資安與生活

雲林科技大學資管系
古東明
2010/5/13

Web Security

網站有毒？


高雄市政府教育局電子報 - 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
NOD32防毒系統警告：IMON - 網絡監視器
有病毒被偵測出來
警告資訊
檔案:
http://www.woai117.cn/bak.exe
病毒：
Win32/AutoRun.NAD virus
註解：
這物件包含一些有害的代碼。
複製到隔離區
顯示警告視窗
傳送檔案作分析
停止
中斷
幫助
關閉
資訊
NOD32
Antivirus System
網際網路
開始
Process Explorer...
高雄市政府教...
NOD32防毒系...
下午 11:34

攻擊原理


竊取資料
瀏覽者
殭屍網路
惡意連結
取得資料
瀏覽網頁
SQL injection
知名網站
犯罪者
5.竊取資訊至伺服器
4.植入惡意程式碼
3.背景導向惡意連結
1.攻擊網站漏洞
2.植入惡意連結
Web Threats !!

所有網頁 圖片 新聞 網上論壇 更多 »

女人國女性購物 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

女人國女性購物社群入口網站

這個網站可能會損害您的電腦。

提供網路開店、網路購物、討論區、電子報專業行銷、心理測驗、貼圖、免費相簿、問卷調查、搜尋引擎、網站登錄、線上學習之女性購物社群入口網站.

www.iamlady.net/ - 類似網頁

女人國免費網路相簿

這個網站可能會損害您的電腦。

女人國免費網路相簿 免費個人相簿、明星寫真、生活攝影、活動貼圖、親子照片、電子賀卡、靈異相片、桌布、桌面下載、圖庫與網頁素材分享。 ... 女人國是女性購物社群入口網站，以下簡稱為本站，其中提供相簿發表平台，使用者必須遵守本站相關規定。 ...

www.iamlady.net/myphoto/Mall_covenant.asp - 類似網頁

大砲開講 女人國女性購物社群入口網站被植入惡意連結

女人國女性購物社群入口網站被植入惡意連結. Roger | 04 Oct, 2007 17:18. 請按我..繼續閱讀全文. ... 女人國女性購物社群入口網站被植入惡意連結 · 創意先進有限公司(HOT)網站被植入惡意連結 · 彰化秀傳紀念醫院網站被植入惡意連結 · 僑光技術學院網站被 ...

www.ithome.com.tw/plog/index.php?op=ViewArticle&articleId=11035&blogId=673 - 28k - 頁庫存檔 - 類似網頁

大砲開講: 女人國女性購物社群入口網站被植入惡意連結

女人國女性購物社群入口網站被植入惡意連結. 女人國女性購物社群入口網站被植入惡意連結，此惡意程式為TROJ_DLOADER.PMG，最近有瀏覽這個網頁的網友，應該要盡速檢查自己的電腦，請各位暫時不要瀏覽這個網站，以免中毒。 惡意連結是放置在某些頁面首頁 ...

rogerspeaking.blogspot.com/2007/10/blog-post_8806.html - 75k - 頁庫存檔 - 類似網頁

Client-Side Attack

- Drive-by-download (瀏覽即下載): 在使用者不知情或是不了解知情況下，下載惡意程式於用戶端電腦當中。
  - Enable Active-X Component
  - 瀏覽E-mail，網頁，橫幅廣告，被導向惡意連結下載惡意程式

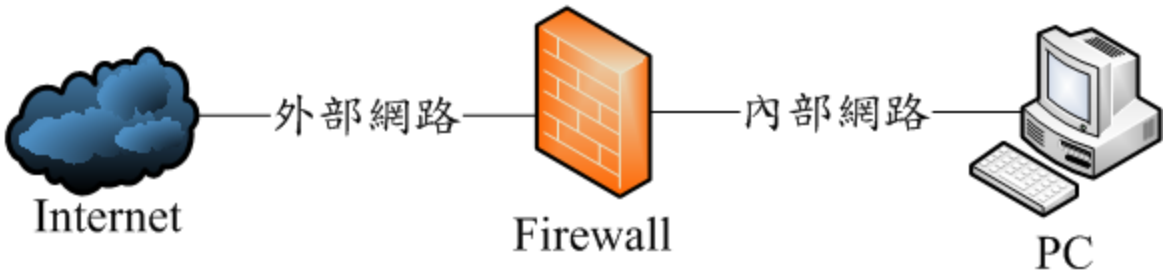
Client-Side Attack

- 如何阻擋Client-Side Attack？
  - 修補Client Application 漏洞，更換新版本
  - 使用網路防毒軟體、防火牆
  - 判定Malicious Server ，建立Blacklist

Firewall

防火牆的定義

- 用來控制網路存取的設備，並阻絕所有不允許放行的流量
- 通常由一組軟硬體所組成，基本上是由一台主機，包含作業系統及安裝防火牆應用軟體而構成，通常建置於網際網路與內部網路之間，作為內部與外部溝通與管制的橋樑



軟體防火牆 V.S. 硬體防火牆

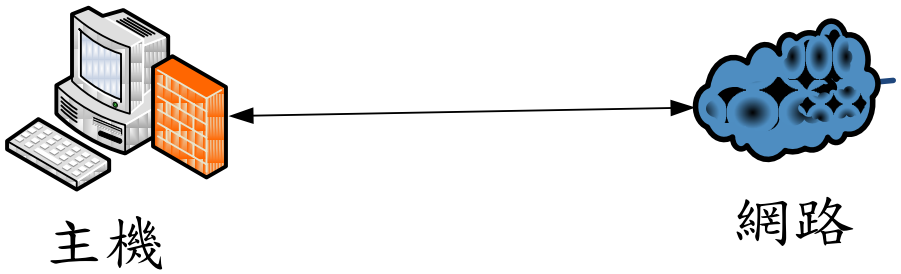
- 軟體防火牆
  - 通用架構的PC硬體
  - Unix或是windows系列的通用作業系統
  - 例：PC Tool 、Checkpoint firewall及Firestarter
- 硬體防火牆
  - 量身訂製的硬體(ASIC)及作業系統
  - 強調高效能，實用性，處理速度
  - 內部實際上也是靠軟體在運作
  - 例：Cisco pix與Netscreen等

防火牆的架構

- 依防火牆的在網路環境中的位置區分
  - 單機防火牆
  - 閘道式防火牆
  - 通透式防火牆(Transparent Firewall)

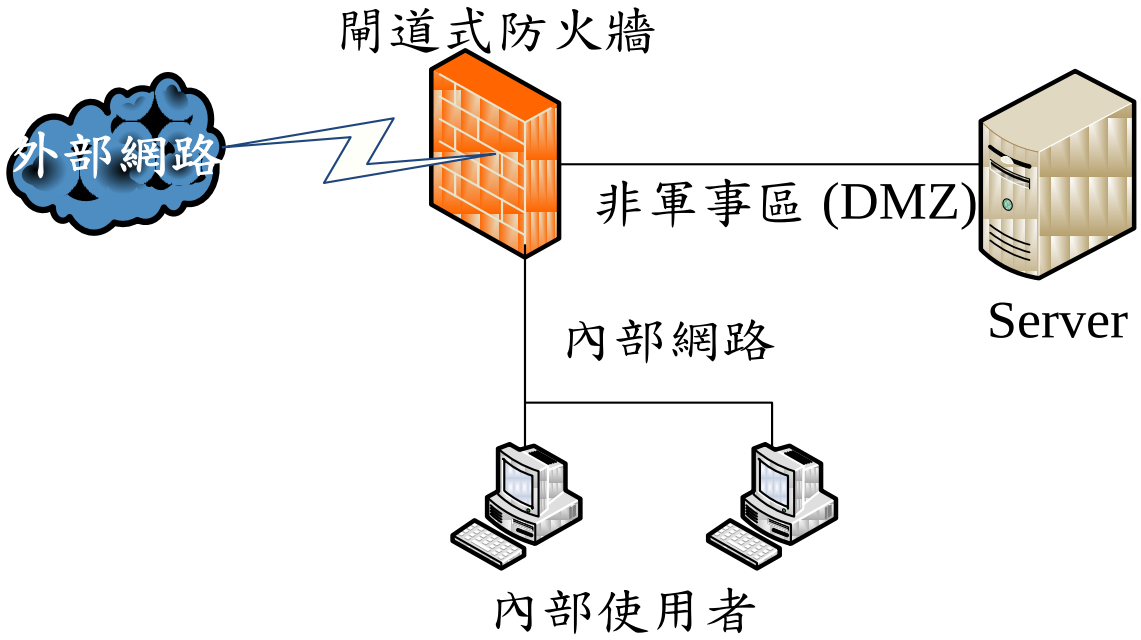
單機防火牆

- 安裝在本機主機上
- 通常為軟體防火牆
- 凡進出本機的封包皆會受到監控
- 保護的範圍僅限本機



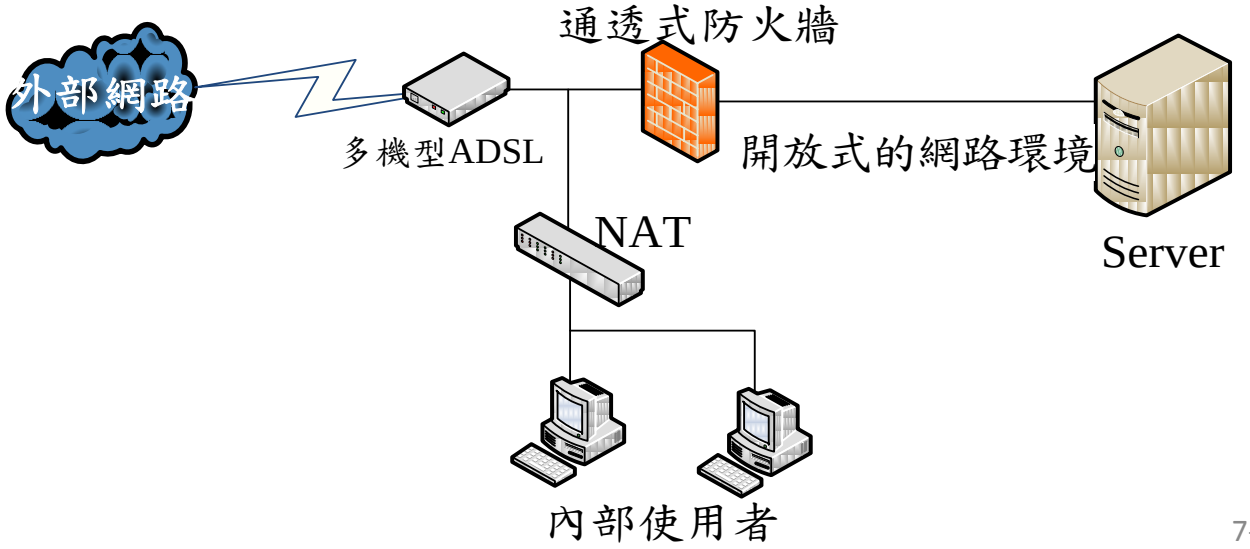
閘道式防火牆

- 部署在閘道位置的防火牆
- 保護的範圍是整個內部網路
- 利用NAT服務隱匿內部使用者



通透式防火牆(Transparent Firewall)

- 部署在橋接器位置的防火牆
- 防火牆本身無須指定IP
- 保護的範圍是位於防火牆後端之伺服器
- 隱密性相當高

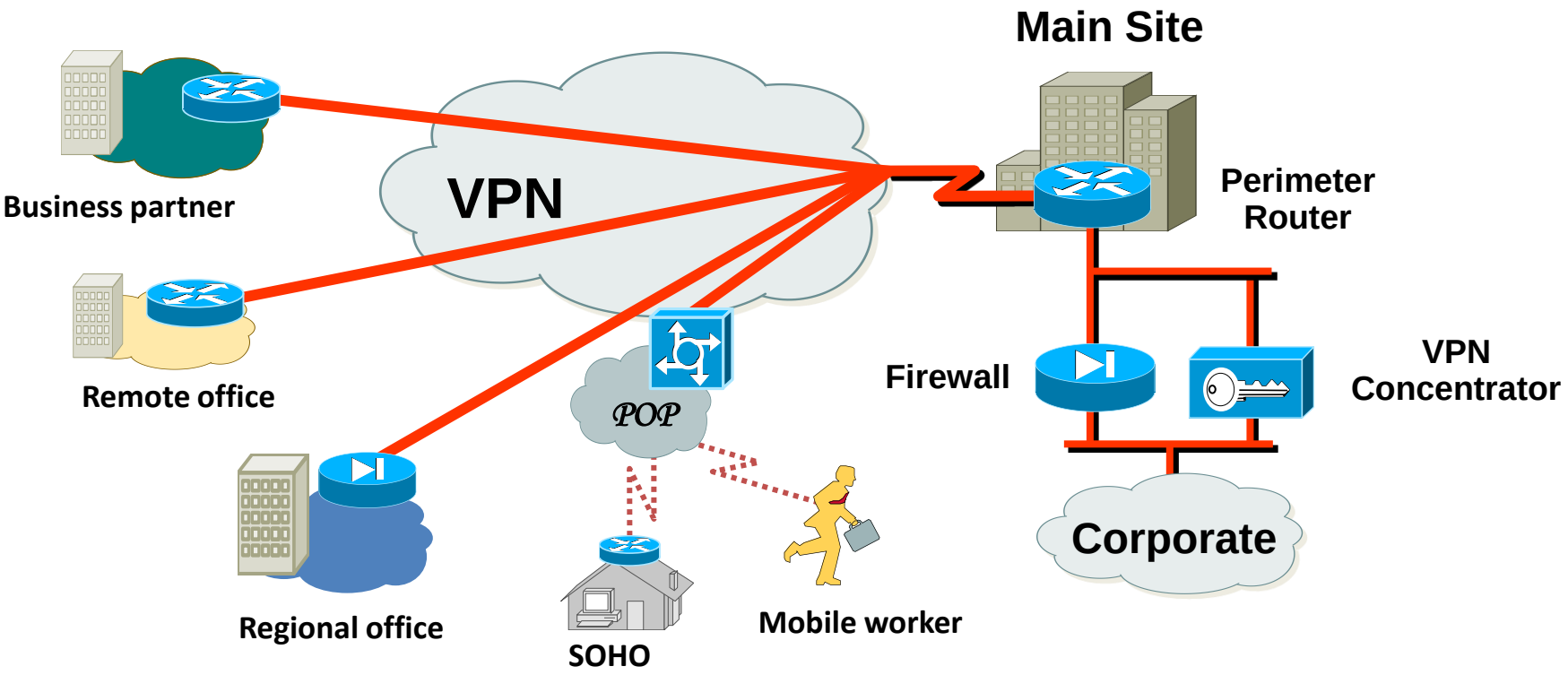


防火牆的限制

- 無法防範全新的攻擊模式
- 無法防範病毒
- 無法管理不經過防火牆的連線
- 無法防止防火牆自己內部的不法行為

VPN & SSL

VPN


Main Site
VPN
Business partner
Perimeter Router
Remote office
POP
Firewall
VPN Concentrator
Corporate
Regional office
SOHO
Mobile worker

VPN (virtual private networks)

- 虛擬私有網路，利用有效的編碼認證和加密演算法來提供資料保護的安全通訊通道。
- ATM等提供虛擬固接線路(PVC)服務的網路。我們也可稱它為IP VPN(以IP為主要通訊協定)。公眾的網路上透過這個虛擬的安全網路，可以用來傳輸公司或是企業內部的資料而不怕被竊取。

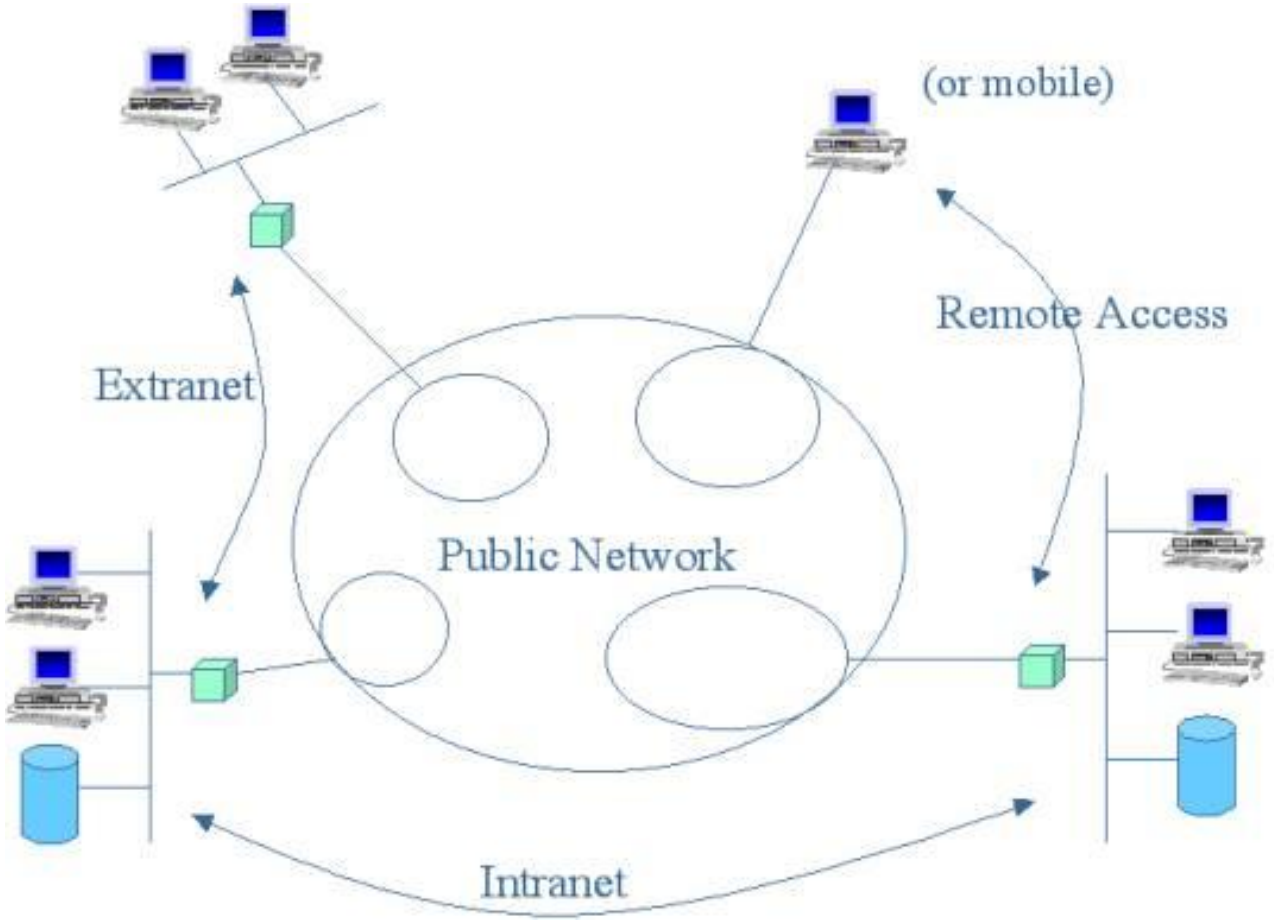
IP VPN相較於傳統VPN技術的不同

- 其和Frame Relay與ATM所提供的固定虛擬線路(Permanent Virtual Circuit,PVC)最大的不同:
  - PVC所有設定權掌握在電信單位
  - 連結的單位越多，相關的終端通訊設備成本越高
  - 管理與設定也很繁瑣
  - PVC也無法立即與世界上任何一個使用Internet的單位連結
- 相反地，運用VPN技術可以在Internet上立即擁有屬於自己的私有數據網路，所以近一代的VPN是指建立在Internet上的IP VPN。

VPN種類--環境應用

- (1) Intranet VPN
  - 適用於企業的總公司及較大的分公司。
- (2) Extranet VPN
  - 適用於諸如汽車業、零件廠商與產險業的整合服務、金融業之間的轉帳與交易、製造業與供應商的生產流程網路、代工行業(OEM)與客戶間的生產與訂單網路.....等
- (3) VPDN(Virtual Private Dialup Network)/(Remote Access)
  - 適用於企業較小的據點及經常出差到各地的業務人員

VPN種類



VPN技術

- **V－－Virtual－－Tunnel－－ PPTP (software)**
  L2TP (hardware)
  IPSec (hardware)
- **P－－Private－－Secure－－ Privacy**
  Integrity
  Authenticity
- **N－－Network－－Internet**
  Intranet
  Extranet

VPN主要採用四項技術

- 穿隧技術(Tunneling)
  - PPTP、L2TP、IPSec
- 加解密技術(Encryption & Decryption)
  - Symmetric、Asymmetric cryptography
- 密鑰管理技術(Key management)
  - SKIP、IKE
- 使用者與設備身份認證技術(Authentication)
  - PAP、CHAP、X.509

入侵者的動機

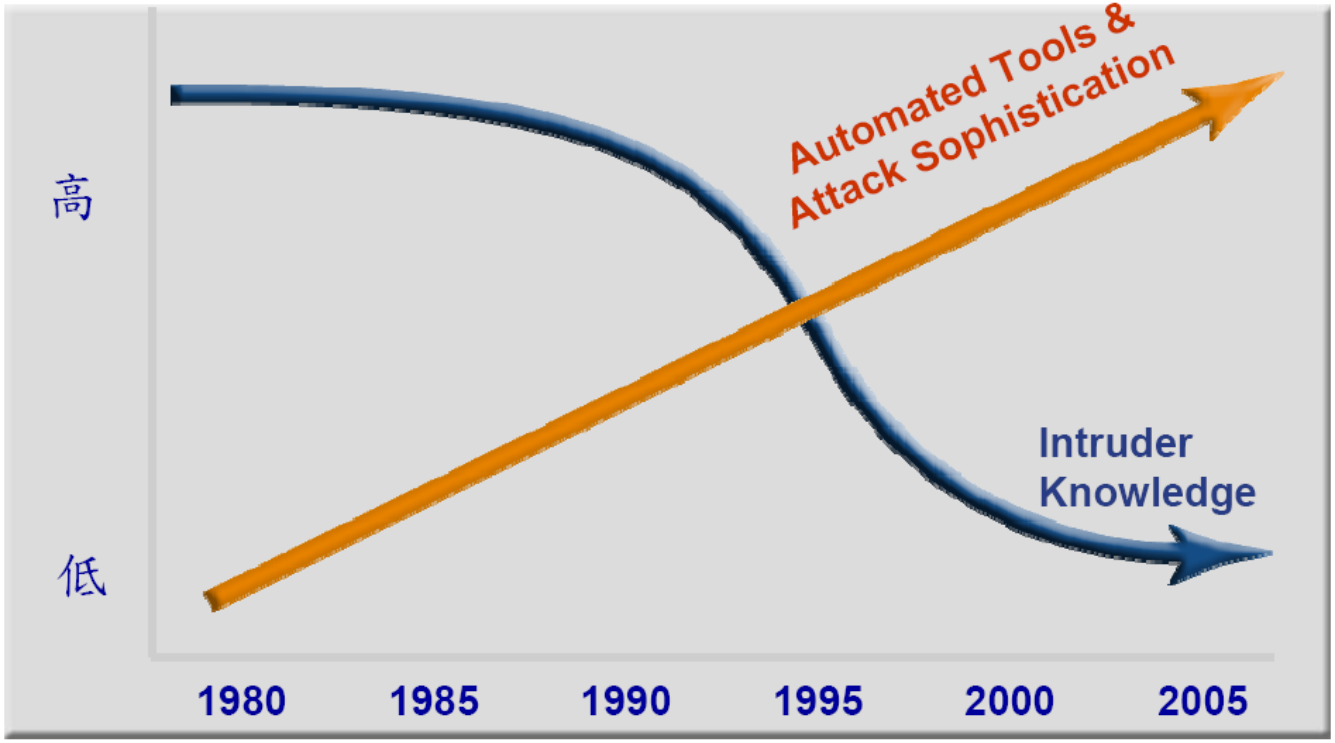
- 檢視系統是否有漏洞
- 好玩、證明自己的功力
- 發洩、表達自己的不滿
- 竊取資料、利益
- 報復
- 變態的破壞

入侵者的目標

- 有弱點的主機
  - Web網站
  - 資料庫
  - 網路設備
  - 提供遠端遙控的主機(shell, remote control)
- 有利益的主機
  - Shell account
  - Game Server
  - 交易主機

當駭客需要豐富的電腦技術知識?

- 要當駭客，不需要太多的技術知識
- 任何人都可以從網際網路下載各種工具



網路釣魚

- 不法駭客將網際網路流量從原本的網站重新導引至另一個看似相同的網站，誘騙人們將使用者名稱及密碼輸入到該偽造網站的資料庫中。

常見的釣魚手法

- Mail信件：釣魚者(駭客)以花旗銀行、eBay、Yahoo!等知名金融網站或拍賣網站的名義，發送主旨為緊急通知的E-mail，要求使用者按下E-mail中的連 結，來更改機密資料。
- 知名網站的超連結：駭客在Yahoo、無名小站等網站提供吸引人之內容，例如：MP3下載、P2P軟體下載等等，引誘使用者點選超連結植入木馬或引誘到假冒網站竊取使用者資料。

常見的釣魚手法

- 可能為詐騙之郵件標題
  - 「請確認您的帳戶資訊。」
  - 要求更新信用卡資訊
  - 「如果您不在48 小時內回應，您的帳戶將會關閉。」
  - 「親愛的客戶，請按一下下方的連結，進入您的帳戶。」

常見的釣魚手法

- 偽裝相似網站名稱：例如台灣土地銀行網址是www.landbank.com.tw，釣魚網站網址是www.1ankbank.com.tw，差別是正牌網站land的第一個字是英文字母「l」，釣魚網站是用阿拉伯數字「1」。
- 無名小站
  - http://www.wretch.cc/
  - http://www.vvretch.cc/

- 遊戲橘子
  - http://tw.gashcard.gamania.com
  - http://tw.gashcard.garnania.com
- 天堂II
  - http://lineage2.plaync.com.tw
  - http://1ineage2.plaync.com.tw

如何減少網路釣魚的危害

- 別隨便按下信件或網站中的網址
- 使用SSL（Secure Socket Layer）機制：這類網站網址開頭為「https://」，而且在IE的右下角落會出現掛鎖圖示來提醒使用者。
- 手動輸入網址
- 輸入帳號密碼前確認網址正確無誤
- 輸入錯誤的帳號密碼
- 經常更換密碼

帳號密碼

Hotmail密碼外洩事件

- 排名第一的密碼是 123456
- 傻瓜密碼(包含生日、身份證、電話號碼
- 安全強度經不起考驗
- 遭破解的機率極高

Hotmail密碼外洩事件

- 以下是前10名常用的密碼：:
- 1. 123456 - 64
- 2. 123456789 - 18
- 3. alejandra - 11
- 4. 111111 - 10
- 5. alberto - 9
- 6. tequiero - 9
- 7. alejandro - 9
- 8. 12345678 - 9
- 9. 1234567 - 8
- 10. estrella - 7

Hotmail密碼外洩事件

- 看到沒，前10名有一半是用阿拉伯數字，就是所謂的傻瓜密碼。
- 提供幾個小訣竅來保護線上密碼的安全。
  1. 用容易記不容易猜的密碼
     - 混合使用數字，大小寫字母和特殊符號，例如!£$@&。
  2. 經常更替
     - 還是老話一句密碼就像牙刷，要經常更替，且不要與人共用。

帳號密碼妙關聯，一般會員知多少

- 身為現在網路的一份子，你有多少組帳號密碼呢？E-Mail就好幾個，還有一堆會員帳號，不是嗎？很顯然的這裡面有很大的商機，但遲遲不見相關應用產品或技術。我大膽的說，帳密問題不解決，未來雲端將沒有安全性可言。

  最近這個夯很大，來做個解說吧！ (facebook)

- 上圖，大家應該頗熟悉這畫面，帳號是取用電子郵件名稱，我甲意，你的密碼是啥呢？有沒想過幾個劇本呢？
  一、電子郵件名稱就是密碼？生日？[太好猜，社交一下很有機會]
  二、密碼是123456。[弱密碼，隨便猜猜]
  三、電子郵件信箱也是這邊登入的密碼。[這劇本非常奧妙，不少人都是用這吧]

帳號密碼妙關聯，一般會員知多少

- 看完帳號部分，接下來也要看一下密碼復原機制。不忘密碼枉為人...XD。

很簡單的機制，我也頗喜歡的，忘記密碼也不用擔心，直接把密碼復原的連結寄到帳號，也是一電子信箱，亦無法變更信箱...讚。這可以玩某種 One-Time Password 的把戲耶，密碼設定到極複雜，用完然後就忘記...XD。

這裡面需要注意幾個問題：
1. 帳號設定使用的電子信箱必須永久有效，不然，密碼忘記可就麻煩了。
2. 帳號設定使用的電子信箱管理權被拿走，這可是一舉淪陷多個帳號。
3. 帳號設定使用的電子信箱密碼忘記，哪，看看信箱的忘記密碼機制能否救了。
4. 啥！密碼復原郵件被當垃圾郵件，收不到@@...XD
5. 這點才是我的重點，兩邊的密碼使用都是一樣的，應該有很多人都是這狀況的，會有啥問題呢？可妙了。

帳號密碼妙關聯，一般會員知多少

- 這時我們先切換到另外一個場景，你曾經填寫過哪些會員資料呢？不會都一五一十的寫吧！

設定電腦密碼的技巧

- 不要用a、b、c等有順序的字母或數字開頭
- 不要以單字、生日、數字做為密碼
- 密碼中的英文最好有大小之分

防拍賣詐騙-推動態密碼鎖

- 拍賣服務及會員中心推出動態密碼鎖（Dynamic Password），防止密碼被駭客破解

小心愛用複製貼上的人

- 對於喜歡用複製、貼上(copy & paste)功能輸入密碼的使用者，得特別當心。只要做簡單的CTRL+C 動作，你就可以驚訝地發現前一秒剛剛複製的資料，下一秒居然出現在陌生的網站當中。

- **STEP1.**輸入”您的剪貼簿可能遭綁架”，按右鍵複製

小心愛用複製貼上的人

- **STEP2.**到示範網站看看發生什麼事，果真出現了”您的剪貼簿可能遭綁架”字眼。

小心愛用複製貼上的人

- 使用網站會員、網路銀行、線上遊戲密碼紀錄在某個文字檔
- CTRL+C…接著 CTRL+V
- **手動輸入密碼與使用者帳戶資訊較安全**

密碼破解

- 軟體介紹
  - 軟體名稱：CopiXP
  - 授權類型：共享軟體
  - 它能將 Windows 視窗中星號 (*****) 背後隱藏的密碼顯示出來並複製到剪貼簿中，讓使用者在遺忘密碼時還有找回來的機會

密碼破解

- 軟體介紹
  - 軟體名稱：Passware Kit Enterprise
  - 授權類型：共享軟體
  - Passware Kit 結合了 25 種以上的密碼回復模組，讓你以十分便利而低成本的方式快速地找回遺失的資訊。

PDF難解的安全問題

- 利用PDF檔案的「/Launch」指令，就能讓PDF檔案去啟動其他程式

- 搭配社交工程手法，在PDF檔案開啟時同 步跳出一個對話框，欺騙使用者按下對話框中的按鈕，就能夠啟動其他程式。
- 目前尚無有效防堵這種攻擊的方法

PDF難解的安全問題

- 陸續有國外資安研究人員指出PDF根本性的安全問題，並驗證了攻擊手法的可行性。
- 這個攻擊手法並不是利用PDF Reader軟體的漏洞，而是利用PDF提供的合法指令，來啟動其他程式。
- 作法屬於合法行為
- 目前尚無有效防堵這種攻擊的方法

PDF難解的安全問題

- 可藉由惡意的PDF檔案去感染一般正常的PDF檔案。
- 開啟正常的 PDF檔案，確認了PDF Reader閱讀軟體已經關閉JavaScript功能。（JavaScript功能會被利用在 背景中下載安裝惡意程式。）
- 接著開啟被動了手腳的惡意PDF檔，然後再開啟原本是正常的PDF檔，開啟之後，就又跳出了瀏覽器視窗，而 且自動連結到一個特定的網站。

PDF難解的安全問題

- 目前已經有人發展出模仿這個手法的套裝工具了。
- 這個問題是PDF 的根本性問題，除非是完全切除這些指令的功用，不然這種運用合法指令的攻擊手法是最難預防的。

網路報稅安全

- 信用卡帳號等資料會有外洩問題
- 5成的人使用過網路報稅
- 僅有 3成左右的人不敢嘗試網路報稅
- 移除P2P 檔案分享軟體
- 去年爆發的網路報稅資料大規模外洩，就是分享軟體惹的禍
- 安裝防毒防駭軟體
- 小心遇上網路釣魚

網路報稅資訊安全

- 網路報稅注意事項
  - 正確網址：http://tax.nat.gov.tw
  - 勿安裝P2P共享軟體，報稅後個人資料移除
  - 勿用公眾電腦報稅
  - 勿在無防毒軟體、防火牆環境報稅
  - 報稅前電腦掃毒
  - 報稅後上網查詢資料上傳情形
  - 勿請他人代為報稅

網路報稅服務資訊安全說明

- 「網路申報繳稅系統」的安全機制
  - 機房管理安全機制
  - 網路安全機制
  - 系統安全防護機制
  - 納稅義務人下載所得資料及上傳申報資料安全機制
  - 報稅軟體安全機制

信用卡網路付款

- 「網路信用卡付款購票」步驟
  1. 先完成訂票
  2. 連上網路信用卡付款網站
  3. 線上信用卡刷卡購票
  4. 取票搭車
- 系統之安全性
  - 採用全球網頁最高加密技術 SSL128bit 以確保您信用卡資料的傳遞安全

網路信用卡付款安全嗎

- 網路信用卡付款安全嗎？
  - 輸入資訊：卡號、到期日、檢查碼
  - 發生冒用交易疑義，而商家不能舉證是否為持卡人使用時，商家須優先承擔被盜刷風險
  - 商店報案，警方就可令ISP交出IP記錄詢線抓到真正的盜刷者
  - 網購時需輸入密碼的認證
  - 線上刷卡會立即傳送簡訊的服務

木馬(Trojan Horse)

- 佯裝成無害的程式
  - 如螢幕保護程式、遊戲或其它類型的應用程式
- 通常由電子郵件或網路下載程式所散佈
  - 不會自我複製->不是病毒
  - 不會自動散佈->不是病蟲
- 被植入後電腦會被遠端的駭客遙控
- 不要執行來路不明的程式

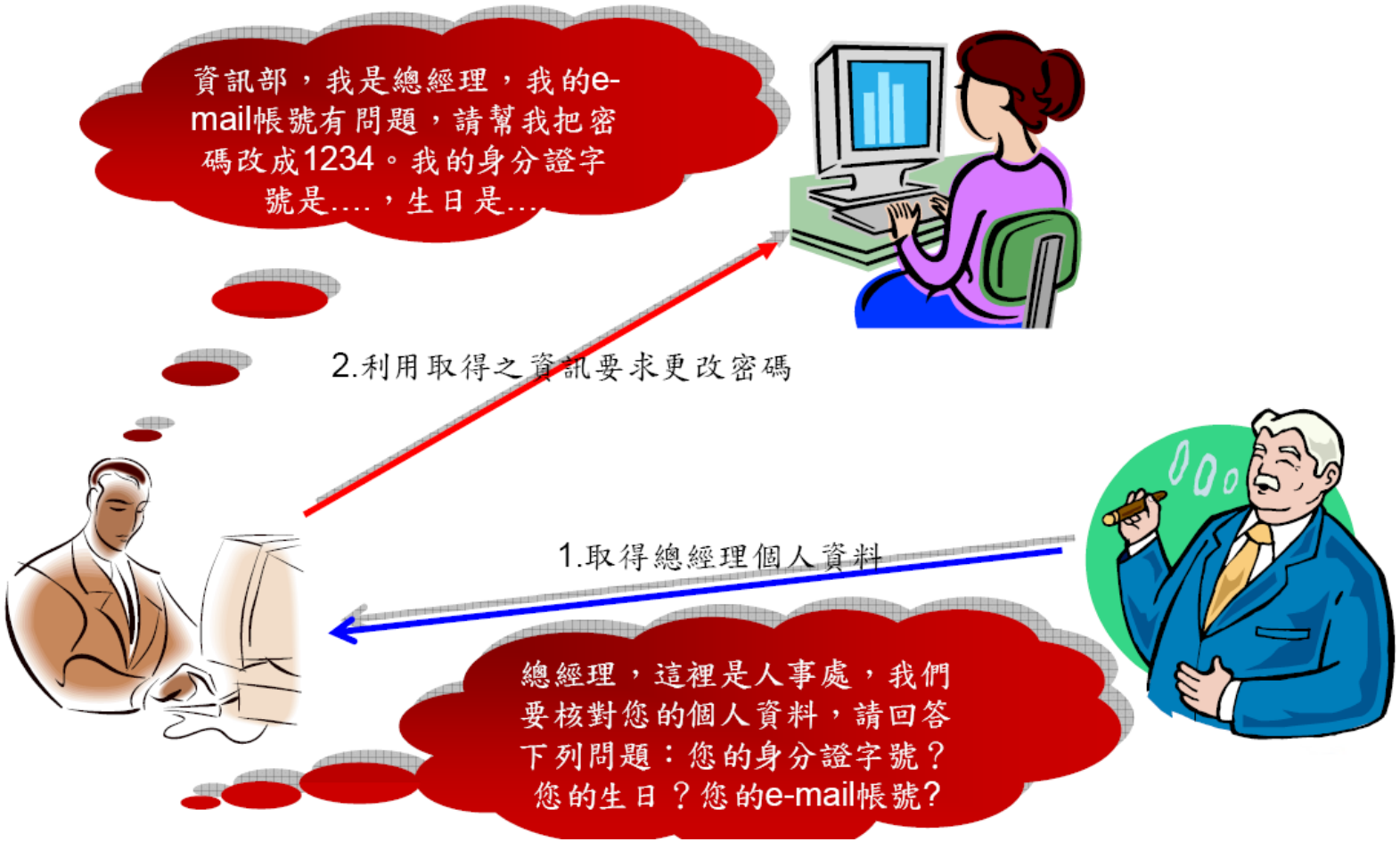
年輕駭客線上遊戲放置木馬程式

- 年僅十七歲的黃姓少年，受到劉姓主嫌教唆，寫出一個新的鍵盤記錄程式，可破解並記錄「天堂」網路遊戲玩家的帳號及密碼。

- 不法分子透過「鍵盤記憶程式」侵入他人電腦，竊取網路帳號密碼及機密檔案。

社交工程

- 利用人性弱點、人際交往上的漏洞
- 不需要使用任何的程式、科技技術
- 常用方式
  - 透過Email
  - 簡訊、電話
  - 親自前往調查
- 獲取帳號、密碼、身分證號碼、姓名、地址
- 或其他可確認身分或機密資料


資訊部，我是總經理，我的e-mail帳號有問題，請幫我把密碼改成1234。我的身分證字號是....，生日是...
2.利用取得之資訊要求更改密碼
1.取得總經理個人資料
總經理，這裡是人事處，我們要核對您的個人資料，請回答下列問題：您的身分證字號？您的生日？您的e-mail帳號?

目標式社交工程共同點

- 長時間臥底
  - 入侵MIS 帳號，潛伏期平均達半年以上
- 社交工程技巧高：
  - 來自同仁的Email: 收集目標對象的信件、平日工作文件電子檔，可延續之前的對談，冒充上司發信/發公文，讓使用者輕易上當。加上某些政府機關允許Client 端接收POP3 Mail，造成安全漏洞**大陸網頁**以收件者有興趣的主題信件（如奧運消息），引導政府員工瀏覽大陸掛馬網頁而中毒

- **攻擊手法：**
- 寄件人來自被冒用的內部員工帳號，內文宛若上層交辦事項，例如指示收件人立即下載教育訓練的PDF檔案。(New！以前的惡意程式植入程式常見的是執行檔，現在改成每天上班都會用到的WORD、Excel、Access、WinZip、RAR、PDF 等應用程式檔案，一旦打開被駭客竄改過看似正常的文件後，惡意程式就會自動執行。)
- 惡意程式下載程式(Downloader)會不斷自網路下載新變種與自我更新，使得傳統防禦方式備受挑戰。
- 攻擊者通常會安裝木馬後門程式於目標機器，有心人士擁有方便的管道，可在受害電腦連線的網路上監聽傳輸資料。

間諜軟體

- 所謂的「間諜軟體」包括間諜程式、廣告軟體、惡意撥號程式、惡作劇程式、駭客工具、遠端存取工具、密碼破解應用程式、鍵盤側錄程式，以及其他未分類的軟體。
- 會在未經使用者同意的情況下進行廣告、收集私人資訊，或修改電腦設定等行為的軟體
- 間諜程式掃瞄並非病毒或惡意的程式碼， 而是危及您隱私的應用程式，允許駭客在您毫無知覺的情況下取得您電腦的控制權。
- 間諜軟體經常隨著下載應用程式的同時，不知不覺地下載到您的電腦上。

被植入間諜軟體的6大徵兆

1. 常常會自動跳出許多廣告視窗。
2. 遊戲或網路帳號、密碼好像被人盜用了。
3. 上網時首頁被改成奇怪的外文或購物網頁，而且無法改回原設定值。
4. 上網速度變慢或者會自動當機。
5. 發現常常有陌生人寄來的email。
6. 網頁瀏覽器出現額外的程式元件，但自己不記得下載過這些元件。

安裝反間諜軟體

- Windows Defender
- http://www.microsoft.com/taiwan/athome/security/spyware/aboutdefender.mspx
- Spyware Doctor™入門版 (從google軟體集安裝)
- http://pack.google.com/intl/zh-tw/pack_installer.html?hl=zh-tw&brand=GPMD&utm_source=zh_tw_TW-et-more&utm_medium=et&utm_campaign=zh_tw_TW
- SpyBot Search & Destroy
- http://www.safer-networking.org/ct/index.html

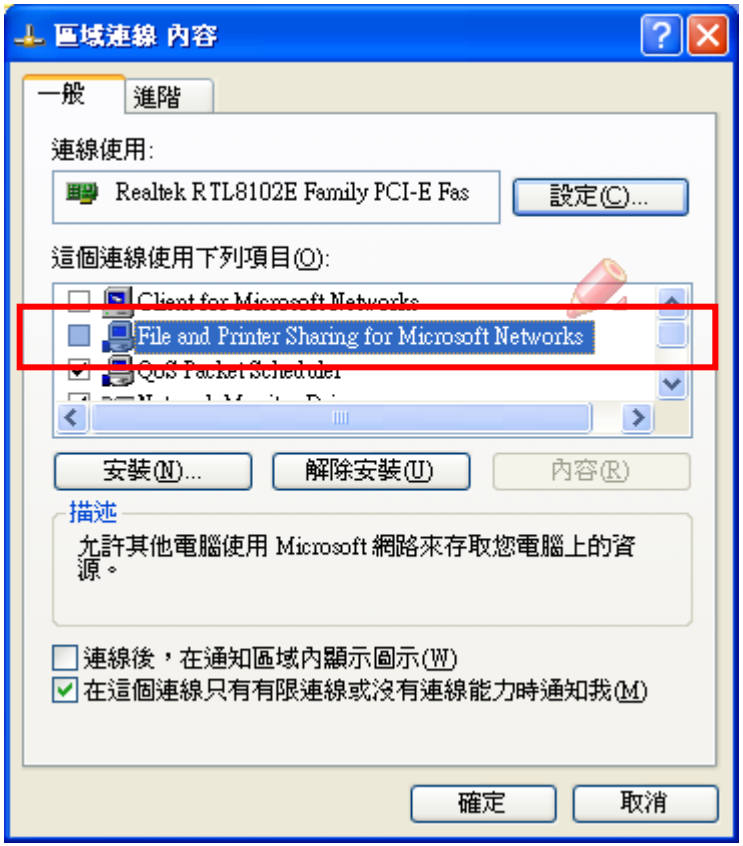
網路芳鄰的資安隱憂

- 網路芳鄰所使用的SFB協定，不僅能在區網中分享，也能用於Internet
- 若主機防火牆保護、共享資料夾未設密碼，或密碼強度不夠，則有心人士很容易透過網路芳鄰竊取資料，甚至取得該主機的控制權

網路芳鄰的資安隱憂

建議：

- 若主機不需要網路芳鄰分享協定時，可將主機內有關 “file and printer sharing for Microsoft network” 網路設定功能取消。
- 共享目錄要設定強度高的密碼，且僅開放讀取權限
- 為防止Internet透過網路芳鄰功能存取區域網路內主機資訊，建議使用防火牆等相關軟硬體阻擋外界對內部主機的port 137-139與445存取


區域連線 內容
一般
進階
連線使用:
Realtek RTL8102E Family PCI-E Fas
設定(C)...
這個連線使用下列項目(O):
File and Printer Sharing for Microsoft Networks
QoS Packet Scheduler
安裝(N)...
解除安裝(U)
內容(R)
描述
允許其他電腦使用 Microsoft 網路來存取您電腦上的資源。
連線後，在通知區域內顯示圖示(W)
在這個連線只有有限連線或沒有連線能力時通知我(M)
確定
取消

取消

網際網路安全守則

網際網路安全守則

- 科技發展日新月異，網際網路威脅亦是如此，提出了 5 項基本原則，協助您在上網瀏覽時保持安全:

- **1. 務必安裝防火牆** :大多數無線網際網路路由器都具備防火牆功能，但仍應安裝軟體防火牆，以提供更周全的保護。

- **2. 務必安裝防毒軟體並定期加以更新。**光是安裝防毒軟體並不夠。病毒碼會不斷更新，因此最重要的是定期掃描系統及更新軟體，確保防護措施維持在最新狀態。

- **3. 在線上購物時，應選擇安全的網站，避免進入不安全的網站。**您可以檢查網址開頭是否為 https:// 來判斷網站是否安全；若網址開頭為 http:// 則表示您在線上購物的過程可能遭人「竊聽」。您還可以檢查瀏覽器視窗右下角是否有一個安全鎖圖示。

網際網路安全守則

- **4. 切勿任意按下連結。**如果您收到來路不明的電子郵件要您「按下連結」時，請先弄清楚其中的「連結」究竟指向何處。只要將滑鼠指向連結，便能在瀏覽器下方看到實際的網址。請不要按下任何可疑的連結。

- **5. 切勿轉寄連鎖信。**許多專業垃圾郵件散播者會四處散發連鎖信，藉此收集有效的電子郵件地址。一旦您將連鎖信轉寄出去，垃圾郵件散播者便可確認您的電子郵件地址仍在使用，然後您將會收到更多相同來源寄來的垃圾郵件

網際網路安全守則

- 密碼定期更新，並制定嚴謹設定原則(至少8個字元,含大小寫字母、數字、特殊字元)
- 關閉不必要的服務(如IIS、FTP、網路芳鄰)
- 只開啟必要的網路連接埠(port)(如FTP:21、WWW:80...)