

# 基隆市地政處102年度 資訊安全觀念宣導

報告人：郁志懿/ Pansy Yu

精誠資訊股份有限公司

Tel: 77201888 ext. 8045

email: pansyy@systex.com.tw

**SYSTEX**  
making it happen 精誠資訊

PayEasy線上購物-陪你Shopping一輩子 - 保養彩妝服飾女鞋-安全網購保證 - Windows Internet Explorer

http://www.payeasy.com.tw/index.shtml

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

★ 我的最愛 PayEasy線上購物-陪你Shopping一輩子 - 保養...

美麗留言板 | 團購 | 企業福利網 | 購物金儲值 | 快樂e點 | 加入會員 | 會員登入

全類別 搜尋

品牌分類 商品分類 超級品牌 Kevin凱文 依霖(小曼) 洪偉明 蔡依林 蔡翠敏 女人我最大 買某趣 量販網

美容保養 | 時尚彩妝 | 造型美髮 | 纖體塑身 | 流行服飾 | 鞋包配飾 | 生活居家 | 親子教育 | 美食保健 | 戶外休閒 | 3C數位 | 大小家電 | 達人獨家 | 旅遊專區

今天加入好康嗎? 適合肉肉腿的裙子 保濕聖水百萬人推 盧小桃推薦保養 倒數2天拿禮物 妳的免費造型師 加入粉絲團

**PayEasy獨創品牌**

- BeautyEasy 自然保養網
- BioBeauty 生化保養網
- BeautyDiy 愛美保養網

**達人專區**

- 彩妝大師 Kevin
- 名媛彩妝 孫芸芸
- 女人我最大 流行天后
- 日潮教主 佑群老師
- 髮妝天后
- 粉刺達人

**The Shirts 歡慶兒童節Big SALE!**

全館單一價 \$499

限量!! 售完為止

護髮造型合一 \$1細腰馬甲 韓美包全館 買大送小 韓童裝均一價 豆漿機9折

**會員服務** 登入/FB、Y!及Google

購物金 訂單查詢 最新公告

**快樂e點** 精選活動 本週最特惠

**死海礦物皂** 任2入388元+49點

超級品牌 TUEDMOC BURT'S BEES GRUTIN ROSE

轉帳

Transfers

繳稅

Tax Payment

繳費

Bill Payment

勞保局資料查詢

Personal Labor Insurance  
Information Inquiry

約定扣繳停車費

Set Up Parking Ticket Payment

查詢

Inquiry

設定變更

Change Settings

機車強制險

Motor Insurance

網路銀行服務

E-banking Service



**請選擇交易選項**  
**Please select a service**

## 注意事項

1. 請確認您所連結的是台北富邦銀行網站(網址: [ebank.taifeifubon.com.tw](https://ebank.taifeifubon.com.tw))
2. 請確認讀卡機已正常連線，並使用有效之晶片金融卡
3. 為了確保交易安全，不進行交易時，請務必登出，並將晶片金融卡取出讀卡機金融卡密碼輸入錯誤連續三次時，即會被系統鎖卡，請洽開戶銀行辦理
4. 為了交易安全，若您執行網路ATM交易時，五分鐘內未有任何操作，本行將強制執行登出交易

登出/Logout



台大醫院網路掛號系統 - Windows Internet Explorer

https://reg.ntuh.gov.tw/webadministration/

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

Google 搜尋 更多設定 >> 登入

我的最愛 台大醫院網路掛號系統

登入 網路(P) 安全性(S) 工具(O)

台大醫院

醫師門診時間表 網路掛號服務 查詢與取消 門診醫師群介紹 醫師看診請假情形 常見問題 English

## 網路預約掛號系統

**NEW** 2012年4月4日(星期三)適逢民族掃墓節及兒童節，本院門診休診，各項檢查、檢驗及復健治療停止服務，不便之處敬請見諒。

- 就醫提醒卡
- 健康教育資訊網
- 睡眠中心網路掛號服務: [成人睡眠門診](#) [兒童睡眠門診](#) [睡眠認知行為治療](#)
- 當日看診進度查詢
- 醫師請假公告(總院)

### 內科系

- 內科部
- 老年醫學部
- 家庭醫學部

### 外科系

- 外科部
- 骨科部
- 婦產部

### 兒童門診

- 小兒部
- 兒童內科
- 兒童外科

### 中心門診

- 血友病中心
- 形體美容中心
- 乳房醫學中心

ezTravel易遊網-機票.訂房.高鐵.無可挑戰.旅行就找易遊網! - Windows Internet Explorer

http://www.eztravel.com.tw/

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

Google 搜尋 更多設定 >> 登入

我的最愛 ezTravel易遊網-機票.訂房.高鐵.無可挑戰.旅行就...

易遊網 ezTravel 鴻鵠遠遊 HH travel.com 實現頂級旅遊者的夢想

國外旅遊 國際機票 國際訂房 國內旅遊 國內機票 國內訂房 高雄出發 頂級旅遊

國外	國內
東北亞	環島之星
東南亞	觀光計程車
港澳	北基宜
大陸	桃竹苗
美加	中彰投
歐洲	雲嘉南
澳洲紐西蘭	高屏
馬爾地夫	花東
大溪地斐	蘭嶼綠島

☒ 國際機票
 ☐ 國際訂房
 ☐ 國外旅遊
 ☐ 國內機票
 ☐ 國內訂房
 ☐ 國內旅遊
 ☐ 台灣高鐵

出發地: 台北

目的地: 選擇地區 選擇國家 選擇城市

航程: 來回

票種: 不限 進階搜尋 搜尋

焦點話題 雪壁奇觀 天天都省 機票降2% 春天吶喊

**旅行・歌頌最美春光**

散步東京櫻阪大道；北海道泡暖湯賞櫻花；關西世界遺產，穿梭櫻花隧道；旅遊中國，驚呼20萬畝油菜花

登入會員 | 加入會員

我的訂單 eMoney 會員服務

**旅型人生**

撮合你的新旅途! GO

出國最夯

九寨溝雙秀8天	23,500起	
---------	---------	--

網際網路 | 受保護模式: 啟動 115%

台灣高鐵網路訂位 > 查詢車次 - Windows Internet Explorer

https://irs.thsrc.com.tw/IMINT/?wicket:bookmarkablePage=wicket-0:tw.com.mitac.webapp.thsr.viewer.Home

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

★ 我的最愛 台灣高鐵網路訂位 > 查詢車次

台灣高鐵 TAIWAN HIGH SPEED RAIL

台灣高鐵網路訂位系統 24hrs

網路訂位 | 訂位紀錄查詢/付款及修改 | 常見問題 | 中文 | English

您所在的訂位步驟： 1. 查詢車次 2. 確認訂位 3. 取票資訊 4. 完成訂位

2012年3月

起訖站	起程站 請選擇... 到達站 請選擇...
車廂種類	<input checked="" type="radio"/> 標準車廂 <input type="radio"/> 商務車廂
訂位方式	<input checked="" type="radio"/> 依時間搜尋合適車次 <input type="radio"/> 直接輸入車次號碼
時間	去程 2012/03/28 約 請選擇... 出發 <input type="checkbox"/> 訂購回程
票數	全票 1 孩童票(6-11歲) 0 愛心票 0 敬老票(65歲以上) 0
查詢早鳥優惠	<input type="checkbox"/> 僅顯示尚有早鳥優惠之車次

開始查詢

網路網路 | 受保護模式: 啟動 115%

歡迎來到 Facebook - 登入、註冊或瞭解更多 - Windows Internet Explorer

http://zh-tw.facebook.com/

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

我的最愛 歡迎來到 Facebook - 登入、註冊或瞭解更多

Google

facebook

電郵地址 密碼 登入

☐ 記住我 忘記密碼?

**Facebook**，讓你和親朋好友保持聯繫，隨時分享生活中的每一刻。

免費註冊  
完全並永遠免費！

姓： 陳（範例）

名字： 君衛（範例）

你的電子郵件：

再次輸入電子郵件：

新密碼：

性別： 選擇性別： ▾

生日： 年 ▾ 月 ▾ 日 ▾

為什麼需要提供我的生日？

點擊「註冊」的同時，表示你同意了我們的[使用條款](#)

完成

網際網路 | 受保護模式：啟動 115%



# 網路改變了我們的生活





資安短片欣賞-Think before you post

**SYSTEMX**  
making it happen 精誠資訊

# Retrevo：35%的美國人曾經後悔自己的線上發文，尤其是iPhone使用者

Retrevo 最近公佈了一項有趣的調查，發現有 35% 的美國受訪民眾都表示曾經在線上發佈了事後悔恨不已的內容，而且越年輕越容易衝動「犯錯」，拿 iPhone 的人又比 Android 和 Blackberry 用戶更容易出現後悔的心情（好像心理測驗），是不是這樣？

根據 Retrevo 的報告，25 歲以下受訪者有 54% 的人表示曾經後悔自己在線上說的某些話，25 歲以上的受訪者則只有 32%，所以說是不是年輕真的容易意氣還是感情用事，話一 po 上網，也跟潑出去的水一樣，很多時候是刪也來不及。

調查也發現，智慧型手機用戶「失手」的機率是其他人的兩倍，其中又以 iPhone 的使用者最嚴重，有 51% 的受訪者都表示他們發佈過他們希望自己從來沒發佈過的內容，Android 用戶大概有 43%，Blackberry 用戶則有 45%，其實也沒有很低。

那究竟手滑的代價有很高嗎？後悔者中有 11% 表示其實後來也沒發生什麼事，15% 說他們有機會可以刪掉那些令人後悔的發文，3% 真的有因為一則發文毀了一段關係或婚姻，6% 造成了一些家庭或工作上的困擾。

所以說，忍一時風平浪靜，喝醉的時候千萬不要拿起你的 iPhone、Android 或是 Blackberry。

# 大綱

- 資訊安全簡介
- 常見的資安問題
- 注意瀏覽網站的潛在風險
- USB 病毒的風險
- 資安教戰手冊
- 回應與討論



# 資訊安全簡介



# 資訊安全控制的疑惑

- 個人電腦都已安裝防毒軟體
- 個人電腦也都已安裝了 Windows 的修補程式
- 資訊中心已經建立各式各樣的資訊安全控制設備
- 防火牆、入侵偵測設備、垃圾郵件防堵軟體
- ...

為什麼仍會有資安事件 ???

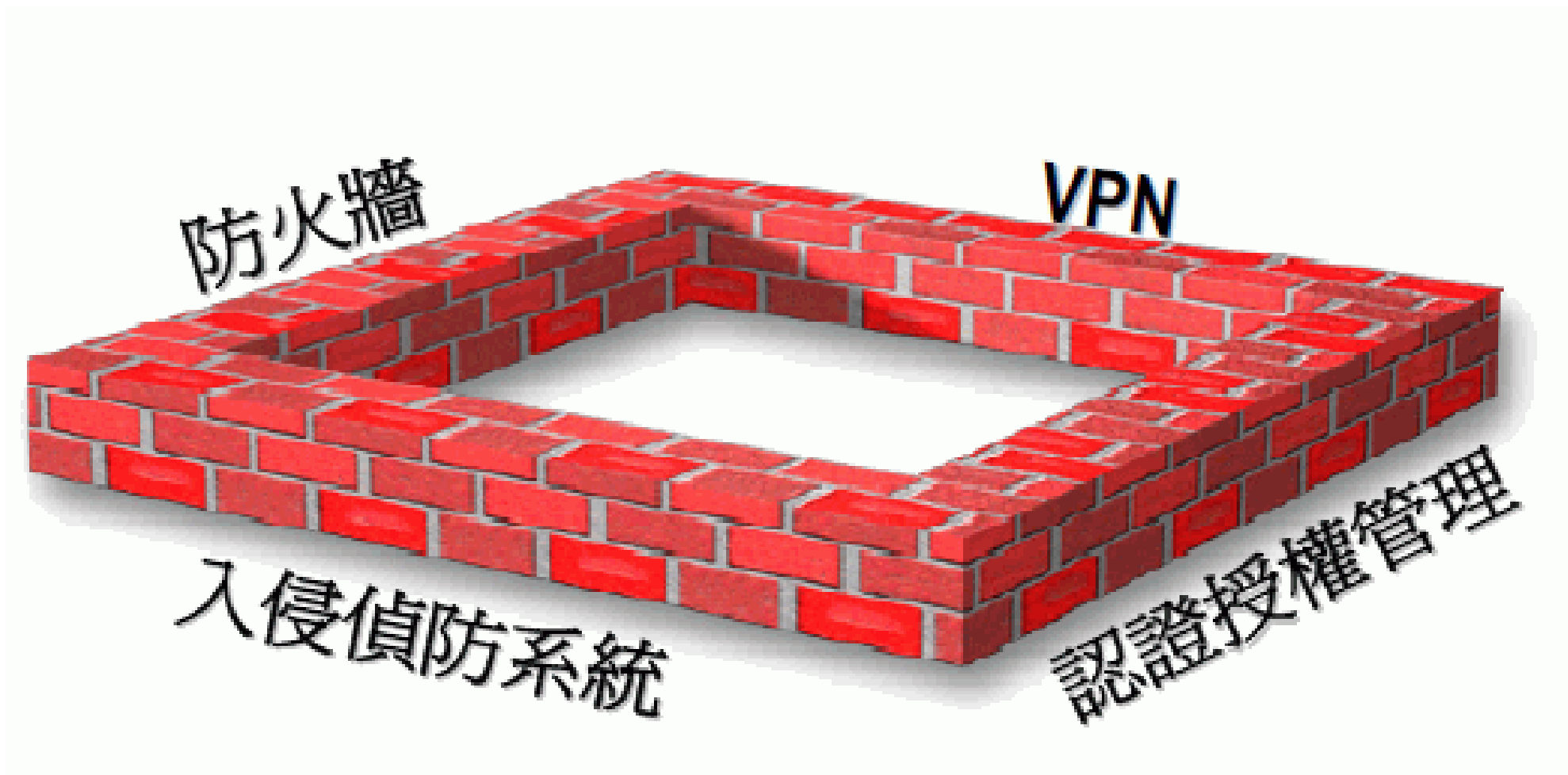
No Management, No Security

沒有管理就沒有安全

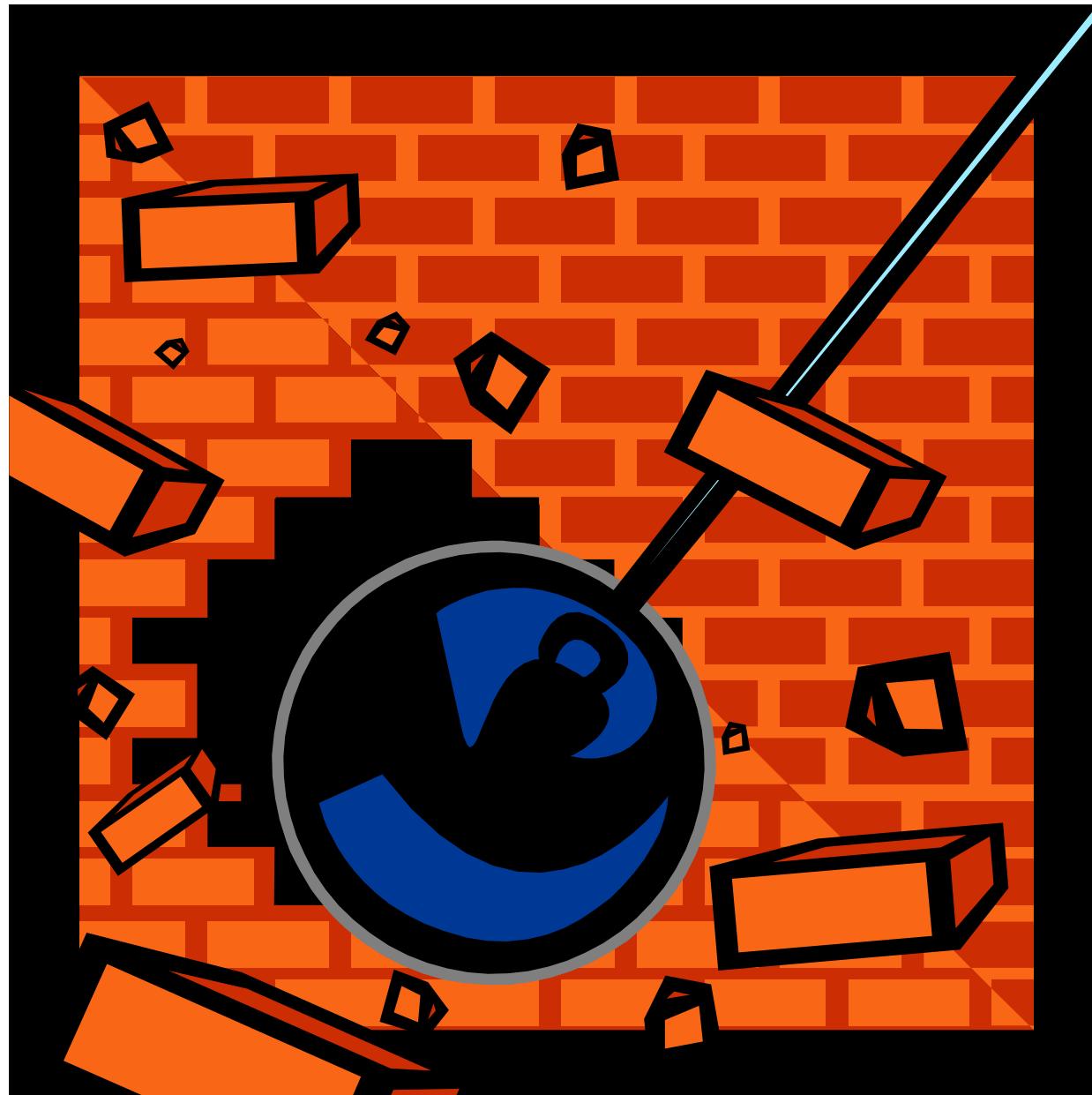


一般都會注意...

## 建立安全的周邊環境



# 直接破牆並不是一件容易的事



# 結果是...

將重要的資料寄  
給非授權的人

嘿嘿.. 我有  
權限

備忘錄放至網路  
留言板

關鍵文件透過印  
表機列印出

將資料、圖檔、文  
件燒錄至CD內

據統計有80%的資料遺失,是因為內部  
人員有意或無意之下所造成的結果



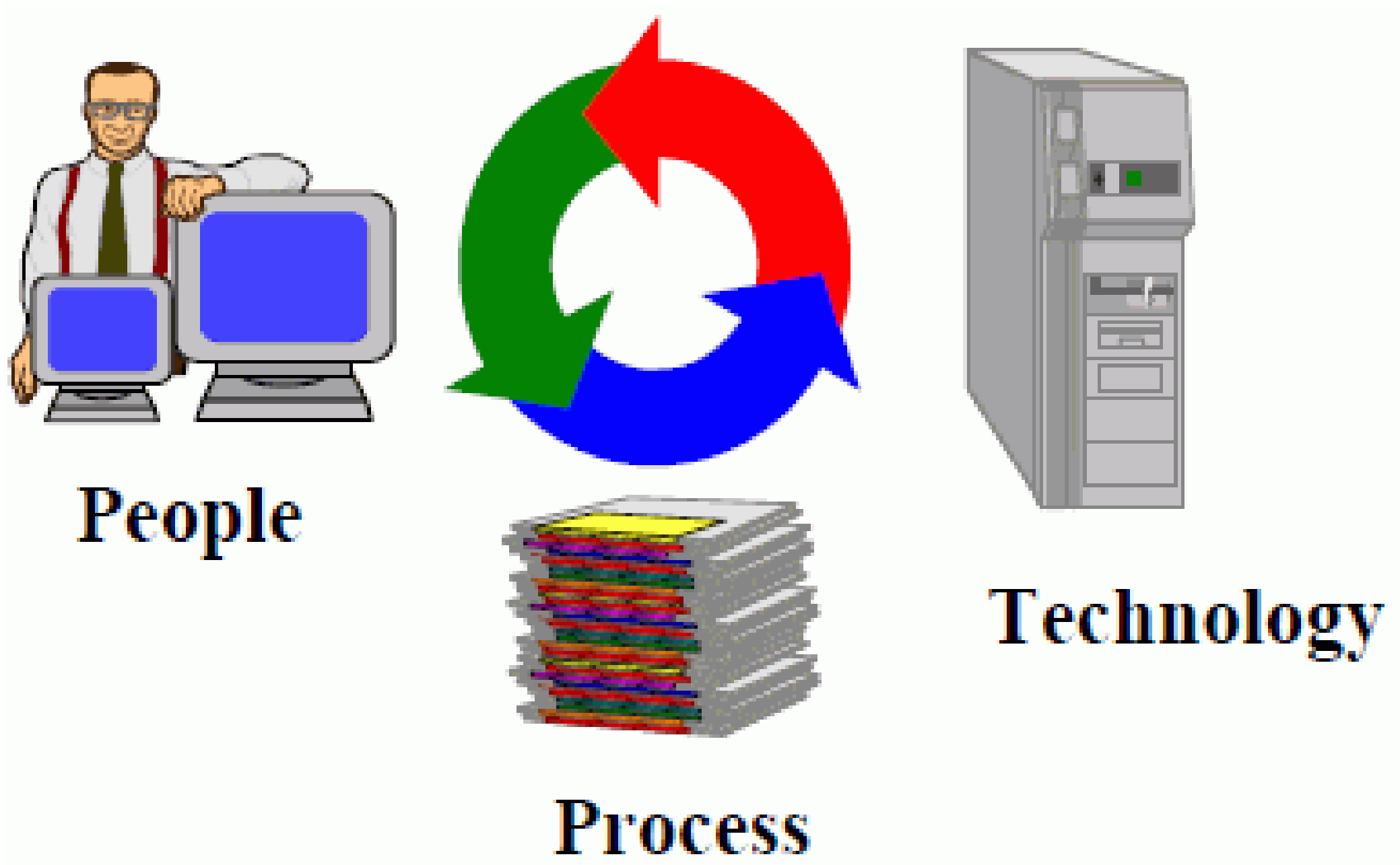
**為什麼是我們的問題？**

**因為我有權限做這些事**

**因為我不知道做這些事是危險的**

**因為我不清楚網路的風險**

# 資訊安全管理重點



# 資訊安全事件定義

- 資訊安全事件指的是任何違反常規的異常行為，其可能**造成資訊系統及網路的安全威脅**。
- 經證明可能**導致資訊系統運作錯誤事件或事故之情形**及其後續所產生之**故障效應**等。
- 從**設備故障、人員差錯、人為事件或自然事件**之類的單一事件到各種事件的複雜組合均**屬於資安事件**範疇內的事件案例。



# 資安事件的類型

- 內部事件

- 遭人為惡意破壞毀損、作業不慎等危安事件。

- 設備故障

- 能直接或間接影響機房安全資訊系統的各個設備的故障可視為資通事件。

- 人員差錯

- 錯誤或不良的維護、錯誤設定和操作員的其他錯誤行為等。

- 其他內部事件

- 內部原因所引起火災、爆炸等對機房安全可能產生重要之影響。

# 資安事件的類型

- 外部事件

- 因外部事件或自然事件所引起某一安全重要系統、元件或建築物故障的可能性，可經由設計和建造中所採取的因應措施，將其風險降低至可接受的程度
  - 病毒感染事件
  - 駭客攻擊（或非法入侵）事件

- 自然事件

- 天然災害：颱風、水災、地震
- 重大突發事件：火災、爆炸、核子事故

# 大綱

- 資訊安全簡介
- 常見的資安問題
- 注意瀏覽網站的潛在風險
- USB 病毒的風險
- 資安教戰手冊
- 回應與討論

# 常見的資安問題

**SYSTEMX**  
making it happen 精誠資訊

# 電腦病毒

## 網路病毒林來瘋 小心doc檔！



作者：林郁平/台北報導 | 中時電子報 - 2012年3月18日 上午5:30

-字 +字

中國時報【林郁平/台北報導】

林書豪在NBA優異的表現，在美國及台灣各地掀起一股「林來瘋」旋風，現在連病毒也搭上這股熱潮！近來網路上就有一個佯裝介紹林書豪故事的惡意文件開始蔓延，民眾一旦打開這個附加檔案，檔案內的惡意程式碼就可以讓攻擊者獲得電腦的控制權，竊取電腦內部及所處的整個網路中的敏感資料。

刑事局警告，民眾最近如果收到電子郵件，發現附檔檔名為「The incredible story of Jeremy Lin the NBA new superstar.doc（NBA超級新星林書豪令人難以相信的故事）」，千萬不要隨便開啟，檔案可能暗藏俗稱「開後門」的惡意軟體。

警方表示，駭客經常會利用熱門的新聞或具話題性的名人，製作暗藏惡意軟體、病毒的相關文件，藉以吸引民眾打開檔案，以四處散布、攻擊目標電腦，像是之前惠妮休斯頓的猝逝，及最新的林來瘋熱潮，發現都被駭客用來當做誘餌。

據統計，去年共有六十一個國家、一千四百餘台電腦遭到入侵，攻擊目標大多針對了一些前蘇聯國家。上個月也發生了另一起攻擊東歐政府辦公室的案例，這些入侵大多鎖定政府的外交等單位，而目前的林來瘋攻擊則持續了這一攻勢。



# 駭客入侵

駭客入侵NASA 恐危及國安 - Yahoo!奇摩新聞 - Windows Internet Explorer

http://tw.news.yahoo.com/%E9%A7%AD%E5%AE%A2%E5%85%A5%E4%BE%B5nasa-%E6%81%90%E5%8D%B1%E5%8F%8A%E5%9C%8B%E5%AE%{ Google

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

★ 我的最愛 駭客入侵NASA 恐危及國安 - Yahoo!奇摩新聞

YAHOO! 新聞 奇摩

搜尋 網頁搜尋

新聞首頁 政治 財經 社會 地方 影劇 運動 國際 生活 文教 健康 科技 影音 專欄 名人娛樂

資訊3C 科學發展 自然環境 科技熱門 瘋蘋果 思科網訊

## 駭客入侵NASA 恐危及國安

中央通訊社 THE CENTRAL NEWS AGENCY 中央社 - 2012年3月4日 上午12:11

(中央社華盛頓3日綜合外電報導)美國國家航空暨太空總署(NASA)去年發生13起重大網路入侵事件。NASA表示,駭客竊走員工憑證、入侵攸關太空任務的重要計畫。這幾起入侵事件可能危及美國的國家安全。

NASA督察長馬丁(Paul Martin)本週就駭客入侵事件向國會作證。美國多個聯邦機構發生一連串安全疏失,NASA遭駭客入侵事件似乎較為嚴重。

根據2月29日公佈的證詞,馬丁表示,NASA去年11月發現IP位址在中國大陸的駭客,入侵NASA噴射推進實驗室(JPL)網路。噴射推進實驗室為NASA重要實驗室,負責管理23艘現役太空船,包括執行木星、火星和土星等探測任務的太空船在內。

馬丁說,駭客取得進出系統的完整權限,讓他們得以修改、複製或刪除敏感資料。駭客還能開設新使用者帳號,並上傳駭客工具竊取使用者憑證,危害其他NASA系統。他們還能修改系統紀錄,隱藏入侵痕跡。

廣告

399元起  
抗UV  
吸排外套

lativ

新聞搜尋 新聞搜尋

# 木馬程式

新聞
新聞專題
即時新聞
新聞簡訊
技術
產品報導
技術專題
IT書訊
IT管理
CIO
IT人物
專欄
新聞總覽
業界動態

## 訂閱電子報

iThome Online提供免費電子報，現在就訂，最新IT訊息每日寄達。

iThome 每日新聞報  
iThome 產品技術報

我要訂閱

## 新Android木馬程式現身

文/陳曉莉 (編譯) 2010-12-30



131 個人覺得這很讚。

+ 我要收藏

行動安全新創公司Lookout宣稱Geinimi是有史以來最複雜的Android惡意程式，不但會竊取Android裝置中的資料，也是第一個具備類似殭屍網路能力的Android惡意程式。

行動安全新創公司Lookout周三（12/29）表示，有一鎖定Android裝置的木馬程式出現在中國市場，Lookout將該木馬程式命名為Geinimi，並宣稱這是有史以來最複雜的Android惡意程式，不但會竊取Android裝置中的資料，也是第一個具備類似殭屍網路能力的Android惡意程式。

Lookout表示，當Android裝置受到Geinimi感染時，除了會將使用者電話上的資料傳送到遠端伺服器外，同時也能接收來自遠端伺服器的指令。

Geinimi一開始是被移花接木到合法的Android應用程式中，特別是遊戲，並透過第三方的Android中文應用程式商店散布，現階段尚不清楚該木馬程式的用途，但可能用來建立惡意的廣告網路或打造Android平台的殭屍網路。

Lookout說明，當Android用戶執行一含有Geinimi的應用程式時，該木馬程式

# 社交工程

## 與社交工程手法混用，惡意文件檔成為有效攻擊手法

上述的數字，隱約透露了一個事實，隨著一般使用者的資安意識逐漸升高，傳統來路不明的執行檔和連結，誘騙使用者點擊的攻擊手法，已經逐漸不那麼有效了；但是文件檔，如PDF、Office文件等，則反而成為了新的可利用手法，如果搭配社交工程的手法，偽裝成使用者認識的寄件者單位或人員，成功率就更高了。

### 1成6的公務人員會打開不明附件



資料來源：行政院國家資通安全會報，2008年6月



# 拍賣詐欺

【新聞】詐騙電話接不停 網拍/中小網購漏很大


帳號：資訊安全專家 [kensan\\_2](#) 張貼時間：2011/06/08 22:29:07

我要回應

 [隱藏](#)

資安人科技網 - 2011年6月6日

龐大的線上購物市場規模，薄弱的消費者安全意識，鬆散的法制環境，蠻不在乎的業者態度，造成了現在個資外洩及網路犯罪詐騙問題。今年8月，在兩岸警力跨國合作下，一舉破獲450多人的跨國詐騙集團，此後165報案件數有明顯下降。根據165的統計，詐騙排名第一的是網拍詐騙

 防毒/防駭/防釣魚

【新聞】RE:詐騙電話接不停 網拍/中小網購漏很大 帳號：jc03 [joyisune](#) 張貼時間：2011/06/09 07:14:05

我要回應

根據165的統計，詐騙排名第一的是網拍詐騙

無本生意又跨國犯罪，21世紀最好賺的行業，再說本刑又輕，就算抓到了根本也不痛不癢！

民怨！民怨！還真是無為而治！

# 兒童上網

**iThome** online

找資料»

請輸入關鍵字

● 全站文章

首頁

新聞

技術

IT管理

研討會

iT邦幫忙

iT邦部落格

小7聚樂部

**BOOST** SPEED, EFFICIENCY, AND SECURITY WITH APPLICATION DELIVERY. **LEARN HOW»**

[寫跨平台Mobile Web簡單了](#)

[IT策略線上資料庫](#)

新聞
新聞專題
即時新聞
新聞簡訊
技術
產品報導
技術專題
IT書訊
IT管理
CIO
IT人物
專欄

## 兒童上網人數增加 交友/個資問題成隱憂

文/郭和杰 (記者) 2009-03-18



成為你朋友中第一個說這讚的人。



研究發現，55.5%兒童相信網路陌生人的身份描述，28.2%喜歡在聊天室和陌生人聊天，24.3%兒童會在網路上給別人自己的個人資料。

一份由政大教授所發表的研究指出，隨著兒童上網人口的增加，「時間管理」、「網路交友」，以及「個資外洩」，成為兒童上網的三大問題。

擔任白絲帶工作站召集人的政治大學數位文化行動研究室教授黃葳葳是在

# 身份盜用

## 美消費者十大投訴 身份盜用居首

新聞日期: 2012/03/06

(綜合報導)據CNN報導，身份盜用連續12年成為美國消費者的最大投訴。聯邦貿易委員會(Federal Trade Commission, FTC)去年共收到180多萬條投訴，其中15%(約28萬條)為身份盜用。

身份盜用多數用於偽造檔案冒領政府福利，這類投訴自2009年來增長11%，占身份盜用投訴總量的27%，其次為冒辦信用卡，占14%。2011年人均投訴身份盜用最多的是佛羅裡達州，其次為喬治亞州和加利福尼亞州。

除身份盜用投訴，第二大投訴為討債，占總投訴量的10%，其次為各類中獎、家中購物。佔據前十大投訴的還有金融服務與貸款、貸款預繳、信貸保護、維修服務，以及互聯網、電話與移動設備提供商及其收費。假裝事主親朋好友或政府機構、公司騙取消費者錢財也赫然在列。

總體而言，去年FTC收到的投訴55%涉及詐騙，消費者遭受的詐騙損失超過15億美元，中位數為537美元；43%的投訴者稱詐騙犯通過電子郵件與其聯繫。

人均詐騙投訴和其它投訴量最多的是科羅拉多州，其次為特拉華州和馬裡蘭州。

FTC發現，消費者要麼是不滿意增多，要麼僅僅是投訴意願上升，去年的投訴量從2010年的150萬增長20%多至180萬。

2011年FTC十大投訴排行:1.身份盜用。2.討債。3.各類中獎。4.家中購物。5.銀行、貸款商。6.互聯網服務。7.汽車業投訴。8.冒充他人騙取錢財。9.電話與移動設備服務。10. 貸款預繳與信貸保護。



# 即時通訊



# 盜用無線網路

民眾悠遊無線網路時，需特別注意，勿隨意盜用別人未加密的「無線網路」，以

分享:      推文  讚

分類：生活情報

2010/06/29 00:15

盜用無線上網 最重罰150萬!



更新日期:2010/盜用無線上網 最重罰150萬!06/28 22:16



民眾在家，要上網除了透過有線網路之外，其實還能使用無線網路，透過無線基地台，走到哪上到哪，不過台北市卻有一名男子，利用無線發送的特性，盜用鄰居家沒有設密碼的無線網路，偷偷上網完全不用付任何網路費，被檢方查出依違反電信法起訴，檢方認定，這種貪小便宜的行為和小偷一樣，最重可判處五年刑期，併科罰金150萬。

這是無線網路基地台，一般民眾裝在家裡，就是想能走到哪，都能上網。小小一台，能夠發射無線網路訊號，也因為如此，台北市有一名男子，看準了這個無線發射的特性，偷偷接收鄰居的無線網路，大肆上網，卻不用付半毛錢，貪小便宜的行徑，被檢察官依違反電信法起訴，像小偷一樣的行為，檢察官說，最重還可能被判刑五年，甚至開罰150萬。

# 離職員工的威脅

## • 上市公司離職員工竊取商業機密損失達3億5千萬元

離職員工 資安 - Google 搜尋 - Windows Internet Explorer

http://www.google.com.tw/search?q=%E9%9B%A2%E8%81%B7%E5%93%A1%E5%B7%A5+%E8%B3%87%E5%AE%89&url=com.microsoft:zh

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

我的最愛 EasyCom資安中文報表系... Tree Menu Module - Pr... 建議的網站 取得更多附加元件

離職員工 資安 - Google 搜尋

離職員工 資安

上市公司離職員工竊取商業機密損失達3億5千萬元, Information Security ... ☆  
2009年3月17日 ... 資安人科技網:資訊安全入口網站,為"資安人"建構全盤掌握資訊安全的交流 ...  
國內從事IC零件通路的上市公司所羅門電子,傳遭離職員工入侵,竊取多項 ...  
[www.isecutech.com.tw/article/article\\_detail.aspx?aid...](http://www.isecutech.com.tw/article/article_detail.aspx?aid...) - 頁庫存檔

從台灣大哥大委外廠商離職員工搞鬼事件學習到的一課 - Information ... ☆  
2009年11月18日 ... 經檢調介入調查,已查出是由台灣大哥大系統委外廠商諾基亞西門子通信公司  
(NSN)的離職員工所為。板橋地檢署於日前依妨害電腦使用罪將陳嫌提起公訴,並 ...  
[www.informationsecurity.com.tw/Forum/reply.aspx?tid...](http://www.informationsecurity.com.tw/Forum/reply.aspx?tid...) - 頁庫存檔

就是資安:[從電影看資安] 早跟你說要小心悲情的離職員工-終極警探4.0 ☆  
2010年2月23日 ... 第二件事就是所謂離職員工的問題。我想台灣企業(尤其是中小企業)最怕離職  
員工的地方,除了擔心離職員工向BSA檢舉公司使用未經授權的軟體外,更怕 ...  
[cyrilwang.blogspot.com/2010/02/40.html](http://cyrilwang.blogspot.com/2010/02/40.html) - 頁庫存檔

中小企業客製化資安維護系列專輯之三小心離職員工的回馬槍-I... ☆  
目前許多公司都制定有資訊安全政策,其中通常都有離職員工的離職作業程序,若能落實確保離職  
員工交回所有公司的電腦設備財產,並且註銷其使用者權限及電子郵件帳號, ...  
[www.i-security.tw/topic/topic\\_sg.asp?id=118](http://www.i-security.tw/topic/topic_sg.asp?id=118) - 頁庫存檔

[PDF] 「景氣寒冬,離職員工打包的不只是私人物品?」「不滿員工」成為機密外洩... ☆  
檔案類型: PDF/Adobe Acrobat - 快速檢視  
刑事警察局於去(97)年3月間破獲一起某企業員工離職後自行成立性質雷同 ... 多便利,但也衍  
生許多新的社會與犯罪問題,其中,最明顯的現象,就是資訊安全 ...  
[www.tntb.gov.tw/core/download/getfile.php?fileName=1007083303...](http://www.tntb.gov.tw/core/download/getfile.php?fileName=1007083303...)

RUN!PC | 即時新聞 | 資訊安全 | MIC: 愈宅愈旺不景氣中的資安商機 ☆  
部份因裁員而離職的員工,在無法自我調適而心生不滿之際,就很有可能會挾怨竊取 ... 因此,因  
應裁員離職風潮可能產生的資安風險,同時也會產生資料外洩防護(Data Loss ...  
[www.runpc.com.tw/news.aspx?id=100271](http://www.runpc.com.tw/news.aspx?id=100271) - 頁庫存檔

# 個資外洩

## PChome網購個資外洩？ 女網友：我被詐騙集團性騷擾！

2009年10月22日 10:01

f 分享 10

+ 分享

記者蘇湘雲 / 台北報導

網路購物讓資料外洩？PChome線上購物被多名網友投訴，刷卡消費後卻接到詐騙集團電話威脅核對銀行資料，甚至有大陸口音男子性騷擾詢問「三圍多少？晚上會不會寂寞？」網友懷疑購物網站外洩了消費者交易資料，笑說「上PChome購物就會免費附送詐騙電話一通。」



PChome線上購物被多名網友投訴，網路購物讓資料外洩。(圖 / 資料照片)

# 垃圾郵件

APR 17 FRI 2009 20:29

## **【新聞】假冒資安廠商 垃圾郵件誘購「防毒軟體」**

電腦病毒讓很多網友都有電腦中毒或是必須重灌系統的切身之痛。資安廠商發現，有打著資安業者名號的垃圾郵件，向網友推銷「防毒軟體」；業者指出，目前還不知道這些軟體是否會真的將商品寄給訂購者，或是這些軟體本身就是電腦病毒。電腦病毒Conficker讓全球很多電腦使用者深受其害，也讓許多擔心自家電腦安全的民眾積極購買防毒軟體或更新現有防毒軟體的病毒定義檔。(撰稿・編輯：韓啟賢)

在此背景下，有一些垃圾郵件自稱是某資訊安全廠商，以協助電腦使用者免於Conficker安全威脅為名，推銷防毒軟體。資安業者指出，這些垃圾郵件會夾帶連結，誘使收件者點選連結到某購物網站去購買防毒軟體。資安廠商賽門鐵克提醒消費者，不要相信這些來路不明的垃圾郵件，而且目前也還沒有確定這些所謂的「防毒軟體」是否會寄到訂購者手中，或是這些軟體本身就具有其它的資安威脅。這家公司的資深技術顧問莊添發說：『(原音)即使如果他真的把一些軟體寄給一般的使用者，事實上，也不要安裝；因為，第一個有可能是盜版的，那第二個有可能是他自己製作的，偽裝的惡意程式。』

另外，由於報稅季節即將來到，也有些垃圾郵件作者，打著稅務單位的名號，以退稅等名義欺騙網友；希望藉此騙取報稅人的個人資訊，包括出生年月日以及信用卡號碼等等。資安廠商提醒民眾，全球的稅務單位很少使用電子郵件與民眾聯繫，因此，如果接獲宣稱來自稅務單位的電子郵件時，要格外注意。



# 惡意網站

## 每月遭受愈5000宗安全威脅 2011 年惡意網站數目劇增 240%

文: Jeff Lau / 新聞中心

網絡應用持續發展，也成為不法份子進行非法活動，複雜網絡犯罪基礎架構亦不斷擴大網絡攻擊，其中據網路安全專家指出，2011 年惡意網站數目劇增 240%，企業平均每月遭受愈 5000 宗安全威脅，網絡威脅中最重大的變化是利用的惡意網絡發送動態的網際攻擊，影響較任何一個攻擊更為持久，預期 2012 將佔所有全新攻擊中的三分之二。

據網路安全專家發表的 Blue Coat 2012 年網路安全報告指出，2011 年網絡威脅中最重大的變化是利用的惡意網絡發送動態的網際攻擊，為互聯網中的分散式網絡基礎結構，主要為了盜取個人資料，或把終端用戶系統改為殭屍網絡，由網絡罪犯創建、管理及維護，用於向無防範意識的用戶長期發出各類攻擊。

目前最常見的惡意軟件交付網絡入口是透過最少阻礙的路徑，使用容易入侵的入口，如搜尋引擎 / 入口網站和電郵，或擁有大量不同使用者的平台，惡意軟件交付網絡透過搜尋引擎 / 入口網站能夠有效地發動攻擊，在 142 個搜尋結果當中便有一個會連結到惡意內容。

[文章索引](#)： [其它 IT 要聞](#)

### GIGABYTE



廣告 advertisement



# 大綱

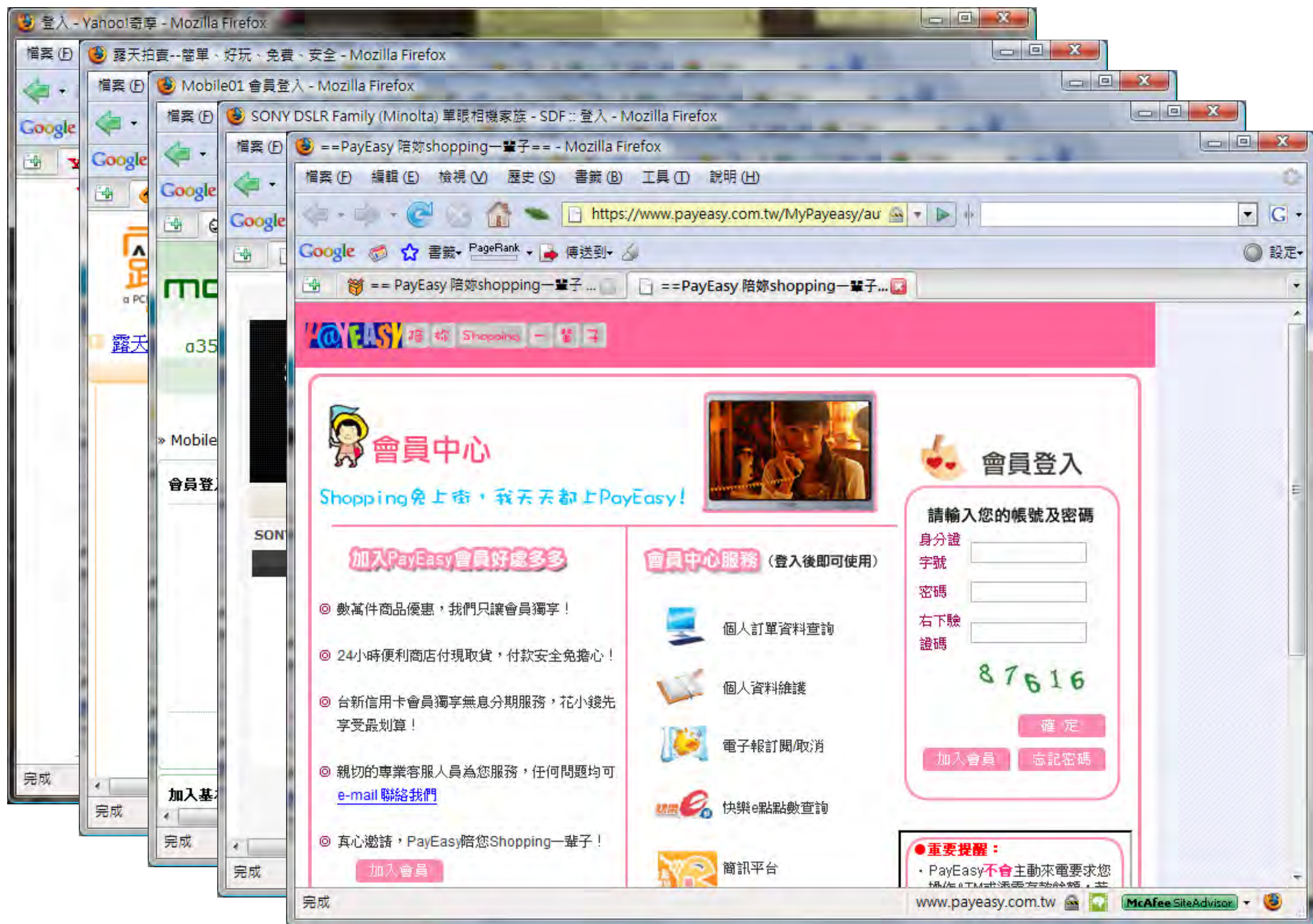
- 資訊安全簡介
- 資訊安全威脅
- **注意瀏覽網站的潛在風險**
- USB 病毒的風險
- 不當密碼的風險
- 資安教戰手冊
- 回應與討論

# 注意瀏覽網站的潛在風險

**SYSTEMX**  
making it happen 精誠資訊

# 以下兩個網址有何不同？

- `http://www.landbank.com.tw`
- `http://www.1landbank.com.tw`
  
- `http://www.landbank.com.tw`
- `http://www.1landbank.com.tw`



# 使用者的行為模式

- 習慣；貪圖方便
  - 密碼過於簡單
  - 在不同的網站中，使用同一組帳號 / 密碼
- 風險
  - 任何一個網站遭受攻擊，詐騙集團即可能利用取得的資訊試著登入其他網站
- 如何避免
  - 改變習慣
  - 使用新技術

# 大綱

- 資訊安全簡介
- 資訊安全威脅
- 注意瀏覽網站的潛在風險
- **USB 病毒的風險**
- 資安教戰手冊
- 回應與討論

# USB 硬碟的風險

**SYSTEMEX**  
making it happen 精誠資訊



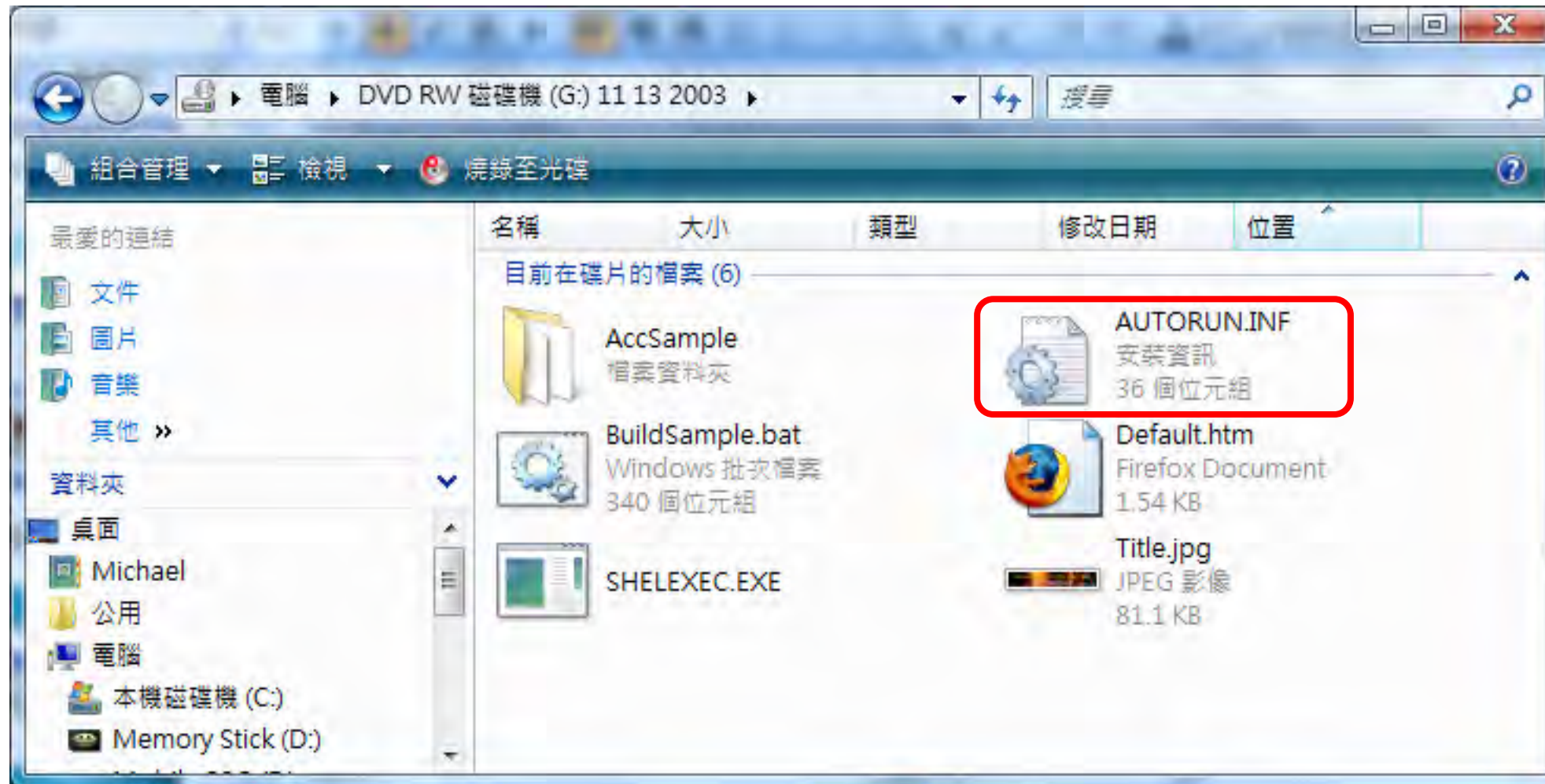
# USB 惡意程式的問題



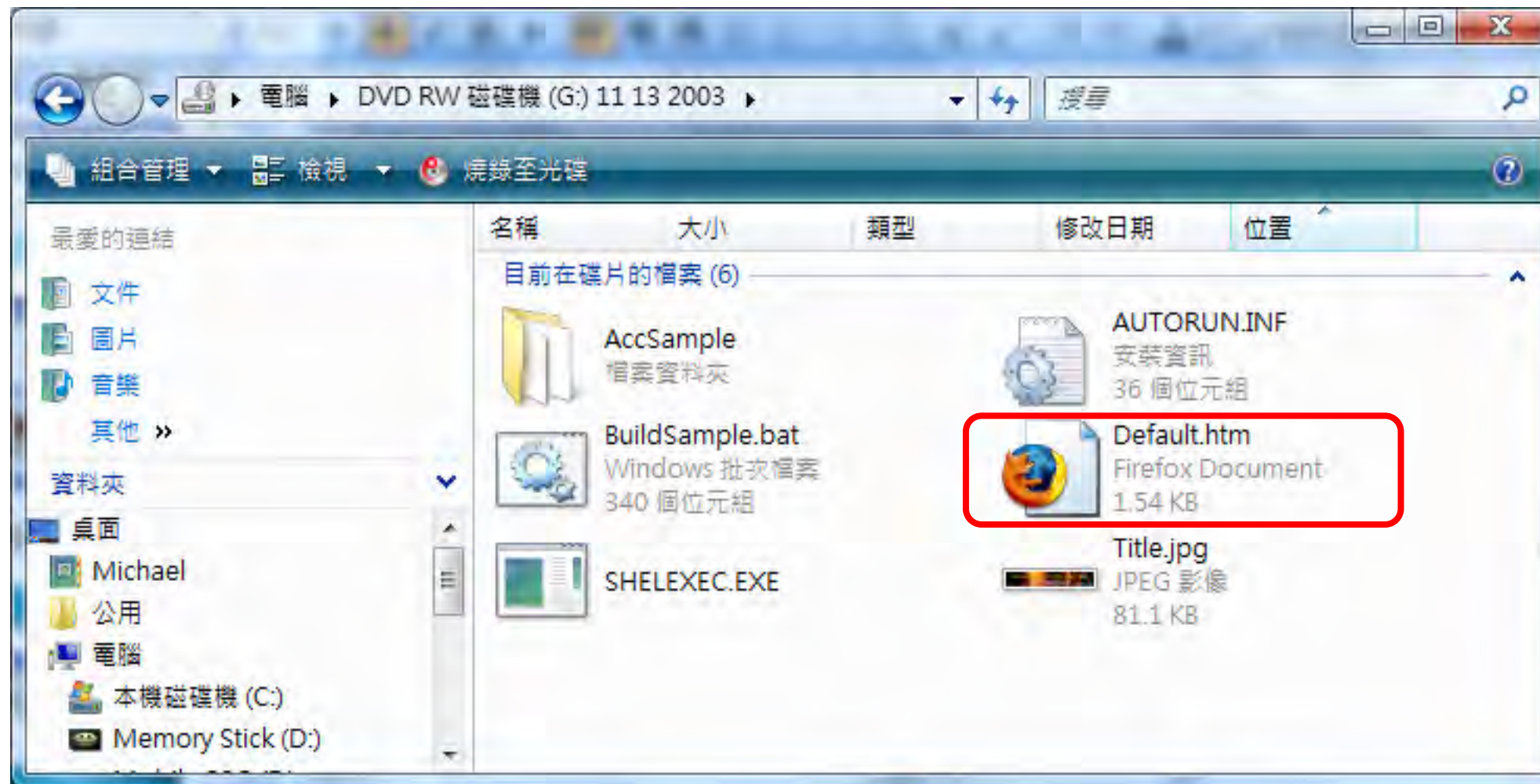
# USB 裝置惡意程式傳播途徑

- USB 惡意程式主要透過 USB 儲存裝置 (USB 隨身碟、大拇哥、USB 外接式硬碟機) 散播。
- 已知目前有許多惡意程式會利用微軟 Windows 作業系統中提供之「裝置自動執行 (Autoruns)」功能進行散播；此類利用 USB 儲存裝置進行散播的惡意程式被稱為「USB 蠕蟲 (USB Worm)」。
  - 「USB Worm」會在磁碟裝置根目錄中寫入一個 autorun.inf 檔案，當使用者插入該磁碟裝置，並從桌面「我的電腦」點選進入該磁碟代號時，預設情況下作業系統會自動讀取 autorun.inf 並執行 autorun.inf 中所指定的惡意程式，進而使惡意程式感染電腦。
- 使用受「USB Worm」感染之 USB 儲存裝置至其他電腦交換資料時，可能感染其他電腦。在受感染的電腦上使用 USB 儲存裝置也可能使正常的 USB 儲存裝置成為帶原體，進而成為散播惡意程式的幫兇。

# 含正常 autorun.inf 的光碟



# 放入光碟後會自動執行的檔案

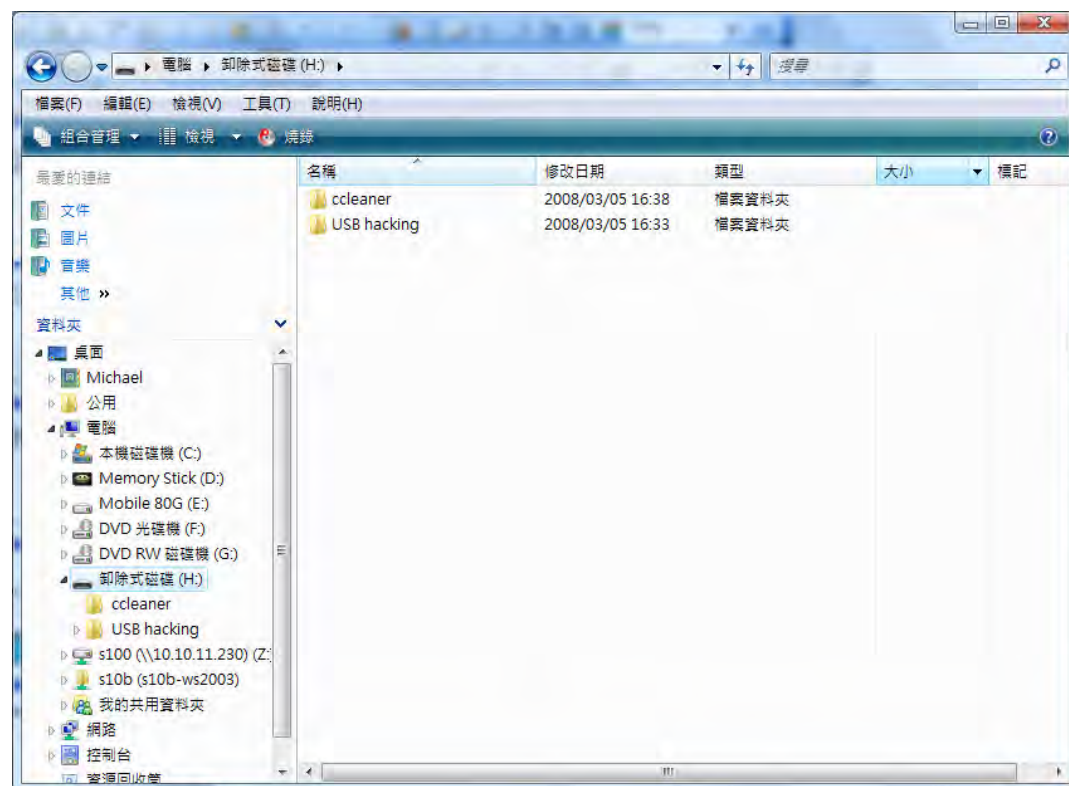


# 預防 USB 硬碟病毒方法

- 停止「自動播放」功能
- 家用電腦如何停止「自動播放」功能
  - 隨身碟連接於電腦時，按住「shift」鍵的方式，暫時取消自動播放

# 預防 USB 硬碟病毒方法

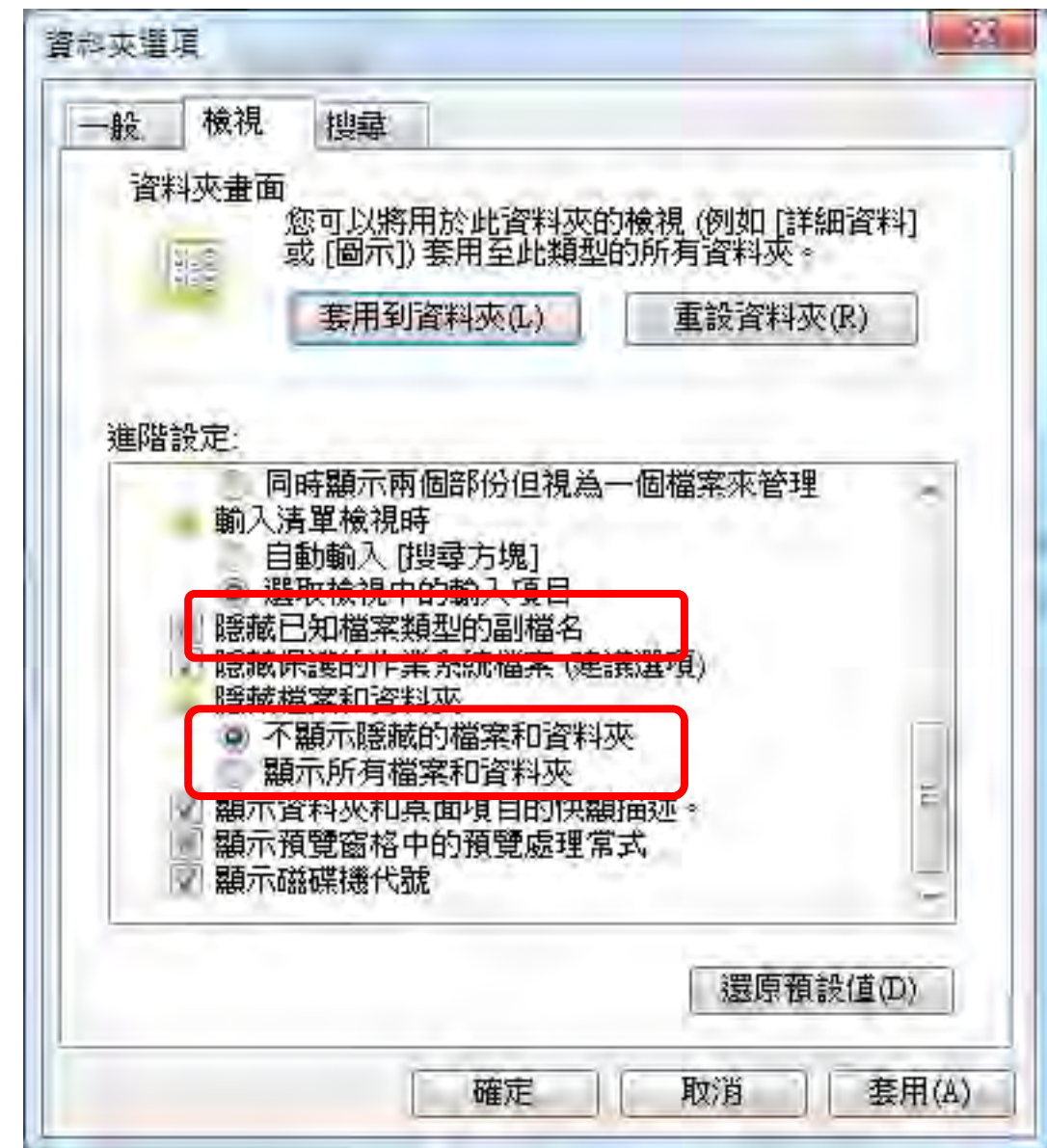
- 不要用 double click 的方式開啟隨身碟
- 因為 double clike 也會執行 autorun.inf
- 請用檔案總管的左邊窗格開啟 USB 硬碟





# 使用安全的電腦設定

- 請取消「隱藏已知檔案類型的副檔名」
- 請選擇「顯示所有檔案的資料夾」



# 大綱

- 資訊安全簡介
- 資訊安全威脅
- 注意瀏覽網站的潛在風險
- USB 病毒的風險
- **資安教戰手冊**
- 回應與討論



# 資安教戰手冊

**SYSTEMX**  
making it happen 精誠資訊

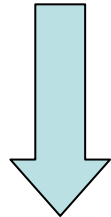
# 使用者責任

- 使用者的態度，對於有效防止非法的使用者存取，以保障安全的工作非常重要。
- 目標：防止未經授權的使用者存取資訊與資訊設施，以及使其避免遭受破壞或竊取。
  - 密碼的使用。
  - 無人看管的使用者設備。
  - 桌面淨空與螢幕淨空政策。

# [密碼設置與使用原則]

- 定期更新密碼
- 設定優質密碼
  - 密碼長度至少要8個字元以上
  - 若想要達到強度足夠的密碼，應該同時混合使用三種類型的字元
  - 避免使用字典中的單字，同時也不應該包含帳號
  - 使用英數字混合時，避免只在最後加上一個數字
  - 避免使用生日、手機號碼等與自身相關之資訊作為密碼
- 不要告訴他人密碼或寫下密碼
- 懷疑密碼外洩立即更新

# 如何設定安全的密碼

- 使用簡單的編碼原則
- 例如：
  - 先想一個句子
  - All things are possible to him who believes
  - Atapthwb!
  - 您可以使用任何句子（中文、英文），任何輸入法！
  - 自己的名-郁志懿
  - M454u\$

# 其他密碼設定技巧

- 輸入法的變型
  - 你好嗎 ( 新注音輸入 )
  - Su3cl3a87 或 su#cl#a8&
- 混合排列
  - abcd + 1234
  - a1b2c3d4 或 a! b@c#d\$
- 錯位
  - birthday
  - ahqsgczx

# 無人看管的使用者設備

- 使用者應確保無人看守的設備獲得適當保護
- 安裝在公共區域的設備(如公用主機、印表機或伺服器)，應有具體的保護
  - 在活動完成時應終止對話，結束畫面。
  - 螢幕保護程式需設定密碼保護。
  - 活動結束時登出系統或主機，再關閉電腦。
  - PC或設備不用時，應使用密鑰鎖或其他安全控制措施，以防止他人非法使用。



# 桌面淨空與螢幕淨空政策

- 桌面淨空

- 重要、機密文件不置於桌上。
- 重要、機密文件下班或離開辦公室前應鎖入安全空間。

- 螢幕淨空

- 設定螢幕保護程式。
- 設定保護密碼。
- 離開座位或暫時不使用時鎖定螢幕。

# 處理公務時的安全防護

- 處理公文時須離線作業。
- 人員勿從網路下載與公務無關之不明程式。
- 公文系統均要求在內部網路處理。
- 不得將與公務有關之內容上傳至網際網路個人儲存空間。

# 要注意什麼？

- 考慮以下狀況
  - 攜帶型資訊設備之使用安全(如:隨身碟)。
  - 列印文件或使用傳真之安全。
  - 桌上型PC的帳號密碼及螢幕保護密碼。
  - 使用E-mail的安全。
  - 防範個人電腦病毒。

# 要注意什麼？(續)

- 考慮以下狀況
  - 個人資料備份。
  - 辦公室、機房進出管制。
  - 非法軟體使用管制。
  - 資訊安全事件的通報。
  - 使用資訊系統的存取權限設定與主管覆核。
  - 人員離調職的帳號異動管理。

# 防範資料外洩

- 防範機密資料洩露方法
  - 減少在公共場所討論。
  - 離開座位，使用螢幕保護程式。
  - 在不使用或下班後將機密文件收妥。
  - 機密文件不遺留傳真機或影印機。
  - 傳真前通知對方領取。
  - 機密文件以碎紙機銷毀。
  - 機密檔案櫃或房間上鎖。
  - 會議室文件帶走及白板擦拭乾淨。
  - 儲存媒體報廢清除內容。

# 妥善處理您的網路相片，避免洩漏太多個人資訊

- 若您在線上共享相片，檢視和下載相片的人可能會存取相片檔儲存的中繼資料。
- 相片是否顯示關於您的資訊？是否吸引歹徒的注意，或成為別人搜尋的對象？
- 相片背景有什麼景物？相片中是否顯示出您的住家號碼、街道特徵、車牌號碼、社區購物中心、學校或其他地標？
- 您是否在相片上標記了完整姓名或其他詳細的身分資料？
- 您的衣服是否有特殊標誌？校名、隊名或社團名稱？還是有您的姓名？
- 相片中有哪些人？若裡面有朋友或家人，他們也可能曝露在危險之中。
- 當您新增人員標籤 (附加於相片、用來識別相片內人物的文字資訊，可詳細說明相片的內涵。) 至相片時，請記得，可以檢視相片的人員也能看見人員標籤。



# 個人資料保護的基本認知

- 親友來信或MSN邀請加入網站會員，務必先回覆 email 或 MSN 做再次確認。以免中毒或受騙，成為下一個為害親友的罪人。

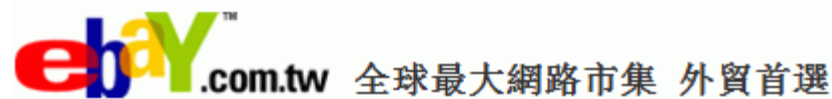


- 許多個資外洩事件，其實問題並非在於網站本身的安全性，而是使用者自己的帳號密碼管理不夠小心
- 要準備多組密碼，採用分級分類的方式共用密碼。因為若只使用一組相同的帳號密碼，一旦外洩，等同所有資料淪陷
- 定期變更重要網站密碼，降低資料外洩的機率以及衝擊

# 網路拍賣詐騙常見特徵

- 保證為新品、公司貨，但價格卻低於市價許多。
- 過往交易與目前所販賣物品種類、價格差距過大。
- 將近一年沒有進行交易，卻突然大量拍賣多款高價商品。
- 提供詳細的圖文說明，但皆複製自網路或其他賣家
- 賣家表明自己位在偏遠縣市，並推拖不肯面交
- 所有拍賣品的結標時間都集中在一兩天之內

**其實拍賣詐騙比電話詐騙還要單純，只要不貪，就不會受騙**



# 別讓工具列幫手成為幕後黑手！

1. 安裝工具列時，請確認程式是直接由官方網站下載，以免暗藏危機。
2. 避免安裝沒聽過的工具列，並且注意安裝軟體過程是否也同時安裝不明的工具程式。必要時可以先上網搜尋相關文章。
3. 工具列安裝越多，電腦記憶體消耗越大，結果會導致系統效能降低，影響工作。
4. 瀏覽器本身的安全性跟瀏覽網站的安全性同等重要。
5. 一旦懷疑電腦內存在惡意工具列，應趕快移除，或通知IT服務中心處理。



# 有備無患 你的備份做對了嗎？

- 不論是紙本或電子檔的重要資料，皆應：
  - 定期備份
  - 存放在不同地方（**異地備份**）
- 資料備份原則：
  - 資料價值較高時應優先備份
  - 選擇適合之儲存媒介進行資料備份工作
  - 按所欲備份的資料型態，選方法進行備份（如：完全備份、選擇性備份、漸進式（增量）備份）
  - 備份的資料需定期做資料回復測試，以確認備份資料的可用性

# 資訊儲存媒體的管理

- 儲存媒體的管理
  - 制訂儲存媒體(如：磁帶、磁片、光碟以及列印報告)的管理方法。
  - 明確記錄所有的管理步驟和授權級別。
- 儲存媒體的報廢
  - 具敏感資訊的媒體應該進行安全保險的保存和處置。
  - 安全收集和報廢所有媒體。
  - 謹選具有經驗及技術的合格合約商。
  - 儘可能記錄敏感資料的報廢，並保留稽核追蹤。
- 儲存媒體的運送安全
  - 使用可靠的傳輸工具或投遞人。
  - 包裝應可保護不受運輸過程中事故造成損壞。
  - 依需要採取特殊的控制措施以保護敏感資料免遭非法公開或修改。

# 電子郵件的安全

- 安裝防毒軟體過濾郵件
- 不隨意開啟郵件附檔
- 防堵垃圾郵件
  - 絕對不回覆垃圾電子郵件訊息。
  - 不購買垃圾電子郵件的廣告商品。
  - 不轉寄串接式的電子郵件，(例如聲稱不轉寄給10 個人就會倒楣的電子郵件)。
  - 要寄送同一訊息給許多收件者時，可採用「密件副本」方式來進行。
  - 刪除寄件者為空白的電子郵件。
  - 使用垃圾電子郵件過濾軟體。
- 垃圾郵件過濾簡易設定
  - 在Web 郵件上設定過濾垃圾郵件寄件者。
  - 利用常見關鍵字過濾郵件。



# 即時通訊軟體使用安全

- 登入密碼最好不要用「**儲存密碼**」記錄於系統內
- 不任意傳遞與分享公司重要資訊或檔案。
- 不任意接收來路不明之分享檔案。
- 使用者必須秉持以公事使用之目的使用企業即時訊息。
- 隨時更新使用端程式。

# 電腦病毒的防範

- 確認防毒軟體隨時運作。
- 勿隨意安裝未經許可的電腦軟體。
- 確保軟體在最新更新狀態。
- 使用有問題立即反應。

# 廣告或間諜軟體的防範

- 使用防火牆阻擋。
- 關閉網路瀏覽器的ActiveX 功能。
- 安裝封鎖彈跳視窗功能的工具。
- 下載免費軟體前仔細閱讀所有相關資訊。
- 學習資料備份基本技巧。

# 駭客入侵的簡易處理

- 定期系統備份。
- 針對可能入侵途徑系統作隔離。
- 蒐集入侵紀錄、檔案等軌跡。
- 追查駭客IP來源。
- 分析資料找出入侵方式並改善。
- 報告相關單位。
- 適時尋求協助。

# 駭客入侵的防範

- 即時更新修正檔。
- 檢視權限設定。
- 日常備份作業。
- 紀錄及檢視稽核軌跡。
- 設定自動時間校正作業。

# 回應與討論

**SYSTEMX**  
making it happen 精誠資訊