
個人資訊安全與社交工程

課程大綱

個資安全的情境

一、紙本往來威脅：

二、通信傳真威脅：

三、社交工程威脅：

網路資安的情境

網路安全威脅

一、行動威脅：

二、網站威脅：

三、病毒威脅：

四、社交工程威脅：

網路資安的重點議題

密碼安全

軟體使用安全

病毒與木馬防護安全

電腦操作安全與資料備份

USB管理

公用存取

電子郵件安全

社交工程

網路釣魚與網路詐騙

日益猖獗的勒索病毒

社會、科技、人性

- 外部威脅

根據全球資料保護領導廠商SafeNet, Inc.的研究指出

- 2014年上半年有超過3.75億筆顧客紀錄因全球559件資料外洩事故而被竊或遺失；
- 在過去連續四個季度，每一季均有一宗重大資料外洩，洩漏超過1億筆紀錄；
- 2014年4月至6月期間，全球共有237件資料外洩事故，涉及超過1.75億筆個人及財務資料紀錄，可此些資料外洩多是由駭客惡意入侵所引起，可見駭客入侵所引起之資料外洩為企業面臨最主要之外部威脅

社會、科技、人性

- 外部威脅

  依據賽門鐵克的報告指出

  - 台灣名列2013年全球整體網路威脅的第九名，在亞洲國家中僅次於中國大陸與印度。
  - 全球「進階持續性滲透攻擊」（Advanced Persistent Threat，以下簡稱APT）日益猖獗，台灣是最常被列為攻擊目標的國家之一，亞太地區有75%的APT駭客會透過各種工具、技術以及程序對台灣進行攻擊(註3)，可見台灣資訊安全的整體風險偏高。

社會、科技、人性

- 內部隱憂

  企業內部之資安隱憂則為員工的不當行為，由於員工可能經手機密性資料，一旦外洩資料，往往導致企業龐大的損失及商譽的損害。

  2011年台北富邦銀行發行的運動彩券，襄理林昊縉利用職權下注，在比賽結束後私自將系統打開重新開賣、下注，不當得利230萬元。

  2014年南韓的39歲朴姓電腦工程師，任職信用評價組織(Korea Credit Bureau)開發可辨識偽卡的軟體，因而有機會存取南韓三大發卡公司KB Kookmin Card、Lotte Card與NH Nonghyup Card的資料庫，自2002年5月到去年12月間多次將資料庫中的個人資訊複製到USB裝置上，共外洩1.04億筆信用卡資訊，約40%的南韓人受到波擊，連南韓總統朴槿惠的個資都遭竊，堪稱是全球最大的個資外洩案。

社會、科技、人性

- 內部隱憂
  - ➢ 內部缺乏完備的資訊安全控制管理和觀念，
  - ➢ 員工因職務之便方便取得

  讓員工有機會不當存取資料、進而外洩資料，往往在發現時已造成相當損害而為時已晚，因此對於有機會接觸個人資料的員工，應該站在
  - ✓ 保護公司、
  - ✓ 保護客戶、
  - ✓ 保護員工的立場 、

  在內部建立適當的監控及稽核機制，以降低潛在的內部風險。

社會、科技、人性

- 新科技而產生的漏洞

  隨著行動裝置、雲端科技的同時，也對資訊安全防護形成相當程度的挑戰，擔心有心人士將內部機密資訊外洩
  裝置本身的安全性，多數資料都是在員工於不知情的狀況下外洩，例如：裝置遭到惡意程式攻擊讓資料遭到竊取。

社會、科技、人性

- 新科技而產生的漏洞

  特別是行動裝置已與生活緊密結合，許多人開始將機密資料放在手機上而面臨外洩風險。
  應該要積極針對行動裝置進行資安檢測；

  網路與行動裝置結合之便利性大幅提升，使用個人電子郵件、個人的資料共享、通訊軟體如Line等，來連絡公司業務亦十分普遍。
  此類個人服務並不在企業的控管範圍內，也有資料外洩之可能。

社會、科技、人性

- 新科技而產生的漏洞

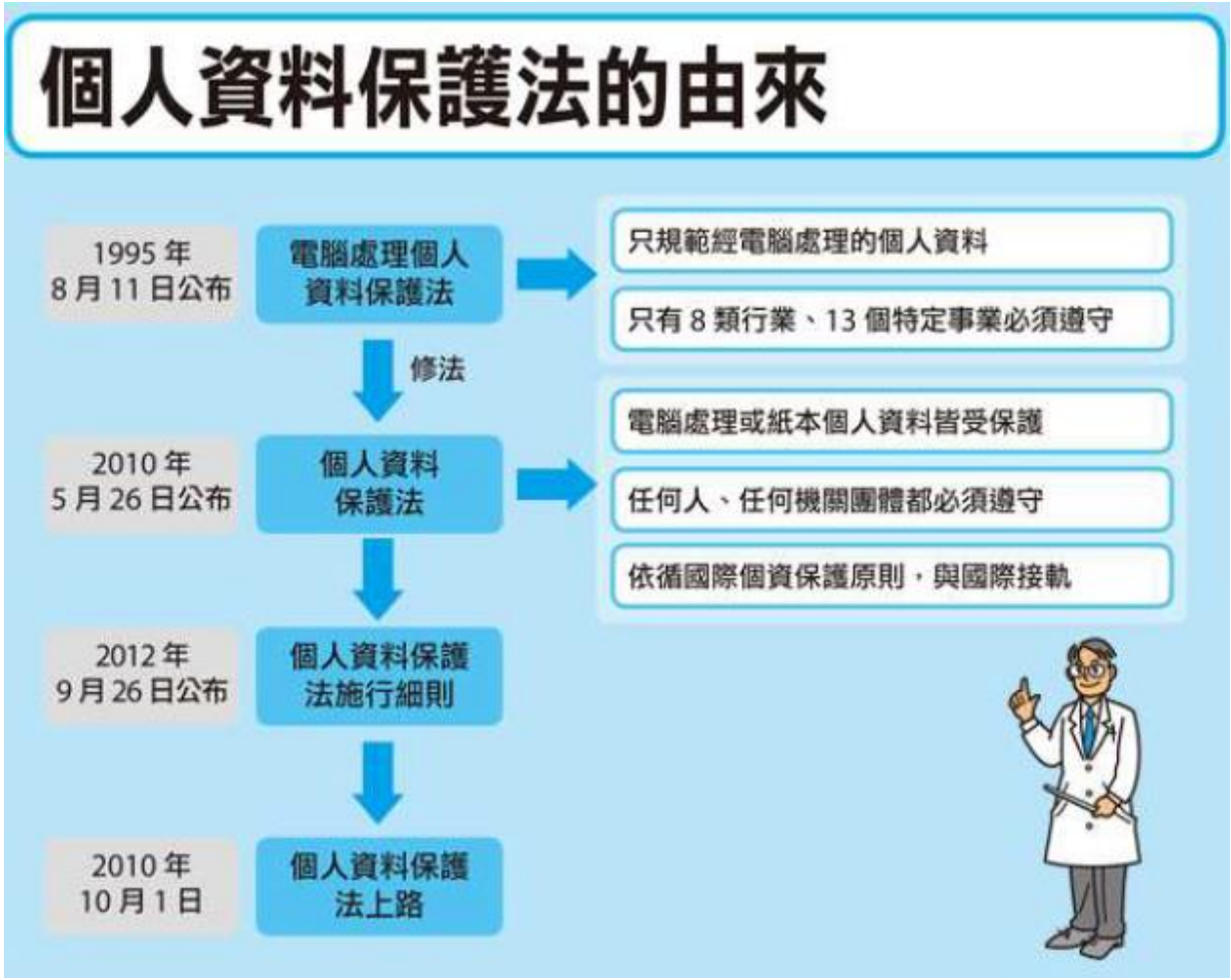
雲端科技的發展，網路銀行，線上交易平台亦隨之發展，又智慧型手機之出現
客戶可在任何時間、任何地點，操作現金以外的銀行業務，這種便利性催化行動銀行的爆炸性成長，然而當越來越多的交易資料存放在雲端，該資安防護能力也就更備受挑戰，業者必
防範隨時可能遭受駭客入侵竊取資料的風險。

動機

- 炫耀(人性)
- 方便(人性)
- 竊取機密檔案/文件
- 針對性資料蒐集
- 線上遊戲、網路購物及網路銀行等服務之有價財產
- 部落格或社群網站之帳號密碼
- 工作商業機密資料
- 跳板(殭屍電腦)
- 監控使用者行為
- 智慧型手機富含使用者個資(通訊錄、E-Mail等)

個資法的沿革

我國自1995年8月1日初次公布之電腦處理個人資料保護法後，在2010年5月26日第一次公布重大的修正，並更名為個人資料保護法(以下稱”個資法”)，2016年個資法全面完整修正施行，也就是在2010年網路普及後將網路資安一併納入處理。



個資安全的情境

個資安全威脅

一、紙本往來威脅：

二、通信傳真威脅：

三、社交工程威脅：

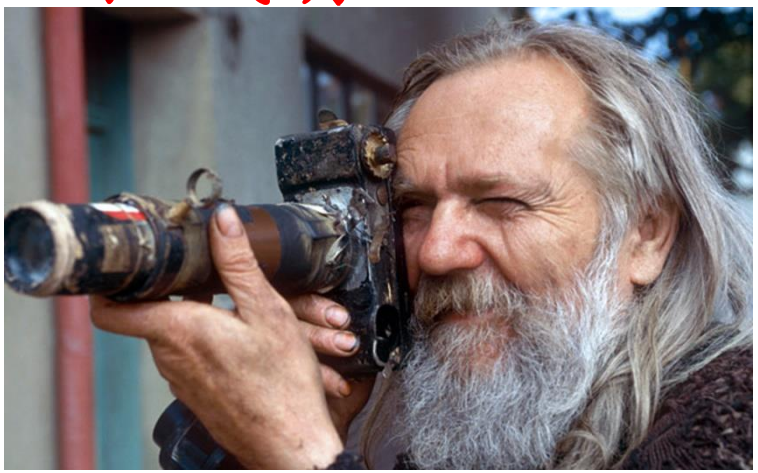
個資安全的情境

個資安全威脅=>一、紙本往來威脅：

錄音機

影印機

相機



流浪漢用「垃圾自製相機」偷拍女人50年，當他的作品曝光後...真的太震撼!

個資安全的情境

個資安全威脅=>二、通信傳真威脅：

傳真機

個資安全的情境

個資安全威脅=>三、社交工程威脅：

書信往來
商業書信
筆友書信

網路資訊安全的情境

網路安全威脅

一、行動威脅：

二、網站威脅：

三、病毒威脅：

四、社交工程威脅：

網路資訊安全威脅有哪些？

「網路無國界」，在科技發達的現代社會網際網路與人們的生活密不可分。以往我們認為只有連上了惡意網站，才會感染病毒或木馬程式，但是後來也發生包括政府、學校，甚至消費、娛樂這些一般大眾會瀏覽的合法網站，皆被利用成為惡意程式感染的主要來源。就讓本專題來告訴民眾，如何安全用網，建立資安防護罩！

網路資訊安全威脅有哪些？

一、行動威脅：

使用者所使用的手機，已經是一部可移動式的電腦，尤其開放的作業平台，等於為駭客開啟了一扇窗，透過各種行動套件，使得這一類的攻擊更容易發起。許多行動裝置，像是數位相機、 GPS 等消費性電子產品，都具備了 USB 介面以及儲存媒體的功能，這些裝置只要一連接電腦，很容易就可入侵成功，並且容易散佈。

網路資訊安全威脅有哪些？

二、網站威脅：

利用瀏覽器安全漏洞的攻擊，使合法網站成為最主要的攻擊目標，尤其是針對 Flash 和 Quicktime 等外掛程式的漏洞，將會使駭客入侵的成功率大幅提升。

網路資訊安全威脅有哪些？

三、病毒威脅：

可透過連結大量散佈，在很短的時間內即感染大量的電腦。有些木馬病毒可以長時間潛伏在目標電腦之中竊取使用者資料。

網路資訊安全威脅有哪些？

四、社交工程威脅：

為竊取有價值的情報資訊，攻擊者會利用郵件或連結夾藏木馬，並且透過系統漏洞來取得目標電腦的控制權。攻擊者偽裝成政府單位或金融單位等機關，配合 email 和語音系統的詐騙手法，使一般人很容易就會掉入釣魚陷阱。

行動威脅

智慧型手機已和現代人的生活密不可分，但在滑介面時，所有的資料，都有可能暴露在遭惡意利用或曝光的險境中。根據調查，臺灣12歲以上的民眾，持有智慧型行動裝置人口約有1,432萬人，普及率已達65.4%，預測2018年將達81.7%。本專題介紹在手機上的資安風險，讓民眾在享受科技的同時也能注意自身的資訊隱私。

行動威脅

智慧型手機，就規格與效能來看，等同於一部可隨手攜帶的微型電腦，然就安全性而言，手機本身的設計與預設組態上可能存在不少潛在弱點。美國國家標準局指出當前行動裝置7大主要資安風險來源如下：

行動威脅

是否安裝不可信任的APP軟體

手機APP軟體最大隱憂為「使用者權限」及「個資外洩」問題。許多手機應用程式的使用條款中，使用者須同意應用程式可存取使用者的個人資料，包含手機狀態、識別碼、GPS定位、連絡人資料、通話記錄、完整網路存取權、擷取執行中的應用程式。很多人往往未仔細瞭解應用程式的存取權限，即按下同意，個人資料便在不知不覺中洩露。

行動威脅

行動裝置本身是否可信任

現在的行動裝置普遍時有越獄（JailBreak）或取得原始管控權力（Root）事件發生，也就是技術性修改行動裝置原有的安全設定，或是作業系統的使用限制，使其無法發揮實質保護功能。

行動威脅

是否連線至可信任的網路

免費Wi-Fi是最具有潛在威脅的上網管道，駭客可藉由Wi-Fi攻擊手機上的應用程式，在其中植入惡意連結，甚至點選木馬連結。

行動威脅

行動裝置連線安全與遺失風險

比起其他裝置，使用智慧型手機最大風險莫過於遺失或遭竊，若手機未設定保護功能，未經授權的人可以直接取得失竊手機內部所有資料。

行動威脅

是否使用安全的資料同步儲存與雲端備份

行動裝置在資料同步與儲存時，可能須與其他系統互動。在行動裝置、遠端備份、個人筆電間傳輸資料若同時連結內、外部網路環境，就會讓惡意程式有機會在設備間傳送。

行動威脅

是否存取不可信任的內容

行動裝置有可能使用不可信任的內容，例如QR Code會被轉譯成相關的連結網址，而惡意的QR Code有可能直接將行動裝置導向惡意網頁。

行動威脅

是否揭露行動裝置GPS定位

內建GPS功能的智慧型手機通常可以執行在地化服務，但在安全方面，具在地化服務功能的行動裝置面臨更大的目標性攻擊風險，有心人士易於利用這些資訊發動攻擊。

行動威脅

手機資安防護三大招

01. 限制惡意程式的安裝。
02. 設定手機不允許安裝非市集中的應用程式。設定手機，取消勾選「設定」內的「安全性」/「應用程式設定」中「未知的來源」。

行動威脅

手機資安防護三大招

03. 養成良好使用習慣

(1) 使用任何通訊軟體與社群軟體，切勿使用懶人密碼。

(2) 絕對不要點選傳送來的訊息裡面的連結。如果是好友送來的訊息，建議與對方確定連結安全之後再開。

(3) 不隨意提供個人資訊，也不轉知簡訊收到的密碼。

(4) 需要使用小額付款的使用者，應啟用「即時消費通知」，若發現詐騙發生務必報警，才可當作是被詐騙證明到臨櫃辦簽結退款。

(5) 安裝手機防毒軟體。

網路資安的重點議題

- 密碼安全
- 軟體使用安全
- 病毒與木馬防護安全
- 電腦操作安全與資料備份
- USB管理
- 公用存取
- 電子郵件安全
- 社交工程
- 網路釣魚與網路詐騙
- 日益猖獗的勒索病毒

課程大綱

- 密碼安全
- 軟體使用安全
- 病毒與木馬防護安全
- 電腦操作安全與資料備份
- USB管理
- 公用存取
- 電子郵件安全
- 社交工程
- 網路釣魚與網路詐騙
- 日益猖獗的勒索病毒

密碼的重要性

- 在電腦的世界裡，帳號代表身分，而密碼則是鎖匙。簡單的說，密碼就是電腦確認身分的方法。
- 駭客想要竊取您的資源，就必須以您或電腦管理者的腳色登入電腦，而兩者皆需要使用密碼。
- 所以說保管好密碼就是防止駭客攻擊最簡單卻最重要的工作

密碼的重要性～1

您可能不曉得…

您的懶人密碼讓駭客輕易破解您的密碼！

使用暴力破解軟體
破解網路相簿密碼

懶人密碼網友最愛

- 密碼管理程式開發商Keeper Security揭露2016年最常見的密碼，高居榜首的是123456，約有17%的網友使用，顯示不少網友依舊習慣使用最簡單的密碼，也曝露出許多網站未強迫使用者設定強大密碼。

Top 25 Most Common Passwords of 2016

RANK	PASSWORD
1.	123456
2.	123456789
3.	qwerty
4.	12345678
5.	111111
6.	1234567890
7.	1234567
8.	password
9.	123123
10.	987654321

（資料來源:keeper Security 2016）

密碼安全管理的對策

安全管理的對策

- 定期更新密碼
- 定期檢查密碼
- 設定優質密碼
  - 避免使用重複數字/單位簡稱/詞語/生日
  - 數字字母符號穿插且不過於複雜(長度在6~15之間, 英數字大小寫及文書符號夾雜)
  - 避免重複使用密碼(1年內部使用舊密碼)
- 不告訴他人密碼或寫下密碼
- 懷疑密碼外洩立即更新

盡量避免的密碼

設定密碼應儘量避免以下情形：

- 避免使用英文字典的字，如：computer、telephone
- 避免全部使用數字
- 避免連號：a12345、b98765
- 避免順序：abcdef、pqrst
- 避免使用a或1開頭的密碼防止字典攻擊（字典攻擊通常從a開頭的字母或1開頭的數字開始）

密碼強度測試

http://password.mx500.com/

測試你的密碼		密碼最低要求
待測密碼:	••••••••••••	• 密碼最低要求8字元 • 最少符合下列四項中三項規則: - 大寫英文字元 - 小寫英文字元 - 數字字元 - 符號字元
密碼隱藏:	☑	
分數:	91%	
評語:	非常 強	

加分項目	型態	計算規則	次數	小計
密碼字數	Flat	+(n*4)	12	+ 48
大寫英文字元	Cond/Incr	+((len-n)*2)	2	+ 20
小寫英文字元	Cond/Incr	+((len-n)*2)	5	+ 14
數字字元	Cond	+(n*4)	5	+ 20
符號字元	Flat	+(n*6)	0	0
密碼中間穿插數字或符號字元	Flat	+(n*2)	4	+ 8
已達密碼最低要求項目	Flat	+(n*2)	4	+ 8
扣分項目				
只有英文字元	Flat	-n	0	0
只有數字字元	Flat	-n	0	0
重複字元 (Case Insensitive)	Incr	-(n(n-1))	0	0
連續英文大寫字元	Flat	-(n*2)	1	- 2
連續英文小寫字元	Flat	-(n*2)	4	- 8
連續數字字元	Flat	-(n*2)	4	- 8
連續字母超過三個(如abc,def)	Flat	-(n*3)	0	0
連續數字超過三個(如123,234)	Flat	-(n*3)	3	- 9

說明

- **優秀:** 已超出最低標準. 總分將會被加分.
- **已達標準:** 已達最底標準. 總分將會被加分.
- **警告:** 針對不好的部份提出勸導. 總分將會被扣分.
- **未達標準:** 未達最底標準. 總分將會被扣分.

Gmail二階段式驗證

課程大綱

- 密碼安全
- ➢ 軟體使用安全
- 病毒與木馬防護安全
- 電腦操作安全與資料備份
- USB管理
- 公用存取
- 電子郵件安全
- 社交工程
- 網路釣魚與網路詐騙
- 日益猖獗的勒索病毒

軟體使用安全

- 授權合法軟體
- 共享軟體
- 免費軟體
- 盜版軟體

軟體類別	慣用的商用軟體	可替代的自由軟體
作業系統	Windows	➡ Linux
辦公室軟體	Microsoft Office	➡ OpenOffice.org
檔案壓縮	Winzip	➡ 7-zip
防毒掃毒	PC-cillin	➡ ClamWin
影像處理	PhotoImpact	➡ GIMP
檔案傳輸	CuteFTP	➡ FileZilla
郵件收發	Outlook	➡ Thunderbird
網頁瀏覽器	Explorer	➡ Firefox
網頁製作	FrontPage	➡ NVU

合法授權軟體?

- 將一份獲得授權的軟體安裝在多部電腦當中。
- 員工將公司內部的軟體帶回家中進行拷貝或散佈。
- 購買升級版為軟體進行升級，卻並未擁有該軟體的合法舊版本授權。
- 不具有學術教育機構的資格，卻購買教育版軟體使用。

共享軟體(shareware)

- 讓使用者試用該軟體，並考慮是否付費購買該軟體。
- 共享軟體於試用期限過後即須付費註冊、停止使用或仍可使用但是有較多限制。
- 注意

  如於試用期滿仍繼續使用即可能會侵犯**智慧財產權**。

免費軟體(freeware)

- 可以自由免費的使用該軟體，並拷貝給別人，而不必支付費用給程式作者，在使用上也不會有日期限制。
- 風險：

  內含惡意程式，如電腦病毒、間碟軟體等，需小心使用勿隨意下載使用來路不明之軟體

常見盜版方式

- 將正版軟體複製給未經授權的使用者
- 在網際網路上非法散佈
- 透過網路非法使用
- 軟體版權授權數不足

合法軟體好處

- 得到原廠的技術支援
- 得到完整的產品介紹和文件
- 有權進行軟體更新和升級
- 避免不必要的風險
- 避免受到法律上的處罰
- 避免傷害他人
- 可以安心使用產品

自行/委外開發軟體安全

- 安全要求分析與規格
- 系統文件管理
- 系統測試資料的保護
- 程式源碼的存取控制與集中管理、版本控制
- 測試資料的保護
- 軟體變更控制程序
- 委外的軟體開發管理
- 技術脆弱性控制，如：Code review、滲透測試
- Shareware 與 freeware 管理

課程大綱

- 密碼安全
- 軟體使用安全
- ➢ 病毒與木馬防護安全
- 電腦操作安全與資料備份
- USB管理
- 公用存取
- 電子郵件安全
- 社交工程
- 網路釣魚與網路詐騙
- 日益猖獗的勒索病毒

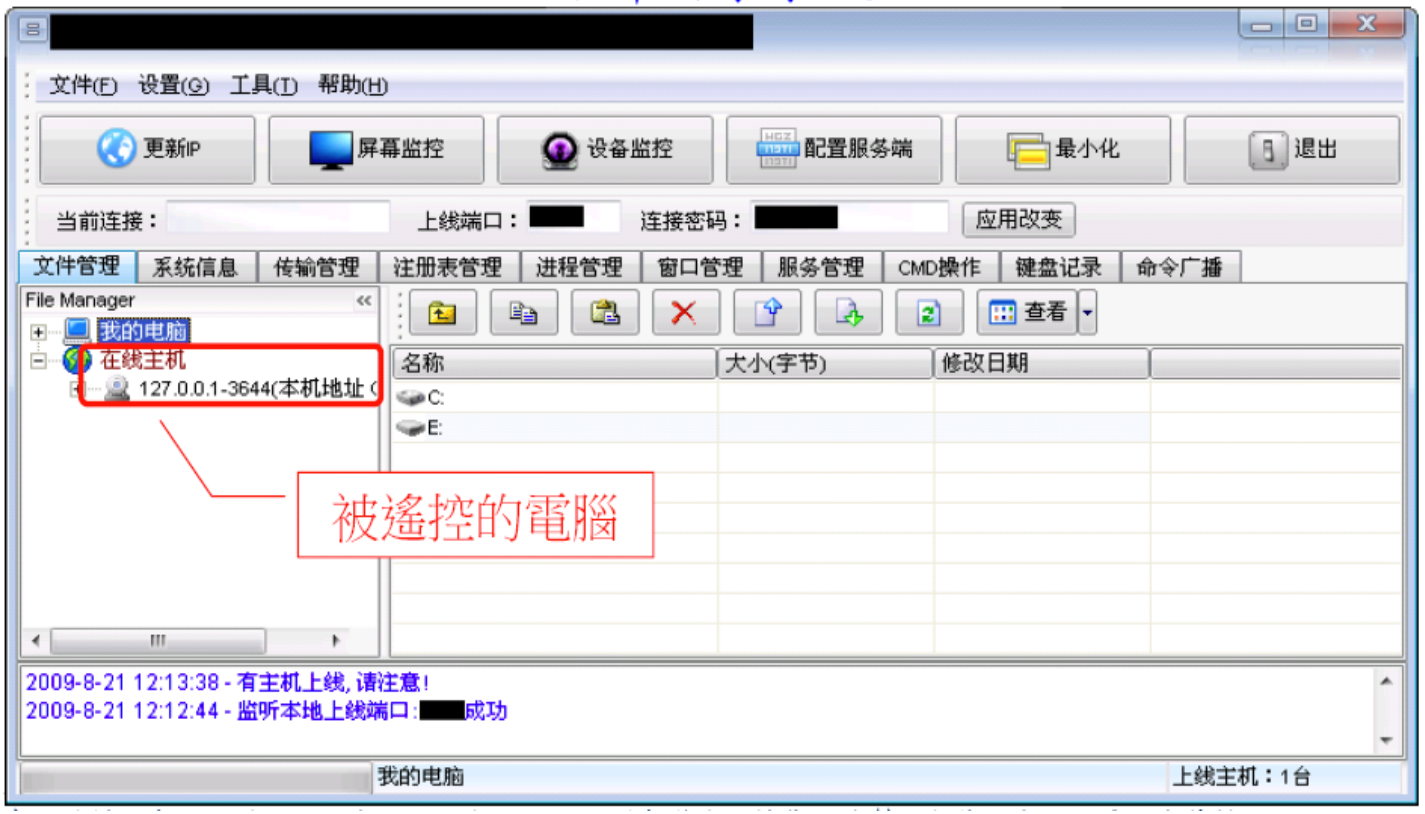
病毒與木馬防護安全

- 病毒
  - 病毒是一種程式，一種會將自己附加在其它程式裡面的軟體，當附加程式被執行的時候，病毒程式也跟著啟動。
- 特性
  - 傳播和感染能力，可能會造成系統損害、刪除程式或者資料。
  - 通常會附著在可執行檔或開機磁片、磁碟，甚至硬碟分割磁區，不過必須附加在其它程式中才能感染另一台電腦，某些病毒也會藉著電子郵件 (E-mail) 感染其它電腦。

木馬程式

所以您要曉得，

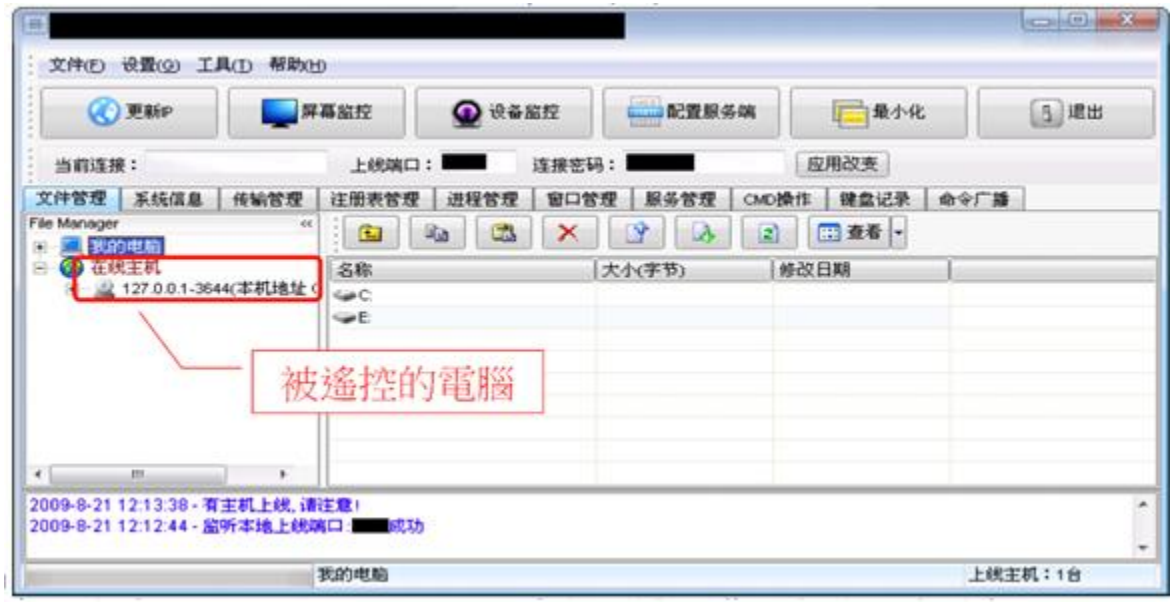
這些木馬程式威力強大，一旦中招，可能就任由宰割了！



本簡報內

木馬程式的威脅

特洛伊**木馬**（Trojan Horse），在電腦領域中指的是一種後門程式，是駭客用來盜取其他用戶的個人資訊，甚至是遠端控制對方的電腦而加殼製作，然後通過各種手段傳播或者騙取目標使用者執行該程式，以達到盜取密碼等各種資料資料等目的。



木馬程式的伎倆

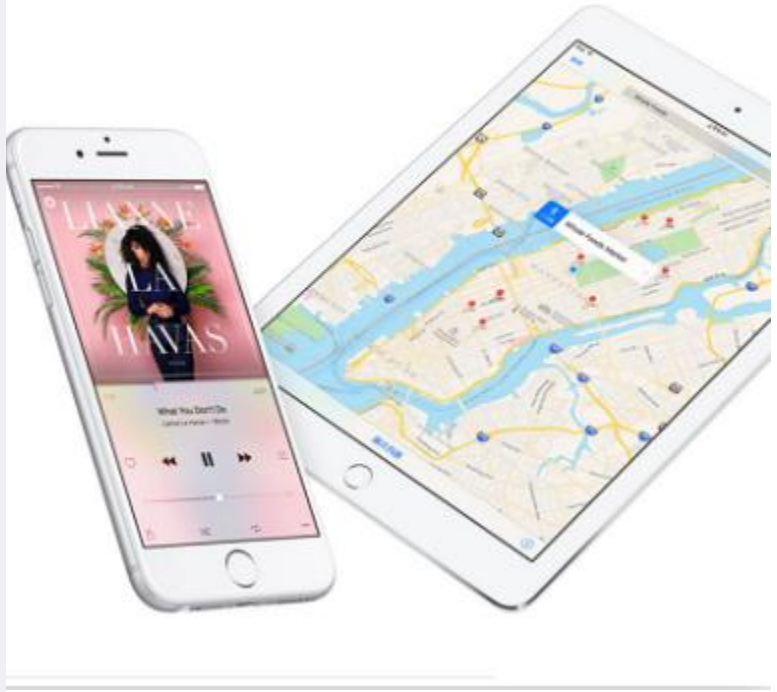
要使用者務必注意這是

01.「詐騙訊息」
02. APP軟體銷售廣告(防毒軟體)

無論如何不要輕信並下載來路不明的檔案！

木馬威脅不分廠牌系統

iOS 9.2.1 主要是修復系統錯誤（圖 / Apple）



建議用戶盡快將裝置升級，修復這個系統漏洞

你(妳)今天臉書(Facebook)了嗎?…

Facebook(安全議題)

Facebook已成為全世界電腦族全民運動，但小心駭客隨棍上。

- 防毒軟體公司發現，已有利用Facebook受歡迎程度的木馬程式，以假的通知信要求使用者以所附連結，誘使使用者點入連結後，散布木馬程式
- 賽門鐵克安全應變中心觀察指出，一份偽造的Facebook帳號通知郵件，告知網路使用者為確保帳號安全性，Facebook已經重新設定其帳號，使用者 若想要知道其新設定的帳號，必需開啟附件中的檔案，而此附檔即藏了木馬程式Trojan.Bredolab.的檔案。若消費者在不知情的情況下開啟此附 檔，則將受到該木馬程式的攻擊。

Facebook登入安全性

病毒與惡意程式防治對策

- **正確的電腦操作觀念**
  - 不任意外流E-Mail Address
  - 不隨意執行來路不明的程式(.exe, .scr, .vbs …等)
  - 不連線惡意的網站
  - 做好系統更新工作
  - 有效的密碼強度
- **個人電腦防護**
  - 防毒軟體
    - 病毒碼確實更新
  - 個人防火牆(如WinXP的ICF…等)

課程大綱

- 密碼安全
- 軟體使用安全
- 病毒與木馬防護安全

➢ 電腦操作安全與資料備份

- USB管理
- 公用存取
- 電子郵件安全
- 社交工程
- 網路釣魚與網路詐騙
- 日益猖獗的勒索病毒

電腦管理對策

硬碟管理區分

- 系統區
  作業系統安裝規畫區
  應用程式安裝規畫區
- 資料區
  所有操作者處理資訊存放區

優點:

- 備份回存管理容易

電腦操作威脅～電腦病毒

- 電腦中毒徵兆
  -電腦系統運行速度異常緩慢
  -上網速度越來越遲緩
  - 異常的系統訊息通知
  - 螢幕顯示異常，例如畫面突然一片空白
  - 來自防毒軟體的警告訊息
  - 電腦無故自動關機或不斷重新開機
  - 瀏覽器自動出現產品廣告或色情網頁
  - 網路流量異常，例如沒有使用網路服務或收發電子郵件，但網路的連線燈號卻一直閃爍

電腦操作威脅～電腦病毒

- 電腦病毒簡易處理步驟
  - 將中毒電腦離線網路作業
  - 設法使防毒軟體運作
  - 以防毒軟體執行病毒的掃瞄於清除
  - 若防毒軟體無法正常執行，則執行以下替代方案:
    - 手動掃毒:
    - 使用未受病毒感染健康的電腦之防毒軟體進行問題硬碟掃毒作業。
    - 透過免費線上掃毒資源,再不危及狀況下連線網路進行 http://www.Kaspersky.com.tw/free-virus-scan
    - 受感染的檔案並執行隔離或刪除動作

電腦操作威脅～廣告/間諜軟體

- 廣告或間諜軟體的症狀
  - 沒有上網卻還是一直看見廣告視窗
  - 網路速度時快時慢
  - 首頁被更改成奇怪的網站
  - 視窗下方的工具列出現許多原本沒有的工具。
  - 瀏覽器多出沒有安裝過的工具列、搜尋工具，而且無法移除。
  - 電腦處理速度變慢或當機頻率增加。

電腦操作威脅～廣告/間諜軟體

- 間諜或廣告軟體的防範
  - 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，例如Google Toolbar。
  - 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
  - 使用至少兩個反間諜軟體程式

電腦操作威脅～駭客入侵

- 駭客入侵的徵兆
  - 檔案及資料庫內容遭到竊取或篡改
  - 不知名的IP來源與電腦連線
  - 系統中異常的服務程式
  - 異常通訊埠開啟
  - 稽核紀錄及檔案中的異常事件
  - 系統帳號的異常增加
  - 系統異常的訊息或行為

電腦操作威脅～駭客入侵

- 駭客入侵的簡易處理
  - 系統備份
  - 可能入侵途徑系統隔離
  - 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
  - 報告相關單位
  - 適時尋求協助

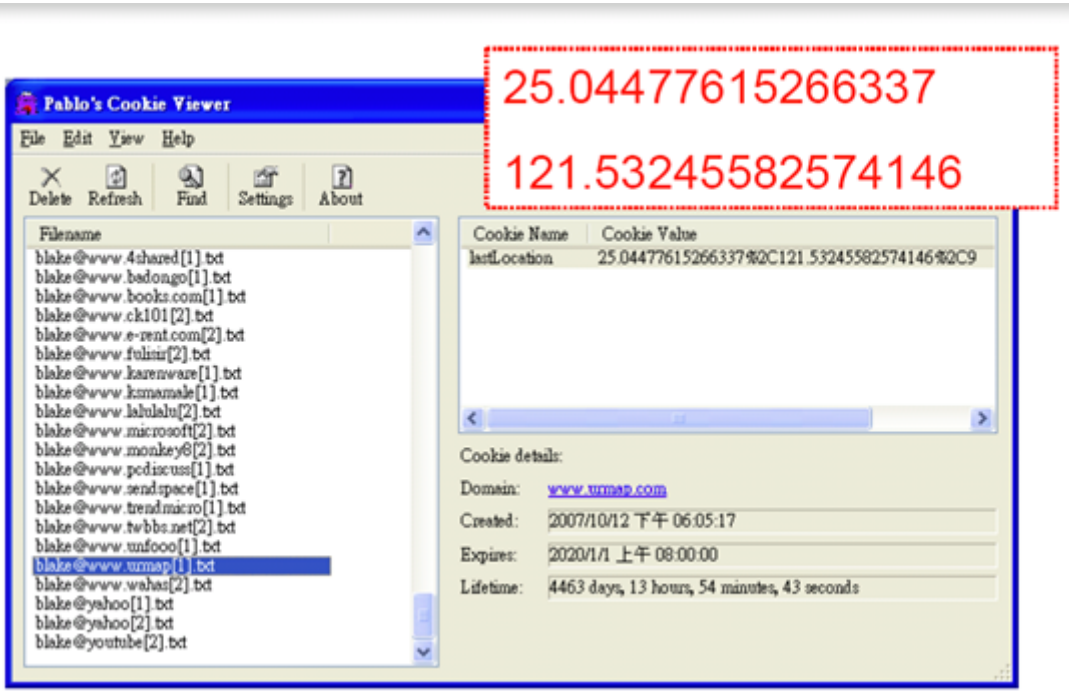
電腦操作威脅～駭客入侵

- 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

Cookies說明

何謂Cookies

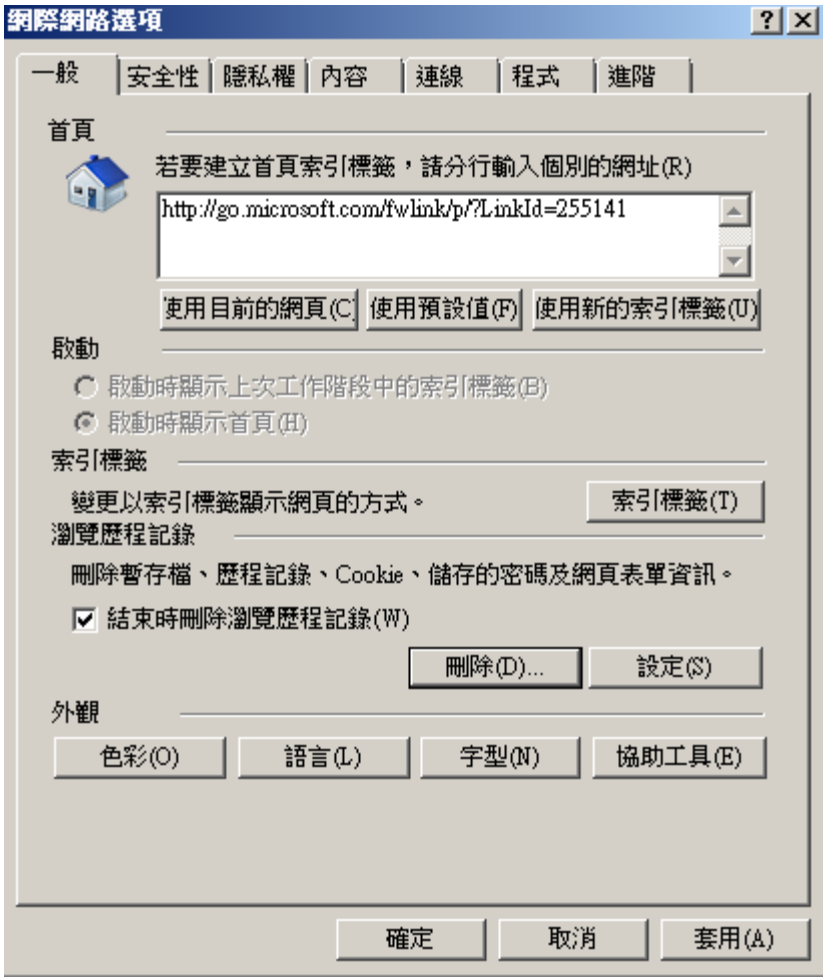
-Cookies是存在瀏覽器中的小型文字檔，記錄使用者瀏覽網頁的資訊，例如瀏覽的網站位址、使用者曾經輸入的資訊等

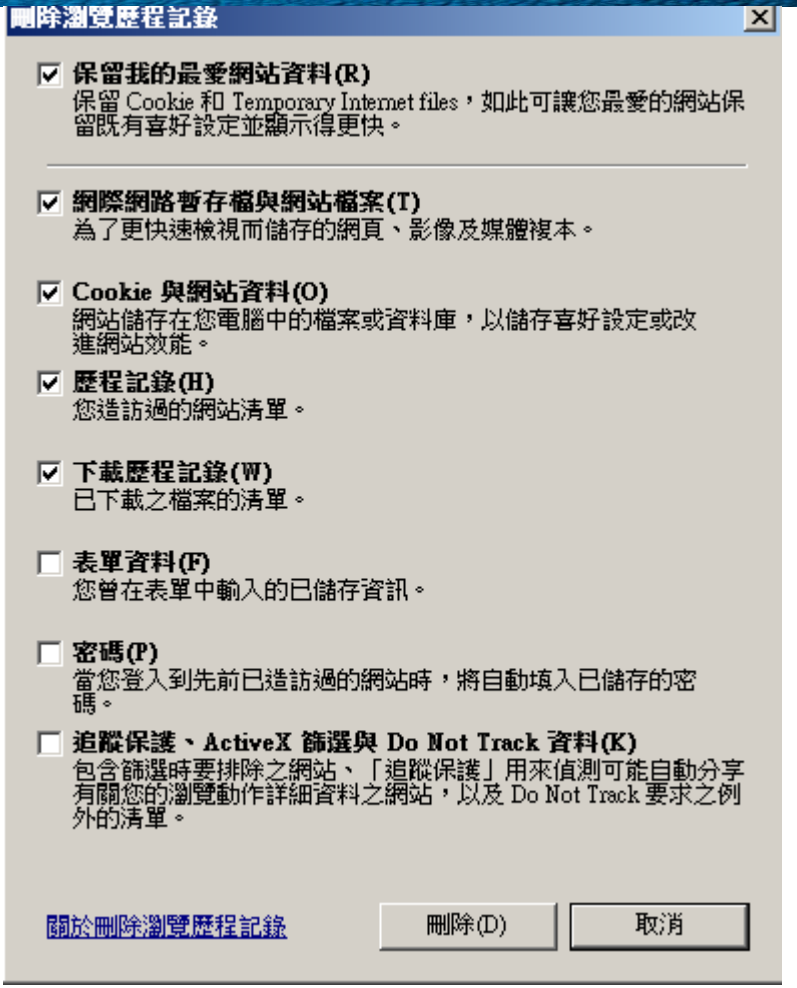


清除電腦上所留的登入資訊

- 以使用Internet Explorer瀏覽器為例
  - Internet Explorer中提供了「自動完成」功能，該功能主要是方便使用者記住曾經在瀏覽器中輸入先前輸入的網址、表單及密碼等訊息。使用者可以調整「自動完成」之設定內容，包括只儲存想要存的資訊，或者根本就不使用該功能。
  - 也可清除已經保留的記錄 。

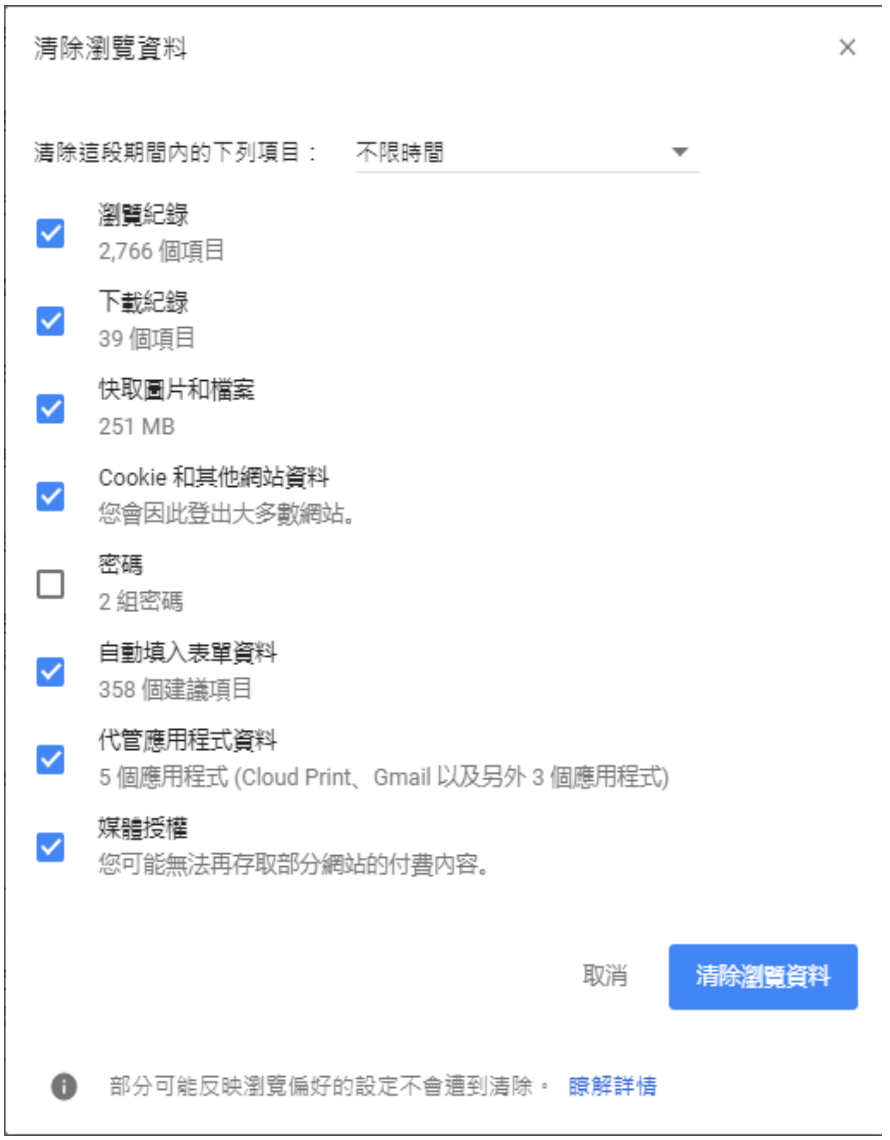
Cookies-潛在危機(IE)





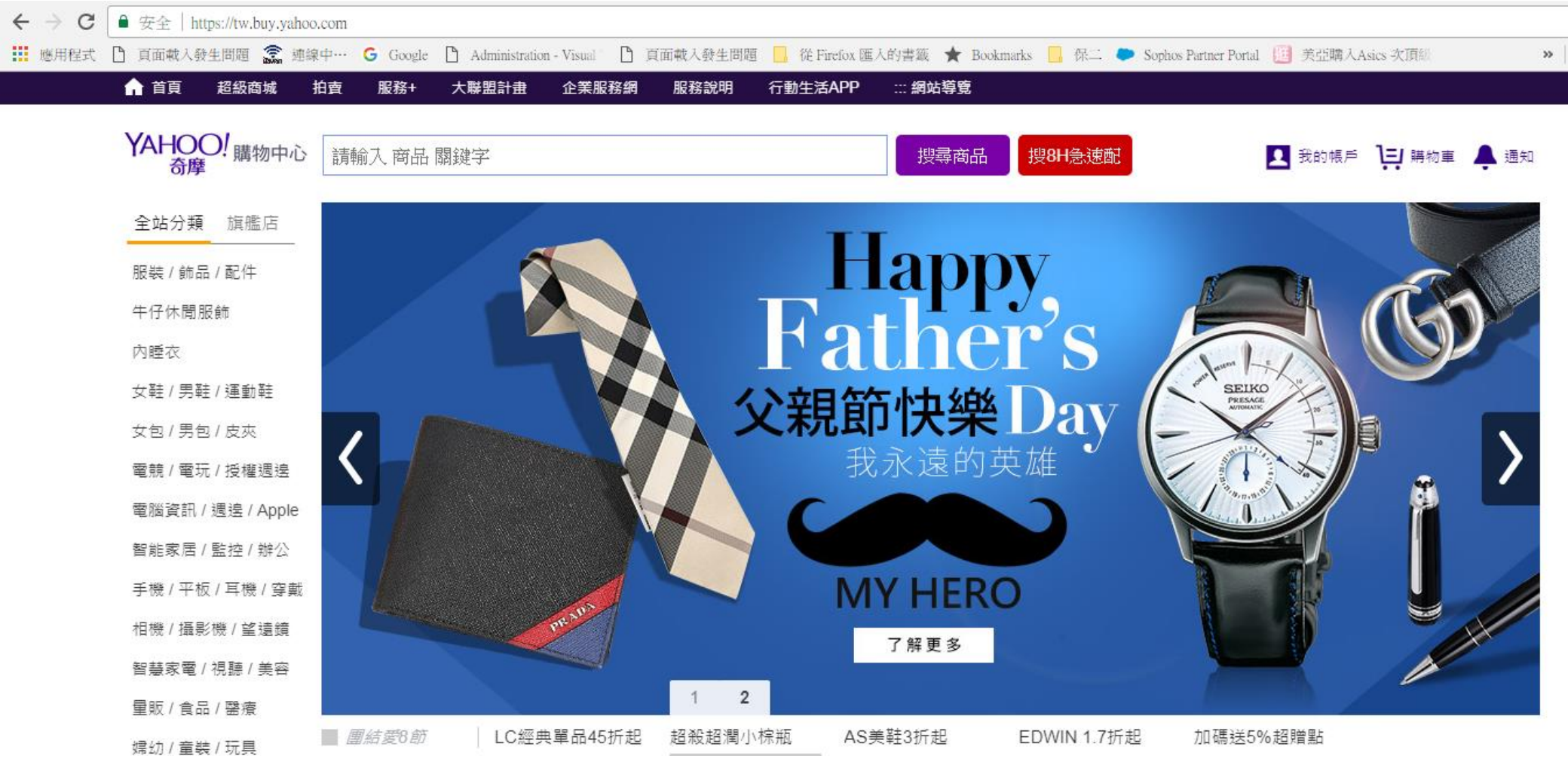
去過哪些網站,輸入過哪些資料、帳號、密碼都是資料可能外洩的來源!

Cookies-潛在危機(chrome)

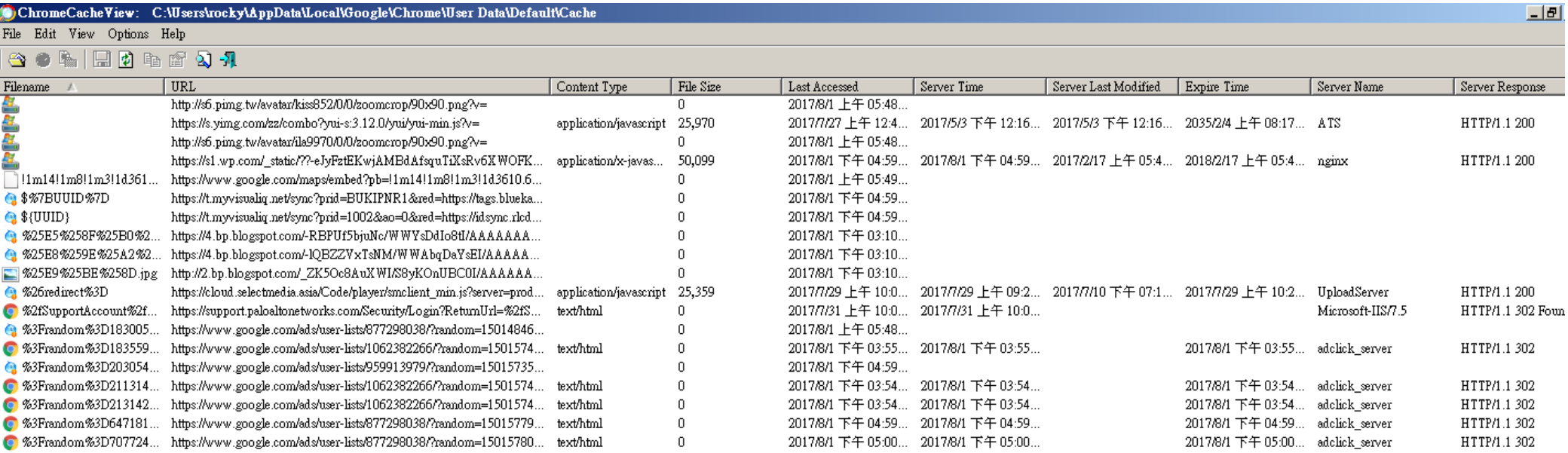


電腦上的暫存檔案，
也可能洩露您曾經做過的操作...

參訪網站


安全 | https://tw.buy.yahoo.com
首頁
超級商城
拍賣
服務+
大聯盟計畫
企業服務網
服務說明
行動生活APP
網站導覽
YAHOO! 奇摩 購物中心
請輸入 商品 關鍵字
搜尋商品
搜8H急速配
我的帳戶
購物車
通知
全站分類
旗艦店
服裝 / 飾品 / 配件
牛仔休閒服飾
內睡衣
女鞋 / 男鞋 / 運動鞋
女包 / 男包 / 皮夾
電競 / 電玩 / 授權週邊
電腦資訊 / 週邊 / Apple
智能家居 / 監控 / 辦公
手機 / 平板 / 耳機 / 穿戴
相機 / 攝影機 / 望遠鏡
智慧家電 / 視聽 / 美容
量販 / 食品 / 醫療
婦幼 / 童裝 / 玩具
Happy Father's
父親節快樂 Day
我永遠的英雄
MY HERO
了解更多
1
2
團結愛8節
LC經典單品45折起
超殺超潤小棕瓶
AS美鞋3折起
EDWIN 1.7折起
加碼送5%超贈點

電腦上的暫存檔案

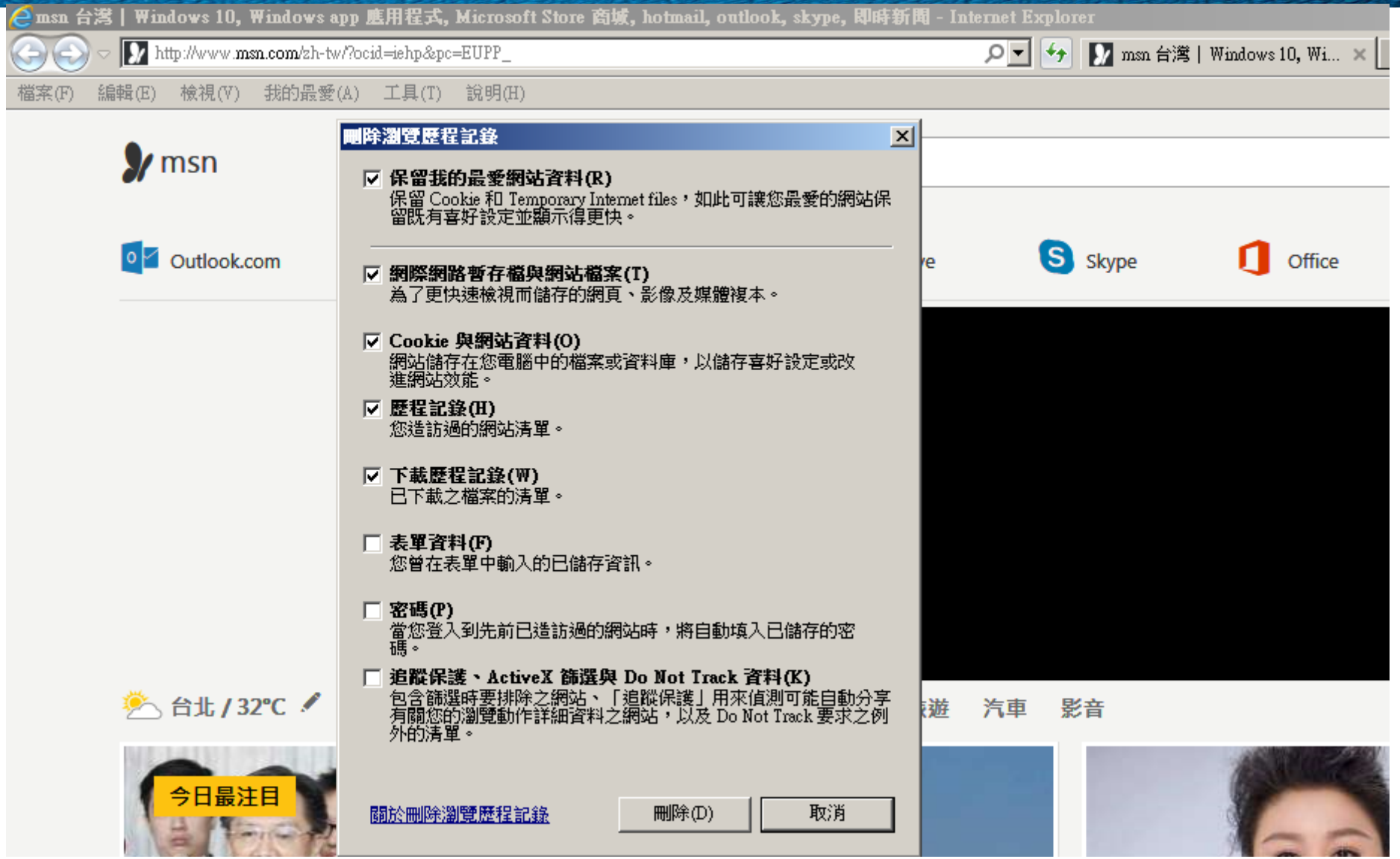

ChromeCacheView: C:\Users\rocky\AppData\Local\Google\Chrome\User Data\Default\Cache

File Edit View Options Help

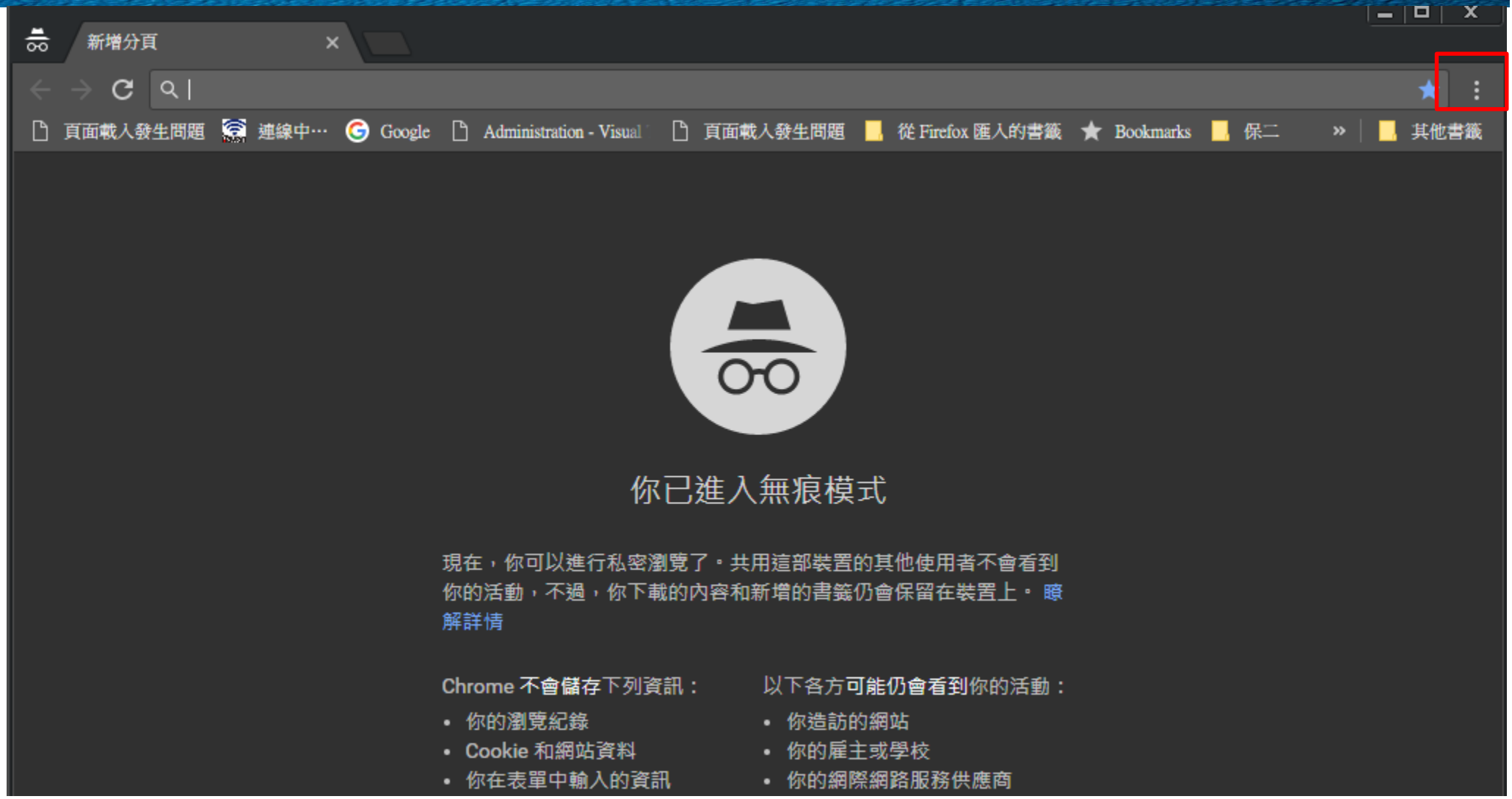
Filename	URL	Content Type	File Size	Last Accessed	Server Time	Server Last Modified	Expire Time	Server Name	Server Response
	http://s6.pimg.tw/avatar/kiss852/0/0/zoomcrop/90x90.png?v=		0	2017/8/1 上午 05:48...					
	https://s.yimg.com/zz/combo?yui-s:3.12.0/yui/yui-min.js?v=	application/javascript	25,970	2017/7/27 上午 12:4...	2017/5/3 下午 12:16...	2017/5/3 下午 12:16...	2035/2/4 上午 08:17...	ATS	HTTP/1.1 200
	http://s6.pimg.tw/avatar/ila9970/0/0/zoomcrop/90x90.png?v=		0	2017/8/1 上午 05:48...					
	https://s1.wp.com/_static/??-eJyFztEKwjAMBdAfsquTiXsRv6XWOFK...	application/x-javas...	50,099	2017/8/1 下午 04:59...	2017/8/1 下午 04:59...	2017/2/17 上午 05:4...	2018/2/17 上午 05:4...	nginx	HTTP/1.1 200
!1m14!1m8!1m3!1d361...	https://www.google.com/maps/embed?pb=!1m14!1m8!1m3!1d3610.6...		0	2017/8/1 上午 05:49...					
$%7BUUID%7D	https://t.myvisualiq.net/sync?prid=BUKIPNR1&red=https://tags.blueka...		0	2017/8/1 下午 04:59...					
${UUID}	https://t.myvisualiq.net/sync?prid=1002&ao=0&red=https://idsync.rlcd...		0	2017/8/1 下午 04:59...					
%25E5%258F%25B0%2...	https://4.bp.blogspot.com/-RBPUf5bjuNc/WWYsDdIo8tI/AAAAAAA...		0	2017/8/1 下午 03:10...					
%25E8%259E%25A2%2...	https://4.bp.blogspot.com/-lQBZZVxTsNM/WWAbqDaYsEI/AAAAA...		0	2017/8/1 下午 03:10...					
%25E9%25BE%258D.jpg	http://2.bp.blogspot.com/_ZK5Oc8AuXWI/S8yKOnUBC0I/AAAAAA...		0	2017/8/1 下午 03:10...					
%26redirect%3D	https://cloud.selectmedia.asia/Code/player/smclient_min.js?server=prod...	application/javascript	25,359	2017/7/29 上午 10:0...	2017/7/29 上午 09:2...	2017/7/10 下午 07:1...	2017/7/29 上午 10:2...	UploadServer	HTTP/1.1 200
%2fSupportAccount%2f...	https://support.paloaltonetworks.com/Security/Login?ReturnUrl=%2fS...	text/html	0	2017/7/31 上午 10:0...	2017/7/31 上午 10:0...			Microsoft-IIS/7.5	HTTP/1.1 302 Foun
%3Frandom%3D183005...	https://www.google.com/ads/user-lists/877298038/?random=15014846...		0	2017/8/1 上午 05:48...					
%3Frandom%3D183559...	https://www.google.com/ads/user-lists/1062382266/?random=1501574...	text/html	0	2017/8/1 下午 03:55...	2017/8/1 下午 03:55...		2017/8/1 下午 03:55...	adclick_server	HTTP/1.1 302
%3Frandom%3D203054...	https://www.google.com/ads/user-lists/959913979/?random=15015735...		0	2017/8/1 下午 04:59...					
%3Frandom%3D211314...	https://www.google.com/ads/user-lists/1062382266/?random=1501574...	text/html	0	2017/8/1 下午 03:54...	2017/8/1 下午 03:54...		2017/8/1 下午 03:54...	adclick_server	HTTP/1.1 302
%3Frandom%3D213142...	https://www.google.com/ads/user-lists/1062382266/?random=1501574...	text/html	0	2017/8/1 下午 03:54...	2017/8/1 下午 03:54...		2017/8/1 下午 03:54...	adclick_server	HTTP/1.1 302
%3Frandom%3D647181...	https://www.google.com/ads/user-lists/877298038/?random=15015779...	text/html	0	2017/8/1 下午 04:59...	2017/8/1 下午 04:59...		2017/8/1 下午 04:59...	adclick_server	HTTP/1.1 302
%3Frandom%3D707724...	https://www.google.com/ads/user-lists/877298038/?random=15015780...	text/html	0	2017/8/1 下午 05:00...	2017/8/1 下午 05:00...		2017/8/1 下午 05:00...	adclick_server	HTTP/1.1 302

凡走過必留痕跡

使用瀏覽器選項清除檔案



瀏覽器無痕模式(chrome)



瀏覽器無痕模式(IE)


InPrivate - Internet Explorer - [InPrivate]
InPrivate
about:InPrivate
InPrivate
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
已開啟 InPrivate
開啟 [InPrivate 瀏覽] 時，您將看到這個指示器
InPrivate
about:InPrivate
「InPrivate 瀏覽」可阻止 Internet Explorer 儲存與瀏覽工作階段有關的資料。這包括 Cookie、網際網路暫存檔、歷程記錄與其他資料。工具列與延伸模組預設是停用狀態。如需詳細資訊，請參閱 [說明]。
若要關閉 [InPrivate 瀏覽]，請關閉此瀏覽器視窗。
深入了解 InPrivate 瀏覽 | 線上閱讀 Internet Explorer 隱私權聲明

資料備份

- 避免因個人電腦當機，造成資料損失
- 避免人為不當操作電腦，將資料誤刪
- 避免因電腦病毒感染作業系統或資料，造成資料損失
- 避免因天然災害，造成資料損失作為資料本身另一種備援，防範不可預期之災害

資料備份政策

可利用資料夾來區分檔案之重要性。個人作業資料建議採取以下備份政策

- 特別重要檔案，每次異動即進行備份
- 每週進行重要檔案備份(選擇性備份)
- 每月進行全部檔案備份(完整備份)

資料備份方式

- 網路磁碟:公司若有規劃共同的儲存地點，如:網路磁碟、檔案伺服器，可優先存放，並由資訊管理人員統一備份
- 網路芳鄰:跟同仁合作，互相開資源分享，設定權限並相互備援
- 隨身碟、CD或DVD燒錄:如公司政策允許使用隨身碟、CD或DVD燒錄，亦是經濟實惠的選擇。

資料備份注意事項

- 備份資料最好存放於另一處所，以分散風險。
- 重要機密資料，可以將資料先加密再備份，保護資料被竊取使用。
- 備份資料應週期性進行回復測試，以確認備份資料之可用性。
- 備份資料的使用，宜有一套管理措施，例如：經過適當的申請與核准程序。

USB的管理

- 密碼安全
- 軟體使用安全
- 病毒與木馬防護安全
- 電腦操作安全與資料備份
- USB管理
- 公用存取
- 電子郵件安全
- 社交工程
- 網路釣魚與網路詐騙
- 日益猖獗的勒索病毒

USB的管理


新增信任裝置
在表格中顯示已定義的下列裝置：
裝置 ID
裝置類型：
名稱： (根據遮罩)
電腦： (根據遮罩)
抽取式磁碟機
更新
裝置類型
裝置型號\裝置 ID
電腦
抽取式磁碟機 ADATA HD710 USB Device\USBSTOR\DISK&VEN_ADATA&PR...
抽取式磁碟機 ADATA USB Flash Drive USB Device\USBSTOR\DISK&VEN_AD...
抽取式磁碟機 Google File-CD Gadget USB Device\USBSTOR\DISK&VEN_GO...
抽取式磁碟機 HTC Android Phone USB Device\USBSTOR\DISK&VEN_HTC&P...
抽取式磁碟機 HUAWEI SD Storage USB Device\USBSTOR\DISK&VEN_HUAW...
抽取式磁碟機 I:\\WPDBUSENUMROOT\UMB\2&37C186B&1&STORAGE#VOL...
抽取式磁碟機 Imation Nano Pro USB Device\USBSTOR\DISK&VEN_IMATION...
抽取式磁碟機 Imation Nano Pro USB Device\USBSTOR\DISK&VEN_IMATION...
允許使用者和/或使用者群組：
Everyone
選取...
說明
確定
取消

USB的管理

小心！USB埠成為企業機密資料外洩管道

因應新版個資法，企業有必要重新檢視所有可能的資料外洩管道，特別是USB儲存設備，這個取得及使用門檻極低的小東西，往往是危害企業資安的致命殺手

USB的管理

◆各型企業的IT預算有限

◆或者是為了迎合管理端的需求

所以對於USB是否要封鎖，或者能夠做到的程度，在實際做法上存在著差異。

USB的管理

利用已安裝好作業系統的隨身碟，再將該電腦設定為從USB啟動，就有可能以替換作業系統的方式，來剽竊電腦中的檔案。

USB中的免安裝程式:

- 木馬程式-惡作劇,個資竊取
- 破壞性病毒程式-干擾, 癱瘓系統

USB的管理

USB隨身碟使用原則

使用隨身碟應遵守下列原則：

一、先執行「安全地移除 USB Mass Storage Device 」。

二、拔除裝置。

三、不儲存機敏性資料，如必須儲存應加密，並於使用後將資料立即刪除。

四、妥善保管避免遺失。

個人使用隨身碟除了要注意上述事項外，在辦公室裡更要提防個人電腦或伺服器裡的機敏資料被有心人士利用隨身碟輕易盜拷。平常除需養成螢幕淨空與機敏資料加密等習慣外，若電腦使用 USB 的機會少，可考慮封鎖 USB 傳輸資料功能，以策安全。

課程大綱

- 密碼安全
- 軟體使用安全
- 病毒與木馬防護安全
- 電腦操作安全與資料備份
- USB管理
- 公用存取
- 電子郵件安全
- 社交工程
- 網路釣魚與網路詐騙
- 日益猖獗的勒索病毒

公共電腦使用安全

- 登入網路服務動作的保護
  - 使用公共電腦時，尤其要注意避免勾選任何的記住帳號或密碼的功能
- 使用公共電腦後，關閉網頁瀏覽器，清除個人相關資料
  - 清除網頁瀏覽記錄/網站上所留下的個人資料/電腦中的**cookie**/隱私權記錄/密碼記錄
- 盡量避免利用公共電腦上網處理重要或私密事務
- 特別注意坐在或站在你旁邊的人
- 更換密碼的頻率要更高

課程大綱

- 密碼安全
- 軟體使用安全
- 病毒與木馬防護安全
- 電腦操作安全與資料備份
- USB管理
- 公用存取
- 電子郵件安全
- 社交工程
- 網路釣魚與網路詐騙

電子郵件使用

就使用者而言

- 垃圾信的數量很多
- 不容易找到想要的信
- 浪費時間
- 刪掉重要信件
- 擔心信箱爆掉
- 網路釣魚

對網路管理者而言

- 伺服器癱瘓
- 網路阻塞
- 浪費頻寬
- 郵件伺服器空間
- 員工生產力降低
- 隱藏資安危機

減低垃圾郵件的風險

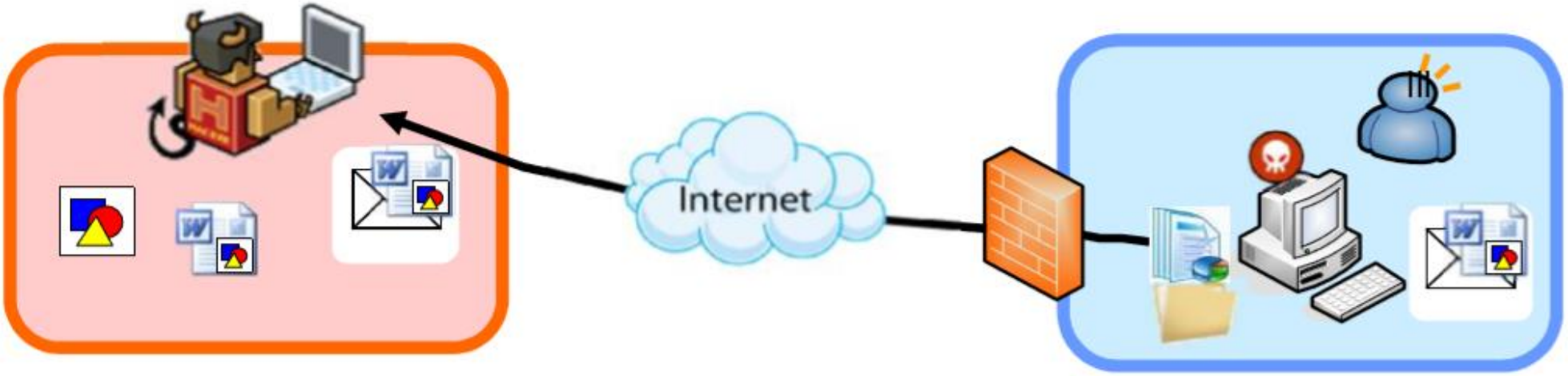
- 絕不回覆垃圾電子郵件，因為這樣會讓寄件者知道你的信箱是有效的。
- 絕不購買垃圾電子郵件的廣告商品，這樣只會鼓勵寄件者持續不斷的寄發。
- 不轉寄串接式的電子郵件(聲稱不轉寄給10個人就會倒楣的電子郵件)
- 使用垃圾電子郵件過濾軟體。
- 留下資料前，記得閱讀每個曾造訪過的網站隱私權保障聲明，了解自己的電子郵件信箱會被使用的用途。

電子郵件社交工程

- 在網路世界最常使用的溝通管道就是電子郵件，因此 社交工程和電子郵件的相互結合，創造了新的詐騙手 法

- 目前這樣的手法已大量被駭客拿來利用，「電子郵件 + 社交工程 + 木馬/後門程式」，駭客能夠取得的不僅 僅是個人資訊，公務機密資料，甚至竊盜網路銀行帳 號密碼、私自進行網路轉帳等行為

電子郵件社交工程攻擊方式



1. 駭客設計攻擊陷阱程式(如特殊*Word*檔案)
2. 將攻擊程式偽裝成附件並夾帶於電子郵件中
3. 寄發電子郵件給特定的目標
4. 受害者開啟電子郵件
5. 啟動駭客設計的陷阱，並被植入後門程式
6. 後門程式逆向連接，向遠端駭客報到
7. 遠端駭客進行資料竊取

社交工程電子郵件手法案例

- 假冒寄件者並設定優先權-利用郵件高或重要優先權，吸引使用者開啟郵件
- 含有惡意程式的附件-偽裝報稅通知訊息
- 含有惡意程式的附件-利用圖示修改與副檔名隱藏方式，引誘使用者開啟
- 含有惡意連結(網路釣魚)

社交工程電子郵件內容

- 令人緊張或鬆懈防備之郵件主旨
  - 關心提醒(請告訴身旁的女性朋友，小心電梯之狼)
  - 誇大聳動(世界末日大預言)
  - 郵件回覆(RE:會議參考資料)
  - 郵件轉寄(FW:簡易規劃日本自助旅行)
- 工作業務、生活時事等相關或令人感興趣之郵件內容 類型
  - 政治新聞、特殊新奇
  - 生活議題、休閒娛樂
  - 社交群體、健康養生

社交工程電子郵件內容範例

郵件主旨	附件
菲律賓槍殺漁民事件真實照片	殘忍的真相.rar
最近超火紅！鄉民的進擊	RCS.DOC
台灣與菲火力比較分析	
十二五時期大陸的經濟戰略對台灣影響	十二五時期大陸的經濟戰略與影響.doc
李x瑞	27G.7z

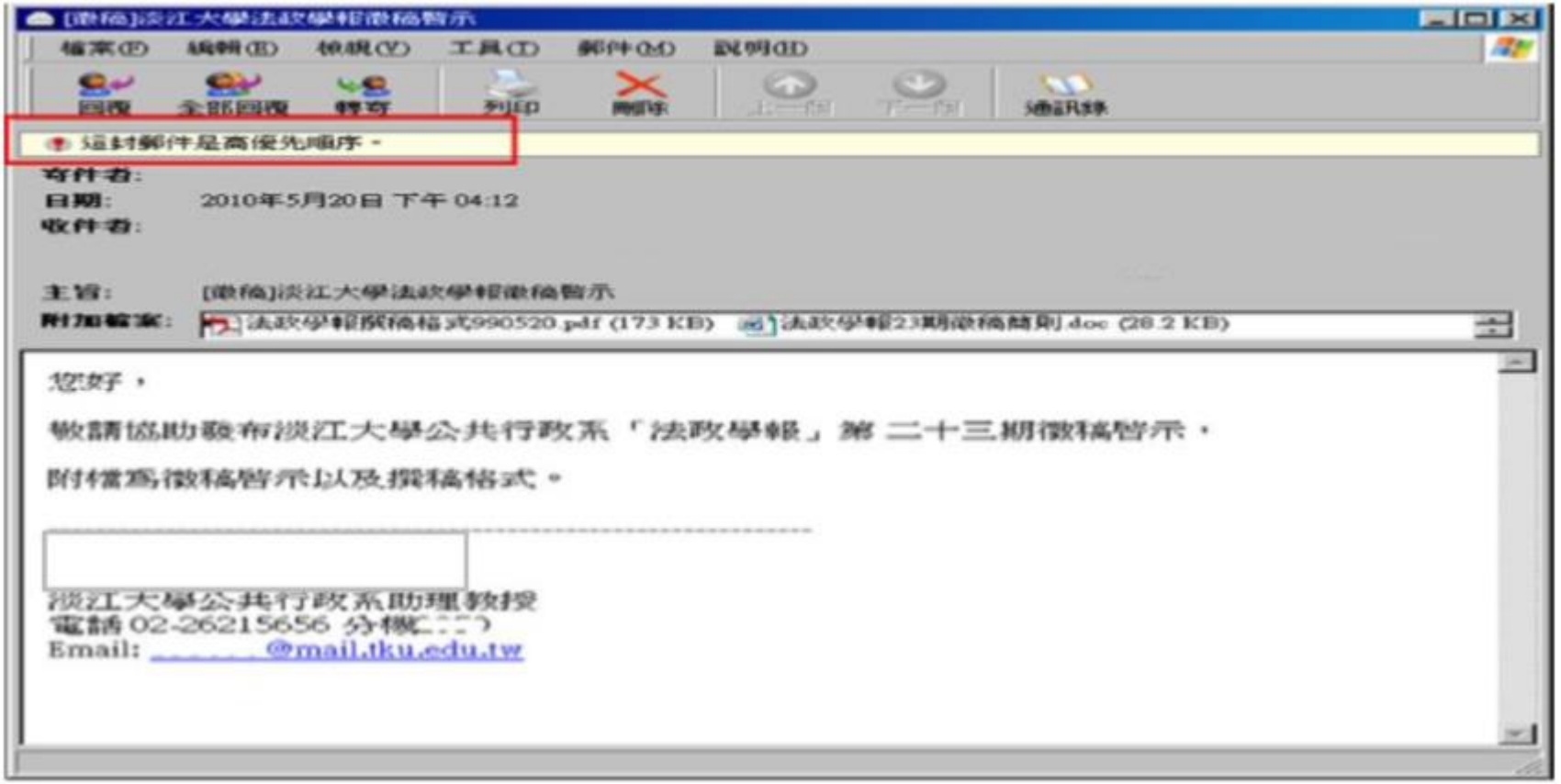
RTLO轉碼字元攻擊，利用檔案名稱編排呈現方式來誘騙使用者執行偽裝後的惡意檔案

社交工程電子郵件手法

- 混淆視聽之郵件寄件者
  - 偽裝身分(王小明、Emily)
  - 偽裝機關(AB銀行、XY商店)
  - 偽裝服務(OX論壇電子報、YAHA新聞)
- 附件夾帶病毒、蠕蟲、木馬程式及殭屍程式等惡意程式
- 郵件本文夾帶惡意連結

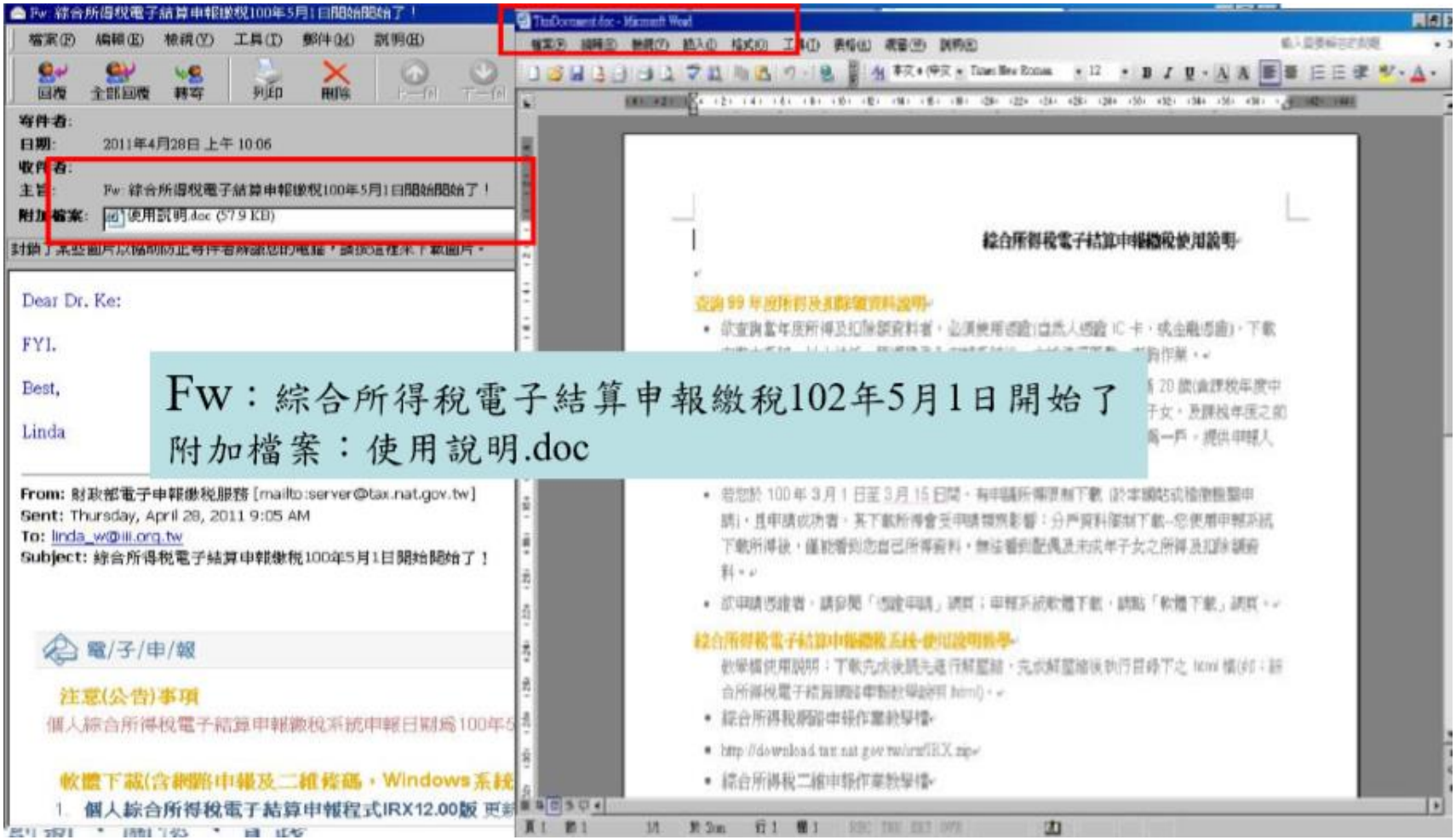
社交工程電子郵件手法案例

- 假冒寄件者並設定優先權-利用郵件高或重要優先權，吸引使用者開啟郵件



社交工程電子郵件手法案例

- 含有惡意程式的附件-偽裝報稅通知訊息

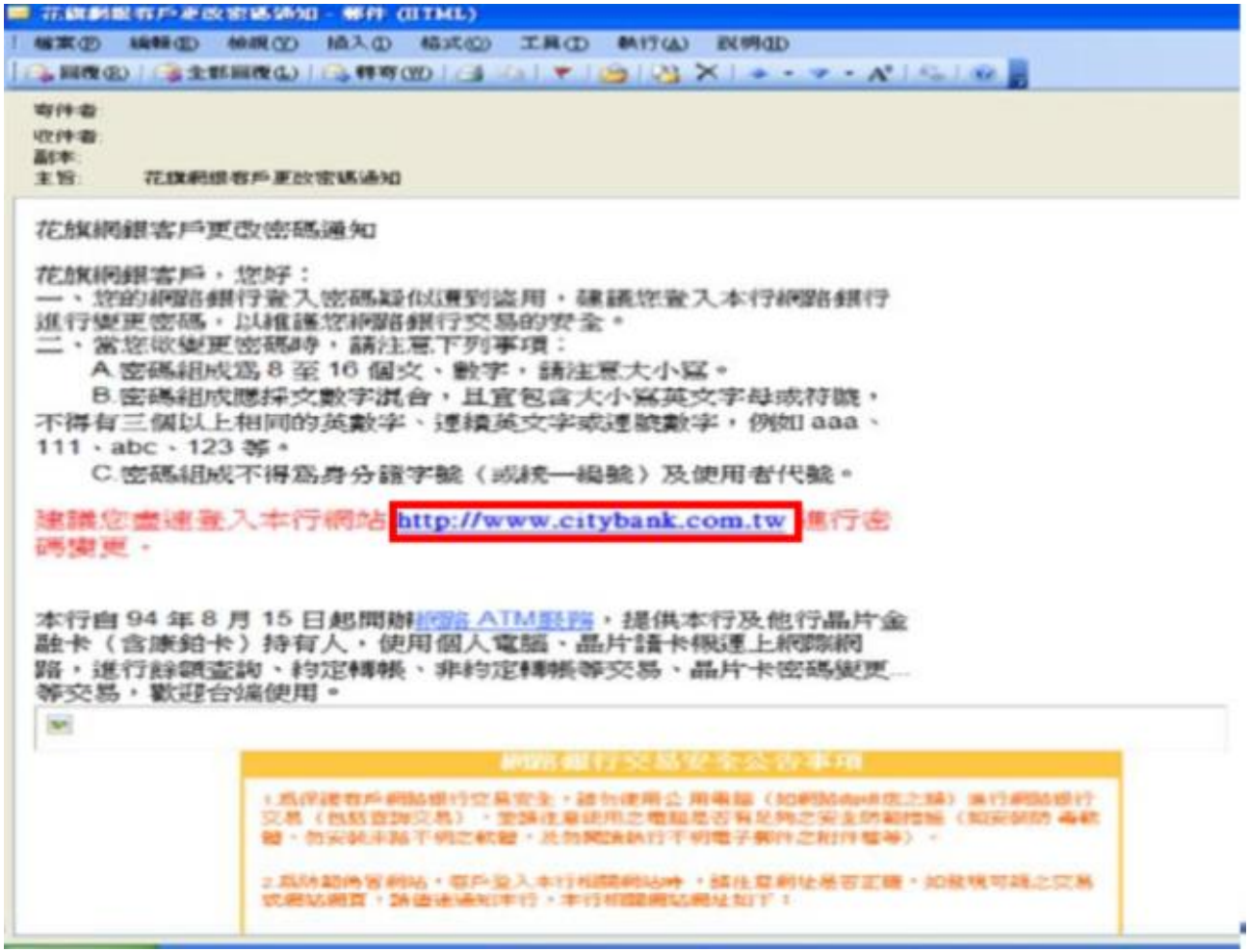


社交工程電子郵件手法案例

- 含有惡意程式的附件-利用圖示修改與副檔名隱藏方式，引誘使用者開啟

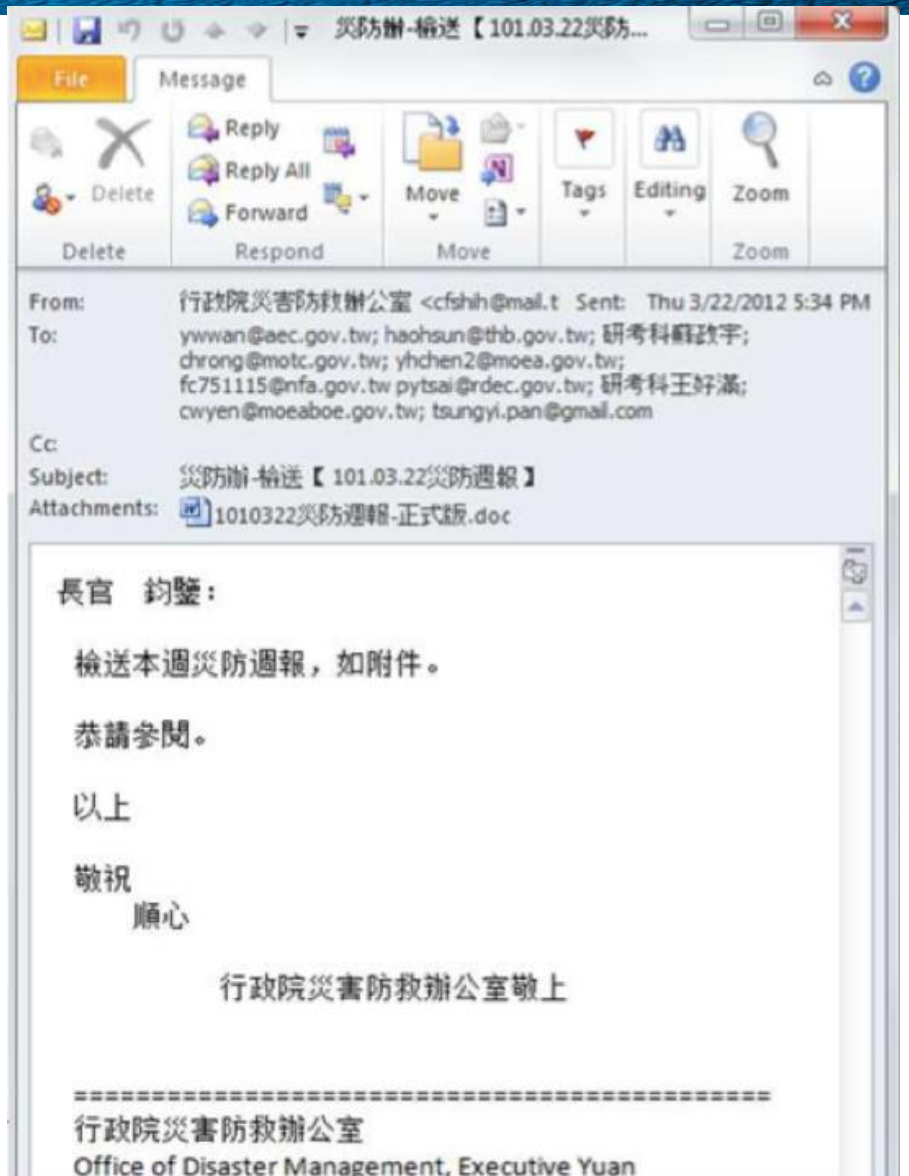
社交工程電子郵件手法案例

- 含有惡意連結(網路釣魚)



電子郵件攻擊的陷阱

- 夾帶惡意程式執行檔
- 內文中的惡意網頁超連結
- Html郵件隱藏遠端下載



電子郵件附件案例

是男人都會珍藏的女神月曆 - Mess...

File | Message

Reply | Reply All | Forward | Delete | Quick Steps | Move | Tags | Editing | Zoom

From: jun.lun <jun.lun@msa.hinet.net> Sent: Tue 3/20/2012 12:56 PM
To: iccoco@doh.gov.tw
Cc:
Subject: 是男人都會珍藏的女神月曆
Attachments: 是男人都會珍藏的女神月曆.doc (84 KB)

《壹週刊》宅男女神月曆

比較《壹週刊》、《FHM 男人幫》及《GQ》出的月曆，我認為《壹週刊》的宅男女神月曆，若不管模特兒的行情、知名度.....等其他因素，其照片拍攝整體水準較為一致，張張皆亮眼，這個設計團隊及攝影師是誰啊？

一月 林依晨

pric 06-Mar-2012 - Message (HTML)

File | Message

Reply | Reply All | Forward | Delete | Quick Steps | Move | Tags | Editing | Zoom

From: Sstarry.shoe <sstarry.shoe@gmail.com> Sent: Tue 3/6/2012 8:53 AM
To: SSTARRY
Cc:
Subject: pric 06-Mar-2012
Attachments: latest_price06-Mar-2012.zip (38 KB)

SSTARRY
SSTARRY@MAIL2000.COM.TW

latest_price06-Mar-2012.zip - WinRA...

File Commands Tools Favorites Options Help

Add | Extract To | Test | View | Delete | F

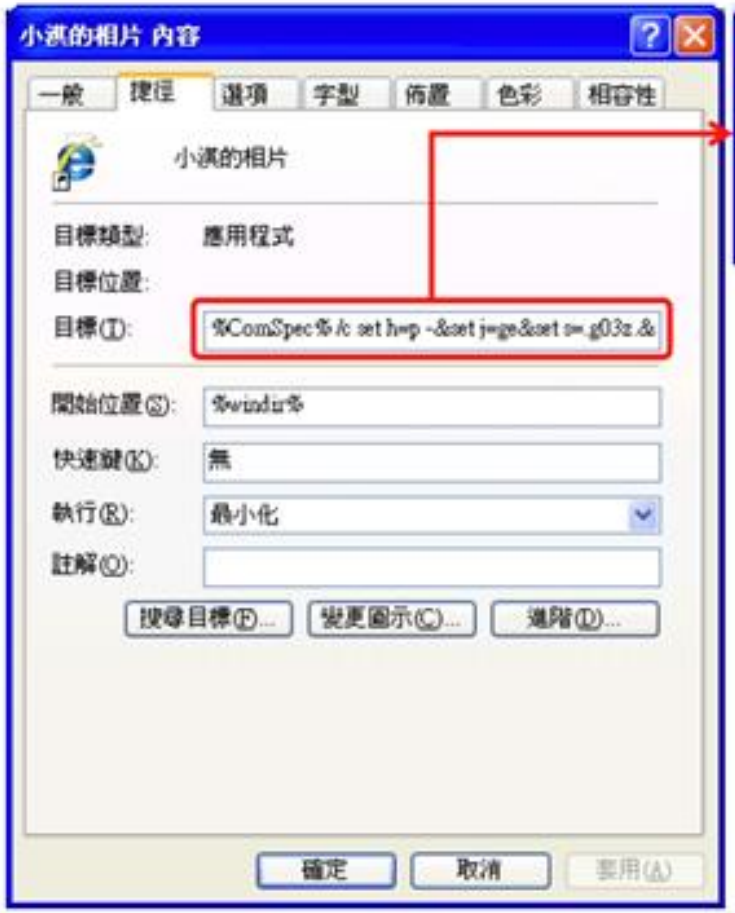
latest_price06-Mar-2012.zip - ZIP archive, un

Name

..

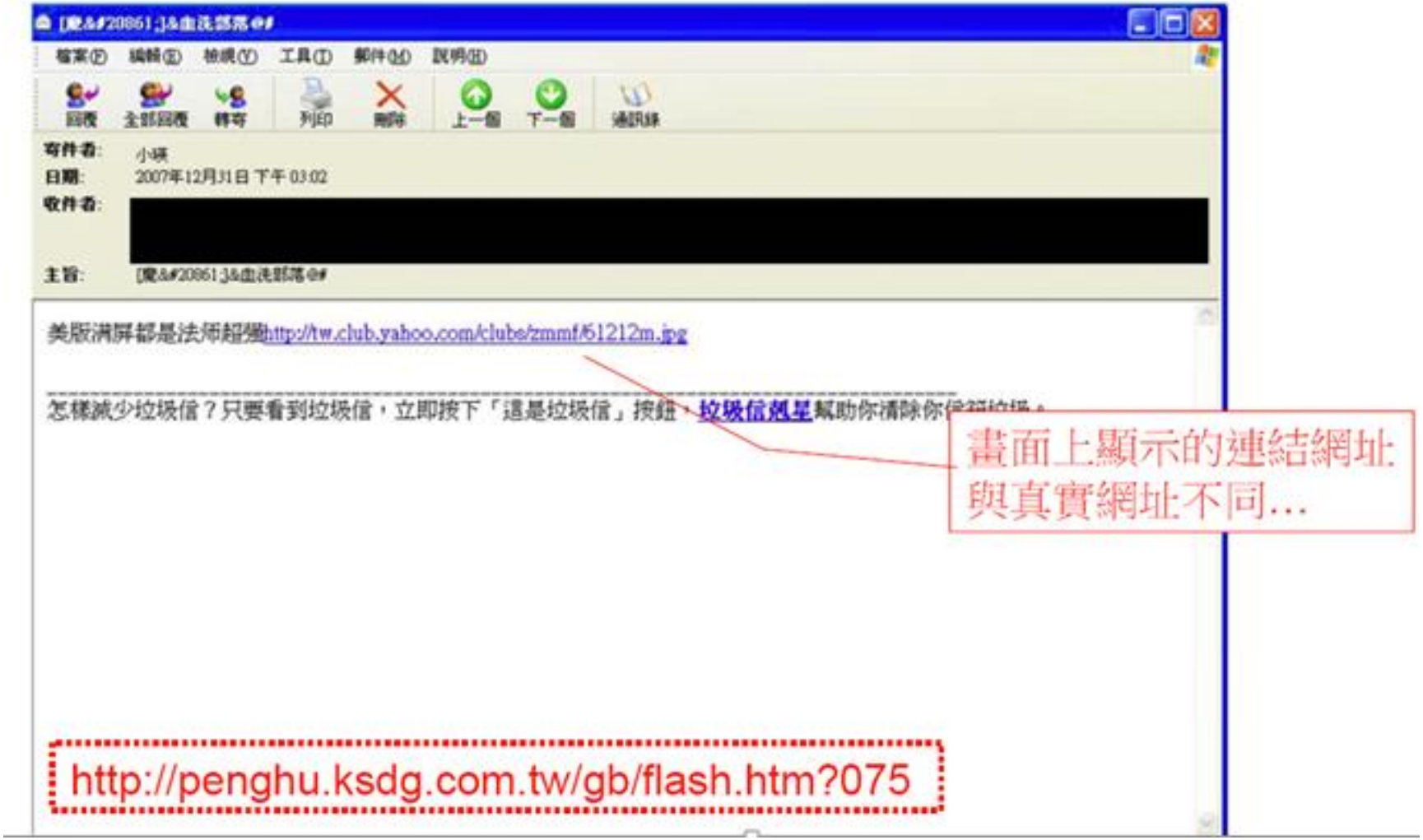
uuztaohzbkqg.exe

「捷徑」攻擊技倆解析

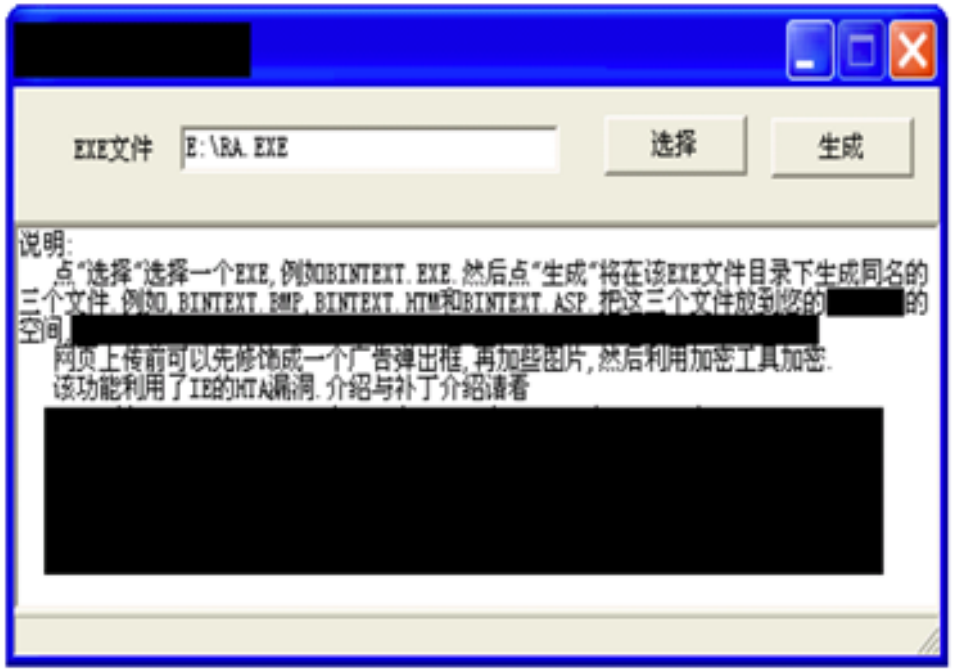


- 捷徑是一串DOS指令的集合
- 此例中，這串指令執行了
  - 連接一個伺服器
  - 下載惡意程式(木馬程式)
  - 執行它！

內文中的惡意網頁超連結



惡意網頁技倆解析



- 利用工具將惡意程式執行檔(.exe)轉檔為.bmp、.htm和.asp三個檔案，放上網頁
- 當您受騙連上這個鏈結網址(.htm)，即下載安裝了這個惡意程式！

電子郵件社交工程防範

面對電子郵件社交工程的態度

- 接收電子郵件時保持警覺心 –寄件人可能是假冒的
  - –內容可能是騙人的
  - –附件可能是惡意的
- 遵守停、看、聽三原則
  - –停：檢視電子郵件防護措施是否落實
  - –看：觀察判斷電子郵件是否有異常
  - –聽：聯絡確認電子郵件是否真

電子郵件社交工程防範

防範之道—停

- 使用電子郵件軟體前、先確認以下設定
  - 安裝防毒軟體，確實更新病毒碼
  - 取消郵件預覽功能
  - 關閉自動下載圖片及其他功能
  - 以純文字模式開啟郵件
  - 設定過濾垃圾郵件機

關閉信件預覽功能

- 關閉信件預覽功能，選取「檢視」「版面配置」
- 不勾選「顯示讀取窗格」

電子郵件社交工程防範

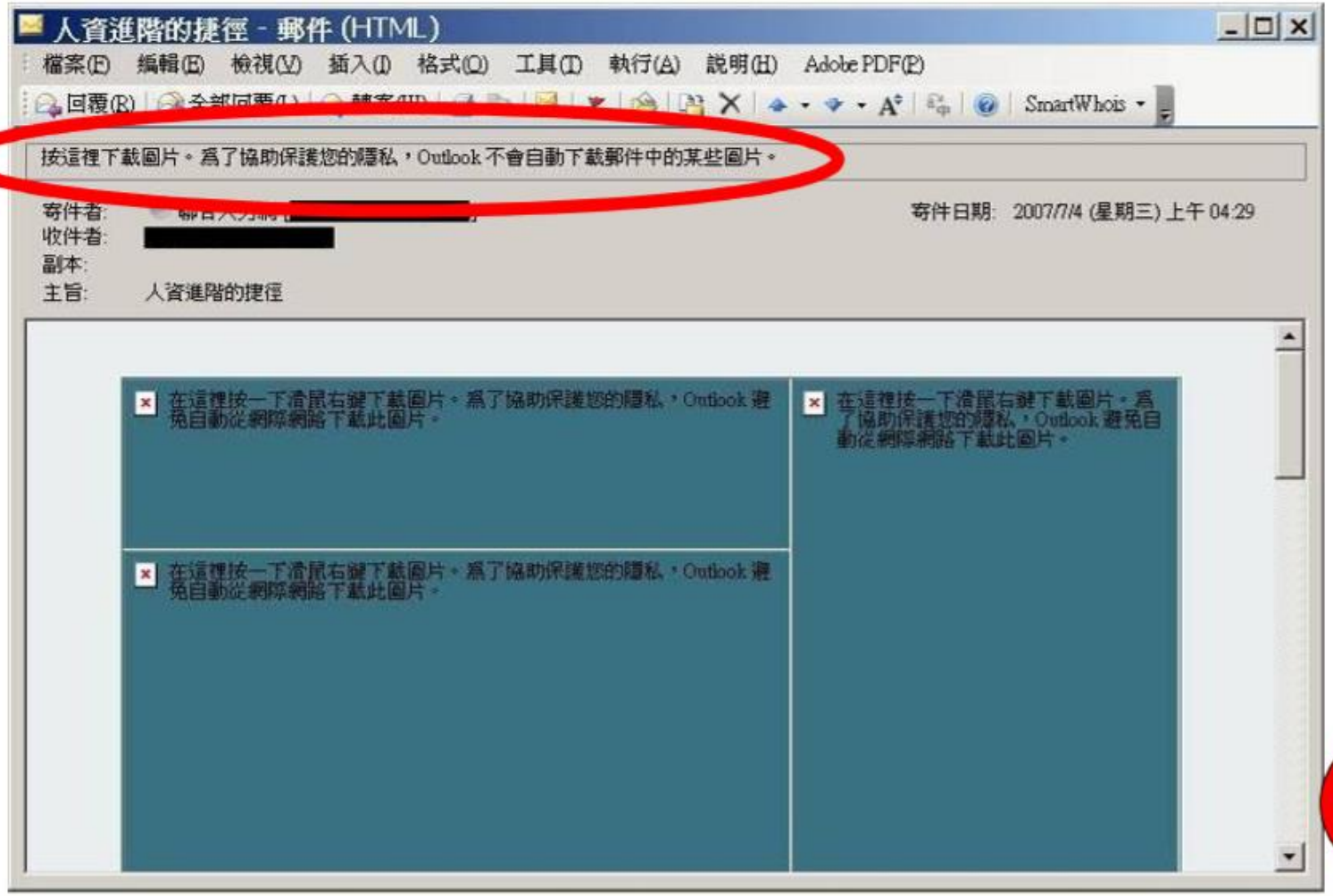
取消郵件預覽功能

電子郵件社交工程防範

關閉自動下載圖片及其他功能

電子郵件社交工程防範

關閉自動下載圖片及其他功能

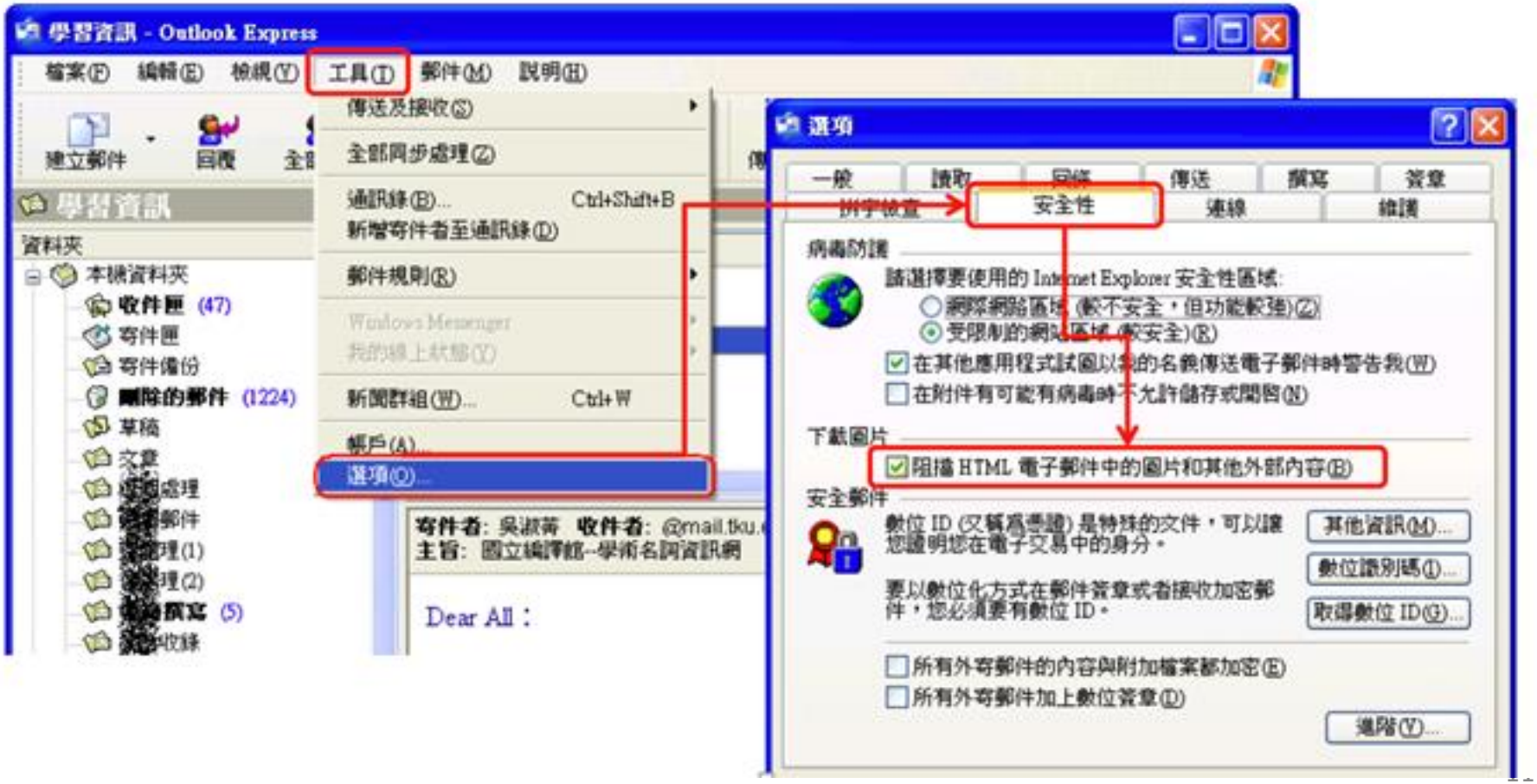


關閉自動下載圖片

Microsoft outlook

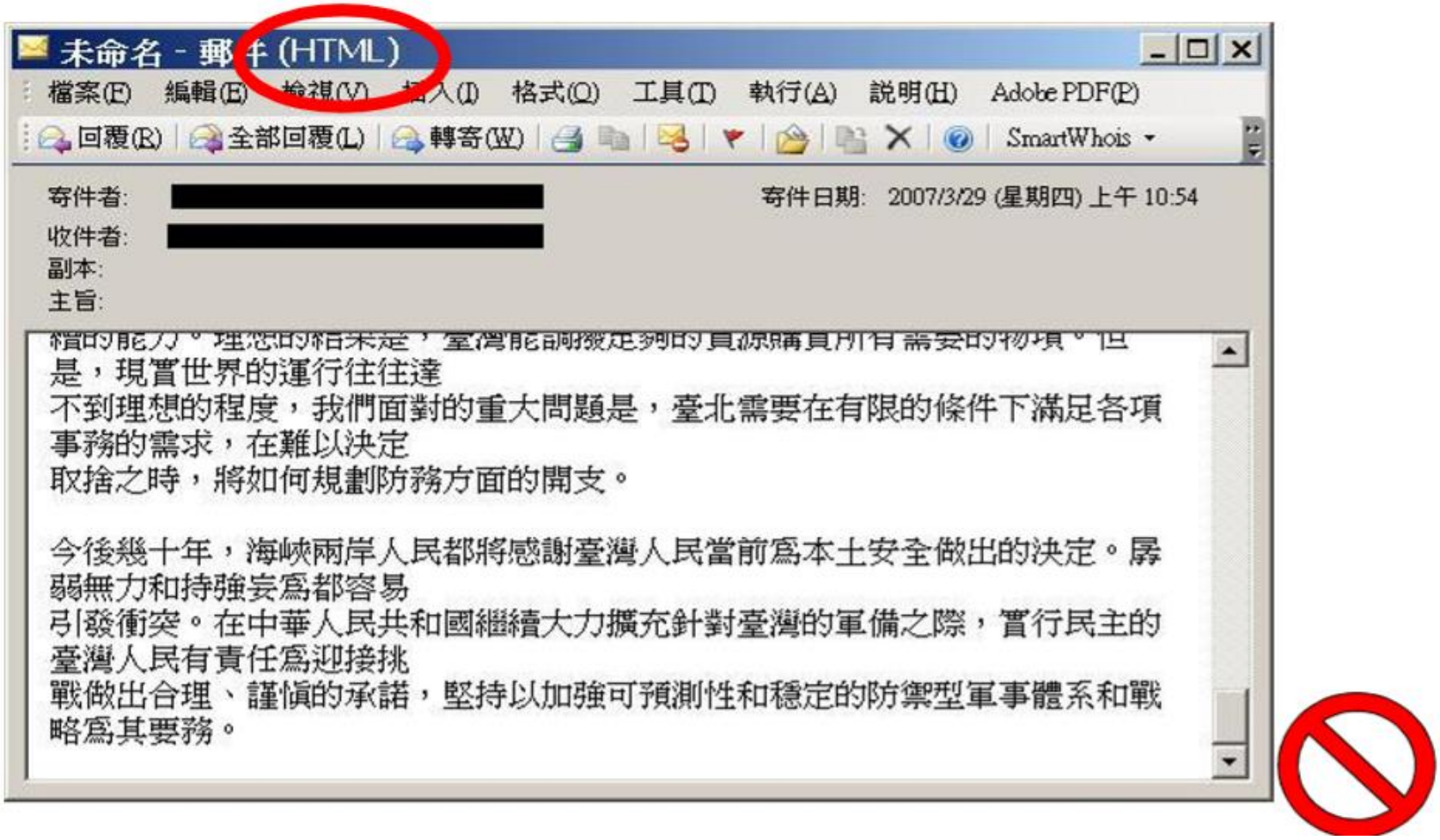
關閉自動下載圖片

Outlook express



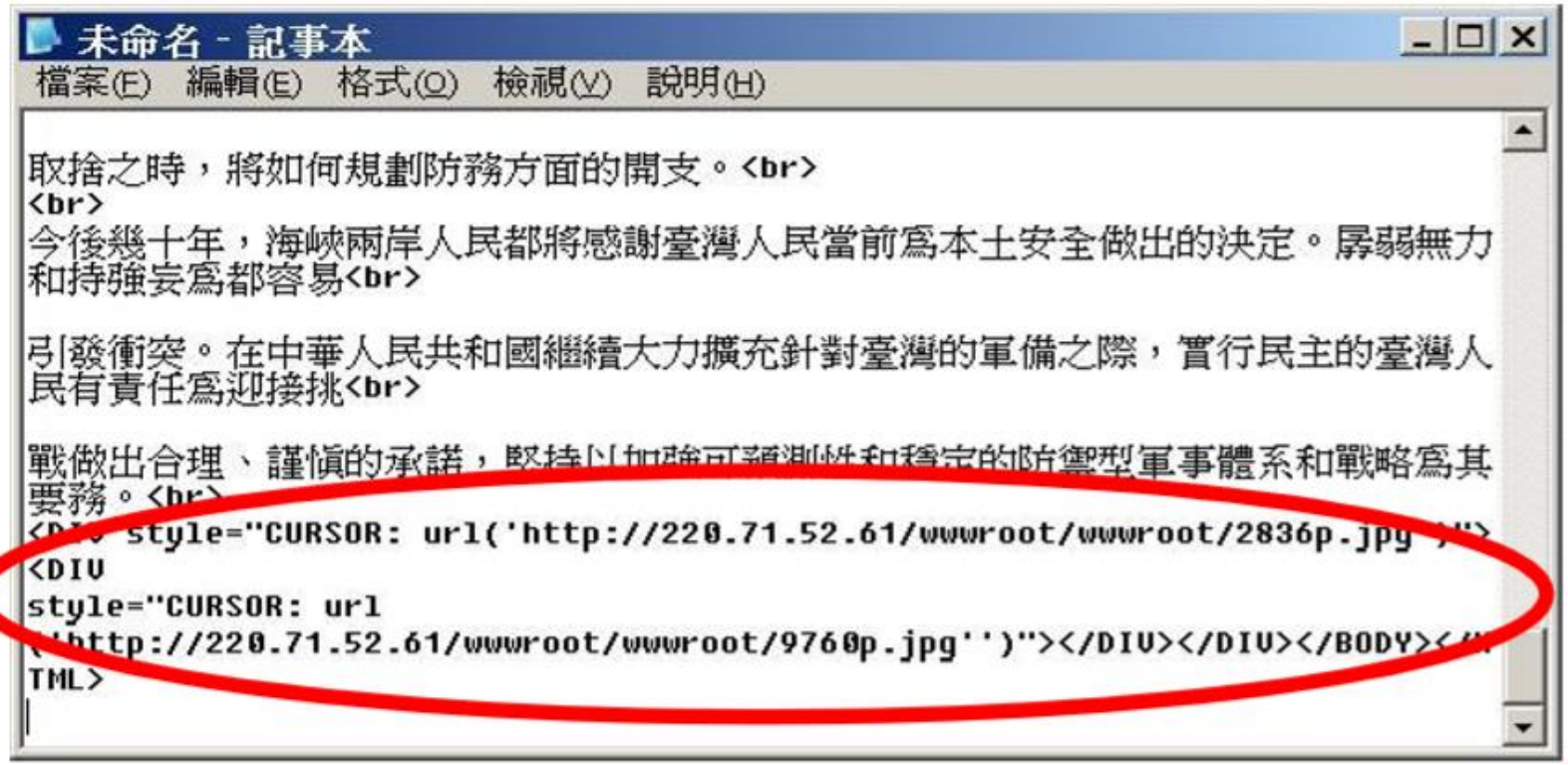
電子郵件社交工程防範

以純文字模式開啟郵件



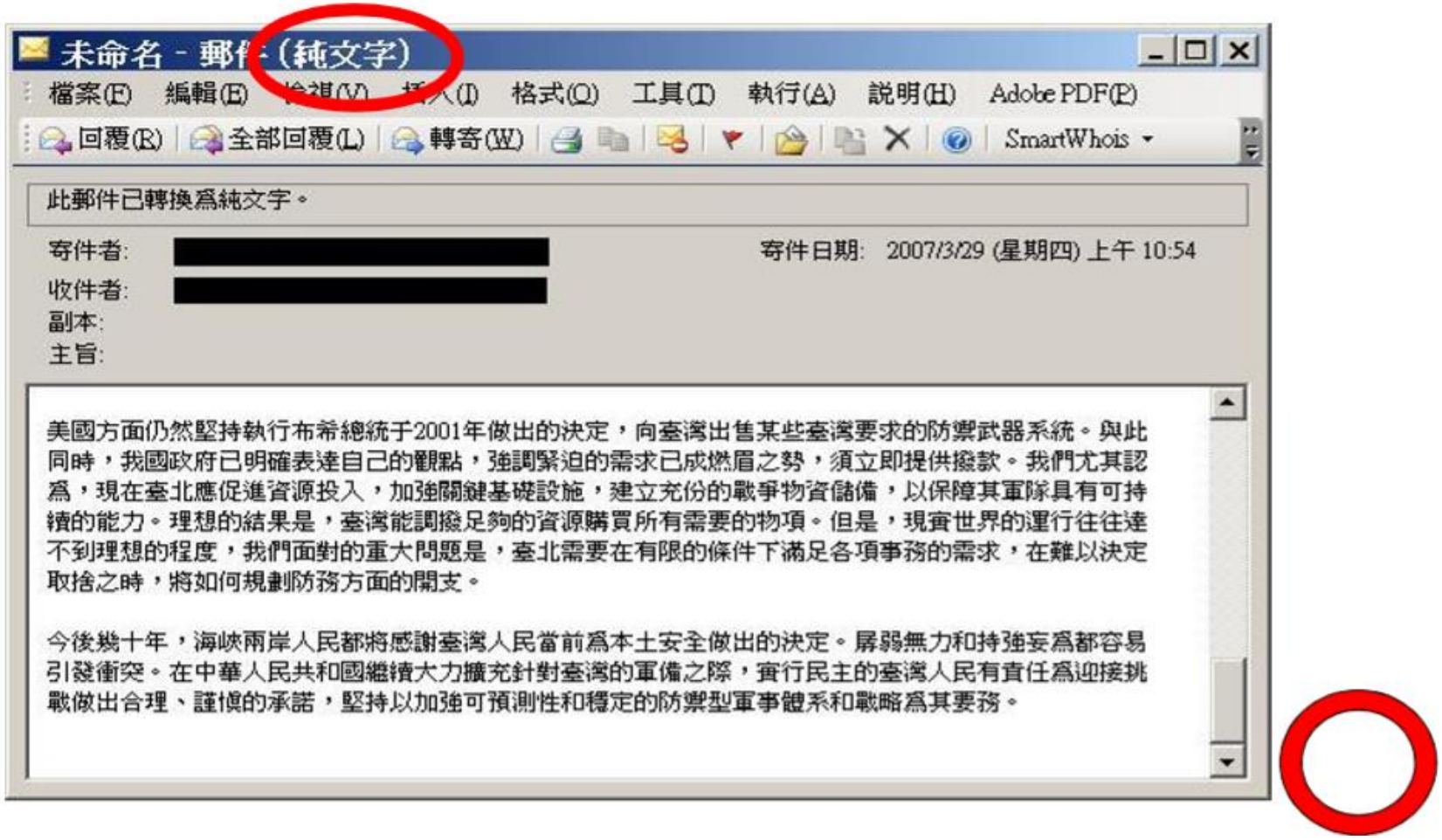
電子郵件社交工程防範

以純文字模式開啟郵件



電子郵件社交工程防範

以純文字模式開啟郵件



以純文字開啟信件

- 以純文字開啟信件
- 選取「工具」「選項」「讀取」
- 勾選「以純文字方式讀取所有郵件

•關閉自動下載圖檔

- 關閉自動下載圖檔
- 選取「工具」「安全性選項」「安全性」
- 勾選「阻擋HTML電子郵件中的影像和其他外部
  內容」

•自我保護措施

- 關閉預覽窗格。
- 非必要閱讀之郵件逕行刪除。
- 設定為純文字讀取模式再開啟郵件閱讀。
- 開啟郵件內含之超連結時先確認連線網址之網域名稱(DomainName)是否足以識別？
- 若為數字IP之網址勿輕易開啟。不隨意輸入資料送出，傳送私密資料時確認是否有啟動加密機制。
- 分辨電子郵件的真偽。

•收取電子郵件應有的正確習慣

- 檢查寄件者的真偽
- 確認信件內容的真實度
- 不輕易開啟郵件中的超連結以及附件
- 開啟超連結或檔案前，確認對應軟體都保持在最新的修補狀態
- 提高警覺，加強危機意識

電子郵件社交工程防範

防範之道—看

- 收到郵件後務必留意
  - 查看郵件來源是否正常(寄件者、寄件來源帳號)
  - 審慎注意郵件中網址的正確性，避免直接點選
  - 標題或內容是否與本身業務相關
  - 無關公務之郵件避免開啟與點

電子郵件社交工程防範

防範之道—聽

- 若懷疑郵件來源務必進行確認
  - 透過電話向對方確認信件真偽
  - 檢視郵件內容之<FROM>資訊

電子郵件社交工程防範

使用者認知教育與管理稽核之落實為資訊安全之基石

停	安裝防毒軟體，並確實更新病毒碼 關閉郵件自動下載圖片及其他功能 純文字模式開啟信件，及取消預覽功能 設定垃圾郵件過濾機制
看	查看郵件來源是否正常 審慎注意郵件中網址的正確性，避免直接點選 標題或內容是否與本身業務相關 無關公務之郵件避免開啟與點閱
聽	透過電話向對方確認郵件真偽

課程大綱

- 密碼安全
- 軟體使用安全
- 病毒與木馬防護安全
- 電腦操作安全與資料備份
- USB管理
- 公用存取
- 電子郵件安全
- 社交工程
- 網路釣魚與網路詐騙
- 日益猖獗的勒索病毒

社交工程的定義

- 社交工程是利用人性的弱點及無知，透過欺騙、威脅的話術來影響或說服他人，以獲得有用資訊的一種技巧
- 常見的社交工程手法-利用電話、手機簡訊、即時通訊等管道， 設計詐騙劇本，假冒身份，電話電子郵件（政治，笑話，養生資訊）網路釣魚，（養眼）圖片，偽裝程式，MSN，讓被害人主動的告知個人機密資訊或 交付財物
- 對特定目標而言，社交工程手法最具滲透力!!

多元化社交工程手法

- 駭客可利用多元複雜的手法進行攻擊，如電子郵件、 即時通訊軟體、社交網站、手機應用程式
- 甚至包含具有連網裝置
- 共同目的為引誘受害者連線至惡意網站、惡意連結及 執行惡意程式
- 可能導致受害者電腦遭駭客控制或執行惡意指令

安全措施最弱的一環-->人性

- 一家公司即使投資了許多資安科技設備，並訓練員工保存機密資料，雇用良好的保全系統，依然可能不堪一擊。
- 人性的因素是安全措施中最弱的一環
- 社交工程即是利用人類容易受騙上當的弱點，破解人性的防火牆，投資金額通常只有電話的費用

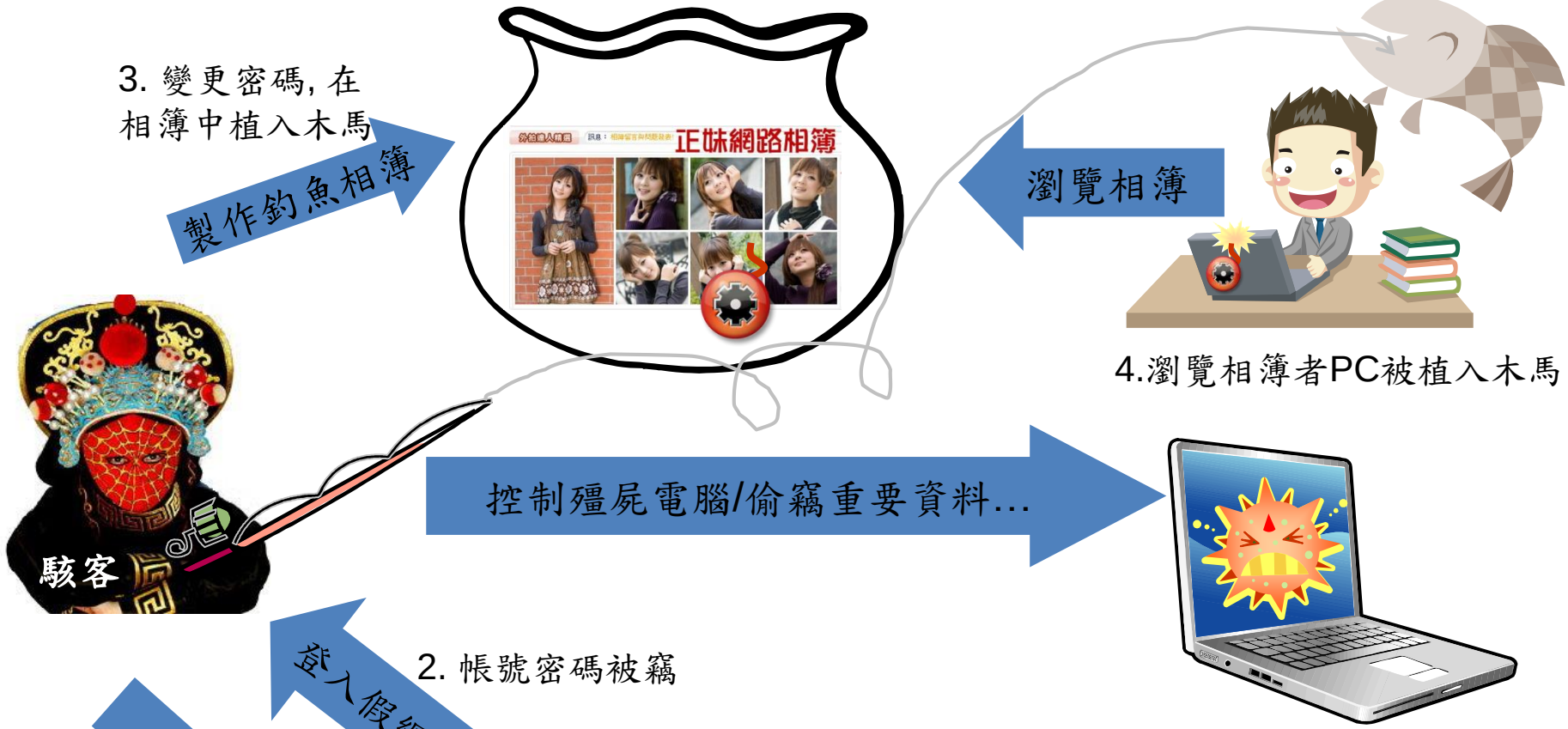
多元化社交工程手法

- 駭客可利用多元複雜的手法進行攻擊，如電子郵件、 即時通訊軟體、社交網站、手機應用程式
- 甚至包含具有連網裝置
- 共同目的為引誘受害者連線至惡意網站、惡意連結及 執行惡意程式
- 可能導致受害者電腦遭駭客控制或執行惡意指令

社交工程攻擊手法

- 電話詐騙(含手簡訊)
- 電子郵件隱藏電腦病毒
- 網路釣魚
- 圖片中的惡意程式
- 偽裝修補程式
- 即時通也是社交工程新途徑

社交工程攻擊手法


3. 變更密碼, 在相簿中植入木馬
製作釣魚相簿
正妹網路相簿
瀏覽相簿
4.瀏覽相簿者PC被植入木馬
駭客
控制殭屍電腦/偷竊重要資料...
登入假網頁
2. 帳號密碼被竊
1. 偽造網路相簿寄維護通知信

社交工程攻擊手法

社交工程-社群網站媒介

利用瀏覽者的好奇心

社交工程攻擊手法

社交工程
-社群網站媒介

臉書病毒又來了！偽裝成瀏覽器擴充元件 駭進帳戶自行更新

cnYES 鉅亨網 作者：鉅亨網鄭杰 綜合報導 | 鉅亨網 – 2013年5月13日 下午3:20

字 +字

微軟報告指出，新木馬病毒的目標是臉書用戶！

新病毒威脅來了！微軟 (MSFT-US) 警告，現有一新惡意軟體偽裝成 Google 瀏覽器 Chrome 和 Firefox 的擴充元件，目標駭進 Facebook (FB-US) 帳戶。

《CNET》報導，微軟報告指出，這個電腦病毒在巴西首度被發現，名稱為「木馬：JS/Febipos.A」，這個病毒會自己更新，就像是一般合法的瀏覽器擴充元件一樣。

一旦下載後，這個木馬病毒會監控受感染電腦是否登入 Facebook，且會試著下載一連串瀏覽器元件指令的配置文件，如此一來這個惡意軟體就可以執行各式各樣的 Facebook 指令，包括按「讚」、分享、發表文章、加入社團、和其他聯絡人聊天等等。

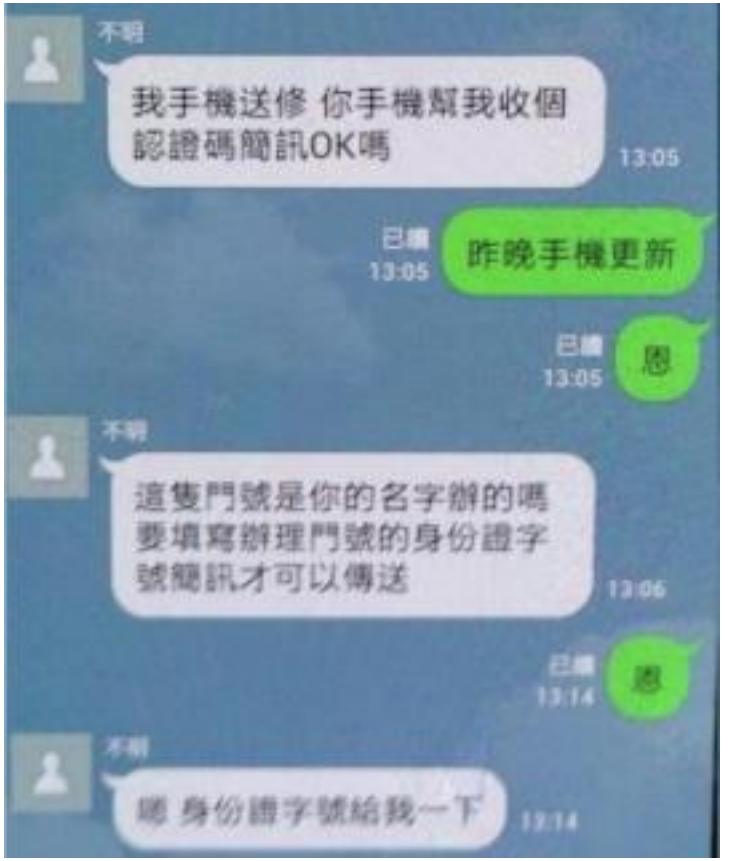
部份變種病毒甚至可以以葡萄牙文發表挑釁發言，且附上其他 Facebook 臉書頁面連結，這些貼文的按讚數和分享次數還在增加當中，顯示病毒感染逐漸蔓延。

不過微軟並沒有明確指出這些惡意軟體是如何自行安裝，也沒有表示多少電腦可能已經受到感染。

社交工程攻擊手法

MSN/LINE詐騙

- 利用信任關係
- 手機門號小額付款
- 假貼圖真釣魚



社交工程攻擊手法

簡訊詐騙

- 短網址
- 簡訊驗證碼

智慧型手機安全嗎？

- 手機已成為駭客攻擊主要目標之一
- 手機惡意應用程式近年大量遽增
- 因為手機與生活網路服務密不可分，結合許多應用服 務，導致手機上儲存機敏資料與執行經濟上的交易 – 例如，個人資料、信用卡號、GPS、網路銀行帳密等
- 許多手機大廠相繼遭揭露存在弱點

其他-社交工程事件回顧

- 美國公平交易委員會指控A大廠美國分公司
  - 未採用安全作法開發行動裝置軟體
  - 未提供工程師軟體安全開發訓練
  - 未檢測安裝於行動裝置上軟體之潛在安全弱點
  - 未遵循眾所皆知及被普遍接受之安全開發流程與實作
  - 未建立供第三方弱點回報與處理之流程機制
  - 未提供移除預先安裝應用程式或元件之功能

其他-社交工程事件回顧

- Loggers(Since 2010, 供客戶支援及問題排除)
  – 收集包含GPS紀錄、使用者號碼、通訊錄、通聯記錄、網頁 及影音觀看紀錄、IMEI、MEID、註冊帳號...等敏感資訊 – 影響：敏感資訊洩漏
- CarrierIQ (Since 2009, 供分析網路及設備問題)
  – 收集包含GPS紀錄、網頁及影音觀看紀錄、文字訊息內容、 應用程式名稱、使用者輸入之keys、行動裝置資訊...等敏感 資訊 – 影響：敏感資訊洩漏、電信服務盜用 (金錢損失)

其他-社交工程事件回顧

假冒銀行通知郵件

引誘使用者到假冒網站
上輸入帳號及密碼

花旗銀行-http://www.citybank.com.tw

駭客

駭客利用使用者
密碼登入真實網站

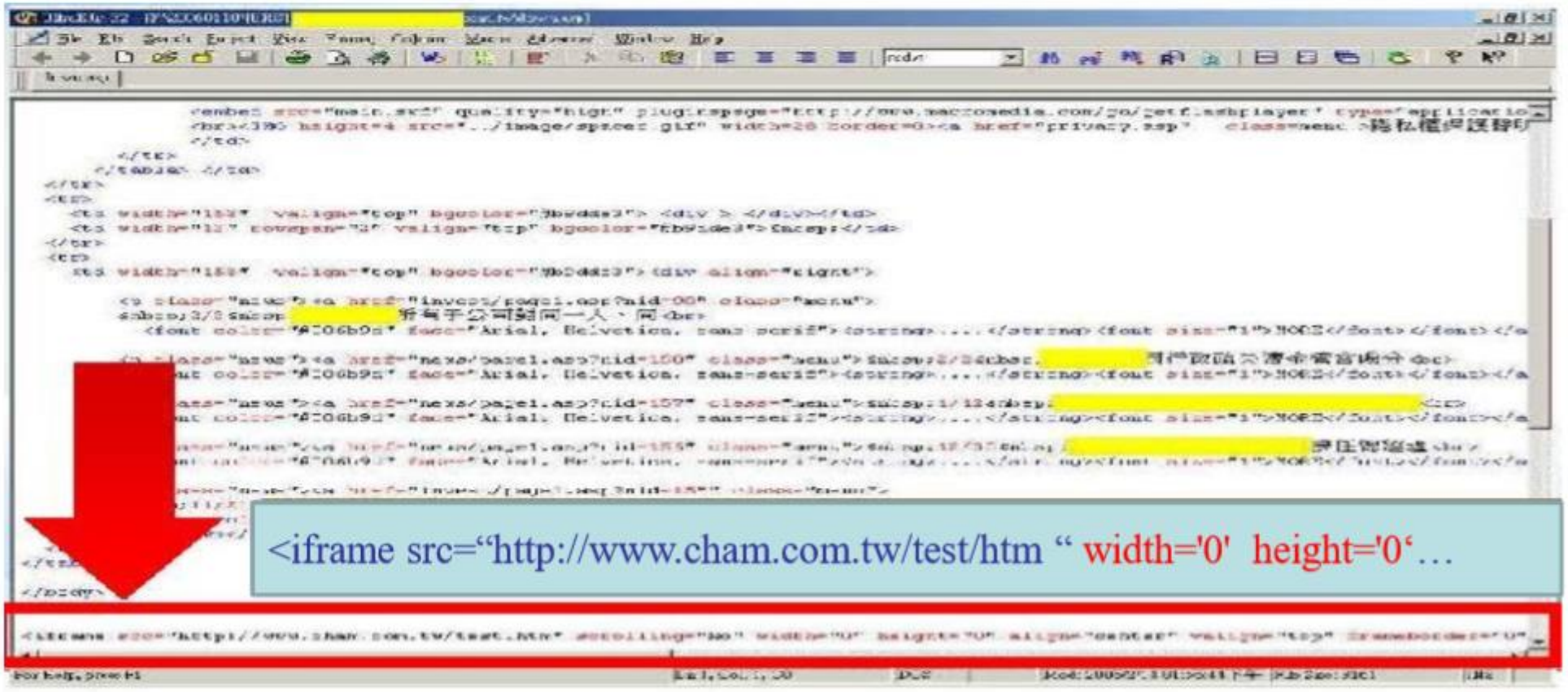
社交工程網頁掛碼

- 網站系統有漏洞未修補，即容易被置入iframe 程式碼 ，受駭成為惡意網站
- 網頁掛碼呈現方式
  - 不破壞原始網頁外觀
  - 嵌入隱藏的網站頁面
  - 嵌入的網頁隱含惡意程式

- 只要防毒軟體沒有偵測到，使用者可能永遠都不知道 被植入惡意程

社交工程網頁掛碼攻擊方式說明

- 嵌入隱藏的網站頁面
  - 參數使用width='0' 或 height='0'



遭受社交工程攻擊之後果

- 電腦被植入惡意程式後門程式
- 行為舉動遭到監視
- 個人資訊與機密檔案被竊取
- 如同監聽般的鍵盤側錄
- 使用者電腦遭感染成為殭屍電腦
  - 當成網路攻擊行動的跳板
  - 被操控並且發動惡意攻

社交工程

威脅的型態與種類或許層出不窮，但弱點發生的根本原因才更值得探究

社交工程手法

- 偽冒身份之電子郵件誘使使用者開啟惡意電子郵件之案例層出不窮
- 通信軟體-LINE, Facebook, Wechart, …
- 假冒網路業者官網.
- 結合社交工程與零時差弱點的精準攻擊，更增加入侵防護之困難度

社交工程

威脅的型態與種類或許層出不窮，但弱點發生的根本原因才更值得探究

- 定期修補軟體漏洞，防範已知軟體弱點所造成的攻擊
- 使用者認知教育與管理稽核之落實仍為根本解決之道
- 目前研考會正在政府機關推動職務憑證與資安防護認知訓練，以降低社交工程電子郵件攻擊之風險

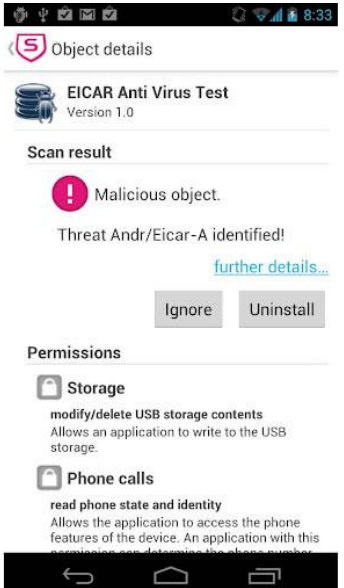
社交工程防範

盡量在APP Store安裝軟體

社交工程防範

盡量少安裝破解的APP

如果還是需要安裝非官方來源的APP，建議安裝第三方的防毒軟體來確保APP的安全性



課程大綱

- 密碼安全
- 軟體使用安全
- 病毒與木馬防護安全
- 電腦操作安全與資料備份
- USB管理
- 公用存取
- 電子郵件安全
- 社交工程
- 網路釣魚與網路詐騙
- 日益猖獗的勒索病毒

網路釣魚

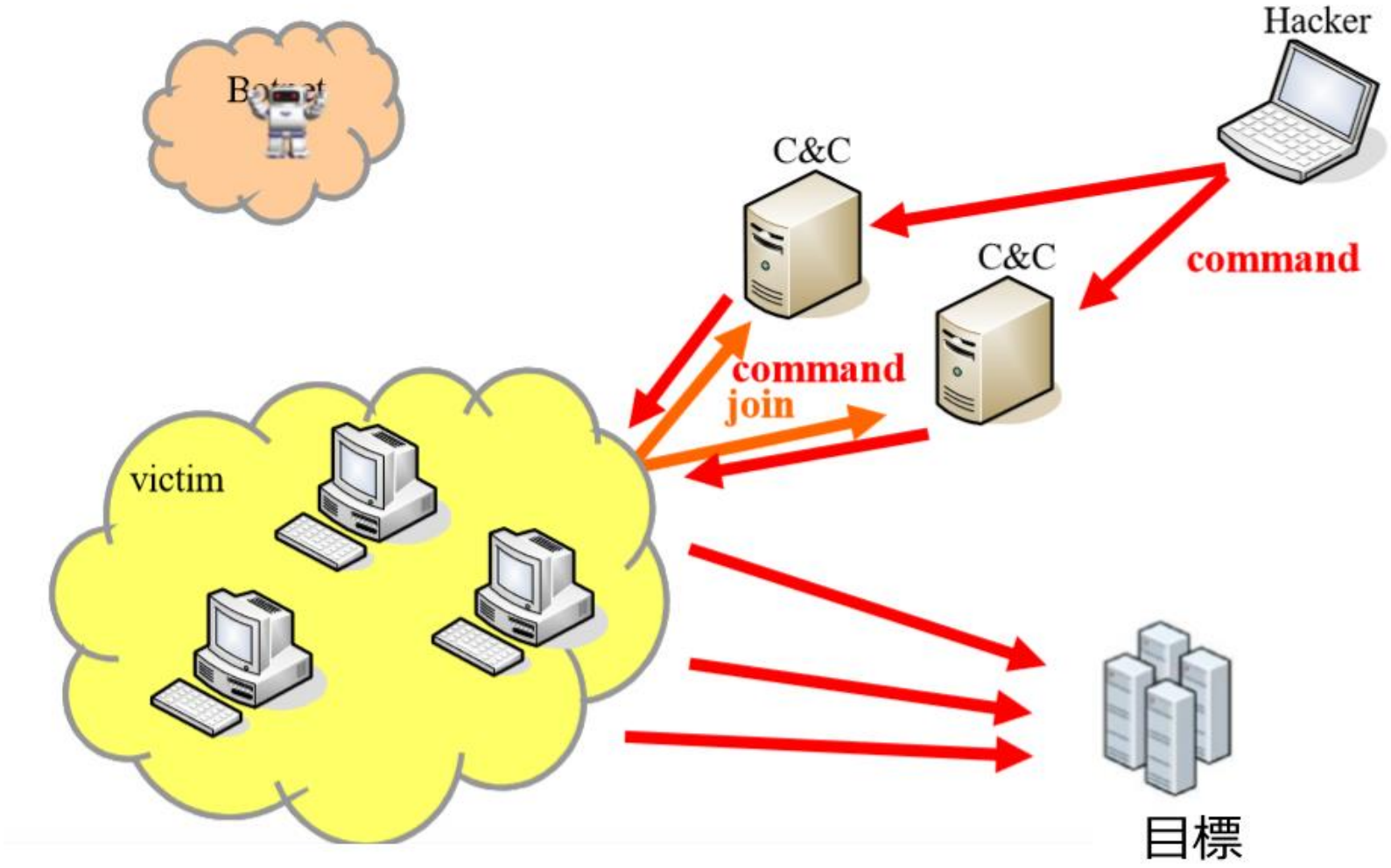
http://www.paypal.com

http://www.paypal.com

殭屍網路(Botnet)

- 殭屍電腦(Bot)
  – 被植入惡意程式的電腦，自動前往C&C報到
- C&C (Command & Control)
  – 駭客挑選開機時間長，網路環境穩定的電腦，作為下達命令 的中途媒介
- 當一群Bot成功前往C&C報到，並且依照C&C上的指 令運作時，即構成殭屍網路(Botnet)

殭屍網路運作方式示意



殭屍網路攻擊方式說明

- 一旦Bot程式植入到受害主機，駭客即可遠端控制受害 電腦，做為攻擊跳板
  - DDoS攻擊
  - 濫發垃圾郵件
  - 蒐集個人隱私資料
  - 散布惡意程式

偽「我的拍賣賣場」陷阱…


Microsoft Internet Explorer
用途 一般住宅
行政區域 板橋
使用坪數 10坪以下
房型 套房
屋齡 新成屋
格局 一房
近捷運 無
近學校 無
近公園 無
近百貨公司 無
電梯 無
電視 無
陽台 無
附家具 無
洗衣機 無
冰箱 無
冷氣空調 無
車位 無
請用滑鼠點擊下邊(前往我的拍賣賣場)
YAHOO! 奇摩 拍賣 前往 我的拍賣賣場
點擊這黃色長長的圖標就可以直接到我另一個賣場~還有很多一元起標商品全面結束營業大出清喔~保證買到賺到~
Yahoo! Taiwan Inc. All Rights Reserved.

進入偽Yahoo釣魚網站

進入偽華航的釣魚網站

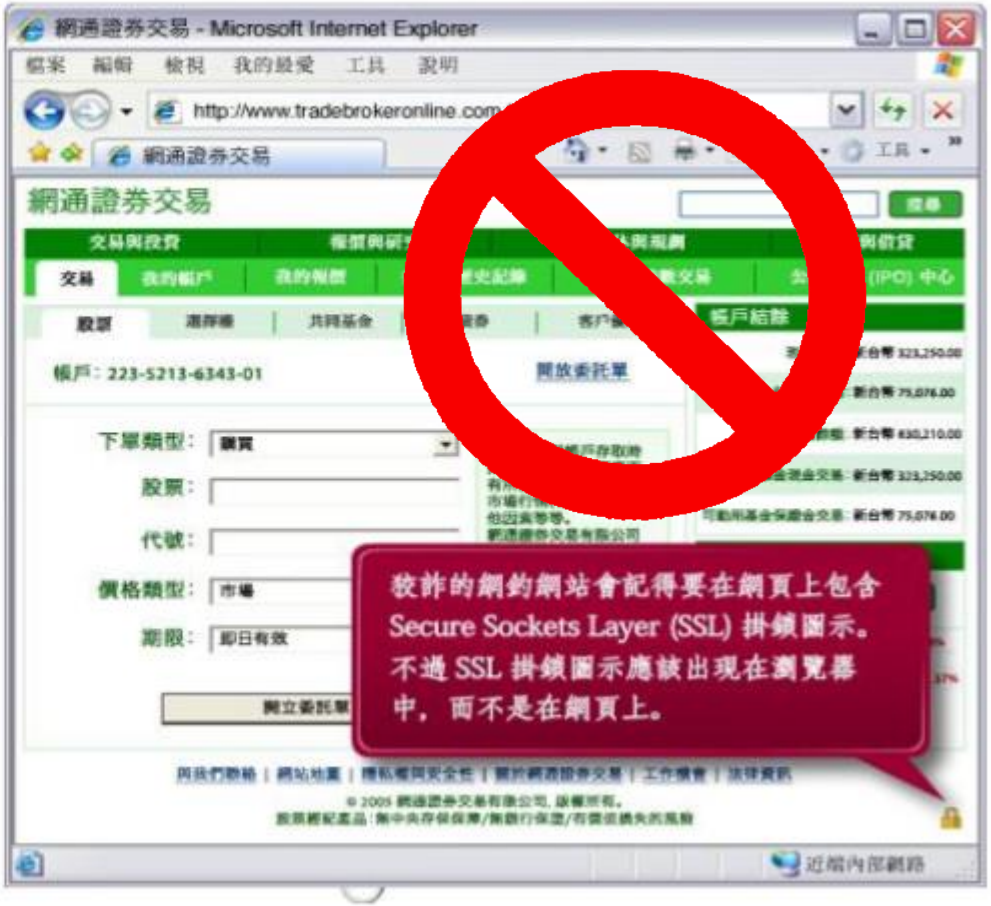

CHINA AIRLINES
華夏 會員專區
班機離到動態 »
// 透過航班時間表，旅程安


中華航空公司 China Airlines - Windows Internet Explorer
CHINA AIRLINES
華夏 會員專區
班機離到動態 »
// 透過航班時間表，旅程安

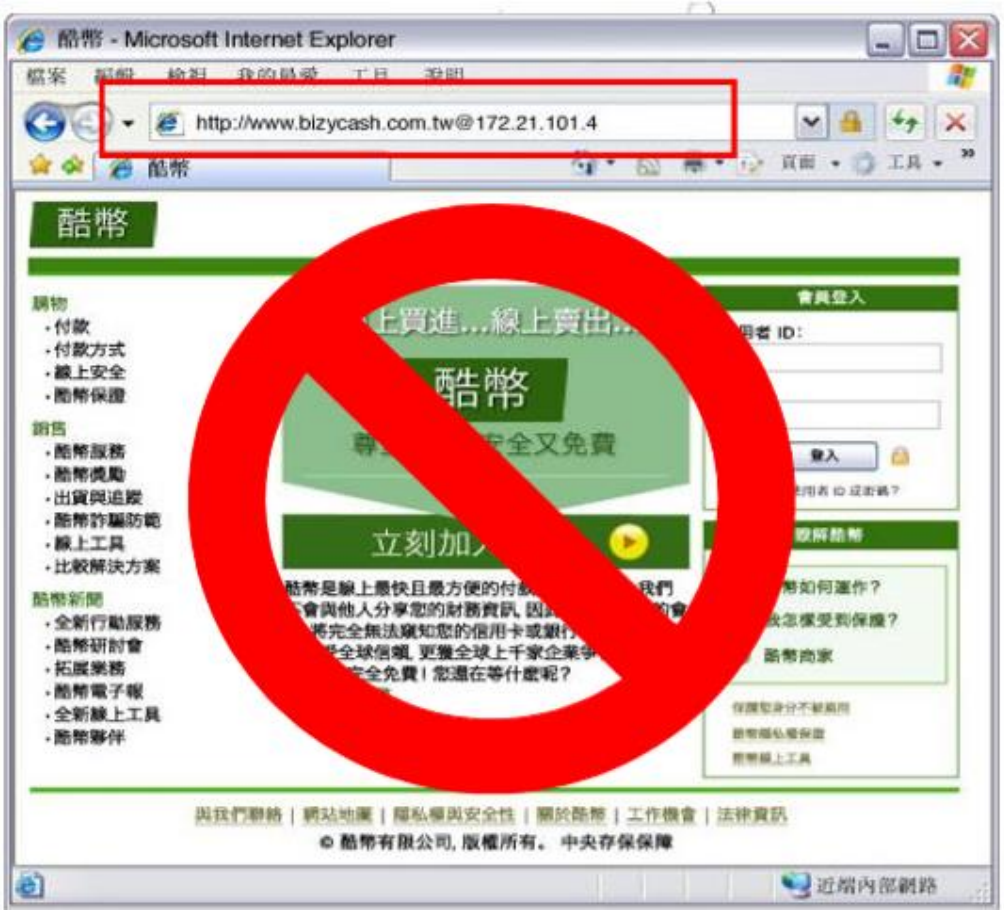

公司 China Airlines - Windows Internet Explorer
http://www.china-airlines.com/ch/schedule/s_check.htm
華航空公司 China Airlines


空公司 China Airlines - Windows Internet Ex
http://www.china-airlines.com/ch/schedule/s_check.htm
中華航空公司 China Airlines

進入偽網通證券交易的釣魚網站



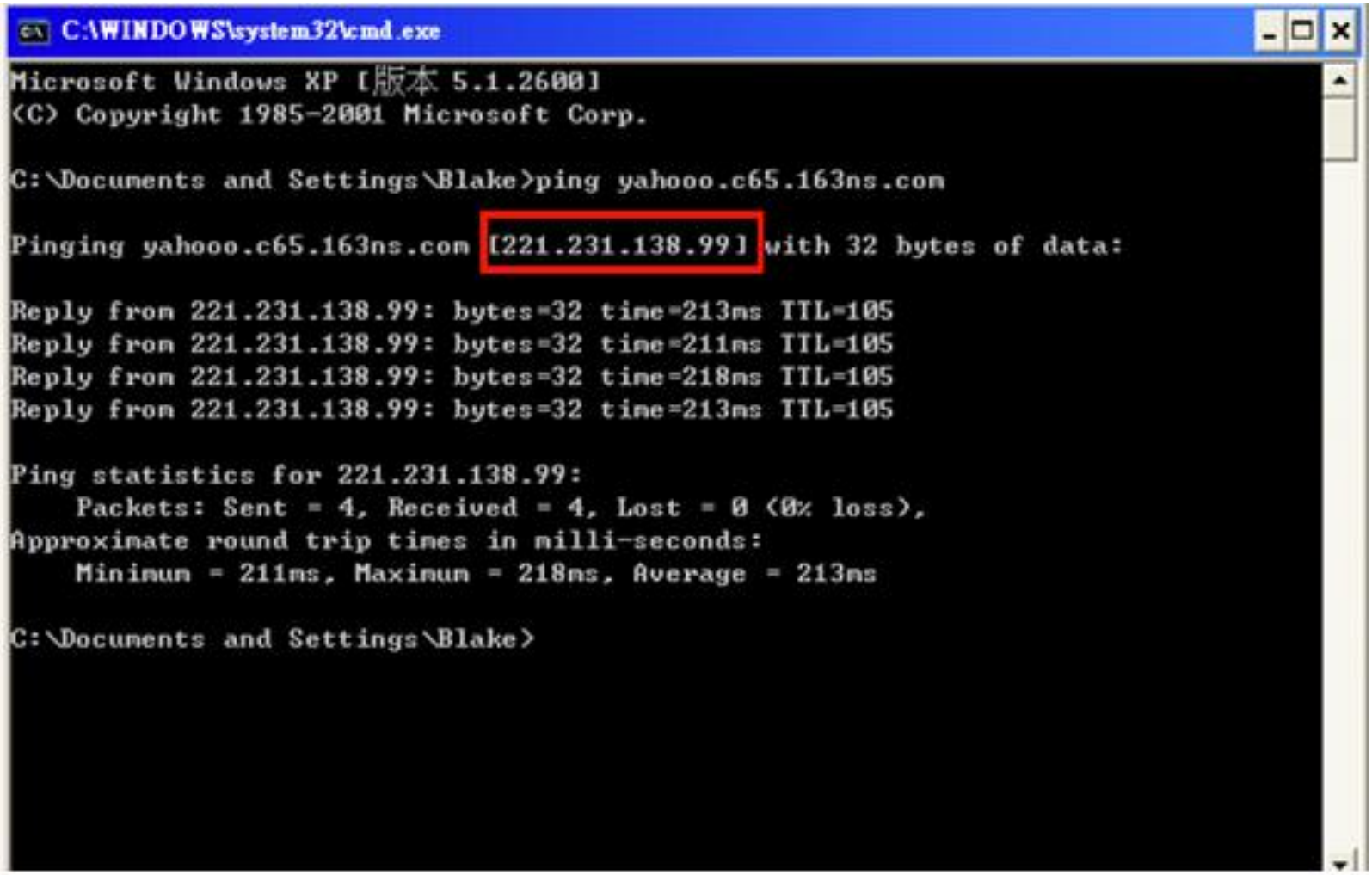
進入偽虛擬貨幣網的釣魚網站



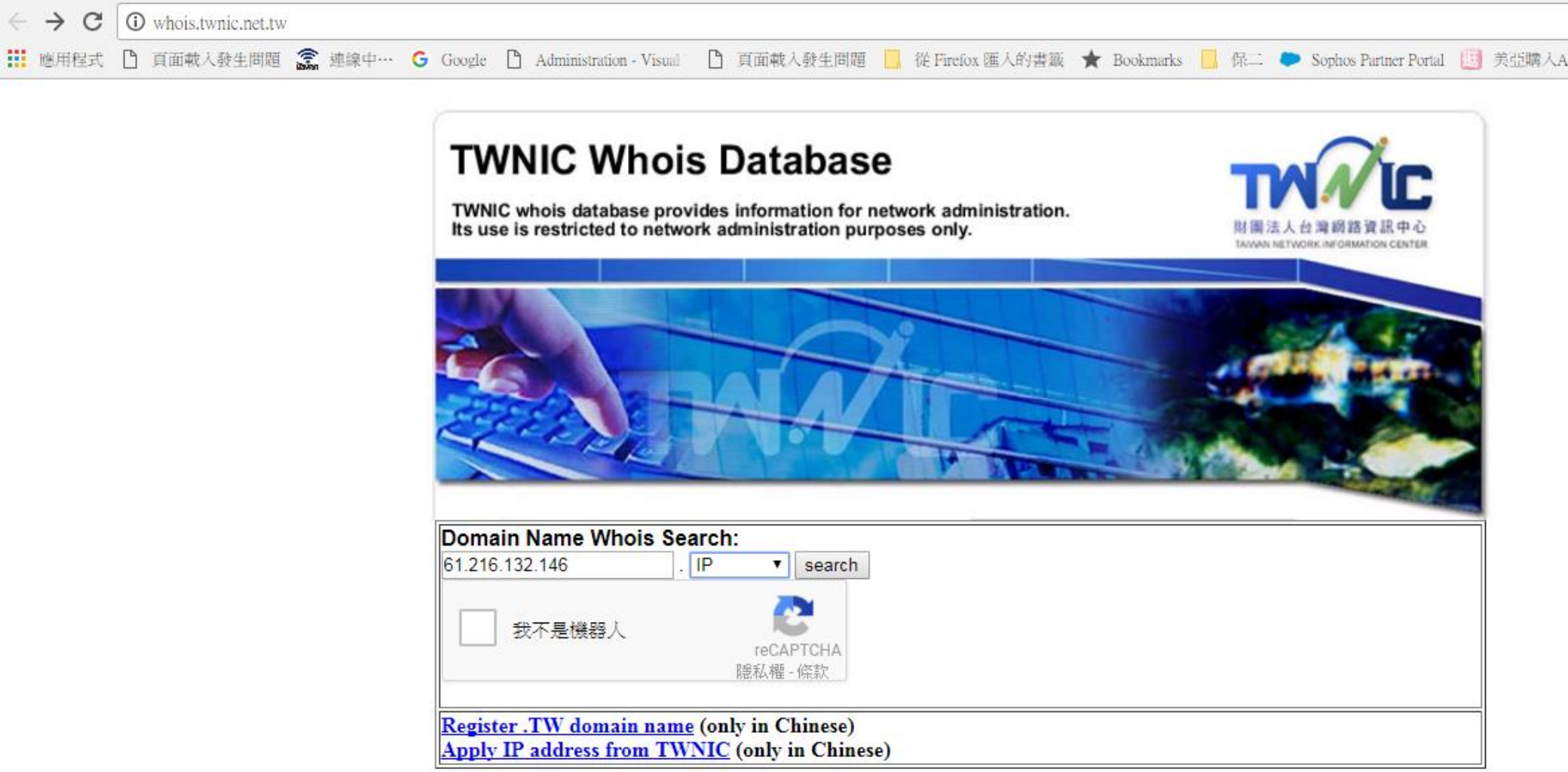
進入偽微軟的釣魚網站


Back
Search
Favorites
Address
http://www.lloginlove.com/
Go
Links
http://www.lloginlove.com/
仿冒微軟Windows Live網站
申請
登入
Hotmail
有智慧的電子郵件 - 快速、簡易，又可靠
Messenger
與生活中的親朋好友保持聯繫
SkyDrive
受密碼保護的免費線上儲存空間
沒有 Windows Live ID？
註冊
只要有 Windows Live ID，即可全面享有 Hotmail、Messenger、Xbox LIVE 和其他 Microsoft 服務。
Windows Live ID：
密碼：
忘記密碼？
記住我的資訊
記住我的密碼
登入
Done
Internet

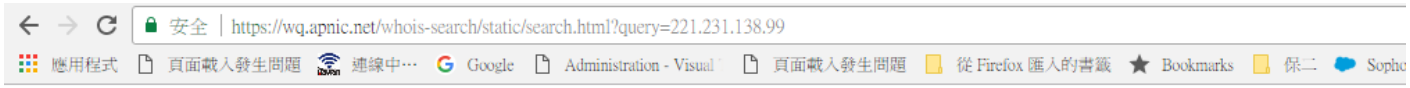
查詢網站IP


C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Blake>ping yahooo.c65.163ns.con
Pinging yahooo.c65.163ns.com [221.231.138.99] with 32 bytes of data:
Reply from 221.231.138.99: bytes=32 time=213ms TTL=105
Reply from 221.231.138.99: bytes=32 time=211ms TTL=105
Reply from 221.231.138.99: bytes=32 time=218ms TTL=105
Reply from 221.231.138.99: bytes=32 time=213ms TTL=105
Ping statistics for 221.231.138.99:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 211ms, Maximum = 218ms, Average = 213ms
C:\Documents and Settings\Blake>

到TWNIC網頁查看看



用APNIC網頁 查詢結果



APNIC

APNIC Whois Search

To assist you with debugging problems, this whois query was received from IP Address:

61.216.132.150

If you experience problems with this form, try the legacy search form.

```
% APNIC found the following authoritative answer from: whois.apnic.net

% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '221.224.0.0 - 221.231.255.255'

% Abuse contact for '221.224.0.0 - 221.231.255.255' is 'anti-spam@ns.chinanet.cn.net'

inetnum:        221.224.0.0 - 221.231.255.255
netname:        CHINANET-JS
descr:          CHINANET jiangsu province network
descr:          China Telecom
descr:          A12,Xin-Jie-Kou-Wai Street
descr:          Beijing 100088
country:        CN
admin-c:        CH93-AP
```

中國

免費分析網站 www.virustotal.com

網路釣魚Phishing

-利用偽造的網頁作為誘餌，詐騙使用者洩漏如帳號密碼等個人機密資料

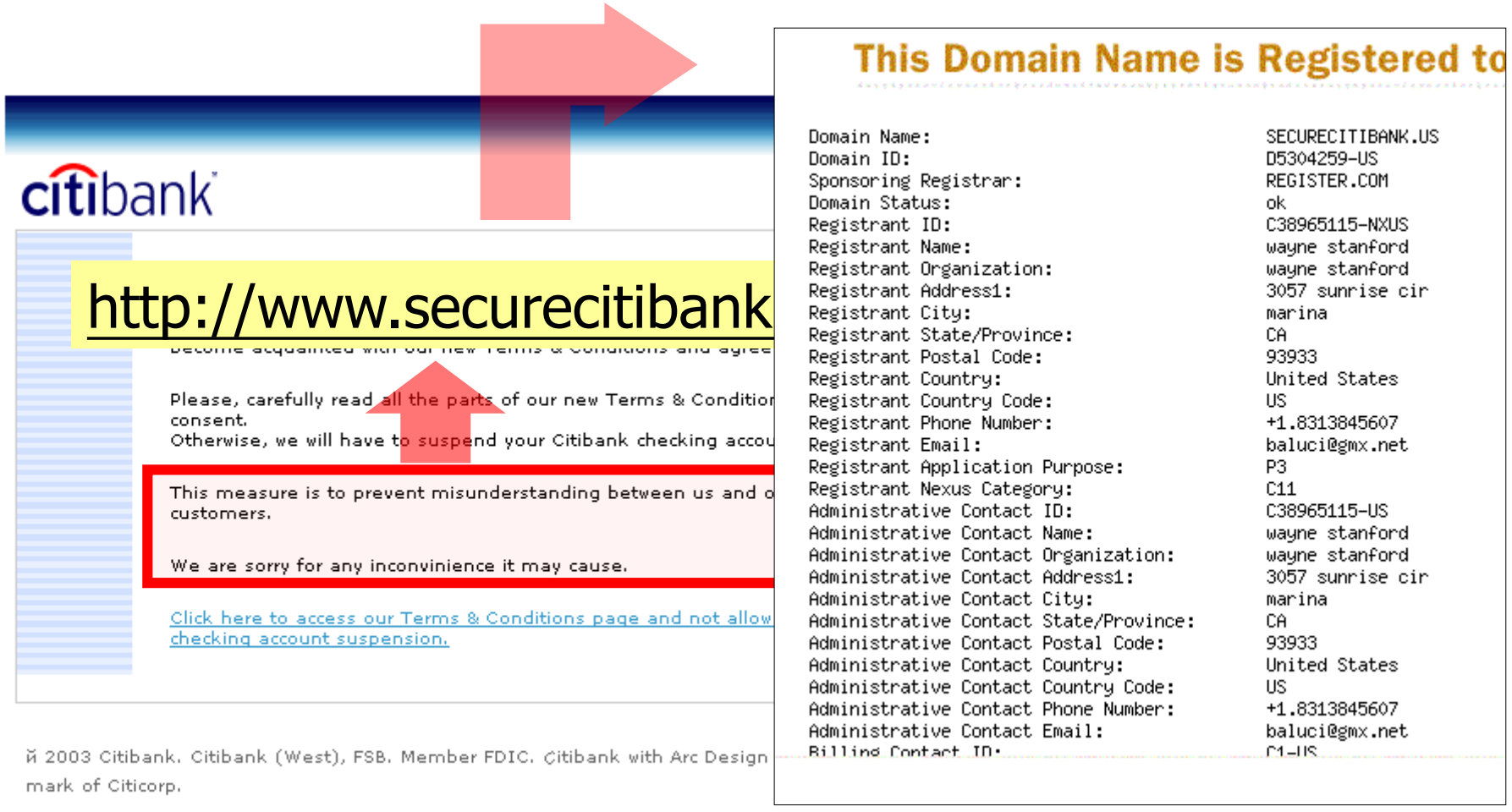
-釣魚網頁畫面與官方網站相同，但其實這個網址並非官方網站

以相似的字元來偽裝網址

例如:以數字的0來替換英文的O

以數字的1來替換英文的I…..等等

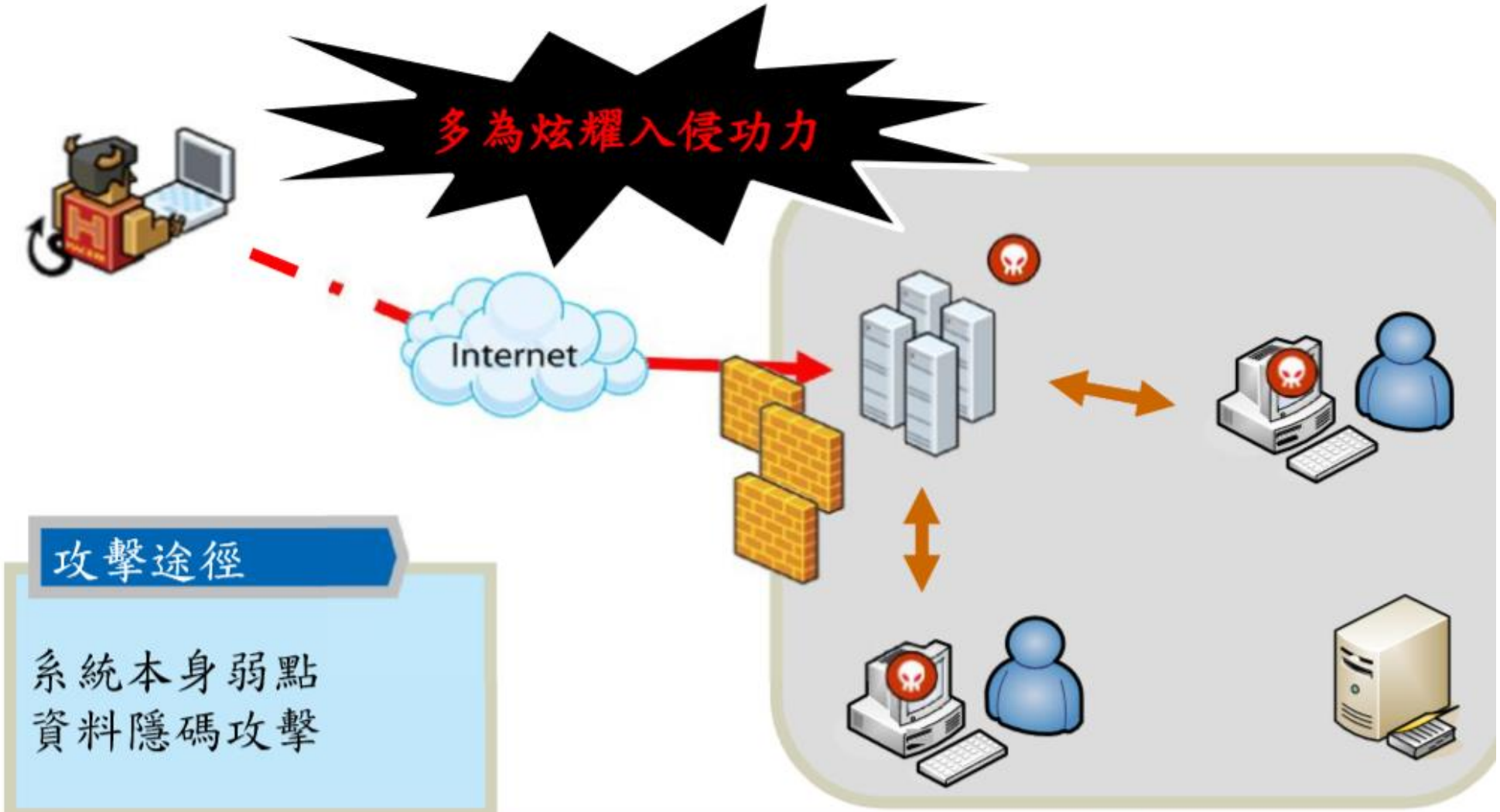
生活中的案例-Phishing



課程大綱

- 密碼安全
- 軟體使用安全
- 病毒與木馬防護安全
- 電腦操作安全與資料備份
- USB管理
- 公用存取
- 電子郵件安全
- 社交工程
- 網路釣魚與網路詐騙
- 日益猖獗的勒索病毒

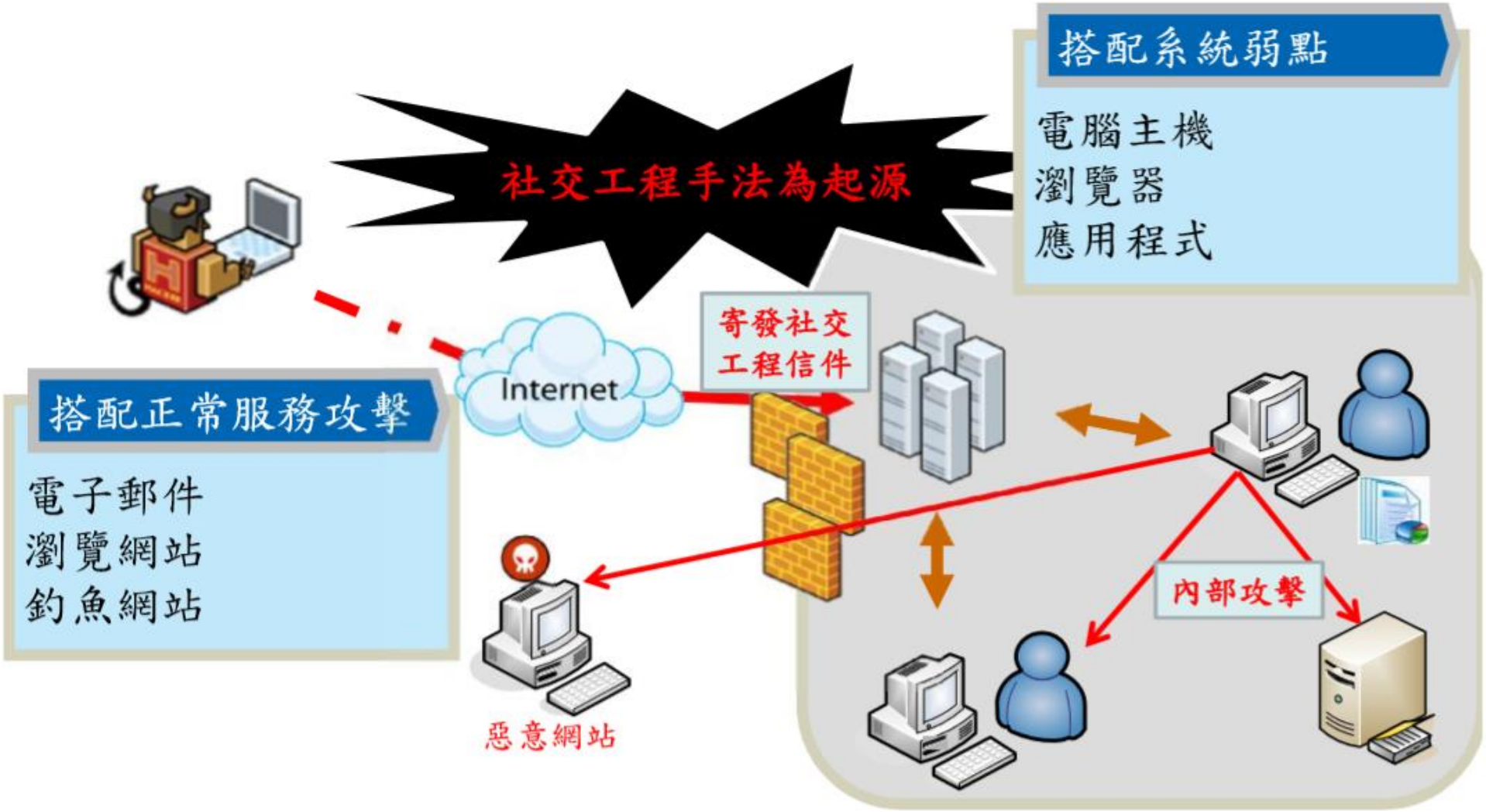
初期勒索



攻擊途徑

系統本身弱點
資料隱碼攻擊

進化勒索


社交工程手法為起源
搭配系統弱點
電腦主機
瀏覽器
應用程式
搭配正常服務攻擊
電子郵件
瀏覽網站
釣魚網站
Internet
寄發社交
工程信件
內部攻擊
惡意網站

勒索軟體WannaCry

勒索軟體感染途徑

- 偽裝成快遞信件...
- 附件夾帶隱藏的惡意程式
- 回報惡意中站,下載金鑰
- 將Pdf / Word / Excel / PowerPoint .... 檔案加密
- 跳出付款解鎖警訊，需要金鑰才可以解開

進入偽微軟的釣魚網站


Back
Search
Favorites
Address
http://www.lloginlove.com/
Go
Links
http://www.lloginlove.com/
仿冒微軟Windows Live網站
申請
登入
Hotmail
有智慧的電子郵件 - 快速、簡易，又可靠
Messenger
與生活中的親朋好友保持聯繫
SkyDrive
受密碼保護的免費線上儲存空間
沒有 Windows Live ID？
註冊
只要有 Windows Live ID，即可全面享有 Hotmail、Messenger、Xbox LIVE 和其他 Microsoft 服務。
Windows Live ID：
密碼：
忘記密碼？
記住我的資訊
記住我的密碼
登入
Done
Internet

假Windows 10更新連結暗藏勒索軟體

- 勒索軟體 Ransomware
- 假冒各種形式
  - Windows 10 update
  - 防毒軟體
  - 解毒軟體
  - …

假冒免費 Windows 10 更新通知信件暗藏勒索軟體

分得出來嗎


土地銀行入口網站 - Windows Internet Explorer
http://www.landbank.com.tw/
Google 日曆
土地銀行入口網站
土地銀行 LAND BANK
www.landbank.com.tw
土地銀行入口網站 - Windows Inter
http://www.landbank.com.tw/
土地銀行入口網站 - Windows Internet Explorer
http://www.landbank.com.tw/
Google 日曆
土地銀行入口網站
土地銀行 LAND BANK
www.landbank.com.tw
關於土銀
土銀業務
最新動態
金融資訊
理財資訊
土地銀行入口網站 - Windows Inter
http://www.landbank.com.tw/

圖片中的惡意程式

明星或色情圖片也是許多惡意程式慣用的社交工程技巧之一，這些都是利用使用者的好奇心來散佈惡意程式，之前Sobig網路病毒出現在某個含有色情內容的網路討論群組，網友點選了其中像是裸照的內容就會感染病毒，而該病毒總共導致了約10億美金的損

讓人很想點入的網頁

林志玲MaggieQ露三點寫眞

檔案(F) 編輯(E) 檢視(V) 工具(T) 郵件(M) 說明(H)

回覆 全部回覆 轉寄 列印 刪除 上一個 下一個 通訊錄

寄件者: 小 玲玲

日期: 2007年8月6日 下午 03:52

收件者: 偉倫;呆呆的小花;呈輝;士平;宇庭 宇庭;宗翰;小 花;小丸子;小喬;小小高;小熊;小白;小白 李文音;小雪老師;小魚 小魚;慧敏;文音;李 A王豪;林柏成 酷仔;林維德;校長;楊建偉;灰姑娘;爹的;玉琳;玉菁;玲;秘a 媽咪;粉粉;育航;致理小瑜;芭樂;芷欣;莊菁菁;萬寶華劉小姐;蘇小韋;蘋果;蝶后;蟲子;邱 詩安;鄭 治武;采;阿 儐;阿豪;陳 小P;陳思帆;雅如;雅如;雅婷姐;電腦老師;電腦邱老師;餅妹;馮慈;醫子;麵功];黃 阿海;奢爸爸

主旨: 林志玲MaggieQ露三點寫眞

附加檔案: 三點寫眞.com (244 KB)

林志玲MaggieQ露三點寫真
亞洲十大名模的狂野挑逗.
性感貼近測試妳的忍耐力到底有多大極限囧囧
來試試吧.....

杜絕網路駭客，保障帳號安全 - 馬上設定 Yahoo!奇摩安全圖章！

假eBay 拍賣詐騙網站

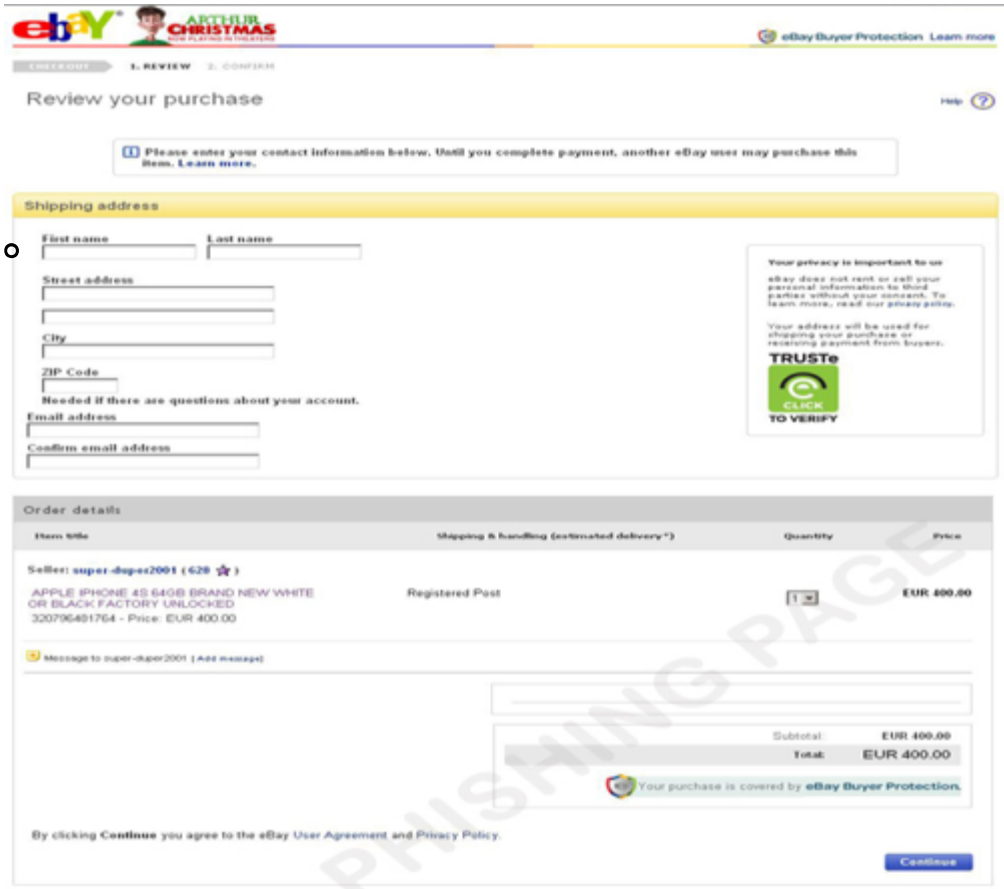
假eBay 拍賣網站的四個破綻:

1.真網站使用美元為貨幣，偽網站使用歐元為貨幣。

2.假網頁上標示的價格便宜得多。

3.網路犯罪分子選擇複製的是有良好評價的賣方。

4.假網頁內的所有連結都是連到正常網站，除了「Buy It Now (立即購買)」是連結到/www.ebay.ie/的網域上外。



降低勒索病毒方式

1. 不要隨意點擊電子郵件中的連結。
2. 不要打開附件，除非你確認內容安全，也知道內容為何。
3. 不要訪問可疑的網站。
4. 不要隨意下載軟體。
5. 要定期將重要的檔案和資料備份，就算中標，損失也不至於太大。

使用者電腦安全部署

- 安裝防毒軟體
  – 更新至最新病毒碼
- 個人防火牆防禦
  – 阻擋非法連線
- 安裝最新系統安全性更新
  – 修補系統上的弱點，避免弱點遭利用攻擊
- 更新應用程式
  – 亦避免弱點遭利用攻擊

結語

- 防護技術是反應攻擊的保護機制
- 新型態攻擊發生時，「人」是安全防範關鍵
- 使用者的資安認知教育為防範的基礎
- 時時刻刻保有警覺心

防護措施沒有100%安全，重要還是在於使用者的行為、使用資訊設施的習慣及對安全的認知。

新型態攻擊發生時，「人」是安全防範關鍵

- 使用即時通訊及社群網站時請避免接受陌生的邀請。
- 社群網站上請避免點擊來路不明的應用程式遊戲與心理遊戲。
- 使用即時通訊時請避免點擊來路不明之連結或檔案。
- 注意塗鴉牆、留言版、電子郵件中的超連結的可靠性。
- 請避免在網路上留下任何可以辨識個人的隱私資訊。


?
Q
&
A
!