SYSWARE

資訊安全概念及網路安全運用

李烜旭 NeoLi
neoli@sysware.com.tw

Who am I ?

- 李烜旭 NeoLi
- 精誠資訊 技術顧問

-Training

Ultimate Hacking
Incident Response & Forensics (Foundstone Washington D.C)
SGS ISO 27001 Lead Auditor
2006 BlackHat and DefCon (LasVegas)

-Certified

Microsoft MCPs、Cisco CCNA、Packet Analysis、
CheckPoint CCSA & CCSE、 BS27001 LA、
Websense CWSE+

SYSWARE

大綱

- 資訊安全概念介紹
  - 資訊安全(CIA)
- 網際網路安全運用
  - 無線網路的潛在風險
  - 電子郵件安全與管理
  - 認識病毒、木馬
  - P2P軟體潛在風險
- 回應與討論

SYSWARE

SYSWARE

資訊安全概念

資訊

- 書面文件
- 電子檔案
- 傳輸中的文件
- 影片多媒體
- 進行中的對話

客戶（業務夥伴）資訊、合約、研發設計稿/文件、作業流程、組織簡介影片、訓練教材等

組織的無形資產

資訊安全

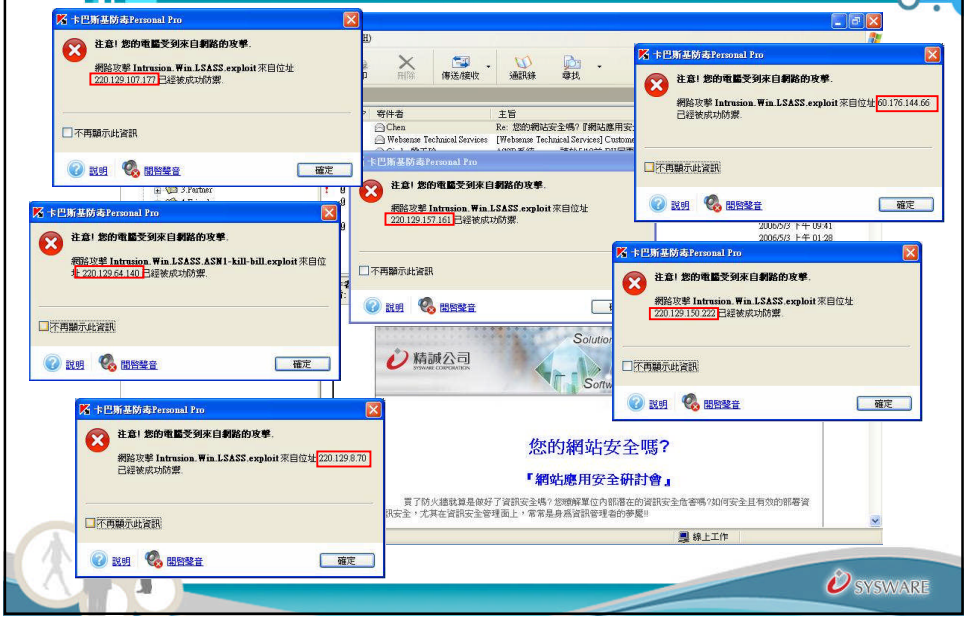
- 定義
  - 保障資訊資產免於〝不可承受的風險〞的所有政策、程序與機制
- 特質
  - 機密性(Confidentiality)
    - 避免未授權的查閱資訊
  - 完整性(Integrity)
    - 避免未授權的竄改資訊
  - 可用性(Availability)
    - 已授權者可經由合法管道使用資訊
- 範圍
  - 環境、設備、人員、資訊紀錄、服務...

資訊安全的重要性

- 資訊是重要的資產
- 現代社會大量的依賴資訊系統的運作
- 個人與組織和資訊系統間的互動構成了現代社會的工作型態，例如
  - Internet網路連線
  - 電子郵件
  - 即時通訊軟體
  - 線上交易
  - …

誰在進行攻擊？

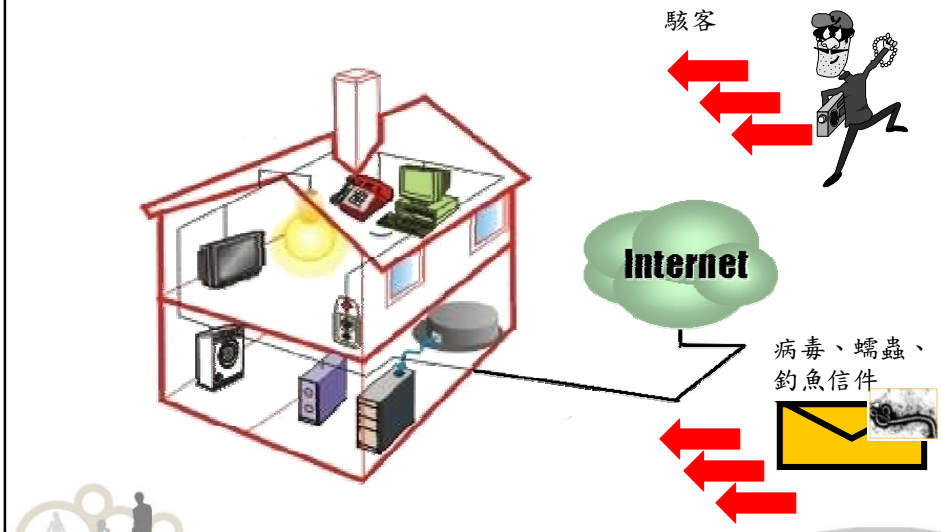
誰在進行攻擊？



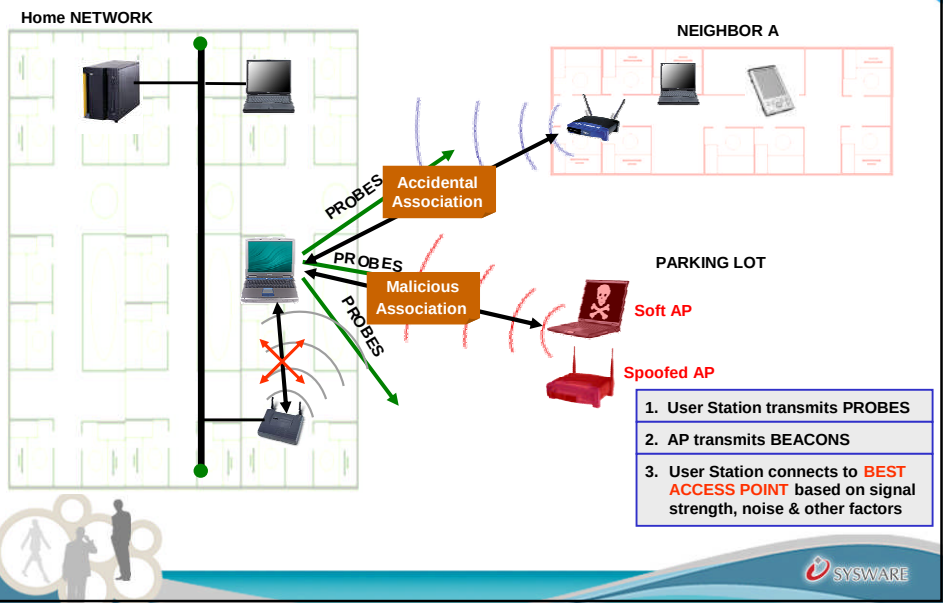
SYSWARE

無線網路的潛在風險

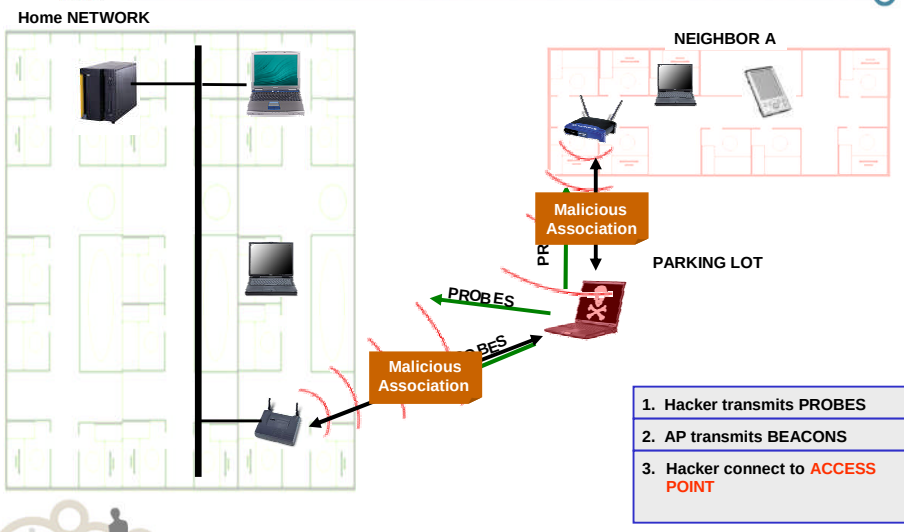
網路的潛在威脅



無線網路的連線與威脅



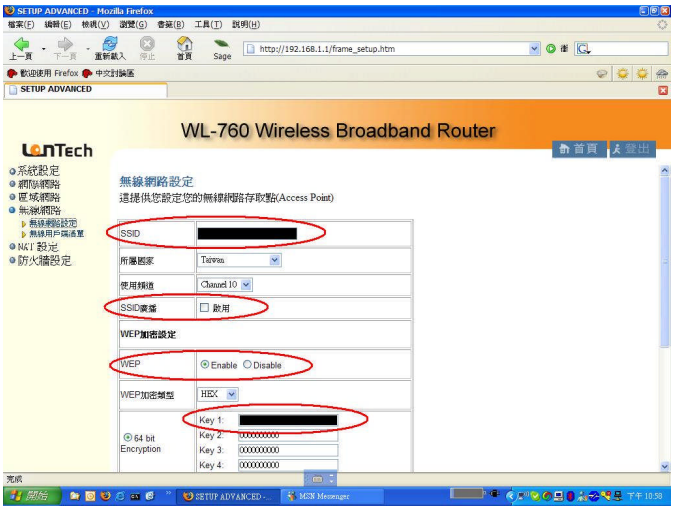
無線網路的連線與威脅



無線網路防護

- 不要廣播SSID (Service Set ID)
- 鎖定MAC (Media Access Control) Address
- 使用WEP (Wired Equivalent Privacy) 加密
- 更改無線基地台管理員帳號 / 密碼
- 儘可能不要啟用DHCP (Dynamic Host Configuration Protocol) 功能
- 養成查看〝日誌〞的習慣
- 不使用時請關閉無線基地台
- 更新最新韌體(Firmware version)

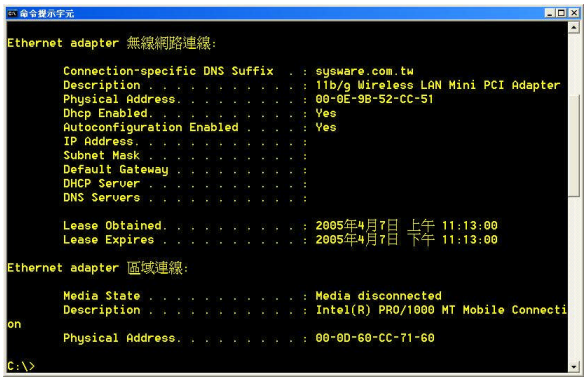
無線基地台安全設定 (1)



SYSWARE

MAC Address

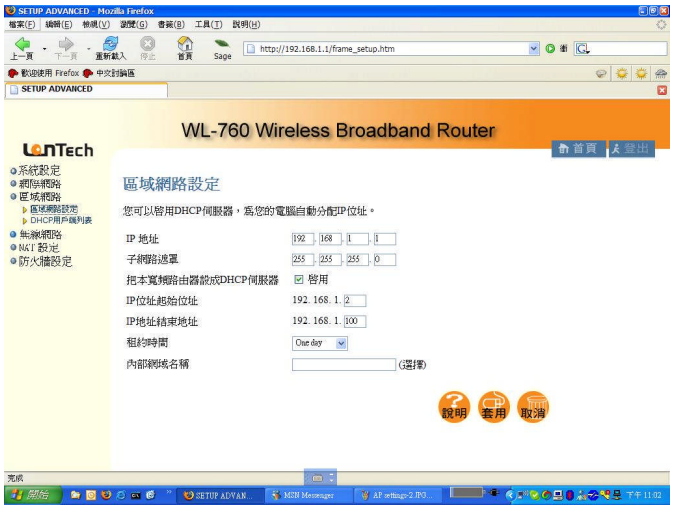
- 開啟DOS視窗
- 執行“ipconfig /all”命令



SYSWARE

無線基地台安全設定 (2)

無線基地台安全設定 (3)



SYSWARE

電子郵件安全與管理

電子郵件

- 電子郵件的威脅
  - 電子郵件仍然是最容易夾帶惡意程式的媒介之一
  - 毫無警惕的打開來歷不明的郵件是非常危險的行為
- 不適當的電子郵件
  - 傳遞色情或其他具有攻擊性內容之不適當的電子郵件可能會面臨法律上的問題
- 垃圾郵件
- 新型詐騙手法
  - Phishing

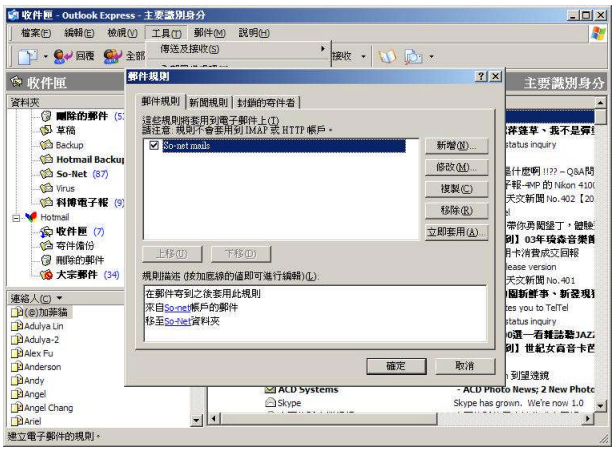
SYSWARE

注意電子郵件的安全

- 〝選項〞-> 安全性〞

如何處理垃圾郵件

- 〝工具〞-> 〝郵件規則〞
- 選用反垃圾郵件軟體 Spam



使用〝郵件規則〞的概念

- 選擇符合〝規則〞的條件
  - 寄件者是...
  - 主旨包含...
  - 郵件本文包含...
  - ...
- 選擇符合〝規則〞的動作
  - 移至特定的資料夾
  - 刪除
  - ...

釣魚信件(Phishing)

citibank

Dear Citibank Member,

As part of our continuing commitment to protect your account and to reduce the instance of fraud on our website, we are undertaking a period review of our member accounts.

You are requested to visit our site, and fill in the required information.

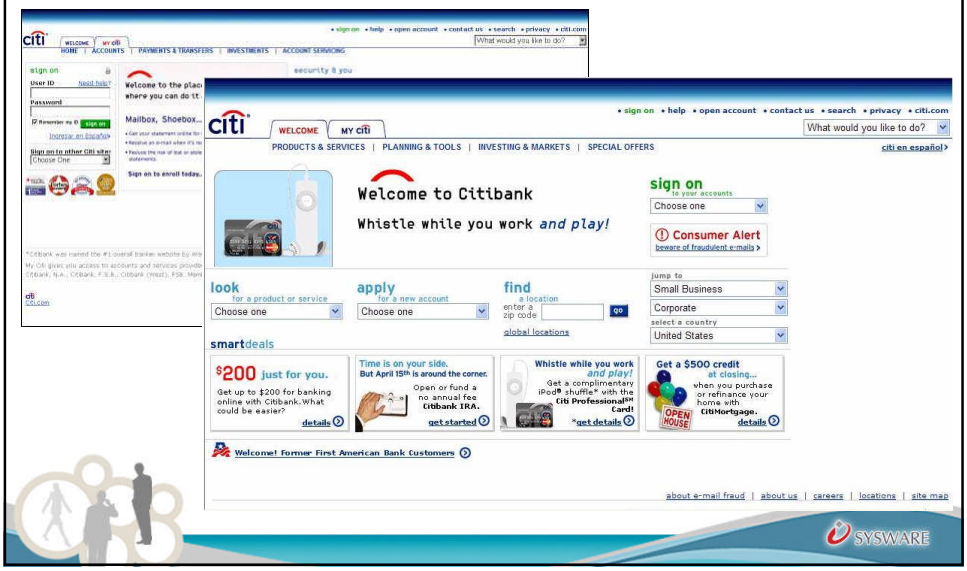
https://web.da-us.citibank.com/cgi-bin/citifi/scripts/login2/login.jsp

This is required for us to continue to offer you a safe and risk free environment to send and receive money online and maintain the experience.

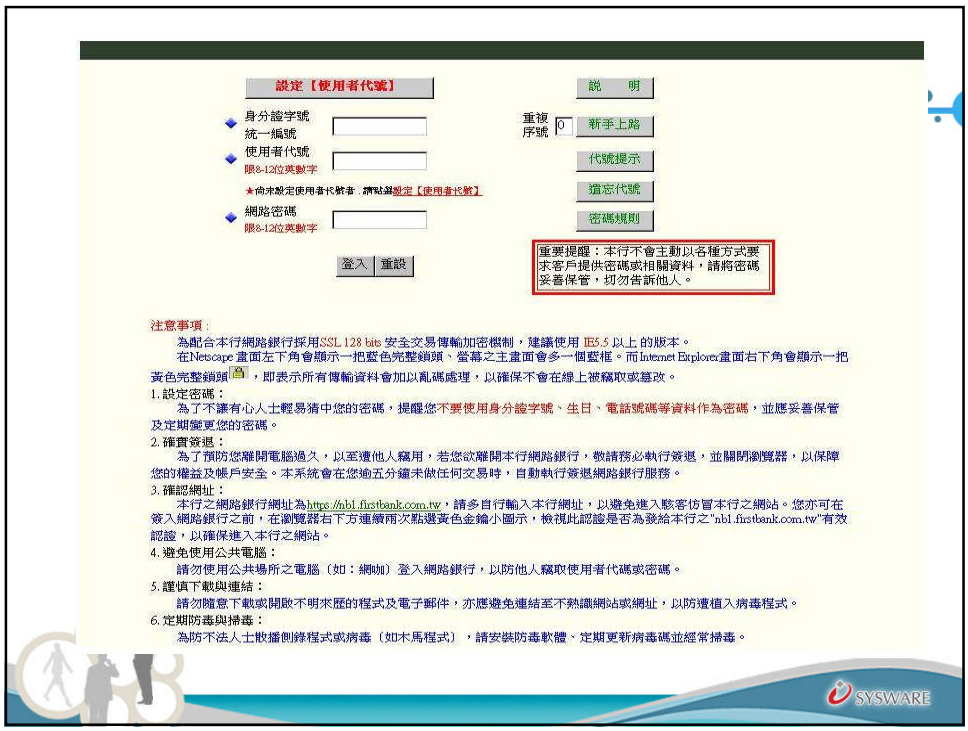
Thank you,

Accounts Management

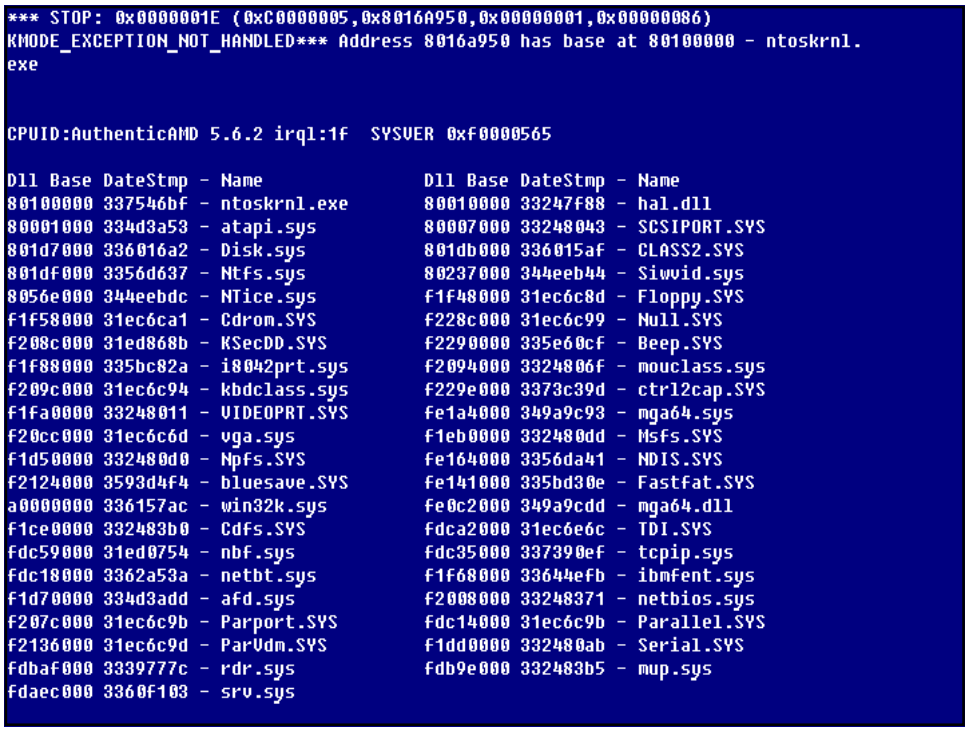
那一個網站是真的呢？


citi
WELCOME
MY citi
PRODUCTS & SERVICES | PLANNING & TOOLS | INVESTING & MARKETS | SPECIAL OFFERS
Welcome to Citibank
Whistle while you work and play!
sign on
Choose one
Consumer Alert
look
apply
find
Small Business
Corporate
United States
smartdeals
$200 just for you.
Welcome! Former First American Bank Customers
about e-mail fraud | about us | careers | locations | site map
SYSWARE


元萬百逾領盜 行銀路網侵入客駭
外銀網路銀行查詢服務為主
肚下吞硬業行銀國美
失損元美億十數
SYSWARE


設定【使用者代號】
說　明
身分證字號
統一編號
重複序號
0
新手上路
使用者代號
限8-12位英數字
代號提示
★尚未設定使用者代號者，請點選設定【使用者代號】
遺忘代號
網路密碼
限8-12位英數字
密碼規則
登入
重設
重要提醒：本行不會主動以各種方式要求客戶提供密碼或相關資料，請將密碼妥善保管，切勿告訴他人。
注意事項：
為配合本行網路銀行採用SSL 128 bits 安全交易傳輸加密機制，建議使用 IE5.5 以上 的版本。
在Netscape 畫面左下角會顯示一把藍色完整鎖頭、螢幕之主畫面會多一個藍框。而Internet Explorer畫面右下角會顯示一把黃色完整鎖頭，即表示所有傳輸資料會加以亂碼處理，以確保不會在線上被竊取或篡改。
1. 設定密碼：
為了不讓有心人士輕易猜中您的密碼，提醒您不要使用身分證字號、生日、電話號碼等資料作為密碼，並應妥善保管及定期變更您的密碼。
2. 確實簽退：
為了預防您離開電腦過久，以至遭他人竊用，若您欲離開本行網路銀行，敬請務必執行簽退，並關閉瀏覽器，以保障您的權益及帳戶安全。本系統會在您逾五分鐘未做任何交易時，自動執行簽退網路銀行服務。
3. 確認網址：
本行之網路銀行網址為https://nbl.firstbank.com.tw，請多自行輸入本行網址，以避免進入駭客仿冒本行之網站。您亦可在簽入網路銀行之前，在瀏覽器右下方連續兩次點選黃色金鑰小圖示，檢視此認證是否為發給本行之"nbl.firstbank.com.tw"有效認證，以確保進入本行之網站。
4. 避免使用公共電腦：
請勿使用公共場所之電腦（如：網咖）登入網路銀行，以防他人竊取使用者代碼或密碼。
5. 謹慎下載與連結：
請勿隨意下載或開啟不明來歷的程式及電子郵件，亦應避免連結至不熟識網站或網址，以防遭植入病毒程式。
6. 定期防毒與掃毒：
為防不法人士散播側錄程式或病毒（如木馬程式），請安裝防毒軟體、定期更新病毒碼並經常掃毒。
SYSWARE


SYSWARE
揭開特洛伊木馬面紗
李烜旭　NeoLi
neoli@sysware.com.tw

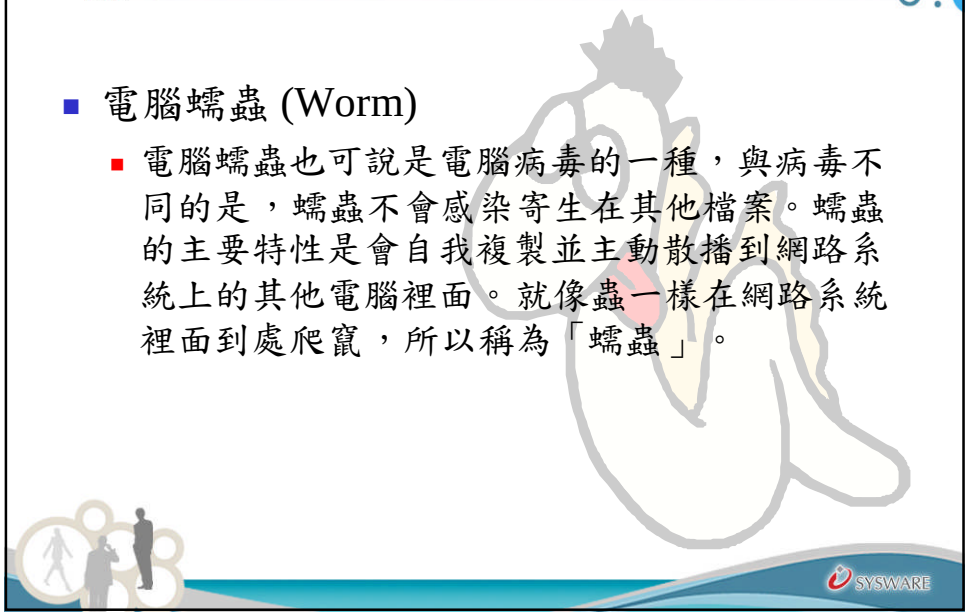


電腦病毒

- 電腦病毒 (Virus)
  - 電腦病毒是一種電腦程式，設計有特定的功能，並且會感染寄生或附著在別的電腦程式或文件檔案裡面。有些電腦病毒就只有自我複製這個單一的功能與目的，有些電腦病毒則會破壞電腦裡面的資料，甚至會破壞電腦系統(如：CIH)。

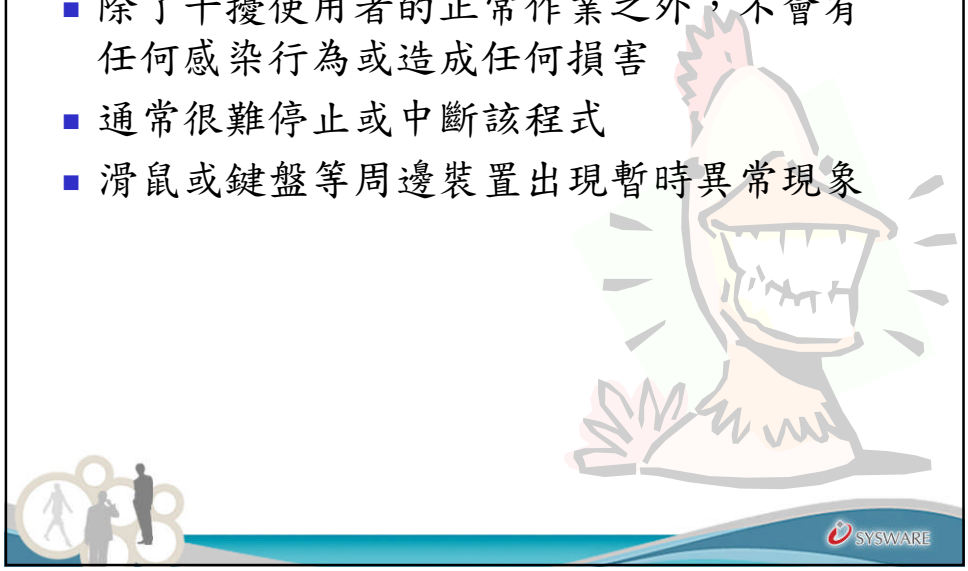
電腦蠕蟲

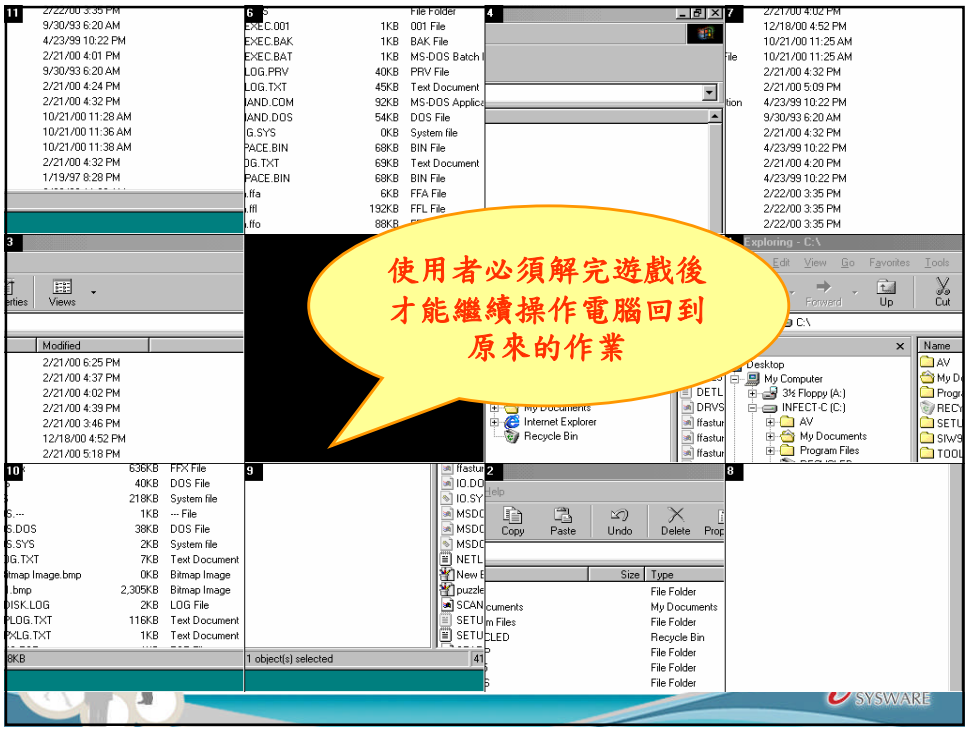
- 電腦蠕蟲 (Worm)
  - 電腦蠕蟲也可說是電腦病毒的一種，與病毒不同的是，蠕蟲不會感染寄生在其他檔案。蠕蟲的主要特性是會自我複製並主動散播到網路系統上的其他電腦裡面。就像蟲一樣在網路系統裡面到處爬竄，所以稱為「蠕蟲」。



惡作劇程式

- 除了干擾使用者的正常作業之外，不會有任何感染行為或造成任何損害
- 通常很難停止或中斷該程式
- 滑鼠或鍵盤等周邊裝置出現暫時異常現象

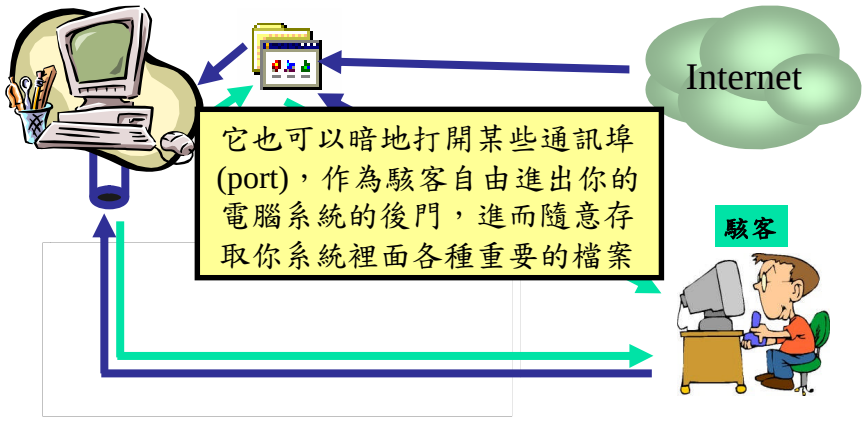




特洛伊木馬

- 特洛伊木馬 (Trojan Horse)
  - 特洛伊木馬 (或簡稱 Trojan) 是一種電腦程式，偽裝成某種有用的或有趣的程式，比如螢幕保護程式、算命程式、電腦遊戲等，但是實際上卻包藏禍心，暗地裡做壞事；它可以破壞資料、騙取使用者的密碼等等。一般定義上，特洛伊木馬不會自我複製，也不會主動散播到別的電腦裡面。

特洛伊木馬駭客工具



駭客工具是一種具有特殊目的惡性程式，它可以設計來做遠端遙控或挖掘某些系統的後門等等。

SYSWARE

[科技專輯]

木馬偷密碼 台新與富邦網路銀行遭盜領

木馬偷密碼 台新與富邦網路銀行遭盜領

國內首度出現網路銀行帳號被木馬程式竊取密碼而盜領的犯罪案例。目前有台新與富邦兩銀行向刑事局報案，並緊急關閉網路銀行的「非約定帳戶」轉帳功能，避免損失擴大。《全文》

木馬入侵 就像在電腦裝針孔

網路族如何避免遭「木馬程式」侵入？專家建議，除了隨時以防毒程式掃描電腦外，最重要的是絕對不要去點選打開來路不明的電子郵件，因爲僅僅可能是打開一封電子賀卡、連結一個網站頁面，都可能導致「木馬程式」侵入你的電腦、竊取你的機密資料。《全文》

駭客功力高 追查不容易

台新及富邦銀行傳出駭客入侵客戶的電子郵件，植入「木馬程式」再竊取被害人網路銀行帳號及密碼，再利用人頭帳戶轉帳盜領。刑事局偵九隊查出，多名被害人存款被轉至國外洗錢，不排除是國外電腦犯罪集團勾結國內不法分子共同犯案。《全文》

SYSWARE

SYSWARE

模擬特洛伊木馬！

SYSWARE

【防範有道】養眼的切勿輕易下載密碼常變更妥善保管

警方昨日公佈查獲不法集團，利用夾藏木馬程式的色情圖片，盜取他人帳號、密碼案。刑事局偵九隊隊長李相臣呼籲使用電腦民眾，除定期對電腦進行全面掃毒工作，對於不明來源色情圖片，切勿輕易下載、觀看，並且注意自身帳號、密碼之保管，定期變更密碼，以防帳號資料被盜用。警方指出，嫌犯等人所散發、張貼的色情養眼圖片，都會取名成引人暇想的名稱，如：台灣的故事尋找山中裸女、各國空姐、好色的客人、林志玲全集系列、馬子舒琪等，以吸引好色人士下載、觀看，藉以植入木馬程式，一般民眾根本很難發覺。警方查獲溫女集團犯案手法，是由台灣集團負責收集帳號前置作業，由大陸集團從事後續網路詐騙等部份。被側錄的帳號都未被更改密碼，遭盜用者無從查覺。警方發現，溫女等人利用這個手法作案，只要曾上過雅虎奇摩家族下載色情圖檔的人，都可能遭到植入木馬程式側錄帳號資料。警方為免受害範圍擴大，除將查扣的帳號資料，交由雅虎奇摩等相關公司清查外，並通知帳號持有人儘速更改密碼。偵九隊隊長李相臣呼籲各網友，定期對電腦進行全面掃毒工作，同時注意自身帳號、密碼的保管，定期變更密碼，並且勿下載不明檔案，以防帳號被側錄、盜用。

SYSWARE

網路安全防護檢測

- 安裝防毒軟體並定期更新病毒碼
- 定期更新Windows Update
- 不要隨意連結不明的網站
- 不要隨意下載不明的程式
- 出現異常現象時，檢測本機狀態
  (工作管理員→處理程序;netstat -an)
- 定期備份(乾淨備份)

SYSWARE

SYSWARE

P2P軟體潛在風險

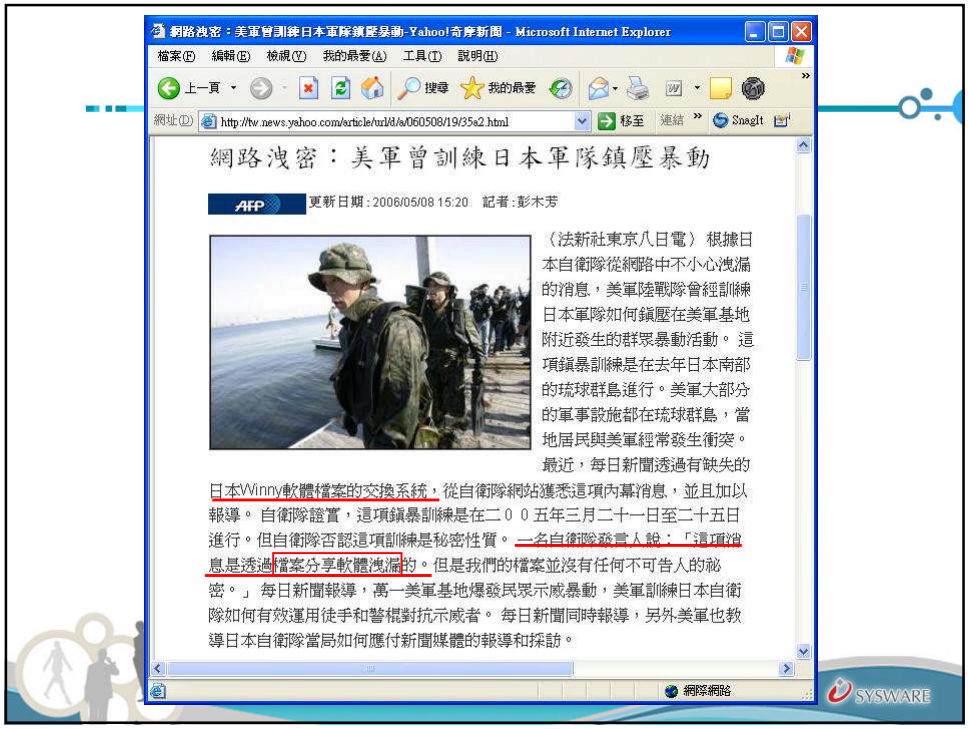
何謂P2P ？

- 「Peer to Peer」是一種點對點通訊傳輸工具,是一種New Internet Directory Service。Website與Browser間的溝通,採用的是HTTP/FTP的標準協定。
- 在HTTP標準協定下,大家所熟悉的Portal Site或Search Engine,幫您分類並搜尋存在網際網路上網站的資訊(Internet Directory Service)。
- P2P傳送檔案時，可以同時連接多個下載點，分散式下載檔案以快速完成檔案下載為目標。

P2P軟體潛在風險

- P2P軟體程式可能遭有心人士放置木馬後門程式，或是病毒蠕蟲。

- 使用P2P軟體工具後，
- 會將MyDocument目錄開放分享。
- 下載影音檔案，多半為mp3、avi、mpeg等，可能造成侵權問題。影響工作或企業、政府形象。


網路洩密：美軍曾訓練日本軍隊鎮壓暴動-Yahoo!奇摩新聞 - 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://tw.news.yahoo.com/article/url/d/a/060508/19/35a2.html
網路洩密：美軍曾訓練日本軍隊鎮壓暴動
AFP 更新日期：2006/05/08 15:20 記者：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，這項鎮暴訓練是在二００五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。」每日新聞報導，萬一美軍基地爆發民眾示威暴動，美軍訓練日本自衛隊如何有效運用徒手和警棍對抗示威者。每日新聞同時報導，另外美軍也教導日本自衛隊當局如何應付新聞媒體的報導和採訪。
網際網路
SYSWARE


SYSWARE
回應與討論

SYSWARE

Thank you ！

沒有百分百的資訊安全，只有有效的風險管理和控制