資安宣導
個資防護

資安顧問　　郭洛坤

大綱

- 上網行為個資防護
- 郵件社交工程防護
- 軟體使用個資防護

上網的個資防護

網路相簿
網路購物
網路搜尋

網路相簿

- **上古時代：**
- 相片是沖洗出來放在相本裡收集，老的時候一頁一頁翻出來看。

- **中古時代：**
- 相片是用彩色噴墨、相片印表機印出來，將四周圍貼滿自己的得意作品隨時看。

- **網路現代：**
- 相片是用手機、數位相機拍好後直接放上網路，迫不及待想跟認識的及不認識的人分享，自己看還不夠，深怕別人看不到。

所以！
當現在科技時代可以用數位相機、手機拍攝，並傳送到網路上，就會衍伸出「個資洩漏」的問題。

網路相簿

- 知名相簿網站：

- 無名小站 (www.wretch.cc)
- 痞客邦 (www.pixnet.net)
- Xuite (www.xuite.net)
- yam天空部落相簿 (blog.yam.com)
- 網路家庭相簿 (photo.pchome.com.tw)
- Flickr相片分享 (www.flickr.com)

網路相簿

- 可是？
- 將相片放在網路上就安全嗎？

- 基本防護設定：
- 我有設定「禁止按右鍵」另存照片。
- 我有設定「相簿鎖密碼」過濾訪客。

- 這樣應該就安全了吧！

網路相簿

- 那使用「相簿鎖密碼」過濾來訪客，沒有密碼就無法看圖呢？

- 重點是？
- 你確定你的密碼設定的很完善？
- 不會被有心人士隨便猜一猜就猜到？
- 或者只要使用網路通通都設相同的密碼？

密碼設定的相關事項

- 需包含英文大小寫、數字及符號。
- 密碼需要 7~8 個字以上。
- 不可以另外寫下　或　存在電腦檔案裏。

密碼背不起來怎麼辦？

- 用鍵盤上　注音符號　的位置。
- c04vupdkru4

- 不會注音符號？
- 發音不正確導致密碼輸錯？
- 改用其他輸入法(倉頡、大易)等
- 測試密碼強度：www.passwordmeter.com

- 當然使用「自己的姓名」當密碼，是個『不好的建議』。
- 比較正確的方法是用：
- 古詩，例如：五言絕句

- 某個自己記得起來的語彙，例如：
- 1l3au4z;62u,6

Case Study

泄密門

網路購物

- 網路購物有二大風險：
- 購物網站本身：
  - 購物網站管理不當(產生漏洞、植入木馬)
  - 購物程式設計不當(產生被人入侵的管道)
  - 購物的流程管理不當(經手訂單的員工、廠商疏失)

- 消費者本身：
  - 電腦本身遭受感染木馬被竊取
  - 每個網站均使用同一組帳號及密碼而洩漏
  - 誤入假的購物網站遭騙
  - 於網拍貪小便宜匯款卻收不到商品

網路購物的注意事項

- 購物網站端：
- 做好網站及程式設計的安全控管。
- 落實客戶資料的保護。

- 使用者端：
- 定期更改密碼。
- 多留意購物網站的公告及新聞。
- 做任何金融交易前，請先確認所使用的電腦當時環境是[乾淨且無毒]的。
- 確認該[購物網站]網站是正確的。
- 定期更新防毒軟體的病毒碼並搭配線上掃毒。

網路搜尋

- 網路搜尋的惡意手法有二：
- 利用「特殊語法」取得隱藏資訊(Google Hacking)
  - 成功後，利用該資訊取得個人資料，或不公開的文件。
  - 例如UNIX Password檔可使用intitle: “index of..etc” passwd或intitle:index.of passwd passwd.bak搜尋密碼檔
- 利用「關鍵字廣告」連結惡意網頁
  - 成功後，利用該惡意網頁植入木馬後竊取個人資料。

Google Hacking

- “Google hacking is a computer hacking technique that uses Google Search and other Google applications to find security holes in the configuration and computer code that websites use.”-Wikepedia
- Keyword(關鍵字)
  - 搜尋相關內容
  - 相關度(relevance)
- Operator
  - 有效過濾資訊

基本語法與關鍵字

- site: (搜尋特定網址)
- inurl: (搜尋特定連結)
- intext: (搜尋網頁內文字)
- intitle: (搜尋網頁標題)
- filetype: (搜尋特定檔案格式)
- link: (搜尋互相連結的網頁)
- “index of“ (搜尋開放目錄瀏覽)
- cache: (顯示網頁在google中的暫存資料)

困擾的是！

不是所有搜尋引擎都會提醒該連結有問題。

就算會提醒也需要掃描時間也不會是立即提醒。

點選了就會感染該木馬。

網路搜尋的注意事項

- 點選搜尋引擎所提供的連結之前，請先注意該連結的網址是否正確。
- 盡量不要使用「不具有惡意連結提醒」的搜尋引擎。
- 可行的話封鎖來自於「中國」的網址。
- 就算真的感染只要防毒軟體與修補程式有更新，至少可以有一定程度的防護。

上網重點項目

- 請勿上傳不適合公開的照片。
- 請勿點選看似好康的「超連結」。
- 做任何網路購物交易前，請記得再掃毒一次確保電腦在無毒的狀態。
- 防毒軟體不要只是有安裝，卻從來沒有全機掃毒過。

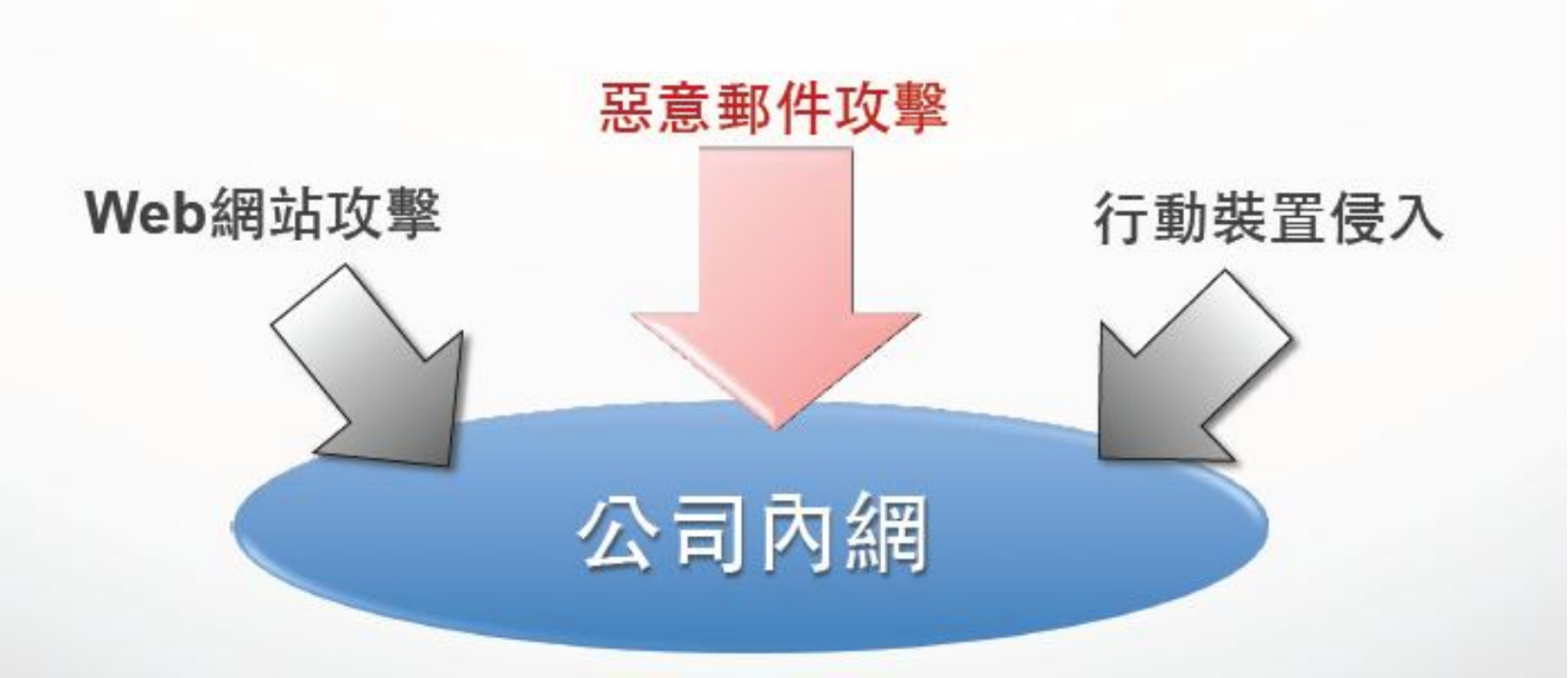
Case Study

PlayStation Network
Sony Online Entertainment

新型郵件社交工程攻擊

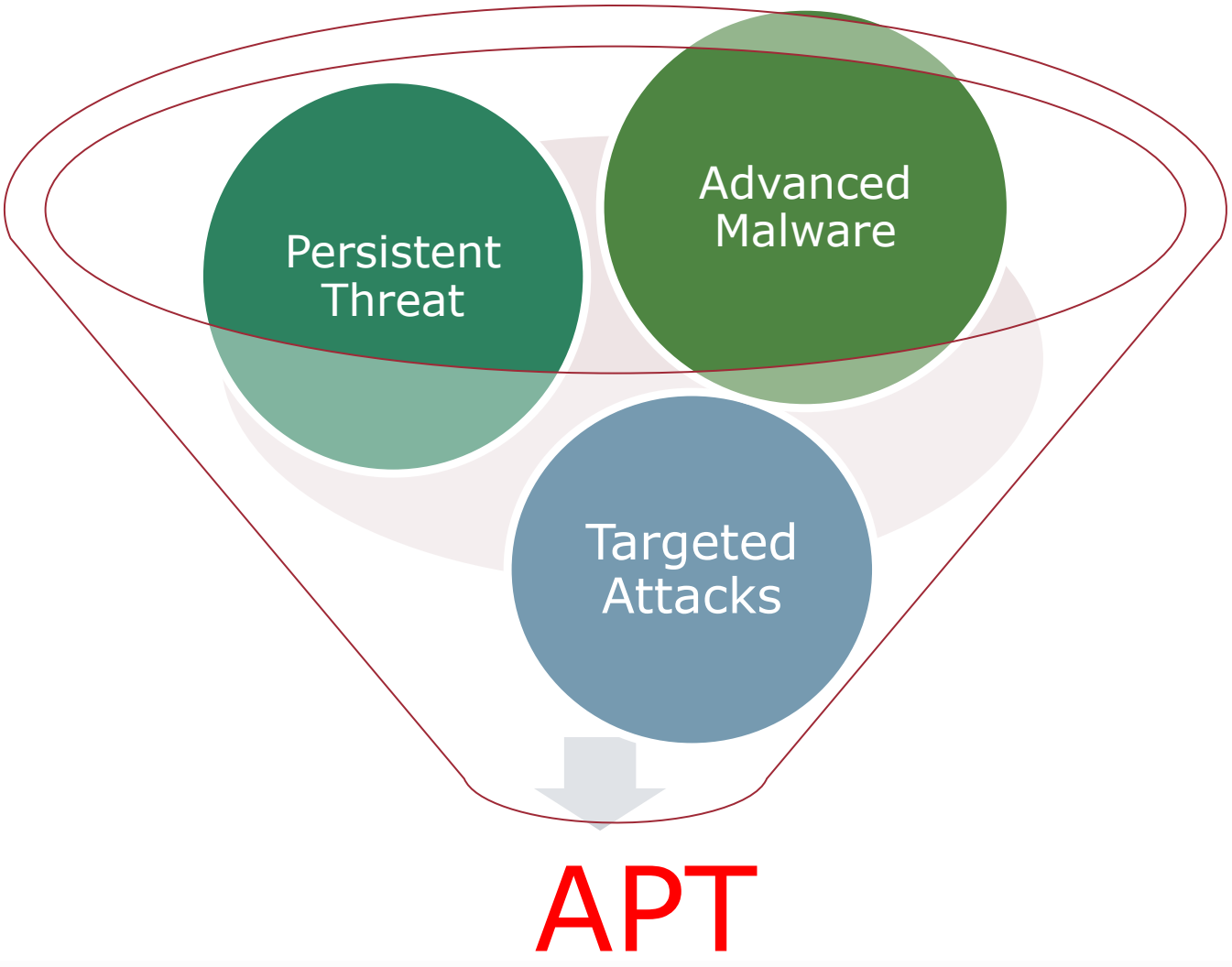
Advanced Persistent Threat
(APT,先進持續性威脅)

APT攻擊管道



APT的攻擊管道中，惡意郵件攻擊為最大宗。

Advanced Persistent Threat



Stuxnet worm

網安／Stuxnet蠕蟲怪客外傳鎖定核電廠？　全球通緝中

2010年10月7日 11:08

記者蘇湘雲／台北報導

趨勢科技6日針對一隻已經危害全球各地許多電腦、名廠

訊，專家指出，Stuxnet的特徵是會自動自我複製，其主

的自動化生產與控制（SCADA）系統，同時SCADA系

客戶該隻惡意程式會藉由USB設備和網路共享進行蔓延

英國經濟學人稍早前報導指出，StuxnetⅡVirusBlokAda

SCADA管理系統軟體WinCC。西門子在7月則於隔月警

連上網路，但Stuxnet可以透過USB傳播，也能透過資料

報導說，Stuxnet同時利用4種完全不同、先前未被公開

產流程和管理系統方面，不太像是惡意駭客所製，而是

但起源和影響還不清楚。據賽門鐵克指出，受感染的電

印度。專家懷疑，Stuxnet可能是鎖定伊朗的核子反應爐

趨勢科技資深技術顧問簡勝財6日指出，這是世界上首隻

7系統的病毒，目的在取得WinCC SQL Server登入SQL

一可允許遠端執行程式碼的MS10-046 Windows 系統漏

伊朗核電廠受到Stuxnet蠕蟲感染

文/陳曉莉 (編譯) 2010-09-27

讚 16 人說這讚。成為你朋友中第一個說這讚的人。　我要收藏

Stuxnet主要的攻擊目標為西門子的自動化生產與控制（SCADA）系統，SCADA系統多半被用在工廠中，目前已蔓延到全球上百個國家，伊朗現為受害最嚴重的國家，境內已有超過3萬台電腦受到Stuxnet感染，大幅領先居次的印尼（約1萬台）。

伊朗新聞通訊社周日（9/26）報導，當地境內首座核能發電廠受到Stuxnet蠕蟲感染，該發電場負責人Mahmoud Jafari已證實此事，但表示僅有部份員工電腦受到感染，而非主要系統。伊朗已派遣專家移除發電廠員工電腦中的病毒，而即將上線營運的核能發電系統並無大礙。

微軟是在今年7月警告視窗作業系統Windows Shell含有安全漏洞，駭客得以透過lnk捷徑檔嵌入惡意程式，當時就發現Stuxnet蠕蟲已藉由該漏洞進行攻擊，並透過各種可攜式USB裝置或網路分享進行感染。

Stuxnet主要的攻擊目標為西門子的自動化生產與控制（SCADA）系統，SCADA系統多半被用在工廠中，Stuxnet蠕蟲除了具備竊取資料的能力外，還能掌控企業控制系統，Stuxnet已蔓延到全球上百個國家，伊朗現為受害最嚴重的國家，境內已有超過3萬台電腦受到Stuxnet感染，大幅領先居次的印尼（約1萬台）。

RSA SecurID Hack?

Shady RAT
(暗鼠行動)

McAfee | Blog Central

Corporate | McAfee Labs | Enterprise

McAfee Labs :

« Previous post in McAfee Labs

Revealed: Operation Shady R

Tuesday, August 2, 2011 at 9:14pm by Dmitri Alperovitch

Download the PDF version of Operation Shady RAT rep

For the last few years, especially since the public r
targeted successful intrusion into Google and two
often been asked by our worldwide customers if th
sophisticated penetrations themselves or if that is
agencies, defense contractors, and perhaps Googl
has been unequivocal: absolutely.

Having investigated intrusions such as Operation
long-term compromise of Western oil and gas industry), as well as numer
disclosed publicly, I am convinced that every company in every conceivable
valuable intellectual property and trade secrets has been compromised (o
majority of the victims rarely discovering the intrusion or its impact. In fact
Global 2000 firms into two categories: those that know they've been comp
know.

Lately, with the rash of revelations about attacks on organizations such as
and others, I have been asked by surprised reporters and customers whet
increasing and if it is a new phenomenon. I find the question ironic becaus
have occurred relentlessly for at least a half decade, and the majority of th
months have, in fact, been a result of relatively unsophisticated and oppo

McAfee揭露大型駭客行動：Shady RAT五年滲透72個組織

文/陳曉莉 (編譯) 2011-08-04

讚 | 5 人說這讚。成為你朋友中第一個說這讚的人。 | 我要收藏

五年來該行動總計駭進全球72個組織，包括22個政府組織、6家鋼鐵與能源企業、13家電子或媒體企業、13家國防承包商．．．；其中，美國佔了49個，居次的加拿大佔了4個，而台灣與南韓皆佔了3個。

比起Anonymous或Lulzsec這類鬆散的駭客組織，資安業者McAfee相信全球仍有許多潛藏的駭客行動尚未被揭露，本周公布了一項該公司五年來持續追蹤的駭客行動—Operation Shady RAT，指稱全球至少有超過72個組織被該行動滲透。

McAfee安全研究副總裁Dmitri Alperovitch將全球前2000大企業分成兩類，一是知道自己的企業已被駭客滲透，二是不知道。雖然Anonymous與Lulzsec一連串的駭客行動喚起大眾對資安的關注，然而這並不是個新的現象，而且相較於那些有規畫且低調的駭客行動，這兩個高調的駭客組織顯得鬆散、簡單，而且是機會主義者。

自2006年起McAfee就開始存取由單一駭客組織所掌控的命令暨控制伺服器，並追蹤該伺服器上的資料，同時將其命名為Shady RAT行動（Operation Shady RAT），五年來該行動總計駭進全球72個組織，包括22個政府組織、6家鋼鐵與能源企業、13家電子或媒體企業、13家國防承包商、4家房


22
6
13
13
4
12
U.S. Federal Government 6
U.S. State Government 5
U.S. County Government 3
Canadian Government 2
South Korean Government 1
Vietnam Government 1
Taiwan Government 1
U.S. Government Contractor 1
United Nations 1
Indian Government 1
Construction/ Heavy Industry 3
Steel Industry 1
Energy 1
Solar Power 1
Electronics Industry 3
Computer Security 2
Information Technology 2
Satellite Communica-tions 2
News Media 2
Information Services 1
Communica-tions Technology 1
Defense Contractor 13
Real Estate 2
Accounting Industry 2
Agriculture 1
Insurance 1
International Sports 5
Economics/ Trade 2
Think Tanks 2
International Government/ Economics/ Trade 1
Political Non-profit 1
U.S. National Security Non-profit 1
Source: McAfee

Protection and mitigation

- Ensure antivirus is up-to-date and active
  - 確保防毒軟體的更新與開啟
- Turn on IPS
  - 開啟IPS
- Use email filtering
  - 使用email過濾
- Patch operating system and software
  - 修補OS與軟體
- User awareness
  - 用戶的意識(教育訓練)

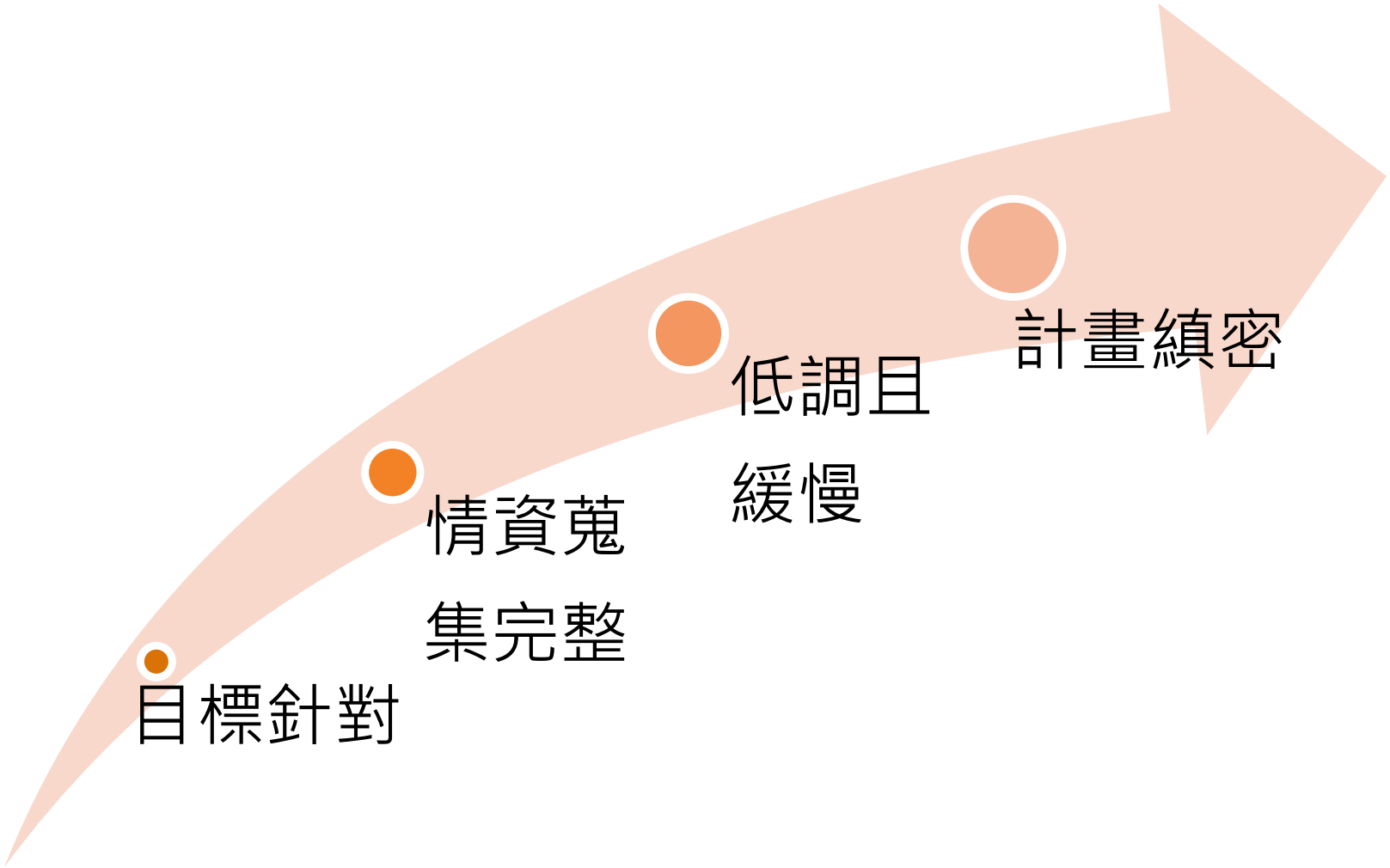
APT有多嚴重?

有多少APT攻擊?

- "分析各國APT樣本來看 APT活動前三大地區(台灣、美國與香港)就占了超過一半比例，其中台灣最高約28% 。綜觀來看，亞洲是APT最主要活動的地區。"
  -- Xecure-Lab

APT Overview

APT攻擊模式



	APT 攻擊	一般網路犯罪
攻擊者	通常是國家贊助或是培養的駭客，有一定規模的組織活動與計畫。	由民間駭客組成，通常與犯罪集團或是從事地下黑市資料交易的集團組成。
受害者	主要以機密資料，如政府機關，政治相關人物，軍火商，高科技公司，高科技研究單位，重要金融公司，民生相關的基礎建設為主。對於受害者有針對性，且有持續性。	主要以個人資料，金融相關資料，如信用卡，網路銀行帳密。對於受害者無針對性，並且沒有區域性。
攻擊目的	情報資料，竊取政府重要資料與高科技成果為主，屬於網路間諜活動 (Cyber Espionage)。	金融資料，將個資與金融資料賣給犯罪集團進行詐騙，以獲利為主。
攻擊武器	最常透過目標式攻擊郵件(Targeted Attack Email)，並搭配Document Exploit，而且都是一般駭客市場很罕見的0Day Exploit為主。觸發後佈署後門程式。	攻擊主要是透過網頁，常用Exploit Pack，以掛馬為最主要手法(Drive-By-Download Exploit)，使用Browser相關的Exploit最多。不同集團用的Exploit都差不多。

郵件社交工程

社交工程之定義

- 社交工程為利用人性弱點或利用人際之信任關係，獲取不當資訊。

- 指不用程式即可獲取帳號、密碼、信用卡密碼、身分證號碼、姓名、地址或其他可確認身分或機密資料的方法。這些方法多半是使用與人互動的技巧。

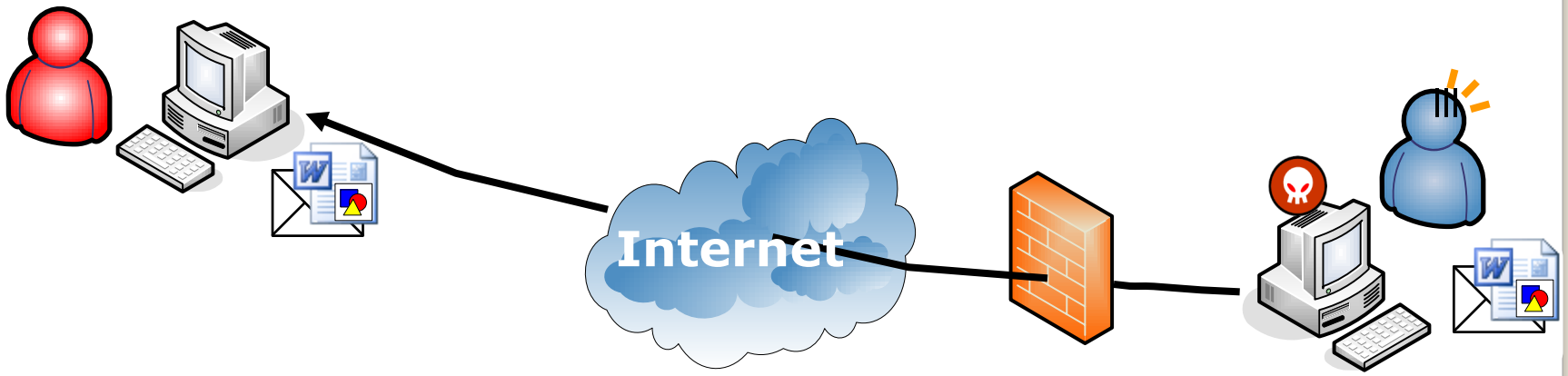
郵件社交工程攻擊之定義

- 利用人性弱點、人際交往或互動特性所發展出來的一種攻擊方法

- 早期社交工程是使用電話或其他非網路方式來詢問個人資料，而目前社交工程大都是利用電子郵件或網頁來進行攻擊

- 透過電子郵件進行攻擊之常見手法
  - 假冒寄件者
  - 使用與業務相關或令人感興趣的郵件內容
  - 含有惡意程式的附件或連結
  - 利用應用程式之弱點(包括零時差攻擊)

社交工程攻擊模式



1. 駭客設計攻擊陷阱程式(如特殊 *Word* 檔案或外部惡意連結)
2. 將攻擊程式置入電子郵件中
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，將被植入後門程式
6. 後門程式逆向連接，向遠端駭客報到

郵件社交工程演練方式

- 攻擊團隊於演練實施期間寄發不同主題之電子郵件（其內含惡意程式碼）。

- 郵件內容區分為：「演藝八卦新聞」、「政治」、「養生保健」、「休閒娛樂」、「教育新聞相關」、「情色」等主題。

- 郵件類型區分為：「網頁類型」、「Word檔案」、「圖檔」等3種類型。

郵件社交工程演練方式

- 當收件人
- 開啟惡意電子郵件或
- 預覽惡意電子郵件或
- 點閱惡意電子郵件所附超連結或
- 點閱惡意電子郵件所附件檔案時，
- 即留下紀錄，

- 做為後續統計
- 惡意電子郵件開啟率及
- 惡意電子郵件點閱率之依據。

郵件社交工程演練範本 (假冒寄件者方式-假冒攻擊)

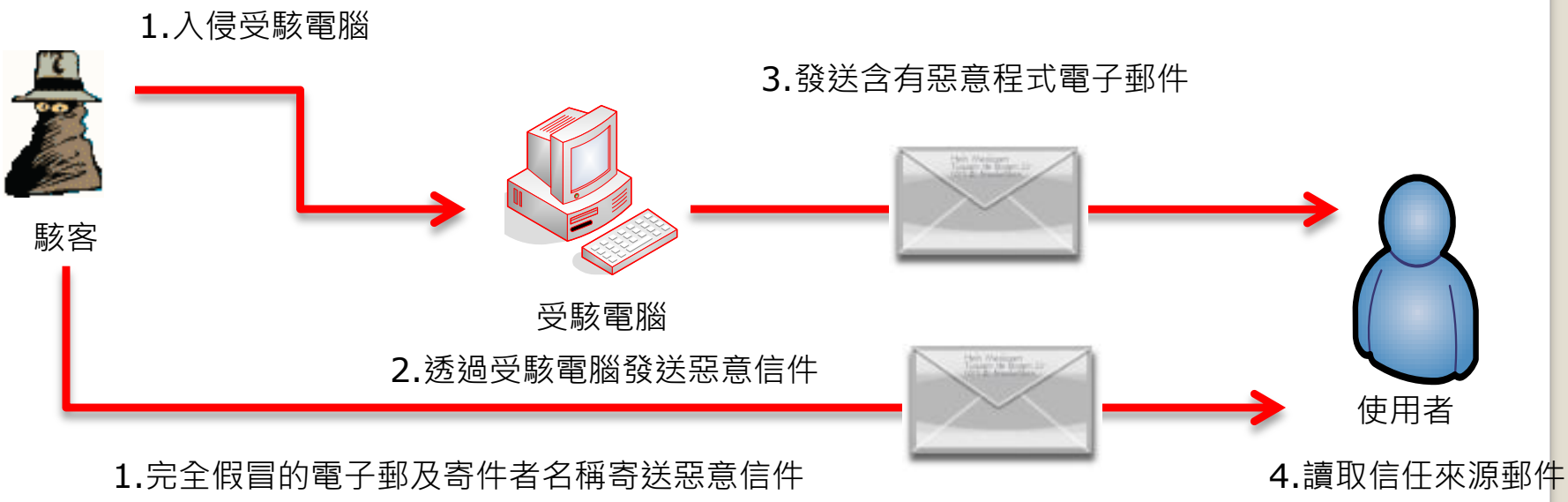
- SMTP 通信規範, *沒有辦法限制驗證寄件人的身份*. 雖然可以用身份驗證機制確保信是由特定人員寄出(例如加上簽章), 但沒辦法防止別人偽造你的 EMAIL 寄出信件. 頂多只能分辨出信是否為假的...

- 寄件人名稱可以是假的
- 超連結的狀態列可以是假的

- 所以整封信件，都是假的!!!!!!!!

郵件社交工程演練範本
(假冒寄件者方式-假冒攻擊)

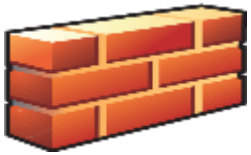
- 由於電子郵件傳送協定弱點，駭客可完全假冒寄件者的名稱以及電子郵件位址，甚至可透過入侵寄件者的電腦來寄發電子郵件。



預覽視窗開啟 或 點選郵件開啟

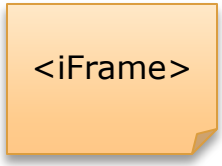
社交工程
郵件

Mail Server



攻擊手

預覽或點選



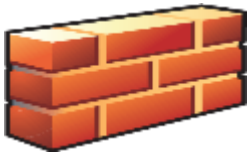
計數用Web
Server

點選郵件開啟後再點選郵件內 超連結

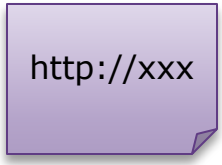
社交工程郵件

Mail Server

攻擊手



點選超連結



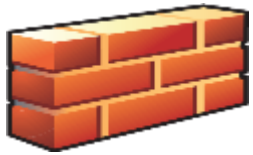
計數用Web Server

點選郵件開啟後再點選郵件內 附件檔

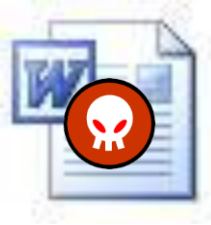
社交工程郵件

Mail Server

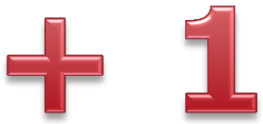
攻擊手



點選附件檔



計數用Web Server



電子郵件掛號信實作

- 使用SPYPIG服務(免費)
  - http://www.spypig.com

- 步驟：
  - 使用網路工具在信件中插入一張小圖片(空白圖片)
  - 當收件者收到之後(即收件者下載圖片)
  - Spypig會寄送信件跟您說對方已經開啟囉

郵件追蹤之術

追蹤信件從哪裡發出來

- http://whatismyipaddress.com/trace-email

郵件追蹤之術-信件從哪裡來

- 貼到以下網址的**Headers**裡面
- http://whatismyipaddress.com/trace-email

Headers:

```
Received: from mail.bccs.com.tw ([192.168.1.11]) by mail.bccs.com.tw
 ([192.168.1.11]) with mapi; Fri, 30 Jul 2010 15:06:17 +0800
Content-Type: application/ms-tnef; name="winmail.dat"
Content-Transfer-Encoding: binary
From: =?big5?B?quGrVLPH?= <jackhwa@bccs.com.tw>
To: =?big5?B?un6p/aX+pL2lcatIvWM=?= <bccs@bccs.com.tw>
Date: Fri, 30 Jul 2010 15:10:36 +0800
Subject: =?big5?B?W7ZnpK2lUqVSuXFdICCnQavnu/K7objcoUGoTal3pOGsT73W
Thread-Topic: =?big5?B?W7ZnpK2lUqVSuXFdICCnQavnu/K7objcoUGoTal3pOGsT73W?=
Thread-Index: Acsvtk6iGWfKdMTBmEqOGpYPQpjP5Q==
Message-ID: <C8789BED.7DB%jackhwa@bccs.com.tw>
Accept-Language: zh-TW
Content-Language: en-US
X-MS-Has-Attach: yes
X-MS-Exchange-Organization-SCL: -1
X-MS-TNEF-Correlator: <C8789BED.7DB%jackhwa@bccs.com.tw>
user-agent: Microsoft-Entourage/13.5.0.100510
MIME-Version: 1.0
X-Auto-Response-Suppress: DR, OOF, AutoReply
X-EsetId: DE64072F5B5D7069C162077B550930
```

Get Source

貼上

Get Source

演練與真實世界還是有出入

退信攻擊
跳板攻擊
密碼猜解

退信攻擊

退信攻擊

- ***收件人不存在導致無法送達郵件***，就會自動將該***退信訊息寄回給原寄件者***
- 利用這項功能，使用*字典攻擊所蒐集到的Email*
- 將***欲攻擊的對象設定為寄件者***
- ***收件者使用其他單位不存在的帳號***
- 然後你就會收到一封***不是自己寄出去的退信***了

跳板攻擊

跳板攻擊

- 當您的*電腦主機本身有啟用SMTP Service* (外寄伺服器服務)，而且*沒有加以防護*時，被有心人士發現，進而不當使用您的網路頻寬及寄信功能，濫寄廣告信件，這就是您的電腦主機被當成廣告信跳板了!!
- 通常受害者不知道自己的電腦安裝了相關服務
- 常見微軟的作業系統，當有*安裝了IIS功能*，*就會一同安裝SMTP(外寄伺服器服務)*，此時若您的網路系統並未安裝防火牆，將 SMTP PORT 25 設為對外阻隔的話 ，基本*上任何人都可以藉由您的 SMTP Service 寄發信件*!! 您的電腦主機，就有可能被有心人士當成廣告信跳板，濫寄廣告信件!!

偽造攻擊

偽造攻擊

- SMTP 通信規範, *沒有辦法限制驗證寄件人的身份*. 雖然可以用身份驗證機制確保信是由特定人員寄出(例如加上簽章), 但沒辦法防止別人偽造你的 EMAIL 寄出信件. 頂多只能分辨出信是否為假的...

- 寄件人名稱可以是假的
- 超連結的狀態列可以是假的

- 整封信件，都是假的!!!!!!!!

附件攻擊

郵件社交工程
防護停看聽

收信軟體安全性設定

- 以微軟的outlook express收信軟體為例，建議進行以下安全性的設定：
  1. 取消「郵件預覽」
  2. 取消「在預覽窗格檢視郵件時自動下載郵件」
  3. 勾選「以純文字閱讀所有郵件」
  4. 設定安全性區域為「受限制的網站區域」
  5. 勾選「在其他應用程式試圖以我的名義傳送電子郵件時警告我」
  6. 勾選「在附件有可能有病毒時不允許儲存或開啟」
  7. 勾選「阻擋HTML電子郵件中的圖片和其他外部內容」

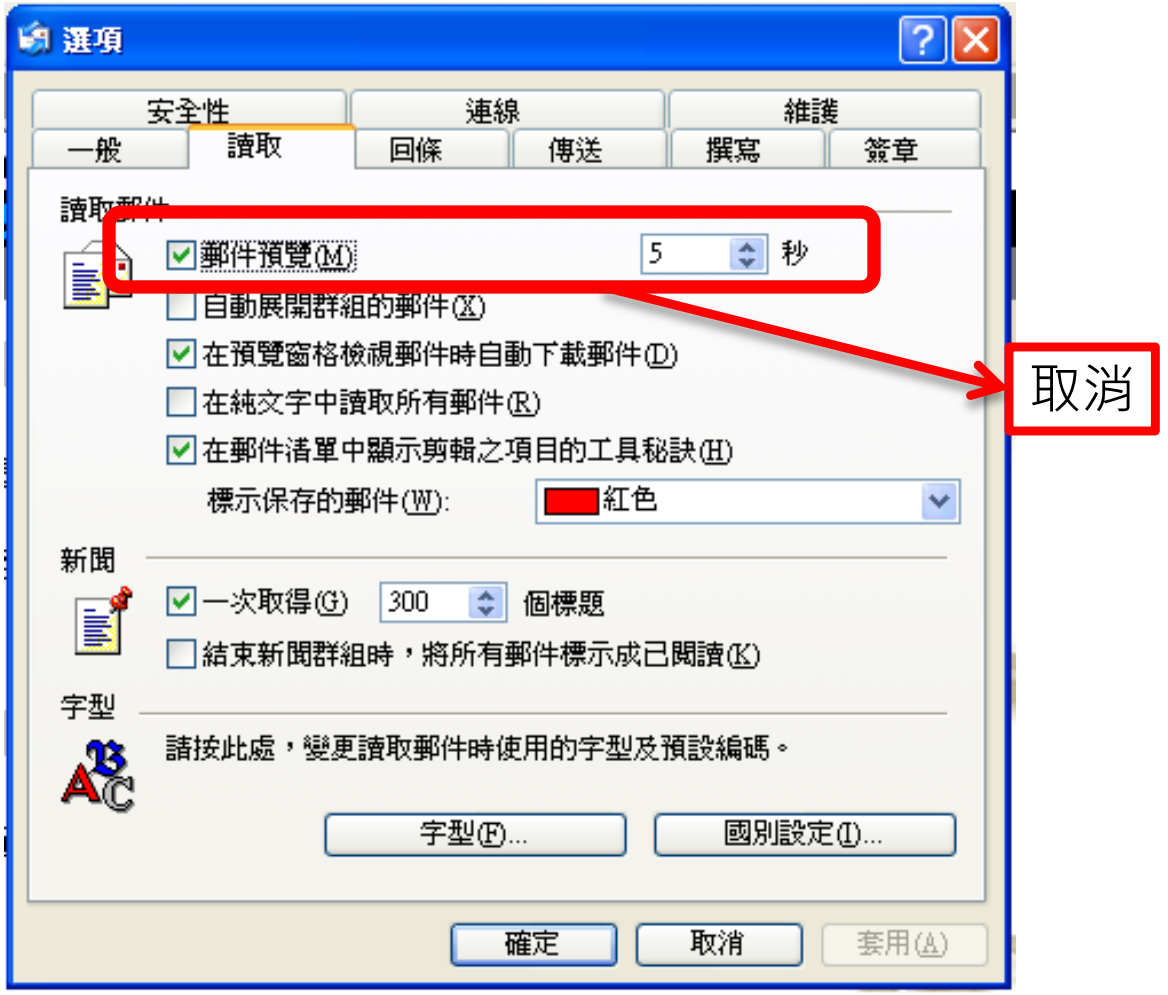
1.取消信件預覽功能


收件匣 - Microsoft Outlook
檔案(F) 編輯(E) 檢視(V) 到(G) 工具(T) 執行(A) 說明(H) Adobe PDF(P)
輸入需要解答的問題
新增(N) 回覆(R) 全部回覆(L) 轉寄(W) 傳送/接收(C) 尋找(I) SmartWhois
郵件
我的最愛資料夾
未讀取的郵件 (8073)
待處理 [17]
所有郵件資料夾
個人資料夾
收件匣 [129]
刪除的郵件 (142)
垃圾郵件 [29]
草稿
寄件匣
寄件備份
搜尋資料夾
收件匣
寄件者 主旨 大小 收到日期
日期: 今天
聯合人力網 人資進階的捷徑 9 KB 2007/7/4 (星期三) ...
績碩科技 想做網站不需花大錢，網站達人~教您如何省錢做... 8 KB 2007/7/4 (星期三) ...
pt-work.com 登録時、10万円お振込みキャンペーン中！即日日... 9 KB 2007/7/4 (星期三) ...
2007台北萬事達 台北萬事達邀你吃大餐做公益 6 KB 2007/7/4 (星期三) ...
人資進階的捷徑
聯合人力網 [redacted]
收件者: [redacted]
有效的招募管理 實操系列課程
名師授課，不同凡響。名額有限，報名從速！
人員招募的工作是企業競爭力的基礎，招募作業做得札實精準，就能真正落實「適才適所」人資管理的最優境界。
有效的招募管理實操系列課程，從理論出發，著重實際操
129 個項目

1.取消信件預覽功能

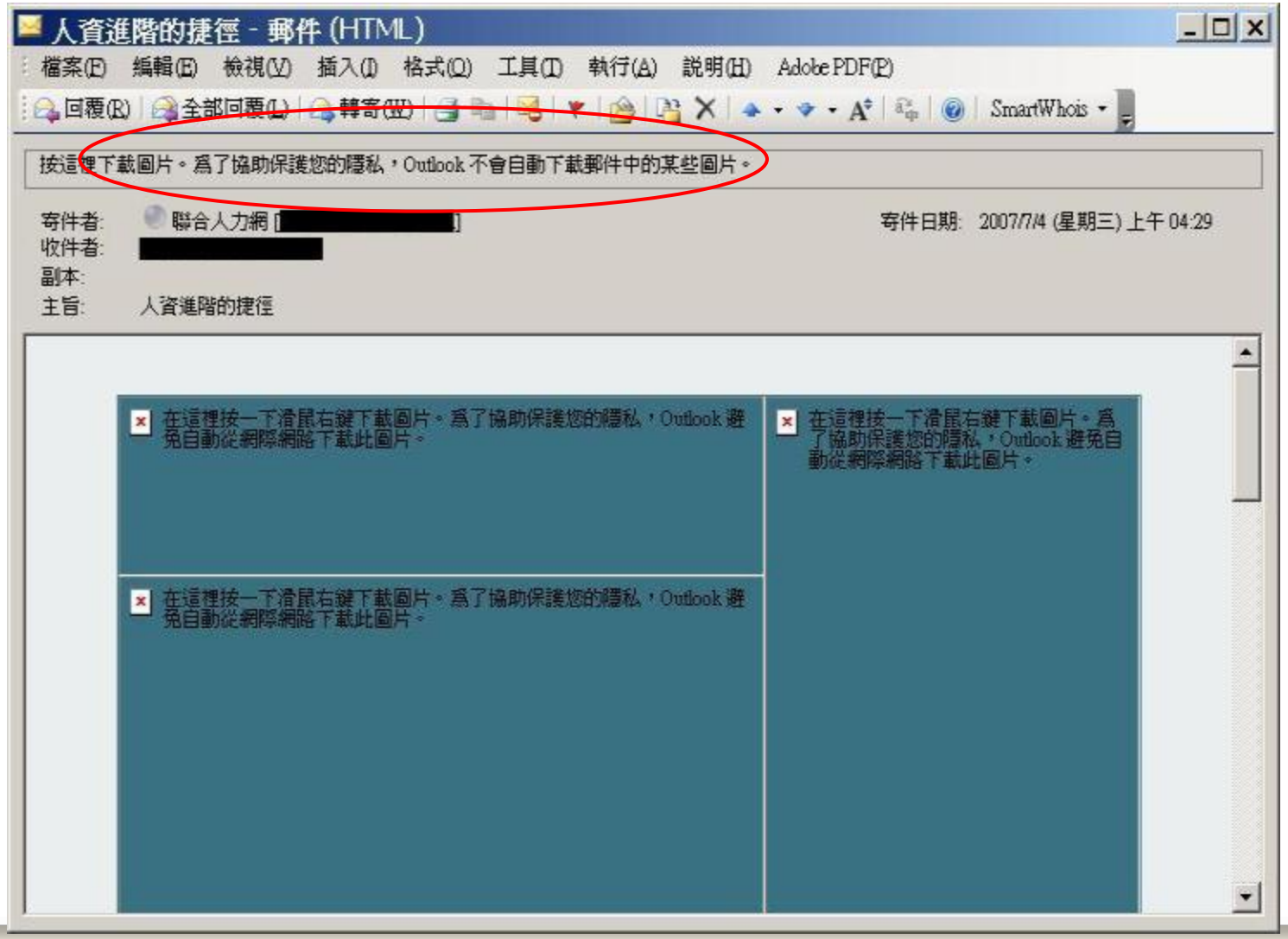

收件匣 - Microsoft Outlook
檔案(F) 編輯(E) 檢視(V) 到(G) 工具(T) 執行(A) 說明(H) Adobe PDF(P)
輸入需要解答的問題
新增(N) 回覆(R) 全部回覆(L) 轉寄(W) 傳送/接收(C) 尋找(I) SmartWhois
郵件
我的最愛資料夾
未讀取的郵件 (8073)
待處理 [17]
所有郵件資料夾
個人資料夾
收件匣 [129]
刪除的郵件 (142)
垃圾郵件 [28]
草稿
寄件匣
寄件備份
搜尋資料夾
收件匣
寄件者 主旨 大小 收到日期
日期: 今天
聯合人力網 人資進階的捷徑 9 KB 2007/1/4 (星期三)
緯鎮科技 想做網站不需花大錢，網站達人~教您如何省錢做... 8 KB 2007/1/4 (星期三)
pt-work.com 登録時、10万円お振込みキャンペーン中！即日日... 9 KB 2007/1/4 (星期三)
2007台北萬事達 台北萬事達邀你吃大餐做公益 6 KB 2007/1/4 (星期三)
日期: 昨天
機器人學校 台北分... FW:★ New! 2007暑期創意機器人科技研習營-----線... 9 KB 2007/1/3 (星期二)
好幸 孩子必讀童書經典 百大排行榜的冠軍故事精選 4 KB 2007/1/3 (星期二)
凡逸 ◆卡爆了，欠錢被討債，卡奴該怎麼辦？ 4 KB 2007/1/3 (星期二)
Winifred 最佳太極拳路,強身健體,防病減壓,通經絡,練精化氣... 5 KB 2007/1/3 (星期二)
Conley {Spam?} bulletin.460d6.pdf attached 15 KB 2007/1/3 (星期二)
Susanna 整合小學 國語文 數學 各大版本，教學重點依重點... 5 KB 2007/1/3 (星期二)
Joy ⊙兒童圖書 遙控飛機 遙控車・船 電子遊戲機 電子... 5 KB 2007/1/3 (星期二)
群豐 看秀看到一半差點被老媽抓包orz 4 KB 2007/1/3 (星期二)
生肖學大全 命理教學,姓名,風水,手相,面相,易經卜卦,八字,生肖... 5 KB 2007/1/3 (星期二)
daisuke yamanaka 登録ありがとうございました 7 KB 2007/1/3 (星期二)
珮逸 ↑完整的健身體系 瑜珈示範 教學，簡單易懂 5 KB 2007/1/3 (星期二)
博客來書籍館 不論你是誰，你想要什麼，這個《祕密》都能給你... 59 KB 2007/1/3 (星期二)
數位教育研究所 全會教育訓練公告一七月份課程快訊，進修學習即... 35 KB 2007/1/3 (星期二)
必備法律常識指... ：夫妻吵架、家庭糾紛或家庭暴力應如何處理？⊕ 5 KB 2007/1/3 (星期二)
詠桂 自然/健康教育最佳輔助教材 幫助兒童解決對人體... 5 KB 2007/1/3 (星期二)
T3領寬~虛擬主機~... 您好!! 慶祝 9周年 現在申請100MB空間，一年只... 4 KB 2007/1/3 (星期二)
129 個項目

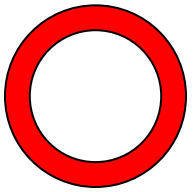
1.收信軟體安全性設定-郵件預覽



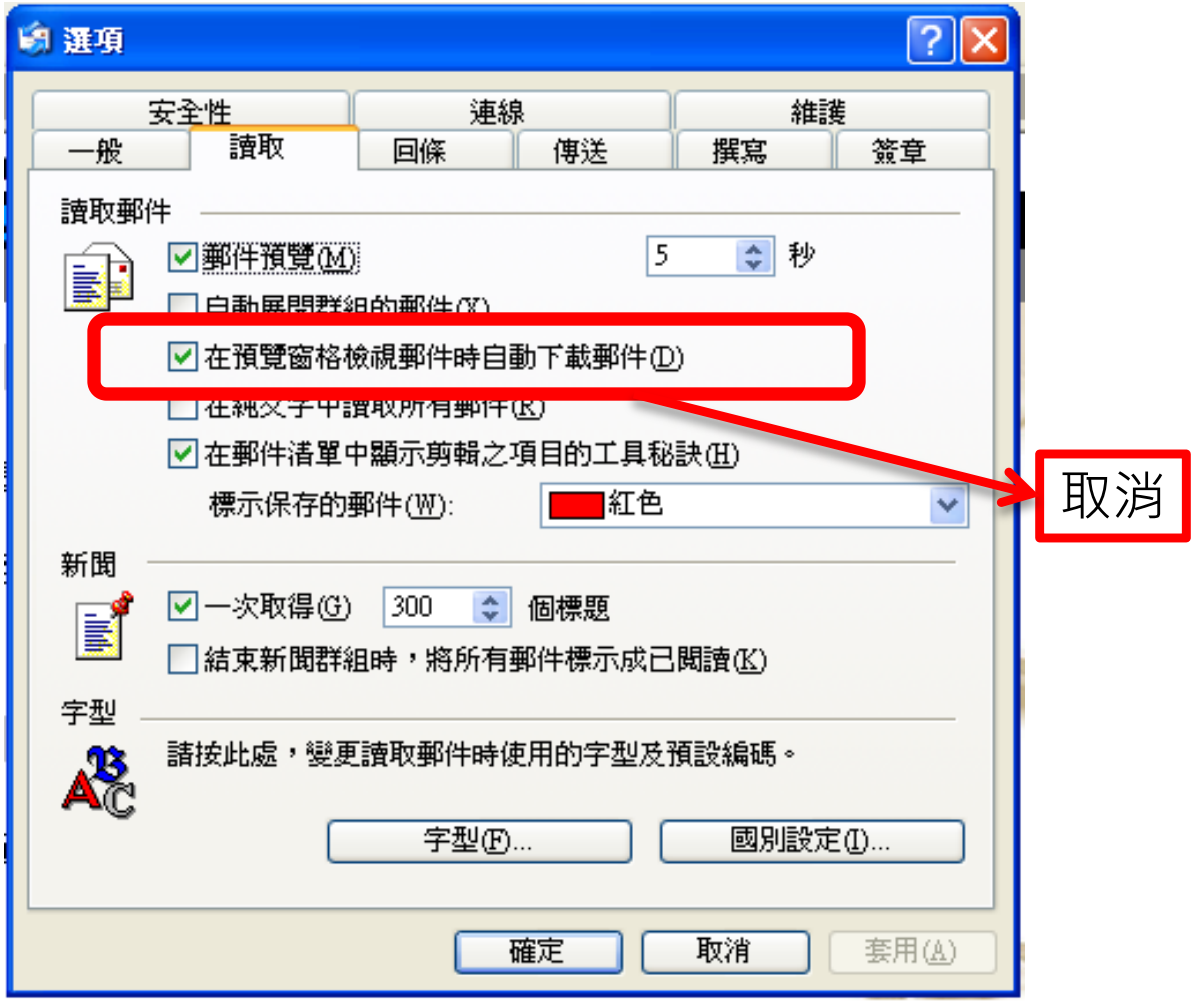
2.關閉信件自動下載圖片及其他內容

2.關閉信件自動下載圖片及其他內容

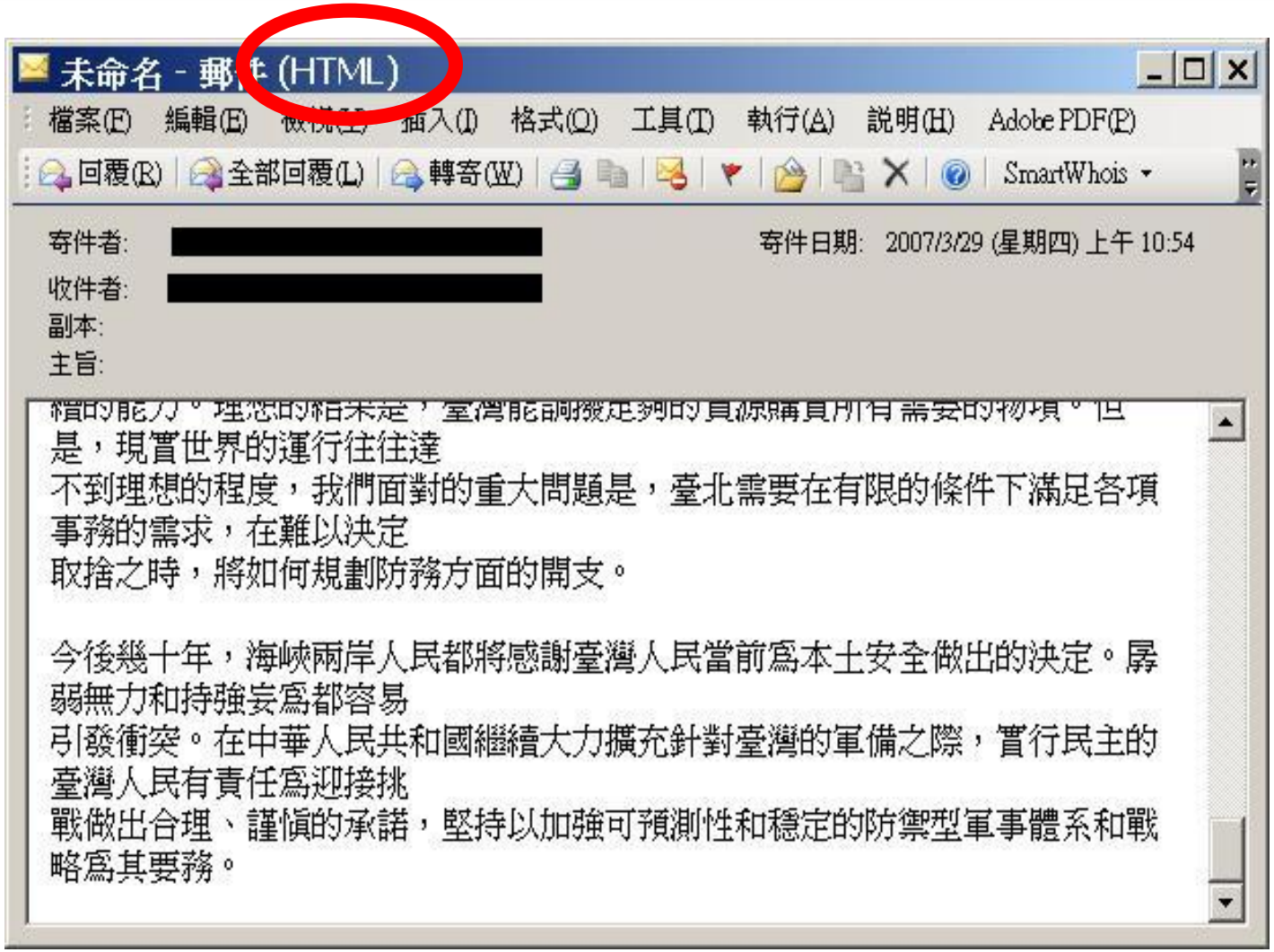




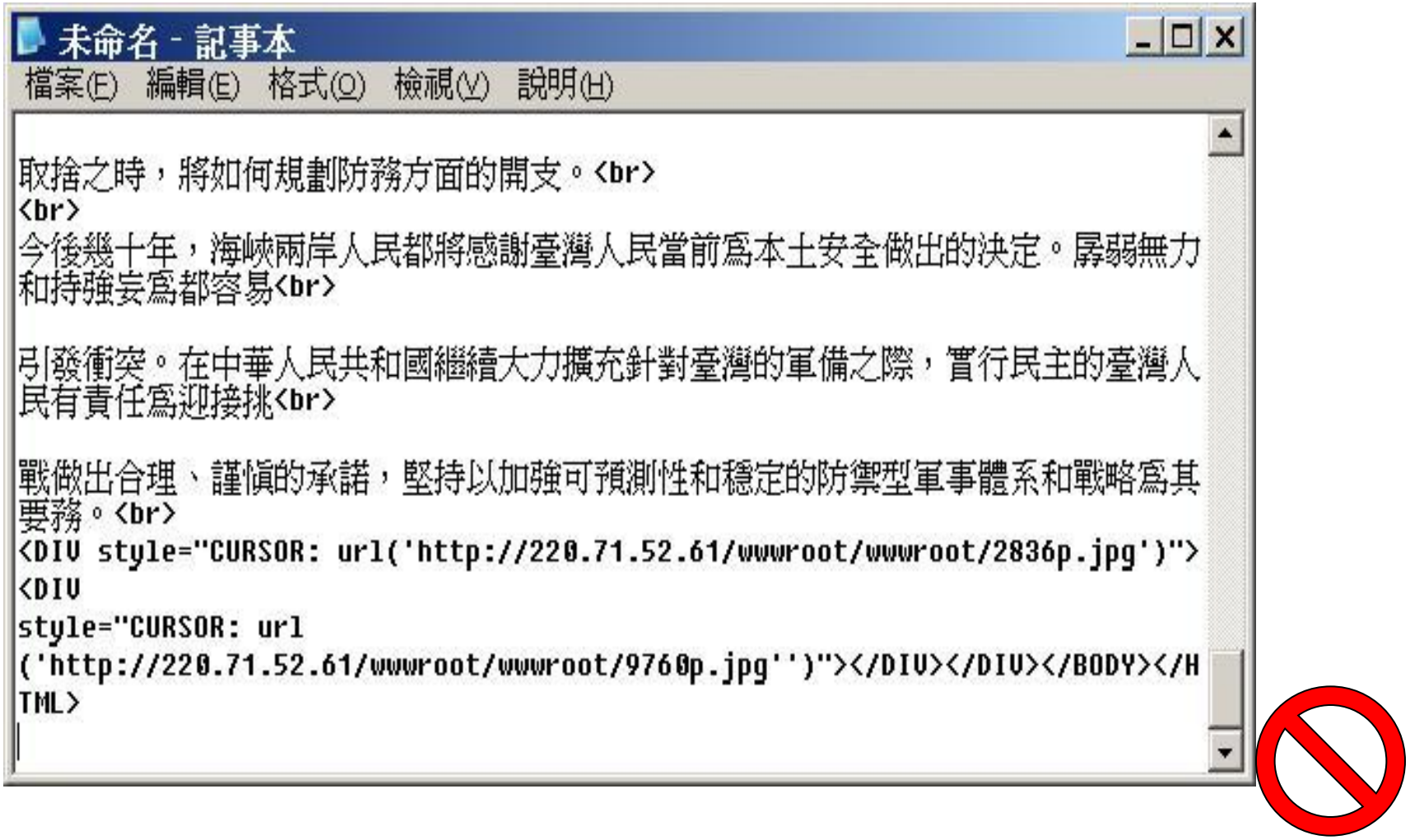
2.收信軟體安全性設定-
在預覽窗格檢視郵件時自動下載郵件



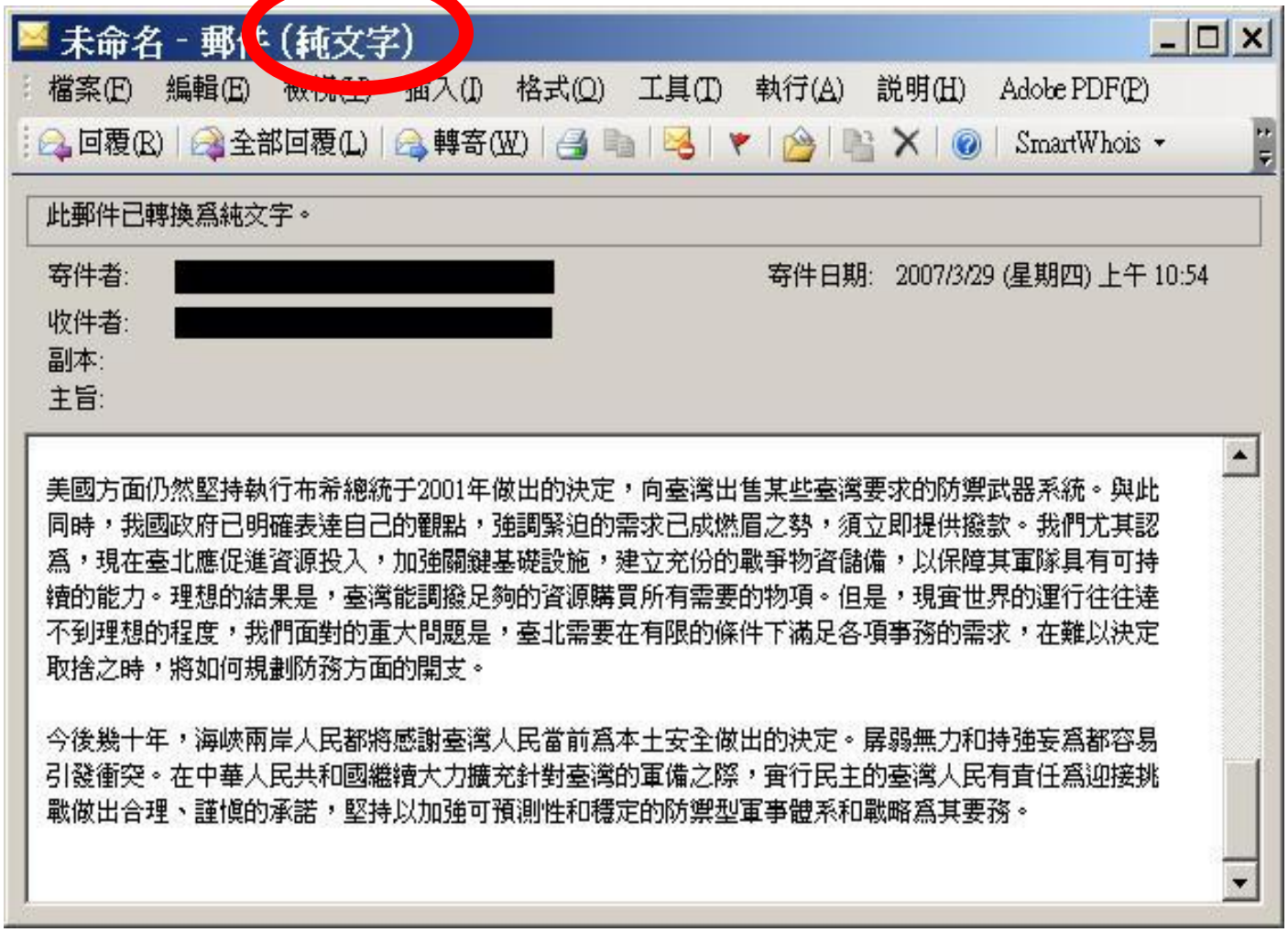
3.以純文字模式開啟信件

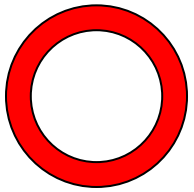


3.以純文字模式開啟信件

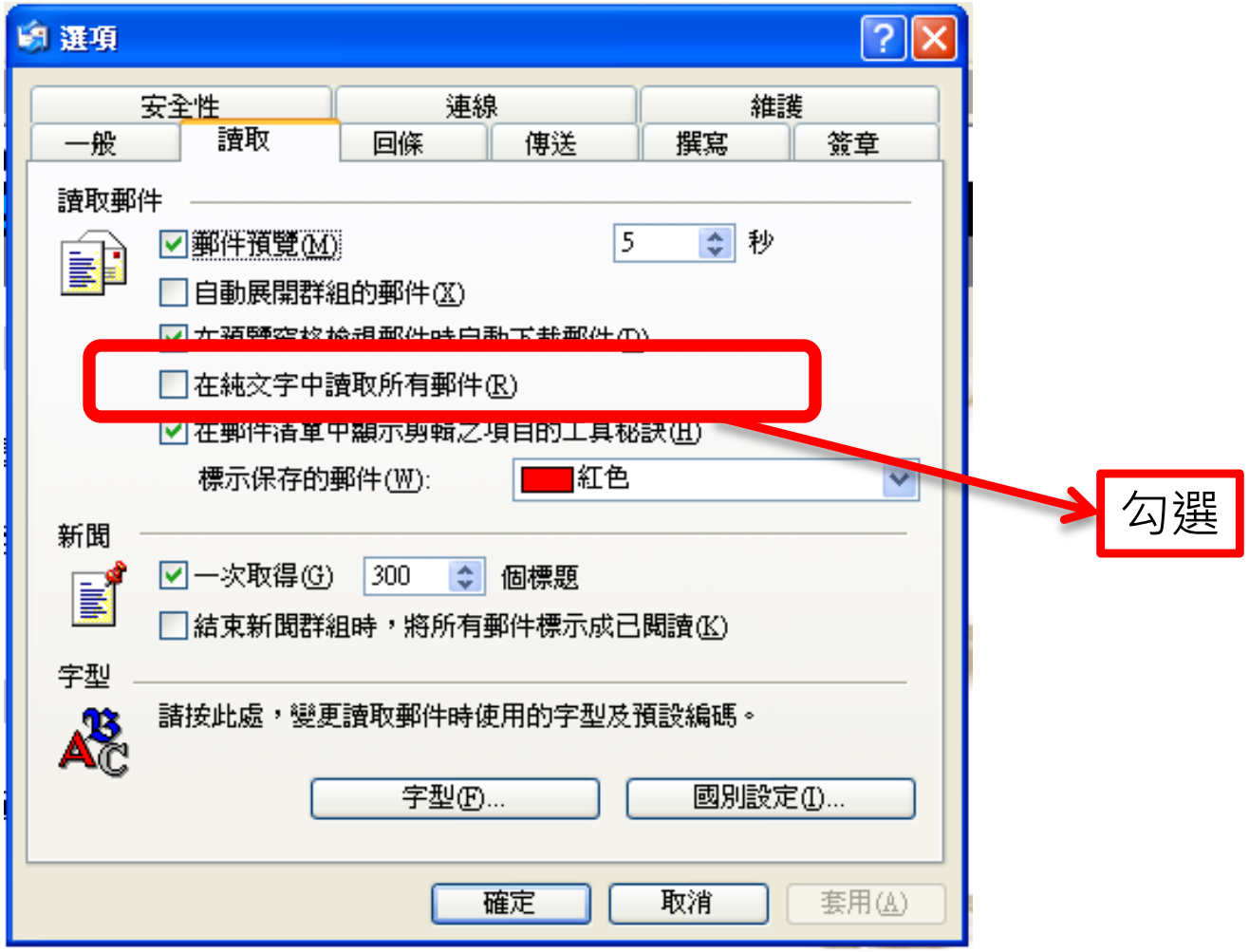


3.以純文字模式開啟信件

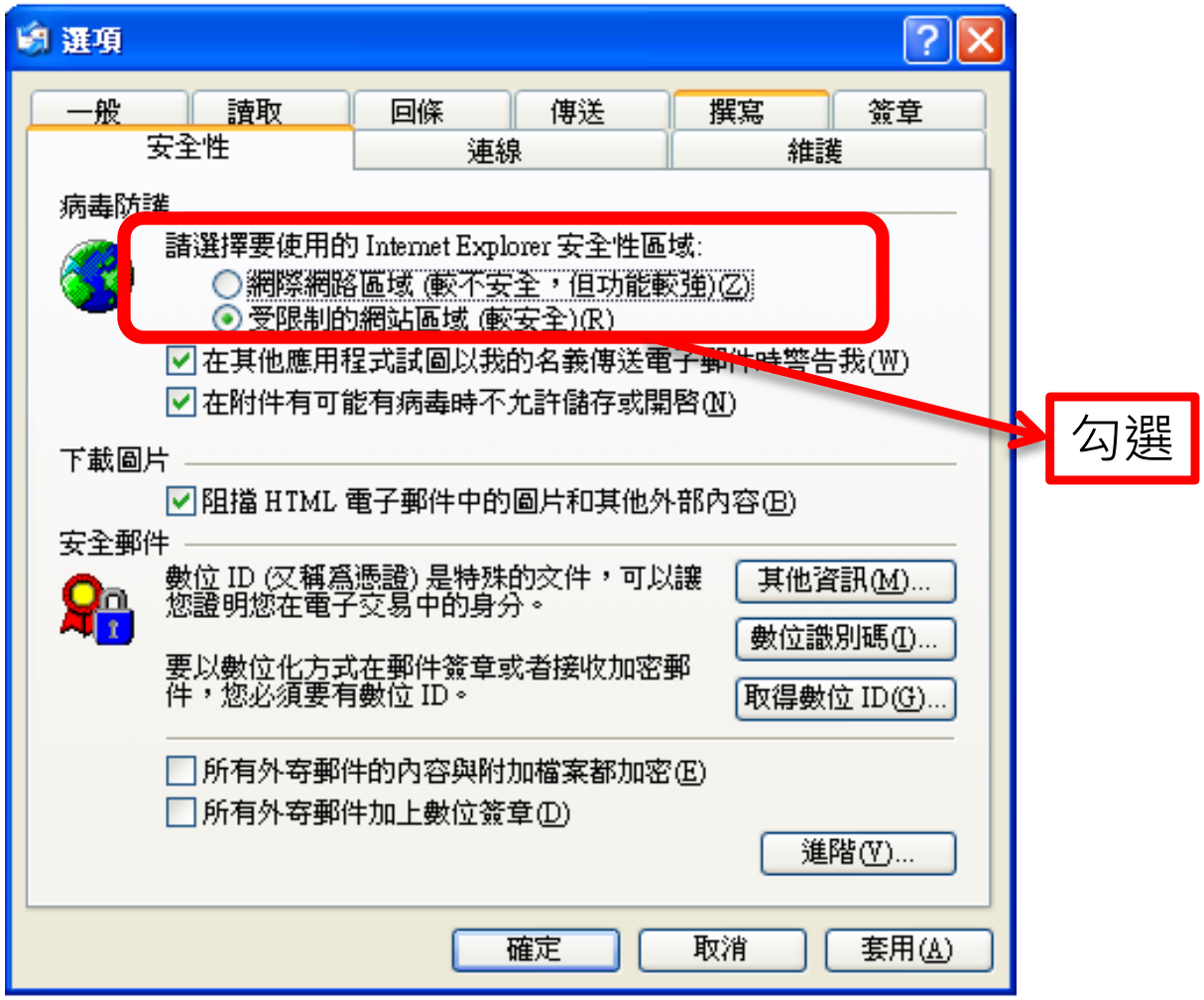




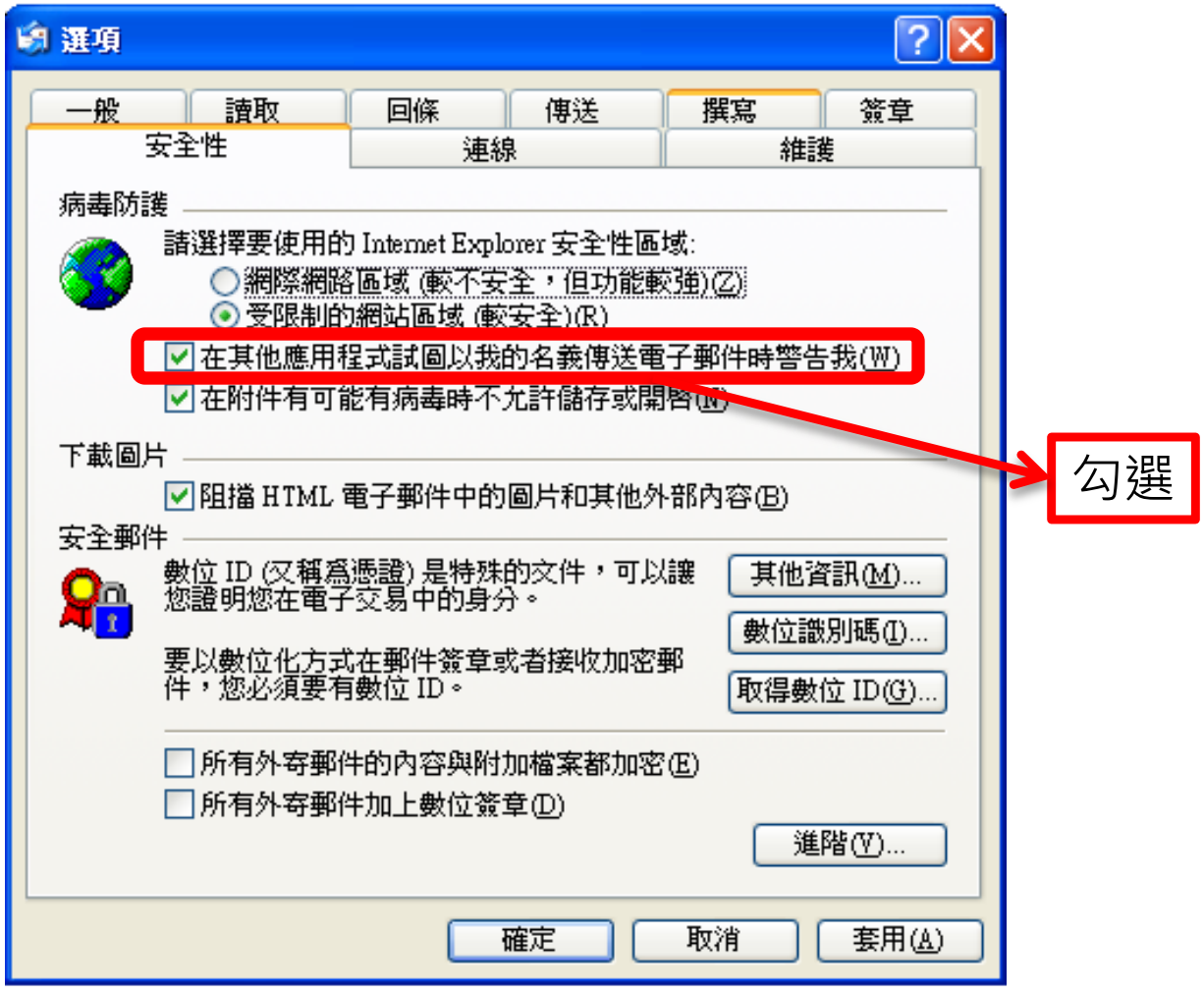
3.收信軟體安全性設定-以純文字閱讀所有郵件



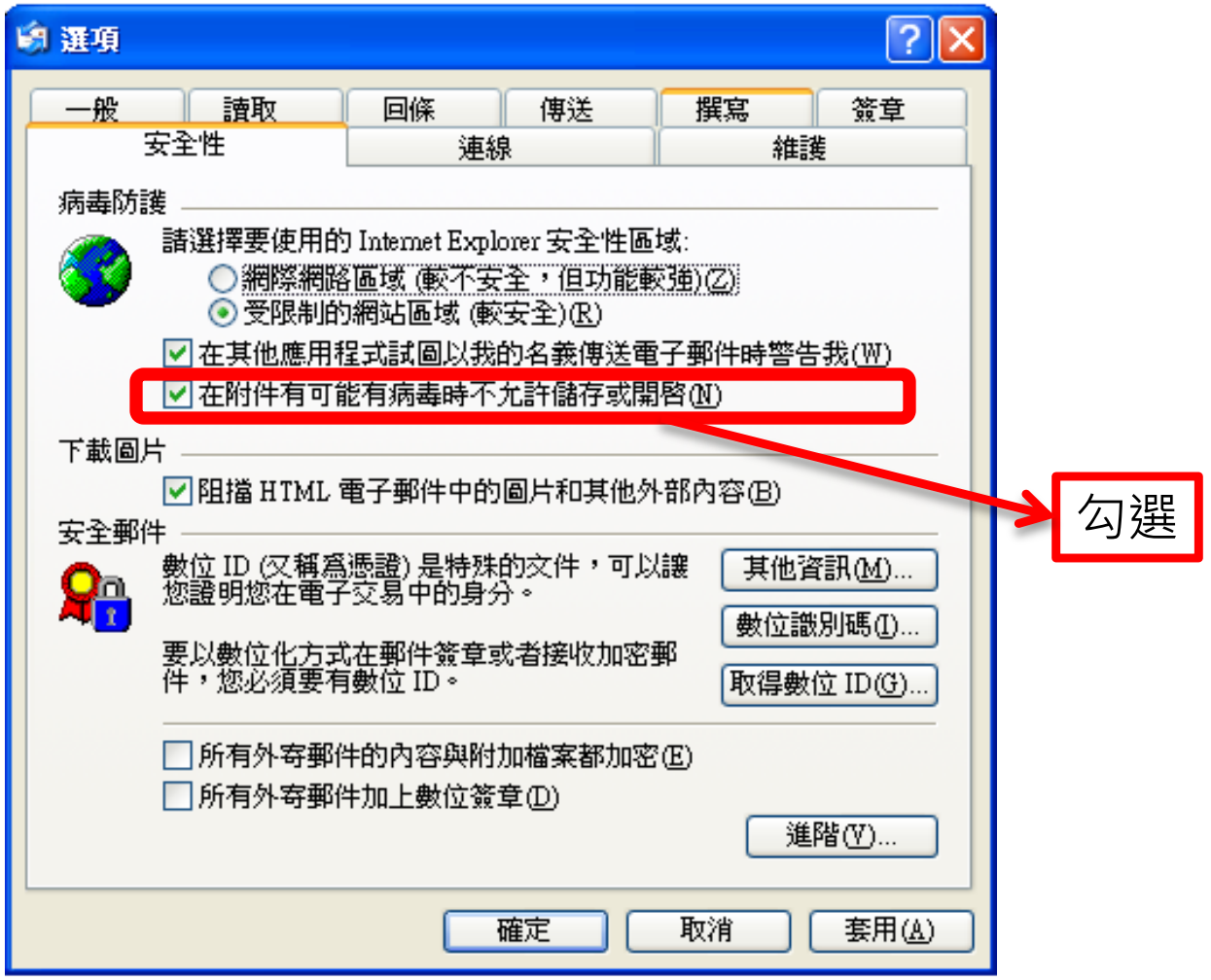
4.收信軟體安全性設定-受限制的網站區域



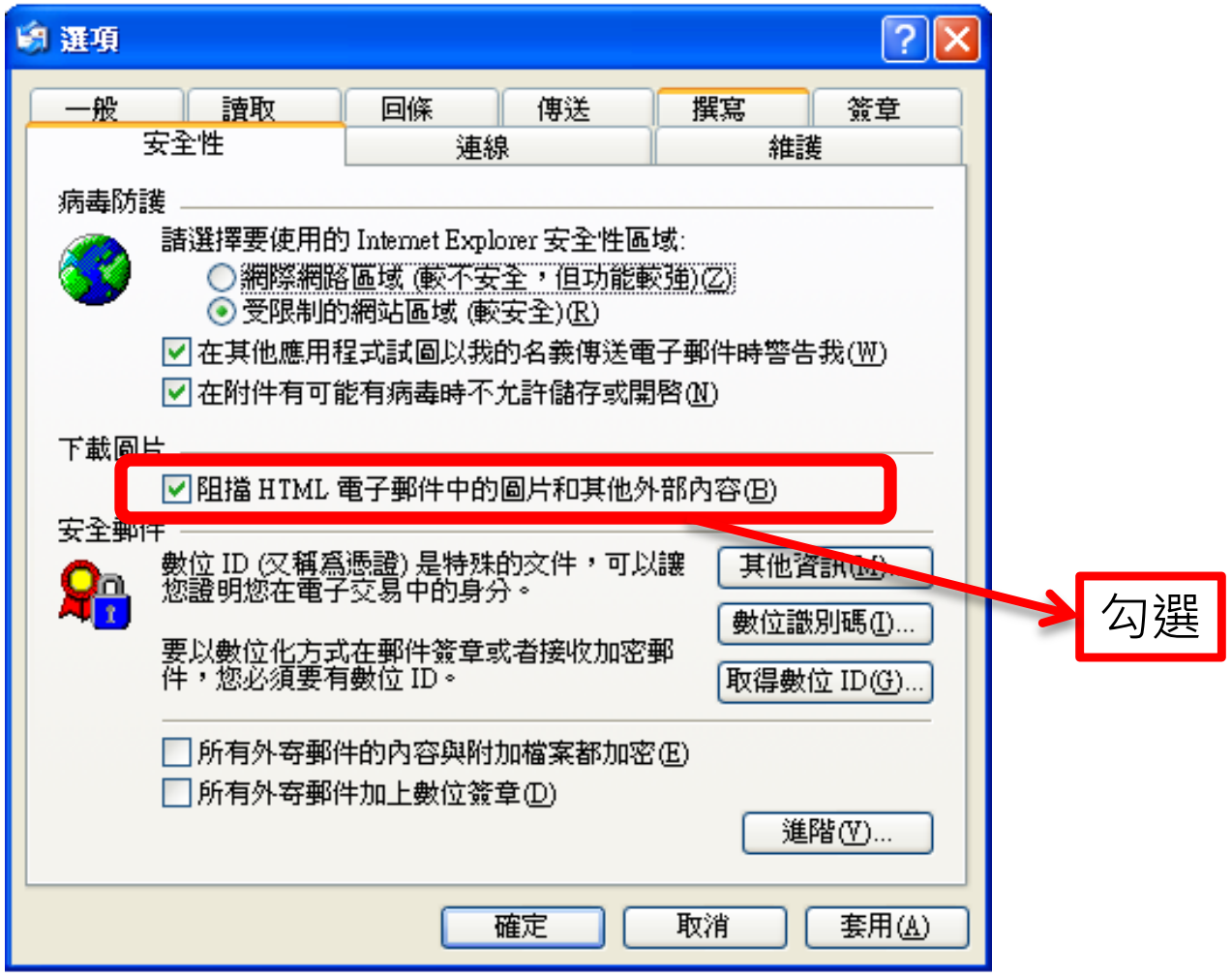
5.收信軟體安全性設定-在其他應用程式試圖以我的名義傳送電子郵件時警告我



6.收信軟體安全性設定-
在附件有可能有病毒時不允許儲存或開啟



7.收信軟體安全性設定-
阻擋HTML電子郵件中的圖片和其他外部內容



使用外部信箱安全建議


Yahoo!奇摩關心您的網路安全
・被假頁面騙了！我的帳號有危險？！
・有人假冒我的帳號賣東西騙錢。怎麼辦？
・懷疑被詐欺？！買東西已經付款卻收不到貨。
KEY
狀況一
天呀~ 我竟然登入了假冒的登入頁面，我的帳號
？！
若您發現或懷疑遇到假冒的登入頁面，請依照以下步驟指
自身安全。
警
提高警覺，請確認Yahoo!奇摩登入頁面。
改
若還能登入Yahoo!奇摩，請立即修改密碼 。
通
通知Yahoo!奇摩客服。
聽
聽從Yahoo!奇摩客服說明處理。

使用外部信箱安全檢測


Gmail - 設定 - Windows Internet Explorer
撰寫郵件
收件匣
星號標記
即時通訊
寄件備份
草稿
所有郵件
垃圾郵件
垃圾桶
通訊錄
Benny Lin
搜尋、新增或邀請
標籤
編輯標籤
邀請朋友
將 Gmail 介紹給：
傳送邀請 剩餘 50 個
預覽邀請
設定
一般 帳戶 標籤 篩選器 轉寄和 POP/IMAP 即時通訊 Web 剪輯 背景主題
轉寄：
停用轉寄
轉寄內收郵件的副本給 電子郵件地址 和 在收件匣保留 Gmail 的副本
提示：您也可以建立篩選器，只轉寄部份郵件。
POP 下載：
瞭解更多資訊
1. 狀態：針對 2007/5/16 起送達的所有郵件啟用 POP 功能
對所有郵件啟用 POP 功能 (包括已經下載的郵件)
對現在起所收到的郵件啟用 POP
停用 POP
2. 當郵件以 POP 存取後
3. 設定電子郵件用戶端 (例如
設定指示
IMAP 存取：
(使用 IMAP 從其他用戶端存取 Gmail)
瞭解更多資訊
1. 狀態：已啟用 IMAP
啟用 IMAP
停用 IMAP
2. 設定電子郵件用戶端 (例如 Outlook、Thunderbird、iPhone)
設定指示
儲存變更 取消
檢查轉寄功能是否被開啟或是轉寄到自己不認識電子郵件帳號
完成
網際網路
100%

防騙停看聽

停	安裝防毒軟體，確實更新病毒碼 關閉信件自動下載圖片及其他內容 以純文字模式開啟信件 取消信件預覽功能 設定過濾垃圾郵件機制
看	信件是否來自政府單位(gov.tw)或教育單位(edu.tw) 標題或內容是否與本身業務相關 其餘信件應視為垃圾郵件
聽	透過電話向對方確認信件真偽 透過電子郵件再次確認

Case Study

HBGary Company Inc.

軟體使用的個資防護

即時通訊軟體
P2P軟體
USB隨身碟
軟體修補
清除、救援、銷毀個人資料

即時通訊軟體：訊息加密程式

- MSN 訊息加密程式
- 程式名稱：MSN Shell
- 下載網址：http://my.msnshell.com
- 程式名稱：SimpLite for MSN Messenger
- 下載網址：http://www.secway.fr/us/products/simplite_msn/getsimp.php

- Yahoo訊息加密程式
- 程式名稱：SimpLite for Yahoo! Messenger
- 下載網址：http://www.secway.fr/us/products/simplite_yahoo/getsimp.php

- 註：以上這些軟體僅適用裝在家用電腦，不適合裝在「辦公室」的環境中。

即時通訊軟體的注意事項

- 最好不使用，如果要使用請記得：
  - 不要隨便接收檔案
  - 不要隨便點選網址
  - 注意訊息傳輸的加密
  - 以及落實掃毒的程序

- 即時通訊軟體也需要經常更新，來避免遭受攻擊。

- MSN更新： http://get.live.com/zh-cht-tw/messenger/overview
- 即時通更新： http://tw.messenger.yahoo.com
- Google Talk更新： http://www.google.com/talk/intl/zh-TW

P2P軟體

- P2P軟體下載已經漸漸取代傳統FTP檔案功能，使得一些地下管道，在頻寬不夠之下漸漸採用點對點分享。(一般稱呼使用P2P下載稱為「養動物」)

- 常用軟體名稱：電驢(eMule)、BT、FOXY、GoGobox

- 為什麼P2P軟體大家都要「禁用」？
- P2P技術現在被濫用於下載有版權的音樂、影片、程式等，做為非法的網路傳輸。且這些經不當管道取得的檔案，對內常發現挾帶病毒與木馬程式、對外常因使用者設定不正確「被動外洩個資與機密文件」。

P2P軟體的注意事項

- 辦公室電腦：禁用。
- 家用電腦：最好不使用、不使用、不使用，是最保險的方法。
- 如果不小心使用請記得：
  - 請設定好分享的目錄(上傳區跟下載區)。
  - 請設定好分享的權限。
  - 請設定好分享的網路頻寬。
  - 每個下載檔案(音樂、影片、檔案等)均要掃毒後才開啟。

- P2P軟體也需要經常更新，來避免遭受攻擊。

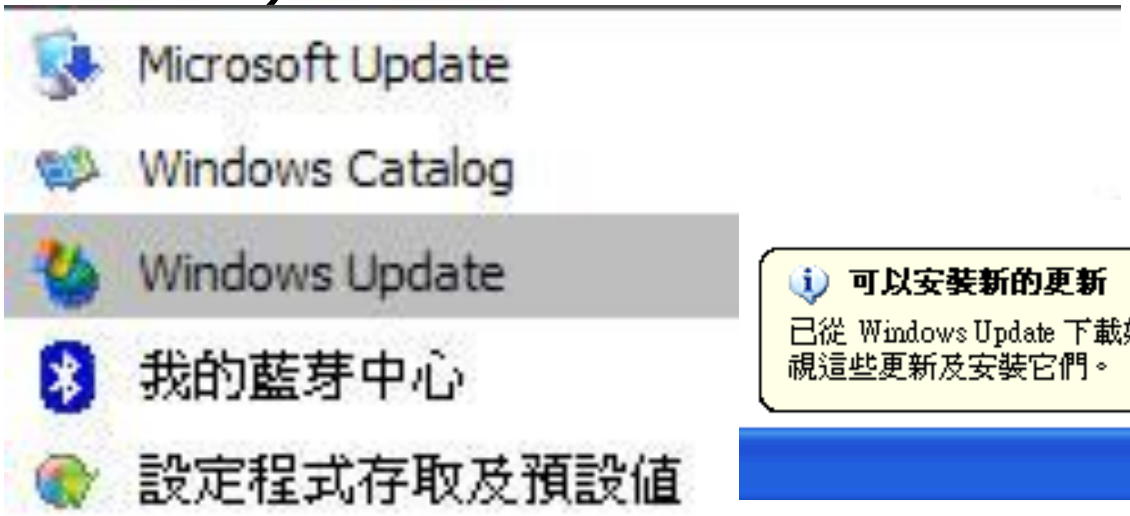
USB隨身碟使用注意事項

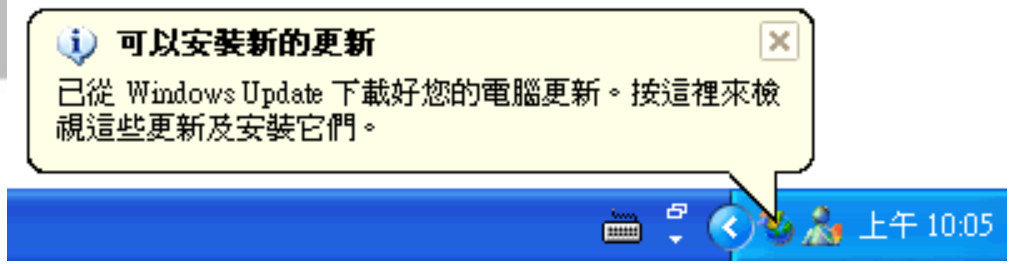
- 隨意將由「網路上下載」或「郵件的附件檔」COPY至隨身碟(大拇哥)中，易造成辦公場所與家用電腦『交互感染病毒與木馬程式』。
- 請搭配防毒軟體掃描隨身碟內的檔案。

軟體修補

- Windows Update (僅更新作業系統本身的漏洞)
- Microsoft Update (會更新Office及所有微軟產品)

- IE 7 or IE 8
- XP SP3
- Adobe Reader
- 壓縮軟體
- 音樂播放軟體





Windows XP Service Pack 3(XP SP3)

- Microsoft 發行 Windows XP 的更新程式，其中會包含在這5年中發行的所有修正程式和增強功能。這些更新程式 (稱為 Service Pack) 提供了方便、全部合一的方式，以存取最新的驅動程式、工具、安全性更新程式、修補程式以及客戶要求的產品變更等。

- 官方下載：Windows XP Service Pack 3 網路安裝套件 (適用於 IT 專業人員與開發人員)
- http://www.microsoft.com/taiwan/download/windows.htm

- 註： 320.9 MB

清除、救援、銷毀個人資料

- 手工清除個人資料
- CCleaner 資料清除軟體
- Recuva 檔案救援軟體
- File Shredder 檔案銷毀軟體

CCleaner 資料清除軟體

- 官方下載：
- http://www.ccleaner.com

- 功能：
- 刪除Cookies，保護隱私。也可以自訂清理時不要刪除的Cookies。

- [清道夫] 功能針對網路瀏覽器、系統記錄檔、系統暫存檔、系統垃圾檔、和各種應用程式的無用檔案進行清潔的工作。有效增加硬碟空間，避免垃圾檔案影響硬碟效率。

- [登錄檔] 清理功能可以有效刪除無用的登錄資料，保持電腦的穩定性與執行效率。如果你發生因登錄檔錯誤而造成不能安裝某些軟體的狀況時，到這裡清潔一下，有時候問題就解決了。

Recuva 檔案救援軟體

- 官方下載：
- http://www.recuva.com

- 功能：
- 每個檔案儲存在硬碟時都會占據一個位置，當你在硬碟刪除檔案後，其實檔案的痕跡還是會遺留在原本的磁區上，只要這個磁區位置還沒有被新的檔案占去，那麼妳就有機會救回誤刪的檔案。而「Recuva」正是利用了這個原理，幫你去掃描、搶救已經刪除的檔案（已經從資源回收桶中移除、或直接刪除的檔案），而從其原理來看，一個很重要的前提是，Recuva 通常只能救回最近刪除的檔案，當你發現不小心誤刪了某個檔案時，不要去進行其它操作，立刻搶救檔案比較有效。

正常使用：

- 搶救硬碟內誤刪資料。
- 搶救隨身碟內的誤刪資料。
- 搶救記憶卡內的誤刪資料。

異常使用：

- 竊取硬碟內誤刪資料。 (維修時？)
- 竊取隨身碟內的誤刪資料。 (COPY資料時？)
- 竊取記憶卡內的誤刪資料。 (沖洗照片時？)

File Shredder 檔案銷毀軟體

- 官方下載：
- http://www.fileshredder.org

- 功能：
- 是一套免付費的軟體，檔案大小約1.15MB，安裝便利、操作也很簡單。安裝只要利用加入檔案或資料匣的方式，選擇要完全清除的檔案或資料匣。

- 這套軟體具備5種不同的檔案覆寫等級，包含簡單的單次與兩次複寫，以及合乎美國國防部標準的「DoD 5220-22.M」，或是7次複寫的「NSA」與35次複寫的最高粉碎等級「Guttman」。

- 不僅可以銷毀單一檔案或資料夾，也可清除無用檔案，騰出硬碟空間。

清除、救援、銷毀個人資料的注意事項

- 使用這些軟體可以有效清除在「家用電腦」上，所存放的個人資料。如果是「辦公室電腦」則需參考資訊安全政策的規定。
- 但如果個人資料是放在相簿網站、購物網站、交友網站上，則這些軟體是清除不到的，所以仍然需要注意上網、收發信件的個資安全。
- 使用「資料銷毀軟體」時請特別留意，因為如果被拿來惡作劇，是沒有藥可以救的。

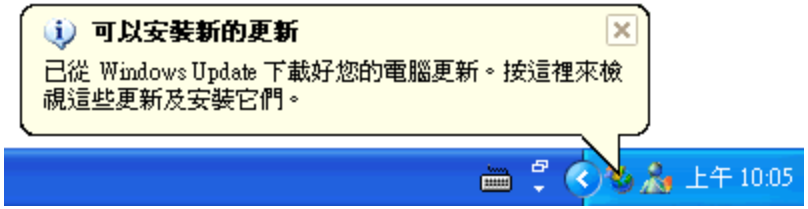
常用工具：檔案偵測(免費)

- Microsoft TechNet Windows Sysinternals
- http://www.microsoft.com/taiwan/technet/sysinternals/default.mspx

- Process Explorer for Windows v10.21
- http://www.microsoft.com/taiwan/technet/sysinternals/Security/ProcessExplorer.mspx

電腦安全性的七大步驟

1. 評估使用電腦的風險，隨時提高警覺不要亂點選
2. 使用防毒軟體及防間諜軟體，並搭配線上掃毒
3. 保持更新作業系統及應用程式等軟體為最新狀態
4. 檢查您的作業系統及IE安全性設定
5. 使用個人(單機)防火牆
6. 建立穩固的密碼
7. 執行日常工作安全性維護，例如：更新、掃毒



CA Hack

Comobo CA
DigiNotar CA

Case Study

你躲過Lizamoon了嗎??

結論

- 上網行為個資防護
- 郵件社交工程防護
- 軟體使用個資防護

問題 與 討論