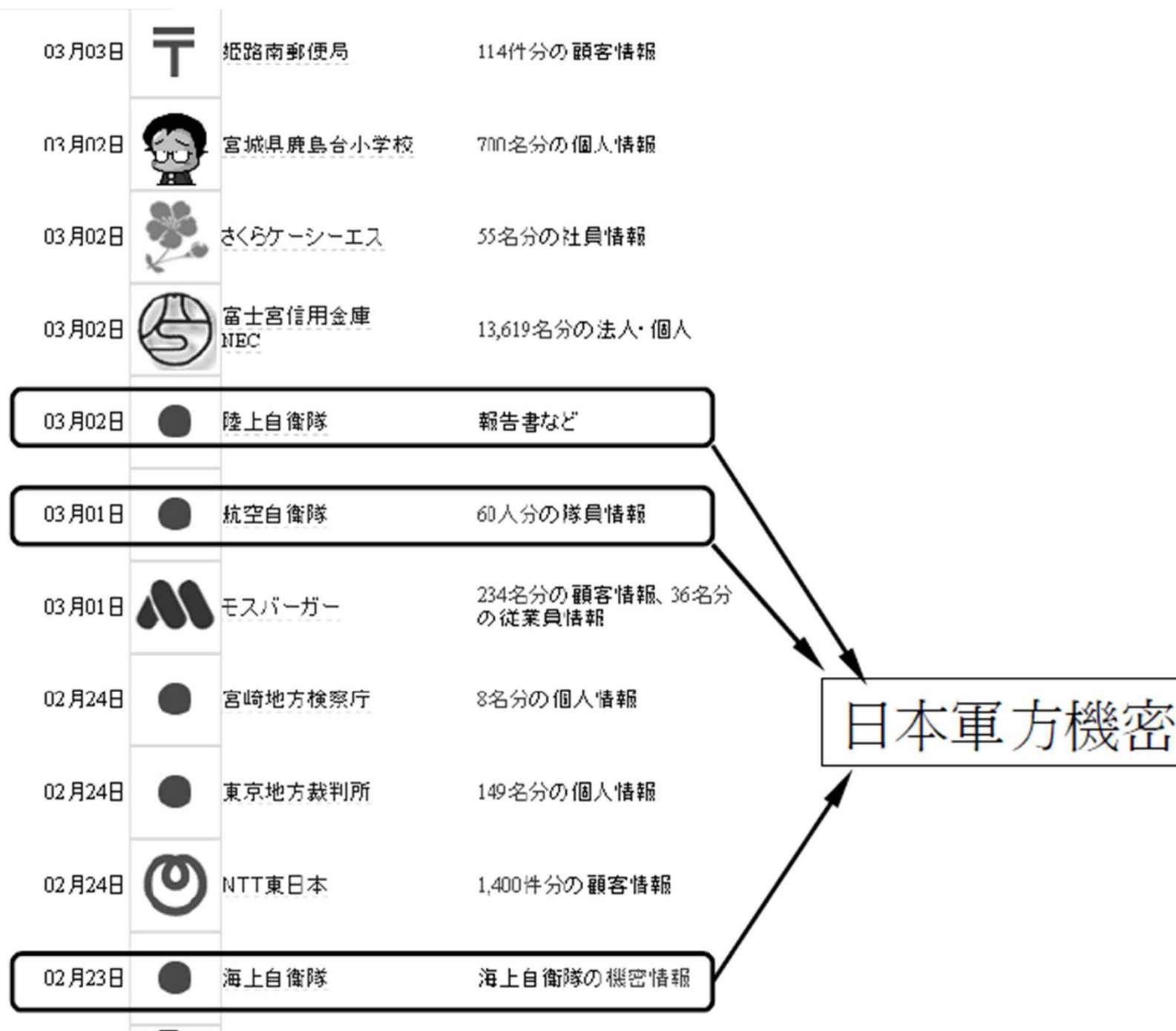
最近，每日新聞透過有缺失的日本Winny軟體檔案的交換系統，從自衛隊網站獲悉這項內幕消息，並且加以報導。

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祕密。」



11月14日		大阪府堺市の配管製造会社	19名分の個人情報 原子力発電所の報告書			
11月10日		NTTドコモ東海	300件の顧客情報	06月23日		北九州市消防局 287名分の個人情報
11月09日		極東ゴム	原子力発電所の報告書	06月19日		熊本県警 39件の警察資料 (Share)
10月11日		秋田県由利本荘市消防署	503名分の顧客情報	06月12日		西日本プラント工業 発電所の資料
10月11日		アフラック	564名分の顧客情報	06月08日		石川県JAつるぎ郷 1,823名分の個人情報 (Share)
09月26日		野村IR	137名分の個人情報	06月05日		ジェイコム 1万5,400名分の個人情報
09月20日		九州電力	火力発電所の技術資料 と個人情報	06月02日		国土交通省 1,800名分の個人情報
08月30日		三菱重工	46力所の原子力発電所の検査情報	06月02日		大阪府貝塚市消防本部 121名分の個人情報
06月24日		愛知県警	6名分の捜査報告書	06月02日		秋田県立横手高校 380名分の個人情報 (Share)
06月23日		三菱電機	原子力発電所の 内部情報	05月30日		愛知県西尾市立中学校 460名分の個人情報 (Share)
06月07日		NECファシリティーズ	395名分の人事考課データ			

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	580名分の個人情報
03月25日		北海道セパタクロ協会	大会参加者の個人情報 ※調査中
03月24日		カーブ・ド・ヴァン萬屋	8,223件分の顧客情報
03月23日		横浜市の事業受託団体	239名分の個人情報
03月22日		日本ジャグリング協会	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		新潟県立養護学校	11名分の個人情報
03月20日		福井市宮葬祭場「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

トレンドマイクロの営業資料がWinnyに流出

トレンドマイクロは27日、同社の営業資料などがP2Pファイル共有ソフト「Winny」のネットワーク上に流出していたことを明らかにした。トレンドマイクロによれば、2005年3月の時点ですでに確認しており、営業先の企業などには個別に連絡し、「ご理解していただいた」という。

トレンドマイクロでは流出した情報の詳細は明らかにしていないが、社内向けの報告書や提案資料といった営業用データであり、顧客リストなどは含まれていないという。同社によれば、トレンドマイクロの社員が上記データを自宅PCに保存。その後、ウイルスに感染して情報が流出したとしている。

なお、この社員は自宅PCにウイルス対策ソフトを利用していなかった。トレンドマイクロは流出禁止などに関するガイドライン（2004年8月以降に）に基づいた処分を行なった。その後、2005年中に処分とは別の理由で退職した」としている。

**資安大廠與網路公司
仍然遭逢劫難**



P2P

- 不要以為抓了檔案無人知道
- 人外有人，天外有天



偵測- P2P 通訊封包特徵 (一般通用原則)



封包檔案選擇工作完成!

首次偵測時間	偵測封包時間	封包類...	發送者 IP 地址	通訊端...	接收者 IP 地址	通訊端...	封 包 內 容
2006/03/14 09:47:17	2006/03/14 09:47:17	TCP	64.62.194.27	18080	172.16.1.100	1165	
2006/03/14 09:47:17	2006/03/14 09:47:17	TCP	172.16.1.100	1165	64.62.194.27	18080	
2006/03/14 09:47:20	2006/03/14 09:47:20	TCP	172.16.1.100	1185	218.167.47.218	7884	
2006/03/14 09:47:20	2006/03/14 09:47:20	TCP	172.16.1.100	1184	218.171.165.228	7884	
2006/03/14 09:47:21	2006/03/14 09:47:21	TCP	218.171.165.228	7884	172.16.1.100	1184	
2006/03/14 09:47:35	2006/03/14 09:47:35	TCP	172.16.1.100	1188	59.114.143.50	5100	
2006/03/14 09:49:08	2006/03/14 09:49:08	TCP	172.16.1.100	1257	202.86.150.73	12247	
2006/03/14 09:49:09	2006/03/14 09:49:09	TCP	172.16.1.100	1258	59.115.232.91	5100	
2006/03/14 09:49:10	2006/03/14 09:49:10	TCP	172.16.1.100	1251	140.129.60.62	5100	
2006/03/14 09:49:10	2006/03/14 09:49:10	TCP	172.16.1.100	1250	220.139.45.95	7884	
2006/03/14 09:49:11	2006/03/14 09:49:11	TCP	172.16.1.100	1253	218.169.84.76	3599	
2006/03/14 09:49:13	2006/03/14 09:49:13	TCP	172.16.1.100	1259	61.230.104.61	7890	
2006/03/14 09:49:14	2006/03/14 09:49:14	TCP	61.230.104.61	7890	172.16.1.100	1259	
2006/03/14 09:49:15	2006/03/14 09:49:15	TCP	61.231.181.122	7884	172.16.1.100	1260	
2006/03/14 09:49:16	2006/03/14 09:49:16	TCP	172.16.1.100	1260	61.231.181.122	7884	
2006/03/14 09:49:18	2006/03/14 09:49:18	TCP	172.16.1.100	1262	218.174.137.237	7890	
2006/03/14 09:49:21	2006/03/14 09:49:21	TCP	172.16.1.100	1261	211.23.128.22	5100	
2006/03/14 09:49:22	2006/03/14 09:49:22	TCP	203.70.2.44	7884	172.16.1.100	1263	
2006/03/14 09:49:22	2006/03/14 09:49:22	TCP	172.16.1.100	1263	220.139.72.207	5102	
2006/03/14 09:49:23	2006/03/14 09:49:23	TCP	172.16.1.100	1264	203.70.2.44	7884	
2006/03/14 09:49:24	2006/03/14 09:49:24	TCP	172.16.1.100	1270	59.116.170.145	16983	
2006/03/14 09:49:24	2006/03/14 09:49:24	TCP	59.116.170.145	16983	172.16.1.100	1270	
2006/03/14 09:49:24	2006/03/14 09:49:24	TCP	172.16.1.100	1267	61.61.178.163	7890	
2006/03/14 09:49:25	2006/03/14 09:49:25	TCP	218.174.137.237	7890	172.16.1.100	1262	
2006/03/14 09:49:27	2006/03/14 09:49:27	TCP	59.115.132.77	5100	172.16.1.100	1273	
2006/03/14 09:49:27	2006/03/14 09:49:27	TCP	172.16.1.100	1273	59.115.132.77	5100	
2006/03/14 09:49:28	2006/03/14 09:49:28	TCP	172.16.1.100	1272	59.116.145.189	7884	
2006/03/14 09:49:28	2006/03/14 09:49:28	TCP	172.16.1.100	1271	219.86.27.34	5100	
2006/03/14 09:49:30	2006/03/14 09:49:30	TCP	172.16.1.100	1276	61.216.102.188	5100	
2006/03/14 09:49:31	2006/03/14 09:49:31	TCP	172.16.1.100	1277	61.217.155.196	5100	
2006/03/14 09:49:40	2006/03/14 09:49:40	TCP	172.16.1.100	1279	218.171.113.164	7884	
2006/03/14 09:49:44	2006/03/14 09:49:44	TCP	172.16.1.100	1282	210.192.215.52	5100	

通訊埠 > TCP 1024

172.16.1.100 單點對外多點

A-PacketMan - 檔案名稱: D:\GNU_TELLA_ezPeer_下載色色_1.Acp 檔案大小: 925 KB					
檔案(F) 編輯(E) 操作(O) 顯示(V) 進階(A) 設定(S) 幫助(H)					
板板	此次	讀檔	讀檔	文字檔	封包檔
複製	複製	尋找	尋找	內容	電話
用戶	主機	即時	詳細	清除	清除
全清	網說	刪除	刪除	網說	開始
停止	設定				
網路封包的通訊記錄已經製作完成，有效記錄 427 個。					
發送者 IP 地址	通訊...	接收者 IP 地址	通訊...	封包內容	
載: (未確定)P2P 傳送自己...	218.171.125.189	6506	192.168.1.135	7047	工具名稱: Mxoe,Foxy,ezPeer,GnuTella等等, 回應解說: 發送端用戶告知其他P2P用戶, 自己為P2P下載端點(
載: P2P 取得連接端點資料	220.139.162.167	15983	192.168.1.135	4341	工具名稱: Mxoe,ezPeer,GnuTella系列等等, 回應解說: P2P用戶回應訊息。 Maximum child connections reache
載: (未確定)P2P 傳送自己...	218.175.160.101	23935	192.168.1.135	7047	工具名稱: Mxoe,Foxy,ezPeer,GnuTella等等, 回應解說: 發送端用戶告知其他P2P用戶, 自己為P2P下載端點(
載: P2P 正在下載分享檔案	218.175.180.185	6158	192.168.1.135	4347	工具名稱: Foxy,ezPeer,GnuTella系列等等, 檔案名稱: 冰原歷險記2 CD1.mpg, 回應解說: P2P用戶下載影片i
載: P2P 取得連接端點資料	218.175.160.101	23935	192.168.1.135	4344	工具名稱: Mxoe,ezPeer,GnuTella系列等等, 回應解說: P2P用戶回應訊息。 Maximum child connections reache
載: P2P 正在下載分享檔案	61.15.84.13	10192	192.168.1.135	4353	工具名稱: Foxy,ezPeer,GnuTella系列等等, 檔案名稱: 楊丞琳-遇上愛MTV.mvb, 回應解說: P2P用戶下載影
載: P2P 正在下載分享檔案	218.175.180.185	6158	192.168.1.135	4347	工具名稱: Foxy,ezPeer,GnuTella系列等等, 檔案名稱: 冰原歷險記2 CD1.mpg, 回應解說: P2P用戶下載影片i
載: P2P 取得連接端點資料	61.30.154.130	17801	192.168.1.135	4300	工具名稱: Mxoe,ezPeer,GnuTella系列等等, 回應解說: P2P用戶回應訊息。 Maximum child connections reache
載: P2P 傳送自己端點資料	220.131.180.217	18039	192.168.1.135	7047	工具名稱: Mxoe,Foxy,ezPeer,GnuTella系列等等, 回應解說: 發送端用戶告知其他P2P用戶, 自己為P2P下載端
載: (未確定)P2P 傳送自己...	218.175.160.101	23935	192.168.1.135	7047	工具名稱: Mxoe,Foxy,ezPeer,GnuTella等等, 回應解說: 發送端用戶告知其他P2P用戶, 自己為P2P下載端點(
載: P2P 已經完成檔案下載	219.68.43.55	4048	192.168.1.135	4372	工具名稱: Foxy,ezPeer,GnuTella系列等等, 檔案名稱: [一本道]-可愛小女生陽台臥室被玩弄.mvb, 回應解說
載: P2P 正在下載分享檔案	61.216.245.44	22221	192.168.1.135	4360	工具名稱: Foxy,ezPeer,GnuTella系列等等, 檔案名稱: 不可能任務3急速搶先版.mvb, 回應解說: P2P用戶下
載: P2P 變更連接端點資料	211.74.220.204	7884	192.168.1.135	4383	工具名稱: Mxoe,ezPeer,GnuTella系列等等, 回應內容: 回應解說: P2P被下載端已經滿載, 或是僅有部份檔
載: P2P 變更連接端點資料	61.231.250.196	7884	192.168.1.135	4384	工具名稱: Mxoe,ezPeer,GnuTella系列等等, 回應內容: 回應解說: P2P被下載端已經滿載, 或是僅有部份檔
載: P2P 已經完成檔案下載	211.75.121.44	5100	192.168.1.135	4381	工具名稱: Mxoe,ezPeer,GnuTella系列等等, 檔案名稱: 不可能任務3急速搶先版.mvb, 回應解說: P2P用戶下
載: P2P 已經完成檔案下載	218.184.36.194	5100	192.168.1.135	4374	工具名稱: Mxoe,ezPeer,GnuTella系列等等, 檔案名稱: A影片-日本-(破曉版56分鐘)潮月雄乃.mpg, 回應解說
載: P2P 變更連接端點資料	218.170.194.5	7884	192.168.1.135	4212	工具名稱: Mxoe,ezPeer,GnuTella系列等等, 回應內容: 回應解說: P2P被下載端已經滿載, 或是僅有部份檔
載: P2P 正在下載分享檔案	221.126.138.27	11160	192.168.1.135	4400	工具名稱: Foxy,ezPeer,GnuTella系列等等, 檔案名稱: [電影]達文西密碼 1.mvb, 回應解說: P2P用戶下載影
載: P2P 正在下載分享檔案	219.71.97.202	9335	192.168.1.135	4387	工具名稱: Foxy,ezPeer,GnuTella系列等等, 檔案名稱: [電影]達文西密碼.mvb, 回應解說: P2P用戶下載影片
載: P2P 變更連接端點資料	59.120.78.236	5100	192.168.1.135	4401	工具名稱: Mxoe,ezPeer,GnuTella系列等等, 回應內容: 回應解說: P2P被下載端已經滿載, 或是僅有部份檔
載: (未確定)P2P 傳送自己...	218.170.207.55	24579	192.168.1.135	7047	工具名稱: Mxoe,Foxy,ezPeer,GnuTella等等, 回應解說: 發送端用戶告知其他P2P用戶, 自己為P2P下載端點(
載: P2P 正在下載分享檔案	61.217.89.81	14078	192.168.1.135	4405	工具名稱: Foxy,ezPeer,GnuTella系列等等, 檔案名稱: 不可能任務3急速搶先版 1.mvb, 回應解說: P2P用戶
載: P2P 正在下載分享檔案	219.71.97.202	9335	192.168.1.135	4387	工具名稱: Foxy,ezPeer,GnuTella系列等等, 檔案名稱: [電影]達文西密碼.mvb, 回應解說: P2P用戶下載影片
載: P2P 正在下載分享檔案	218.167.188.251	4626	192.168.1.135	4412	工具名稱: Foxy,ezPeer,GnuTella系列等等, 檔案名稱: 冰原歷險記2 CD1.mpg, 回應解說: P2P用戶下載影片i
載: (未確定)P2P 傳送自己...	125.228.123.214	24542	192.168.1.135	7047	工具名稱: Mxoe,Foxy,ezPeer,GnuTella等等, 回應解說: 發送端用戶告知其他P2P用戶, 自己為P2P下載端點(
載: P2P 已經完成檔案下載	60.244.60.149	7719	192.168.1.135	4431	工具名稱: Foxy,ezPeer,GnuTella系列等等, 檔案名稱: 冰原歷險記2---驚中---國語發音 2.mpeg, 回應解說: P
載: P2P 已經完成檔案下載	125.228.213.170	5100	192.168.1.135	4441	工具名稱: Mxoe,ezPeer,GnuTella系列等等, 檔案名稱: A影片-日本-(破曉版56分鐘)潮月雄乃.mpg, 回應解說
載: (未確定)P2P 傳送自己...	125.228.123.214	24542	192.168.1.135	7047	工具名稱: Mxoe,Foxy,ezPeer,GnuTella等等, 回應解說: 發送端用戶告知其他P2P用戶, 自己為P2P下載端點(
載: P2P 已經完成檔案下載	220.140.18.25	5100	192.168.1.135	4424	工具名稱: Mxoe,ezPeer,GnuTella系列等等, 檔案名稱: 冰原歷險記2 CD1.mpg, 回應解說: P2P用戶下載影片i
載: P2P 已經完成檔案下載	61.225.166.208	18643	192.168.1.135	4452	工具名稱: Foxy,ezPeer,GnuTella系列等等, 檔案名稱: 不可能任務3急速搶先版.mvb, 回應解說: P2P用戶下
載: (未確定)P2P 傳送自己...	218.170.207.55	24579	192.168.1.135	7047	工具名稱: Mxoe,Foxy,ezPeer,GnuTella等等, 回應解說: 發送端用戶告知其他P2P用戶, 自己為P2P下載端點(
載: P2P 正在下載分享檔案	202.85.155.200	9265	192.168.1.135	4450	工具名稱: Foxy,ezPeer,GnuTella系列等等, 檔案名稱: 冰原歷險記2-冰河世紀CD1.mpg, 回應解說: P2P用戶



P2P

- 侵權：告訴乃論
 - 只是看對方要不要告而已
- 後果
 - 影響校譽
 - 前科
 - 個人名聲
 - ...等





網路相簿

- 無名、痞客邦…真的安全嗎？





舒舒
35pictures



無名破解~3p(上
過新聞)
185pictures



無名破解
20pictures



無名破解~畢業
旅行
28pictures



無名破解
84pictures



無名破解
41pictures



無名破解
31pictures



無名破解
18pictures



18禁2
155pictures



18禁3
50pictures



轟動一時
80pictures



18禁
20pictures



瑤瑤~殺很大
910pictures



婷婷~傻咩露點為都
不知道
22pictures



Ssindy~傻咩露點為
都不知道
89pictures



網路相簿

- 私密資料、圖片避免放在網路上
 - 沒有絕對安全的網路空間
 - 只要上傳至網路、其他人遲早會看見
- 密碼須不易被猜出
 - 想難猜一點的密碼



外接設備

- ATM讀卡機
 - 用完網路銀行、網路ATM記得抽出金融卡
- Webcam網路攝影機
 - 用完後關電源或拔除
 - 彩虹橋木馬與Webcam偷拍





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





良好習慣

- 定期換密碼
- 避免在公用電腦(網咖)登入私密帳號
 - 電子信箱
 - BBS (ptt批踢踢...等)
 - 網路遊戲
- 在家玩。
- 很難知道公用電腦是否安全



良好習慣

- Key Logger (鍵盤側錄)



- 其他無法得知的隱形木馬…等等
- 現在的病毒也會錄影



良好習慣

- 定期掃毒
 - 使用正版防毒軟體
 - 免費防毒軟體
- 常見病毒移除工具

- Combofix

- <http://www.bleepingcomputer.com/combofix/how-to-use-combofix>

- EFix

- <http://reinfors.blogspot.com/>





良好習慣

- 開啟防火牆
- Windows Update
 - 使用正版作業系統
 - 勿用破解檔





良好習慣

- 登入帳號、記得登出(Logout)
 - 避免遭(上機)盜用





良好習慣

- 譬如說被別人偷玩Facebook...





結論

- 回家做更新
 - 瀏覽器、Windows Update
- 掃毒
 - 防毒軟體、Combofix/EFix





謝謝

南投區域網路中心

100年9月15日

