

資訊安全宣導 電子郵件安全簡介

資訊安全管理系統顧問 洪嘉駿

諮詢 輔導 訓練 稽核 . 永續營運

大綱



電子郵件社交工程簡介

電子郵件社交工程攻擊手法

預防電子郵件社交工程攻擊

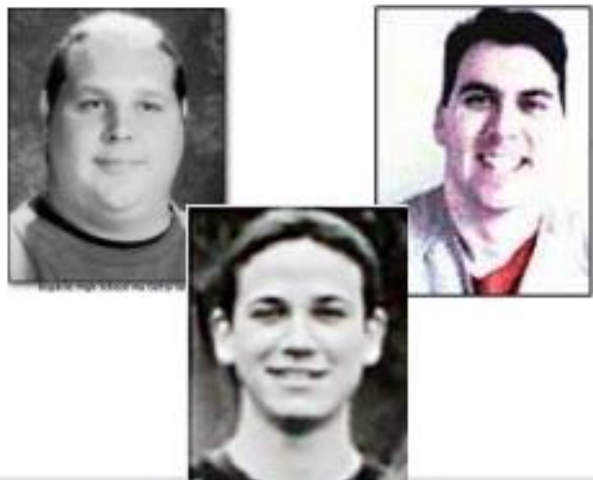
名 vs. 利 – 病毒作者動機今昔大不同

過去的犯罪者

- 介於**14至34**歲的男性
- 對電腦狂熱
- 單身、宅男
- 證明自身之電腦能力

今天的犯罪者

- 利用殭屍網路
- 竊盜他人之機密資料、帳戶密碼
- 擾亂金融、通訊系統
- 特定政治立場



惡意攻擊方式今昔大不同

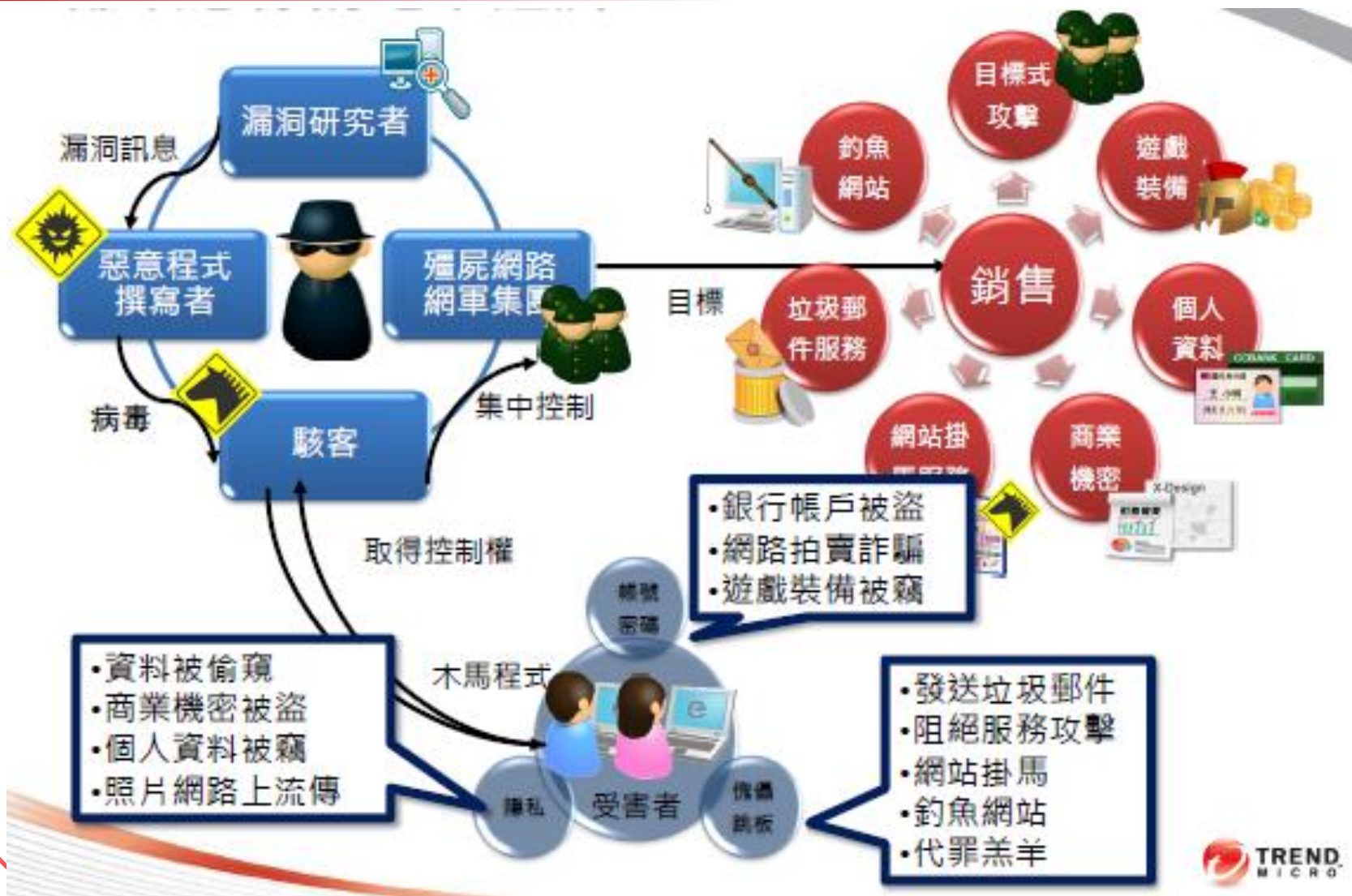
過去的攻擊

- 毀損資料
- 癱瘓個人電腦(如蠕蟲病毒)
- 癱瘓內部網路

現在的攻擊

- 竊取機密資料
- 加密個人資料進行勒索
- 將個人電腦做為跳板
- 將個人電腦作為殭屍電腦
- 癱瘓外部網路(DDoS)

難以想像的地下經濟



網路上釣什麼魚？

- 密碼
- 銀行帳號
- 提款卡、信用卡號碼
- 信用卡認證碼
- 電話號碼、住址
-

攻擊現象之竊取個人隱私

駭客入侵拍女子裸照 PO她部落格嗆聲

【記者黃良傑／屏東報導】還在連線的電腦不要亂放，並時常留意鏡頭有無不正常開機，因為駭客就在你身邊，小心全裸被偷拍還不自知！

男大學生扮駭客炫耀

新竹縣21歲曾姓男大學生扮駭客，侵入屏東縣

動開啟、式」，再隨上的攝電放在床動攝影機曾某窺見房內的私密談話與活動。

曾姓大學生只為證實自己可炒熟別人部落格的能耐，竟惡作劇地把陳女全裸影像，PO到陳女自己的部落格上，供不特定人進入瀏覽。4月13日晚，陳女進入雅虎奇摩網站自己的部落格，驚見自己出浴的裸體畫面，嚇得花容失色。



**駭客種入殭屍病毒後
遠端遙控開啟電腦上的攝影機並上傳**



攻擊現象之竊取虛擬貨幣



駭客入侵某單位主機， 作為跳板盜取受害者的帳號

線上遊戲的玩家，2008/6/18他玩遊戲玩到一半，卻莫名被踢下線，他嘗試重新登入，連續10幾分鐘都無法登入，等到再度順利登入上線，發現有20幾項寶物已不見，估計價值台幣7、8萬元。

攻擊現象之網路勒索

網路勒索新手法：不付錢就刪除你的硬碟資料？！

作者：編輯部 -01/03/2013



網路勒索存在已久，最近歹徒又想出新手法，向受害者宣稱不付款就會刪除電腦硬碟中的資料，不過安全公司指稱這只是歹徒的威脅話術，讓受害者處於壓力和恐懼的情況下，以達到詐騙金額的目的，實際上該勒索軟體並不具備刪除資料的功能。

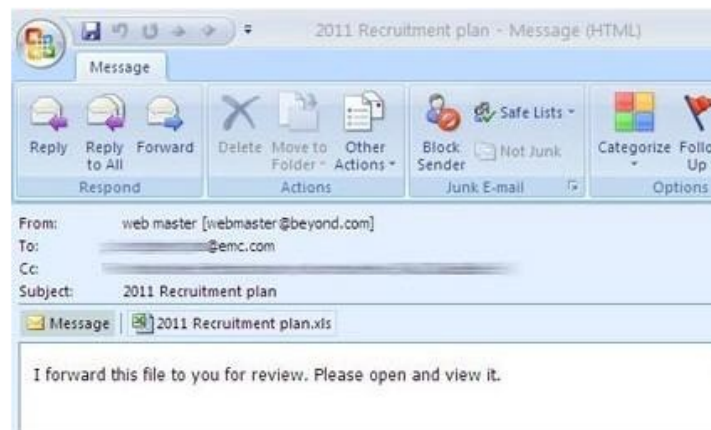
近來資安公司發現一款最新的Ransomlock木馬變種程式，會向受害者勒索現金，還宣稱如果不付款的話就會刪除你電腦中的資料，賽門鐵克(Symantec)將之稱為Trojan.Ransomlock.G，其他防毒廠商則稱之為Reveton。

一旦電腦感染木馬程式Trojan.Ransomlock.G，螢幕上就會顯示一段訊息：「如果你試圖自行解開你的電腦，將會導致你的作業系統完全格式化，電腦中所有的檔案、影片、照片、文件都將被刪除。」此外，相較之前的版本，這款新的變種病毒還把勒索金額從200元美金提高到300美金，並設下48小時的付款期限。

駭客運用社交工程電子郵件或偽冒身分電子郵件侵入個人電腦，使用者不慎開啟夾帶惡意(後門)程式附件檔，隨時洩露機敏機料。機關同仁不當上網，無意間下載惡意軟體或後門程式。

· 2011 年 3 月 – RSA :

歹徒寄了兩封標題為「2011 Recruitment Plan」（2011 年度徵才計畫）的信件給員工。這兩封信件實為網路釣魚 (Phishing)，引發了後續的資料外洩事件。□




RSA APT 事件中的網路釣魚 (Phishing) □

· 2011 年 4 月 – 洛克希德馬丁：

在 RSA 遭到攻擊後隔月，駭客以從 RSA 竊得的 SecureID 通過身分認證，侵入武器製造商洛克希德馬丁。

05 七月, 2013 14:58

冒用健保局名義, 攻擊中小企業案, 使用惡名昭彰的Ghost遠端存取木馬
由 TrendLabs 資安趨勢 發表於 [APT攻擊/APT 進階持續性威脅 (Advanced Persistent Threat, APT)]
(414) 閱讀, (0) 引用, (0) 回應,  推文 (0)

Follow Us on:



 有 1 個人覺得讚。趕快註冊來看看朋友對哪些內容按讚。

作者: Maharlito Aquino (威脅研究員)

從逮捕勒索軟體集團的首腦之一, 到成功打下Rove Digital(請參考:趨勢科技協助 FBI 破獲史上最大殭屍網路始末), 我們可以時常地看到執法單位和安全廠商間的合作行動, 並且有著豐碩的成果。這一次, 台灣刑事單位和趨勢科技合作偵破駭客假冒健保局, 盜取萬筆中小企業個資案件, 解決利用知名的Ghost遠端存取木馬家族所進行的APT-進階持續性滲透攻擊(Advanced Persistent Threat, APT)目標攻擊。執法單位也逮捕了一名對象。



BKDR_GHOST (又名Ghost遠端存取木馬或TROJ_GHOST), 是有名的遠端存取木馬 (RAT), 常常被用在目標攻擊, 也被資安威脅份子和網路犯罪分子廣泛的使用。

在這起目標攻擊內, 攻擊者透過特製的魚叉式網路釣魚 (Phishing) 電子郵件將BKDR_GHOST派送給不知情的目標。上述郵件包含一個會去自動下載該惡意軟體的連結。而且它會偽裝成健保局的來信, 好產生足夠的說服力來吸引目標點入並執行這惡意軟體。

為了避免被偵測, 攻擊者將這些電子郵件設計成為包含一個連結, 將使用者導到一特定網站, 並自動下載看起來是官方檔案的RAR壓縮檔。此外, 為了進一步讓使用者願意去打開壓縮檔內的檔案, 攻擊者利用了一個舊卻有效的文件命名詭計, 將多個空格加到文件副檔名 (在這案例內是DOC) 和可執行副檔名 (在這案例內是EXE) 之間。這方法還是很有效, 多個空格會將真正的副檔名隱藏起來。因為壓縮檔視窗並不大, 趨勢科技的威脅解決方案可以利用ATSE 9.740.1046來將利用這種伎倆的惡意軟體偵測為HEUR_NAMETRICK.A。

南海升溫 越陸駭客也開戰

2014-05-13 中央社 中央社河內13日電

越南與中國大陸南海地區主權之爭越演越烈之際，兩國駭客先在網路上開戰。越南駭客為抗議中方在南海架設鑽油平台，攻擊多個大陸政府網站，大陸駭客則入侵數百個越南網站回擊。

越南媒體今天報導，統計顯示，截至目前為止已有超過**220**個越南政府機關和企業的網站遭自稱來自大陸的駭客入侵，駭客將五星旗放上首頁中央，並留下攻擊原因起源於兩國南海衝突的留言內容。

越南網路安全專家表示，遭到大陸駭客攻擊的主要是地方政府與小型企業的網站，網站安全系統具有漏洞，容易被駭客攻入。他說，越南網站這次遭到駭客攻擊，未造成嚴重後果，但是他建議，越南網站管理者應重新檢查安全系統，以免再度遭到駭客攻擊。

中國大陸近日在南海海域架設鑽油平台探勘石油，引起越中船隻對峙事件，導致兩國關係陷入緊張。越南當局指責中方此舉違反聯合國海洋法公約等國際法並侵犯越南主權。

雙方過去曾經因南海爭議問題而多次發生駭客網路上互相攻擊的類似情況。

南韓事件

- 爆發時間：2013/3/02下午2點
- 範圍
 - 6家企業約32000台主機中斷服務，無法啟動
 - 金融業
 - 新韓銀行(Shinhan Bank)
 - 農協銀行(NongHyup Bank)
 - 濟州銀行(Jeju Bank)
 - 媒體業
 - 韓國放送公社(KBS)
 - 文化廣播(MBC)
 - 南韓新聞頻道(YTN)
- 衝擊
 - 營運中斷
 - 金融業: ATM、臨櫃交易、線上交易全面停擺
 - 媒體業：節目無法播出，對外網站無法運站
 - 由於植入自我毀滅性惡意程式，系統檔案被損毀，電腦主機及伺服器無法開機，導致儲存資料無法還原




Google極光行動：內網桌機 首遭入侵

- 在Google極光行動資安事件中，首遭入侵的不是外部主機，而是內網桌機。當時Google員工瀏覽某含有惡意程式的網站，該頁面載入有shellcode的JavaScript程式碼會造成IE瀏覽器溢位，進而執行FTP下載程式，並從遠端進一步抓了更多新的程式來執行（其中部分程式的編譯環境路徑名稱帶有Aurora字樣，攻擊方以此命名專案），隨後以SSL加密通道與遠端攻擊方進行互動，監聽竊取該機器登入Google伺服器的帳號密碼等資訊，自此成功滲透竊取部分智財與重要人士帳戶。

數十年來始終不變

行政院：中國網軍資訊操演 警政署等部會遭入侵

2003/09/03 12:41  Video



網路駭客開戰？機關企業防恐攻擊

記者朱蒲青／台北報導

行政院政務委員蔡清彥3日在院會中提出臨時提案表示，包括警政署在內的政府部會，最近遭到中國網軍入侵，駭客利用「木馬程式」有計畫在政府部會資訊佈建，伺機發動攻擊，這是一

種資訊戰的操演。游揆相當重視這項訊息，要求5日之前各部會匯報遭入侵情形給「國家資通單位」進行修復，若發現網站遭入侵卻未通報，將依情節懲處。

政院發言人林佳龍說，國家資訊通報單位最近查獲警政署等數十個部會被駭客入侵，經追查發現，駭客來自中國某個網站，他們入侵台灣的方式，包括利用民間公司運用這個管道然後入侵政府部會網站。

數十年來始終不變

大陸網軍入侵 海巡署3,000機密外洩

2012-07-06 07:11 | 新聞速報 | 【報導／戴志揚】



海巡署日前發生遭到中共網軍攻破網路防火牆竊取機密資料的嚴重資安事件，本刊獨家掌握，列為情治機構的海巡署情報處伺服器遭到網軍攻擊，造成

在此同時，海巡署也首次發生情報處遭惡意程式侵入，並陸續將情報處存放於伺服器內的機密資料竊取的重大資安事件，遭竊的機密文書高達三千件以上，這也是海巡署成立十一年來首次遭到駭客大舉攻擊。

海巡署人員透露，時序才剛進入六月，海巡署通資部門機房工程師，突然自電腦上收到重要警訊，顯示有惡意程式正潛伏在伺服器內，四處流竄尋找弱點攻擊，而且發現有內部資料不斷流出。

資訊安全部門的人員立刻進行搜尋，果然在情報處的伺服器內，發現有一筆資料已經打包好，並緩緩地流出。資安人員見狀大為緊張，立刻將網路封鎖阻止資料外流。

憂的是，連國安局相關面對中國網軍攻

中國網軍對我政兵，尤其歷次總統及惡意程式攻擊我逐年增加。

根據國安內部資料顯示，中國網軍的數目至少接近十萬人，每天針對全球政府及企業進行二十四小時攻擊，台灣正是其中的一個主要重要目標。

數十年來始終不變

法務部遭駭 重大案件機密恐外洩 【2012/9/19 11:50】

Ads by Google

最殺遊戲徵才，16歲可申請 www.lccnet.com.tw

遊戲公司徵才培訓，挑戰月薪3-6萬 夠熱血，會一點電腦，請立即接受挑戰！

〔本報訊〕週刊爆料，中國網軍駭客日前「駭」進法務部的「一審辦案系統」，近期重大案件恐遭竊取，而法務部證實，資訊處曾被駭客入侵，對於電腦遭駭，自嘆「技不如人」，引發網友抨擊，直言「懲處咧？預防再發咧？」

壹週刊報導，法務部內部一審辦案系統遭中國駭客入侵，時間長達2個月，期間前鬧得沸沸揚揚的案件，包括總統陳水扁獄中健檢報告、行政院前祕書長林益世涉貪案，甚至是富少李宗瑞涉性愛照片案的被害人個資等，恐已被竊取，機密外洩；對此，法務部表示，內部資訊處的電腦曾遭駭，對於中國駭客能輕易破解防毒軟體與程式，表示「技不如人」。

此話一出，引起網友討論，罵聲連連，有人痛批「網安不如人，竟然還可任意放任連接網路，真是有夠害啦！（台語）」有人則猜測「內神通外鬼的可能性比較高」，調侃是「故意被駭」，要法務部「別再推給電腦」，還有人質疑「一句技不如人就可以帶過？」直言「懲處咧？預防再發咧？」

駭客攻擊對象 台灣居世界之冠



作者：記者林政忠/台北報導 | 聯合新聞網 – 2013年3月25日 上午2:33

字 字

南韓日前遭到駭客惡意攻擊，大型電視台和銀行的電腦網路同時癱瘓，連美國第一夫人蜜雪兒個人資料也驚傳外洩。資安相關官員透露，駭客攻擊活動最頻繁的國家，台灣排行全世界之冠，從軍事、政治乃至金融商業，已籠罩著「駭客危機」。

駭客動一動滑鼠，癱瘓城市網路或盜取金融鉅款，不再是電影或小說的虛構情節。資安問題已達國安層級，美國國防部去年宣布，如果偵測到網路攻擊的立即威脅，美國軍隊可以傳統飛彈反擊，不惜發動實體戰爭。

資安專家透露，台灣是駭客攻擊活動最頻繁的國家，勝過美國、香港、中國大陸，主因是「多數駭客來自對岸」；行政院日前召集內部資安會議，對於部分行政機關、駐外單位都曾「淪陷」，府院高層大感震驚。

駭客攻擊可分為三種等級：一般是「大眾性攻擊」，例如竊取帳號、密碼。其次是「目標式攻擊」，針對公司企業的金錢或一般資料。最高等級是「進階性永久攻擊」，竊取政府機密或企業的智慧財產權。

資安官員指出，組織型駭客對國安、兩岸、金融稅務資料最感興趣，但總統府、國安會、陸委會、財政部的資安是最高防密等級，駭客多採取「迂迴突破」，攻擊駐外使館、地方政府、學校民間單位等「脆弱點」，被突破的情形超乎預料。

承認吧，在座各位是目標

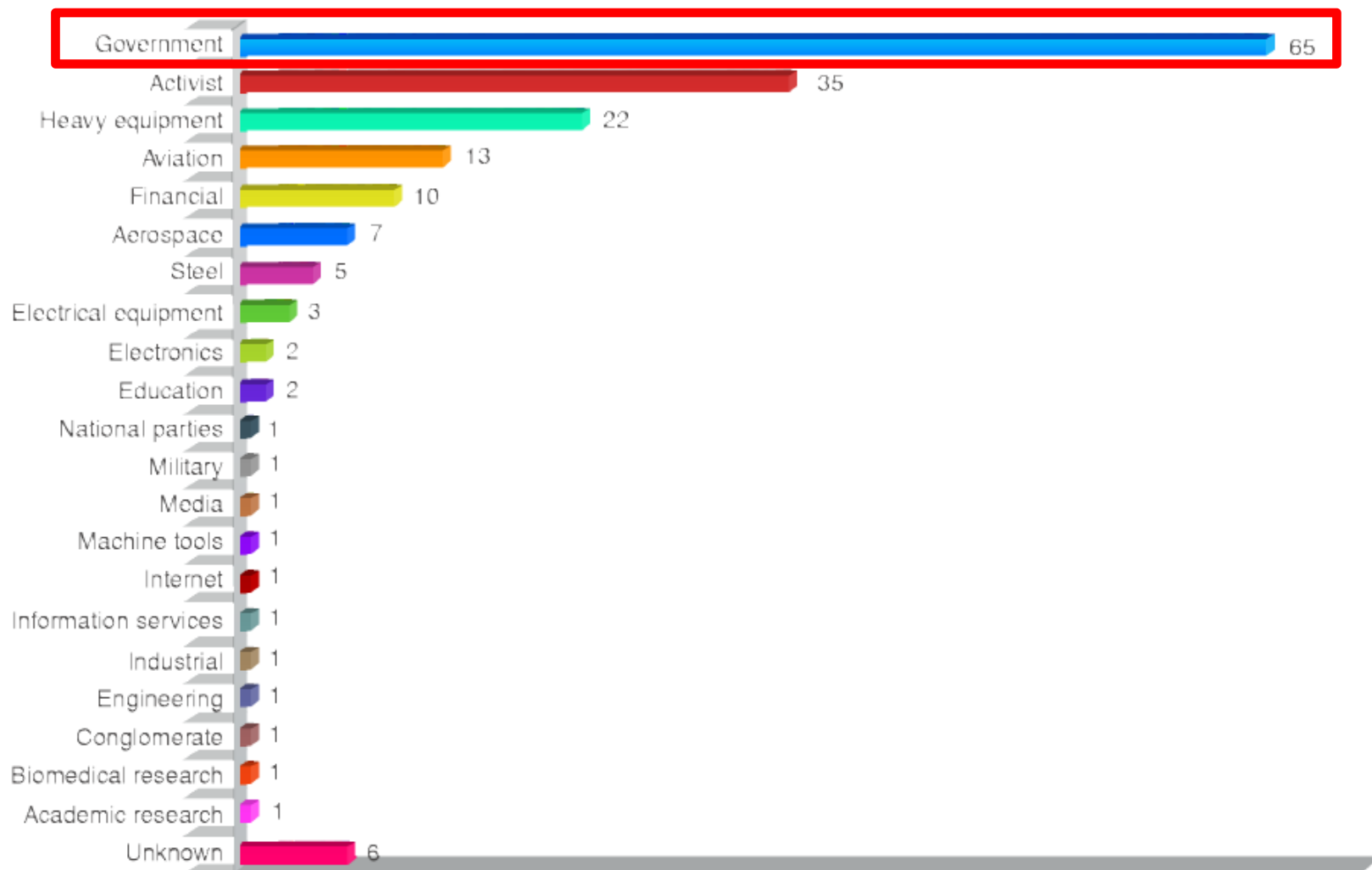


Figure 1. Breakdown of C&C servers by country

總算有人打開潘朵拉盒子了！

蔡得勝：我們的個資可能都被竊了！



康仁俊

2013年3月20日 12:15

8.7 萬

26

3

f 讚

f 推薦

g +1

記者康仁俊／台北報導

國安局長蔡得勝今（20）日坦承，中共網駭對台灣的傷害相當嚴重，甚至可以用個資做交叉分析，同時中共目前已經從竊取軍情資料，轉向蒐集高科技及商業機密，「我們的個資可能都已經被竊了！」

蔡得勝今日在立法院國防委員會答覆國民黨立委林郁方質詢時表示，中共網駭問題



國安局長蔡得勝表示，中共網駭問題嚴重，「我們的個資可能都被竊了！」（圖：記者康仁俊攝）

每天的網路行為

- 開機
- 點選網頁
- 打開電子郵件
- 文書處理
- 遊戲
- 影片、音樂
-

什麼是社交工程

- 社交工程是利用**人性的弱點**進行詐騙，是一種**非「全面」技術性**的資訊安全攻擊方式，藉由人際關係的**互動**進行犯罪行為。
- 以人為本
- 手法萬萬種
- 技術門檻較低

這個也是社交工程

大綱



電子郵件社交工程簡介

電子郵件社交工程攻擊手法

預防電子郵件社交工程攻擊

社交工程電子郵件攻擊流程

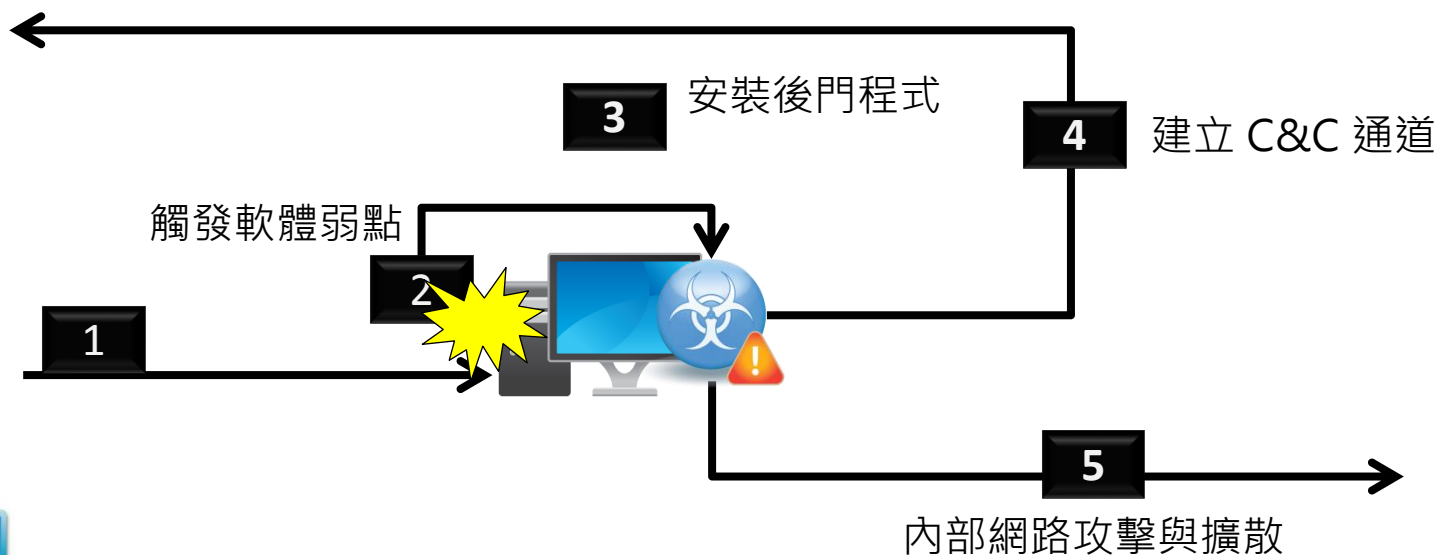
攻擊階段

控制階段

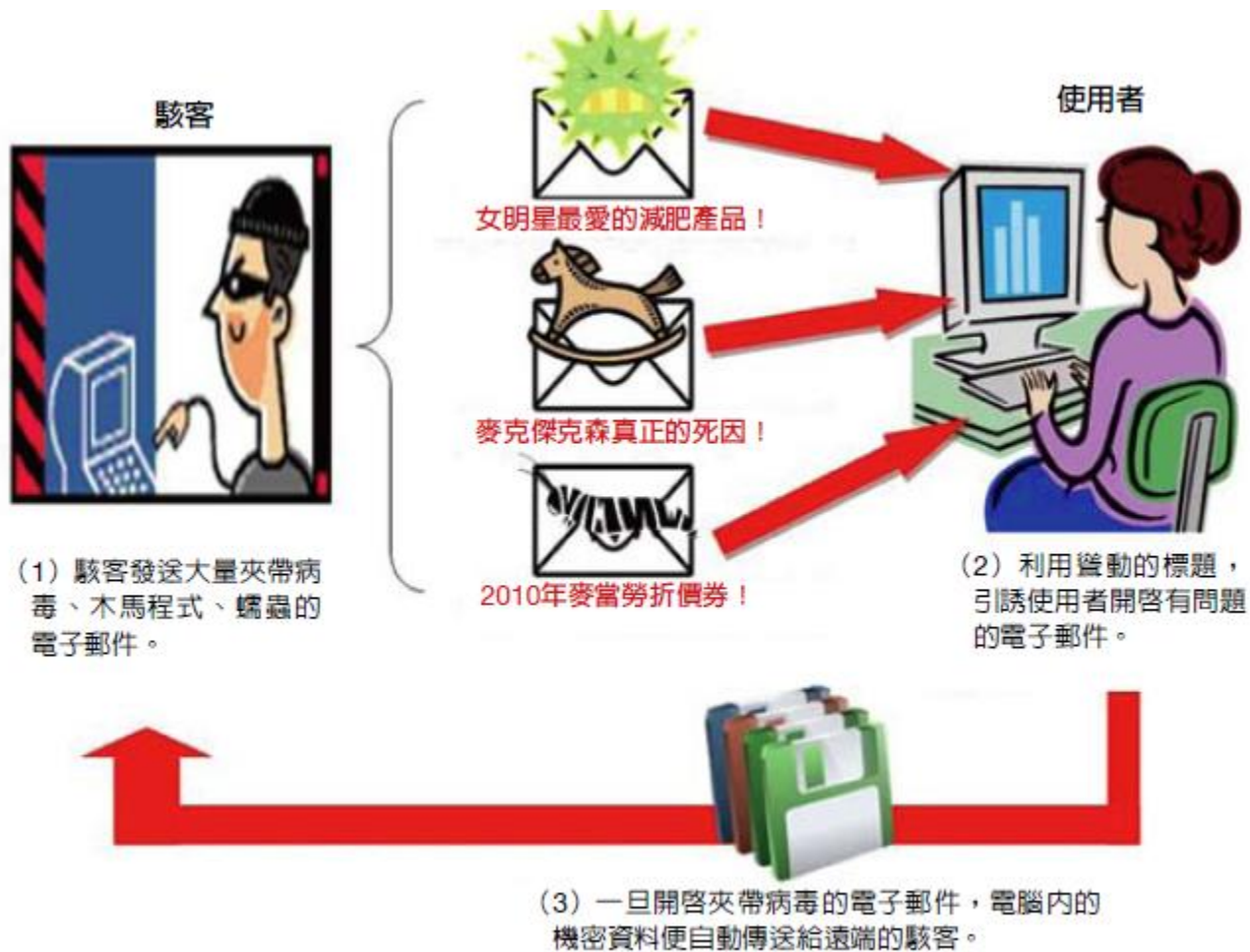
活動與擴散階段



夾帶惡意附件的
社交工程信件



電子郵件社交工程



社交工程可應用之弱點

- 好奇心
- 貪念
- 助人的天性

社交工程常應用之題材

- 政治
- 色情
- 休閒
- 贈品、抽獎
- 新聞事件

廣告-折價券

肯德基折價券 - 郵件 (HTML)

郵件 增益集 Adobe PDF

回應 動作 垃圾郵件 選項 尋找

寄件者: admin [admin@mcdonalds.com.tw] 寄件日期: 2009/9/11 (星期五) 下午 01:04
 收件者: benny
 副本:
 主旨: 肯德基折價券

山胡椒木 煙燻蜜汁 烤雞腿

超省自由配 一個網板有找

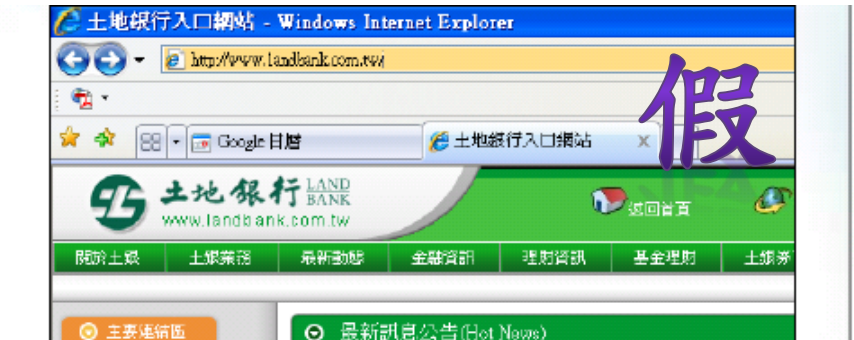
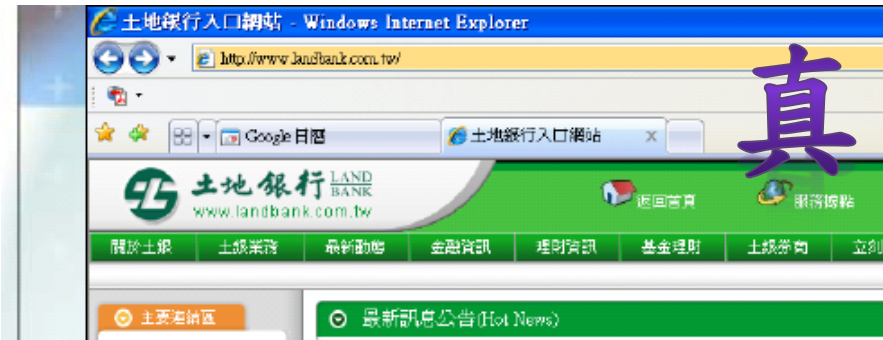
四種貨品 \$169 原價 \$46

列印優惠券 轉寄好友

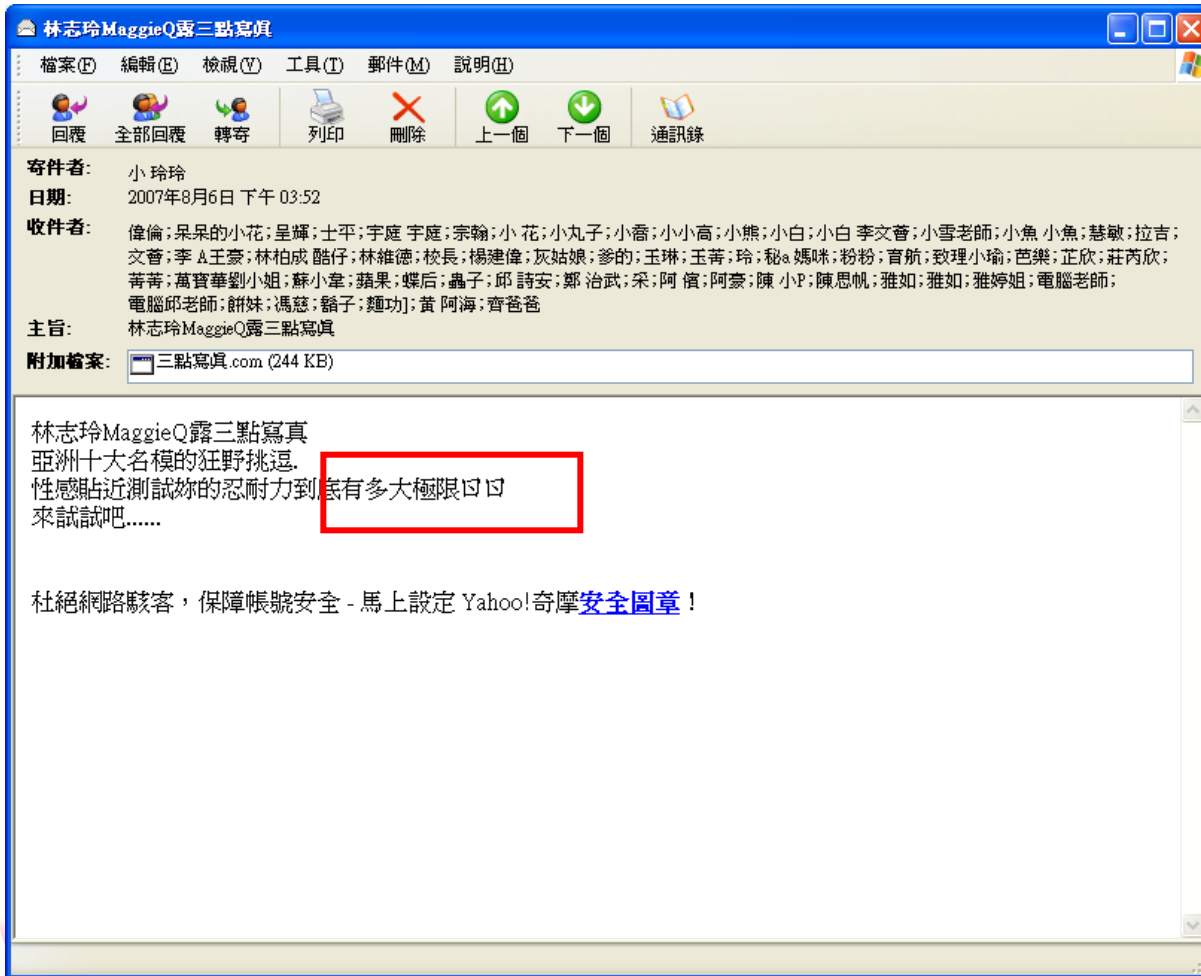
*本優惠券不得與外送優惠服務同時使用, 彩色與黑白列印皆適用
 *炸雞恕不開放選擇部位

<p>肯德基早餐 三角薯餅 9-28</p> <p>\$15 原價 \$25</p> <p></p> <p>★使用期限2009/8/31-2009/11/29 ★本優惠限早餐時段使用 ★本券不適用肯德基外送服務 ★產品以餐廳供應為準, 並只限用乙次 ★本券不得與其他優惠活動同時使用 ★肯德基保有修改優惠的權利 ★僅限供應早餐的肯德基餐廳使用</p>	<p>肯德基早餐 肉鬆蛋餅捲 9-21</p> <p>\$25 原價 \$35</p> <p></p> <p>★使用期限2009/8/31-2009/11/29 ★本優惠限早餐時段使用 ★本券不適用肯德基外送服務 ★產品以餐廳供應為準, 並只限用乙次 ★本券不得與其他優惠活動同時使用 ★肯德基保有修改優惠的權利 ★僅限供應早餐的肯德基餐廳使用</p>	<p>肯德基早餐 皮蛋瘦肉粥加肉鬆 9-22</p> <p>\$35 原價 \$42</p> <p></p> <p>★使用期限2009/8/31-2009/11/29 ★本優惠限早餐時段使用 ★本券不適用肯德基外送服務 ★產品以餐廳供應為準, 並只限用乙次 ★本券不得與其他優惠活動同時使用 ★肯德基保有修改優惠的權利 ★可更換同價格鮮奶茶 ★僅限供應早餐的肯德基餐廳使用</p>	<p>肯德基早餐 金黃雙薯蛋燒餅 9-23</p> <p>\$40 原價 \$48</p> <p></p> <p>★使用期限2009/8/31-2009/11/29 ★本優惠限早餐時段使用 ★本券不適用肯德基外送服務 ★產品以餐廳供應為準, 並只限用乙次 ★本券不得與其他優惠活動同時使用 ★肯德基保有修改優惠的權利 ★可更換同價格歐式燒餅 ★僅限供應早餐的肯德基餐廳使用</p>
--	---	--	--

釣魚連結



色情郵件標題



休閒活動



The screenshot shows a web browser window with the address bar displaying "D:\mail\02-妖怪村\index.htm". The page title is "南投鹿谷鄉妖怪村". The main content of the page is a paragraph of text and a photograph. The text describes a festival held in the 7th lunar month, featuring various yōkai puppets and music. Below the text is a photograph of several people in colorful yōkai costumes (including a pink one with horns, a yellow one, a white one, and a blue one) standing in front of a traditional red torii gate. The browser interface includes standard navigation buttons and a menu bar with options like "檔案(F)", "編輯(E)", "檢視(V)", "我的最愛(A)", "工具(T)", and "說明(H)".

將在農曆七月舉辦妖怪大集合活動。日本鬼偶敲著大鼓，咚咚聲中，不同造型的妖怪也現身，隨著音樂扭腰擺臀，有時還擺出張牙舞爪的模樣，在一旁的小朋友嚇得哭出來。

[台灣，妖怪出沒？！來溪頭妖怪村 - 松林町抓妖吧！](#)



很多人會開啟觀看和熱心地轉寄...

The image shows two overlapping windows from a Windows operating system. The background window is an email client titled "安!幫忙.幫忙找人!!!". It displays the following information:

- 寄件者: 我是~豆 (/=^0^=)/
- 日期: 2008年9月22日 下午 11:22
- 收件者: [Redacted]
- 主旨: 安!幫忙.幫忙找人!!!
- 附加檔案: Pic00325.zip (272 KB)

The email body contains the following text:

安 安!
請幫忙轉寄: 不會花您太多時間, 拜託囉!!
我的愛女小彤五歲被強行抱走 !!!
警方查了幾天都沒線索 只好透過網路管道請大家幫忙了
夾帶的是相片是被抱走的前幾天照的 那天剛好是穿這身衣服
有線索的請 聯絡 0921811 [Redacted] 田為

The foreground window is WinRAR, titled "Pic00325.zip - WinRAR (evaluation copy)". It shows the contents of the ZIP archive:

Name	Size	Packed	Type
..			資料夾
彤彤.scr	332,949	270,217	螢幕保護裝置

The file "彤彤.scr" is highlighted with a red box. The status bar at the bottom of the WinRAR window indicates "Total 332,949 bytes in 1 file".

這就是結果

駭客散佈連接YouTube假網址誘使用戶中毒

中央社 (2007-08-29 23:35)

轉寄好友 列印

〈中央社記者康世人新加坡二十九日專電〉英國SophosLabs全球網路安全研究中心今天警告網路用戶，要注意駭客散佈一封提供假YouTube Video網址下載影片的電子郵件，這封電子郵件會誘使網友連接含有惡意軟體或木馬程式的網站，必須提高警惕。

SophosLabs指出，駭客組織利用最近當紅的YouTube數位影片分享網站，大量寄發標題為「Dudeyou gonna get caught, lol」、「LOL, dude

廣告



無法顯示網頁

目前查閱的網頁無法使用。網站可能發生技術問題或瀏覽器設定。

請嘗試下列：

- 請按 [重新整理] 按鈕，或者稍後再試一次
- 如果在網址列輸入網址，請確定未拼錯任何
- 要檢查您的連線設定，請按[工具]功能表，[項]。在[連線]標籤按[區域網路設定]。設 (LAN) 系統管理員或網際網路服務提供者 (IS
- 要檢視您的網際網路連線設定值是否正被值 Microsoft Windows 檢驗您的網路並自動探索

大綱



電子郵件社交工程簡介

電子郵件社交工程攻擊手法

預防電子郵件社交工程攻擊

有下列症狀的同仁請注意了

- 太有正義感
- 太有愛心
- 好奇寶寶
- 太容易被唬



不用打：

0800XXXX000

內政部要求

- 內政部102年度-電子郵件社交工程演練計畫
- 本部及所屬資安責任等級列A、B級機關預計102年度惡意郵件**開啟率**、**點閱率**分別降至**10%**及**6%**以下。

測試成功定義

- 信件預覽-開啟率
 - 偵測受測者於收到警覺性測試信件後，預覽信件圖片或內容。
- 連結點選-點閱率
 - 偵測受測者於收到警覺性測試信件後，開啟信件並點擊信件中之URL連結或附檔。

讀取信件要領

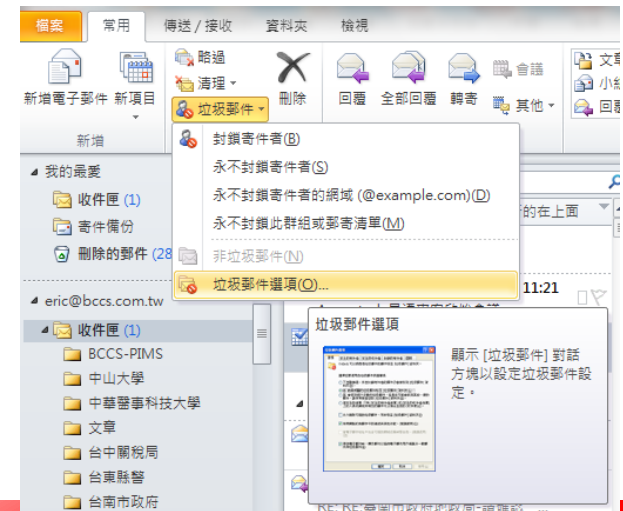
- 先確認寄件者。
 - 是否為您認識的人或業務需要。
- 確認郵件主旨。
 - 是否為奇怪的主旨, 或與寄件者不搭的主旨。
- 確定郵件內容是否與寄件者或主旨有關
- 確定郵件內容是否得宜。
 - 例如是否得提供個資料機敏資料。
- 是否非得開啟附件或點選連結。
- 是否須向寄件者確認。

讀取信件注意事項

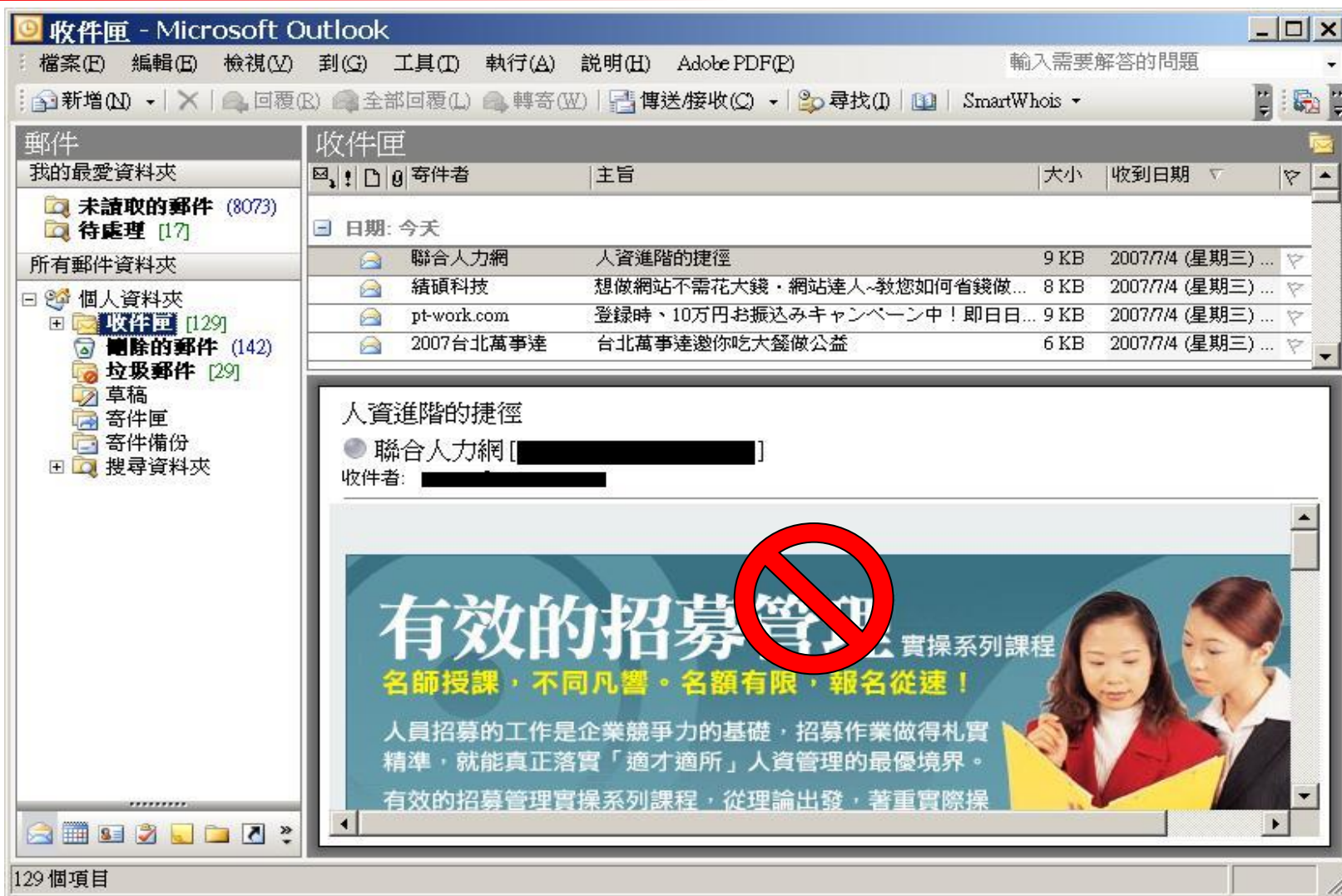
- **寄件者**是很容易假冒的，若發覺信件內容與寄件者之前所寄的內容差異大時，請向寄件者詢問（例如此寄件者原先都寄中文信，而收到其英文信.....）。
- 來路不明之信件不予理會，**直接刪除**或避免按照信件內容指示行事，也**不要開啟附加檔案**，以免導致中毒或資料外洩。
- 遇到任何要求**提供密碼或個人資訊**的情況，請勿理會。系統之管理者決不可能要求使用者以**mail**方式回覆密碼。
- 若要求提供資料之信件，可先詢問承辦單位是否屬實，且不用該信件或網頁提供之查詢資訊。
- 天上很難掉下來禮物，愈好康的信件愈有問題，例如點選連結或回信即可得到禮物。
- 看似無害之信件也儘可能不要開啟，如廣告信件。
- 不要點選不明信件中的連結網址，**最好自己輸入**，以免被偽造的網址所欺騙。

使用者防護停看聽(1)

- 停 – 使用任何電子郵件軟體前，必須先確認以下設定
 - 必須安裝防毒軟體，並確實更新病毒碼
 - 審慎開啟郵件及其附件或連結
 - 必須取消郵件預覽功能，避免無意開啟郵件
 - 設定過濾垃圾郵件機制
 - 建立電子郵件驗證機制



取消郵件預覽功能



The screenshot shows the Outlook interface with the 'View' tab selected. The email list is displayed with columns for 'Sender', 'Subject', 'Received Date', 'Size', and 'Category'. The selected email is from 郭瑞祥 (Guo Ruixiang) with the subject '已接受: 昱通專案... 會議' (Accepted:昱通專案... 會議), received on 2013/3/26 at 11:02 AM, with a size of 5 KB. A red circle highlights the 'Subject' column header and the subject text of this email.

Sender	Subject	Received Date	Size	Category
吳秀娟	Accepted: 昱通專案... 會議	2013/3/26 (週二) 上午 11:21	7 KB	
郭瑞祥	已接受: 昱通專案... 會議	2013/3/26 (週二) 上午 11:02	5 KB	
黃淑琦	RE: 有關筆電電池... 比較	2013/3/25 (週一) 下午 6:15	14 KB	
Wang, Vicky-tw (Kaohsiung)	RE: 臺南市政府地政...	2013/3/25 (週一) 下午 4:28	77 KB	
陳柏翔	事件通報&委外程序書	2013/3/25 (週一) 上午 11:42	282 KB	
郭瑞祥	P-02-001個資差點及分類分級...	2013/3/25 (週一) 上午 11:39	65 KB	
Wang, Vicky-tw (Kaohsiung)	3/26 臺南市政府地政局-撥證	2013/3/25 (週一) 上午 10:33	152 KB	

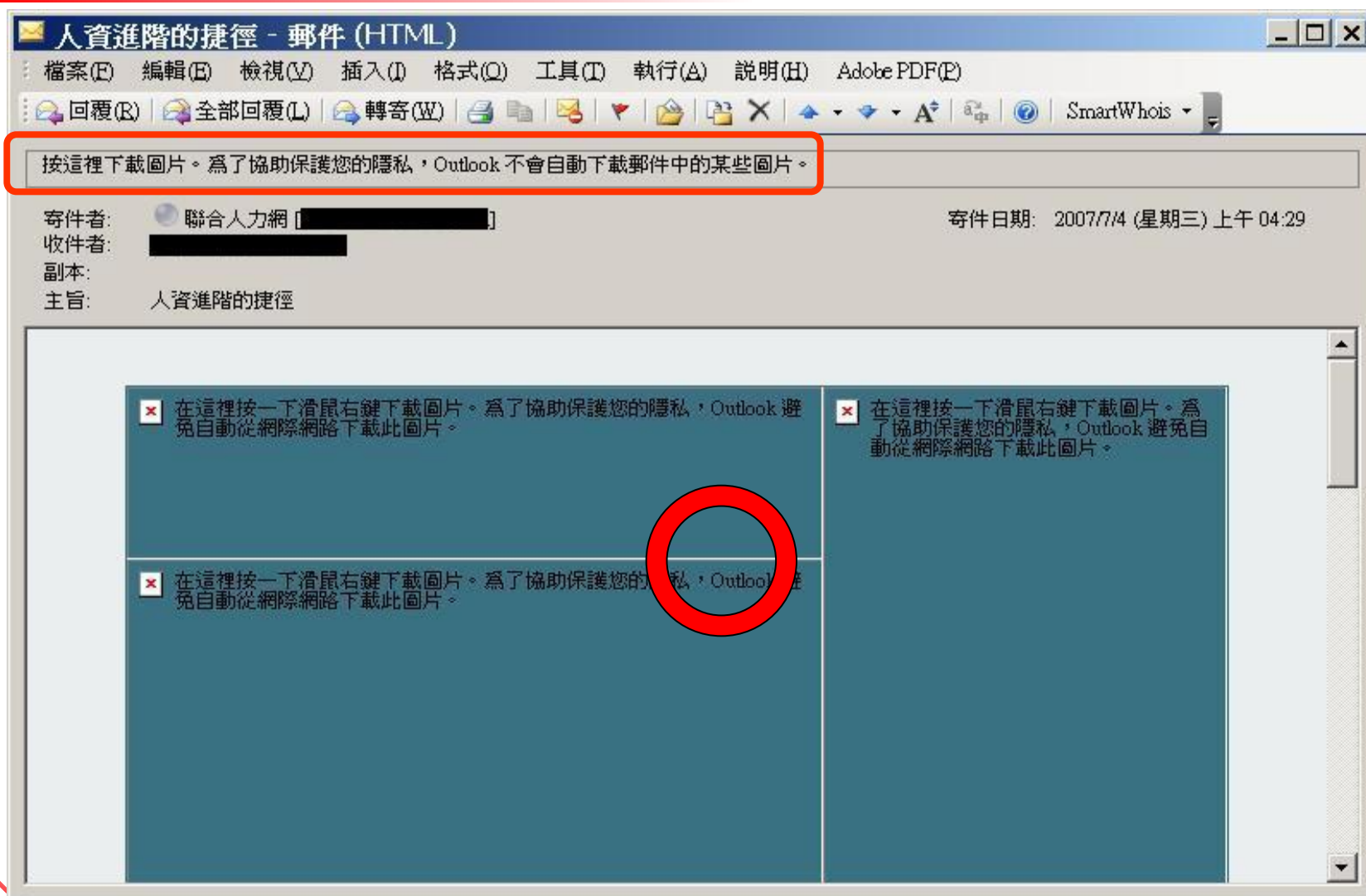
關閉信件預覽功能

- Windows Live Mail
 - 選取【檢視】／【版面配置】
 - 不勾選【顯示預覽窗格】
- Outlook express
 - 選取【檢視】／【版面配置】
 - 不勾選【顯示預覽窗格】
- Outlook 2010
 - 選取【檢視】／【讀取窗格】
 - 選擇【關閉】
- Outlook 2007
 - 選取【檢視】／【讀取窗格】
 - 選擇【關閉】

關閉郵件自動下載圖片及其他內容



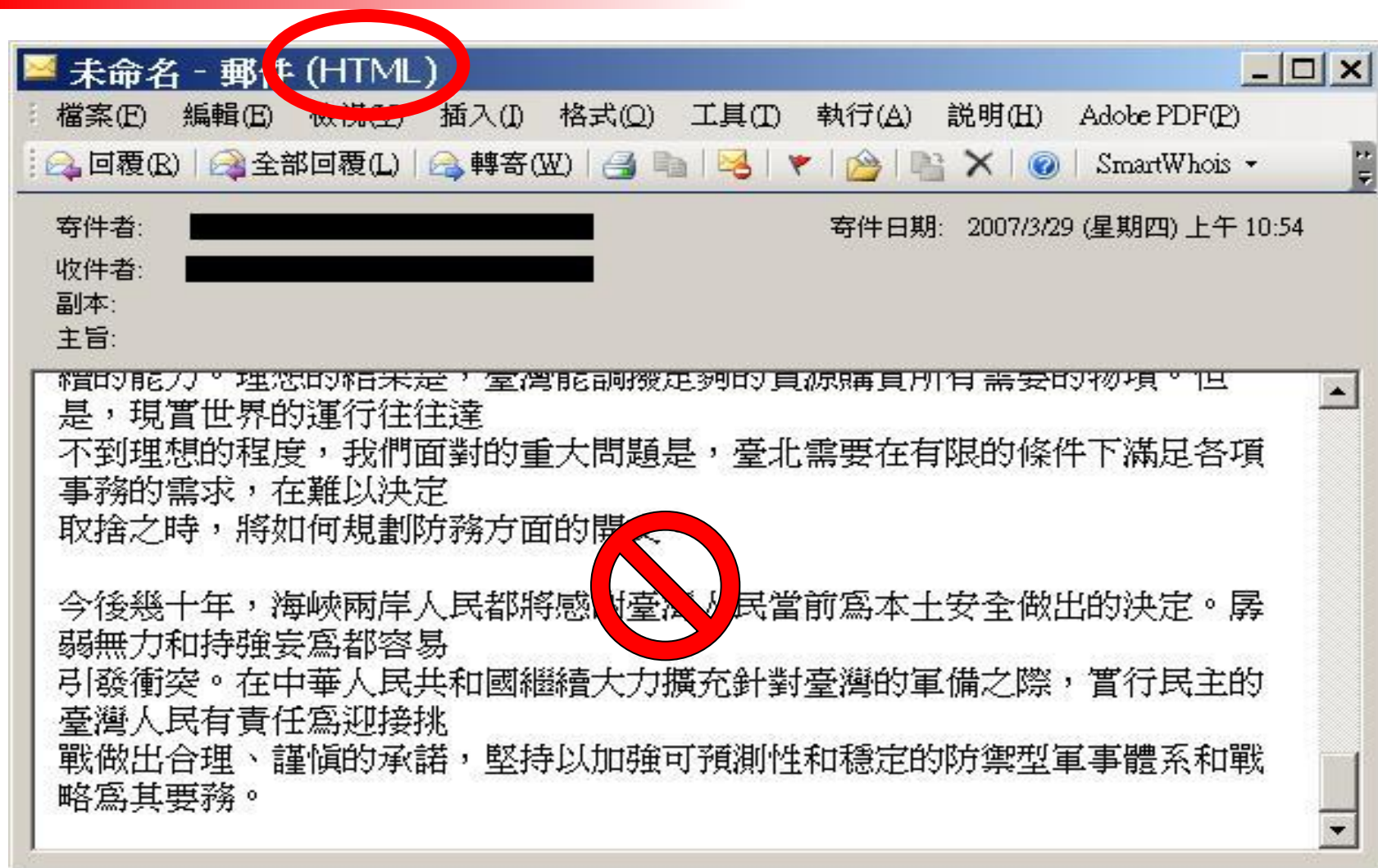
關閉郵件自動下載圖片及其他內容(續)



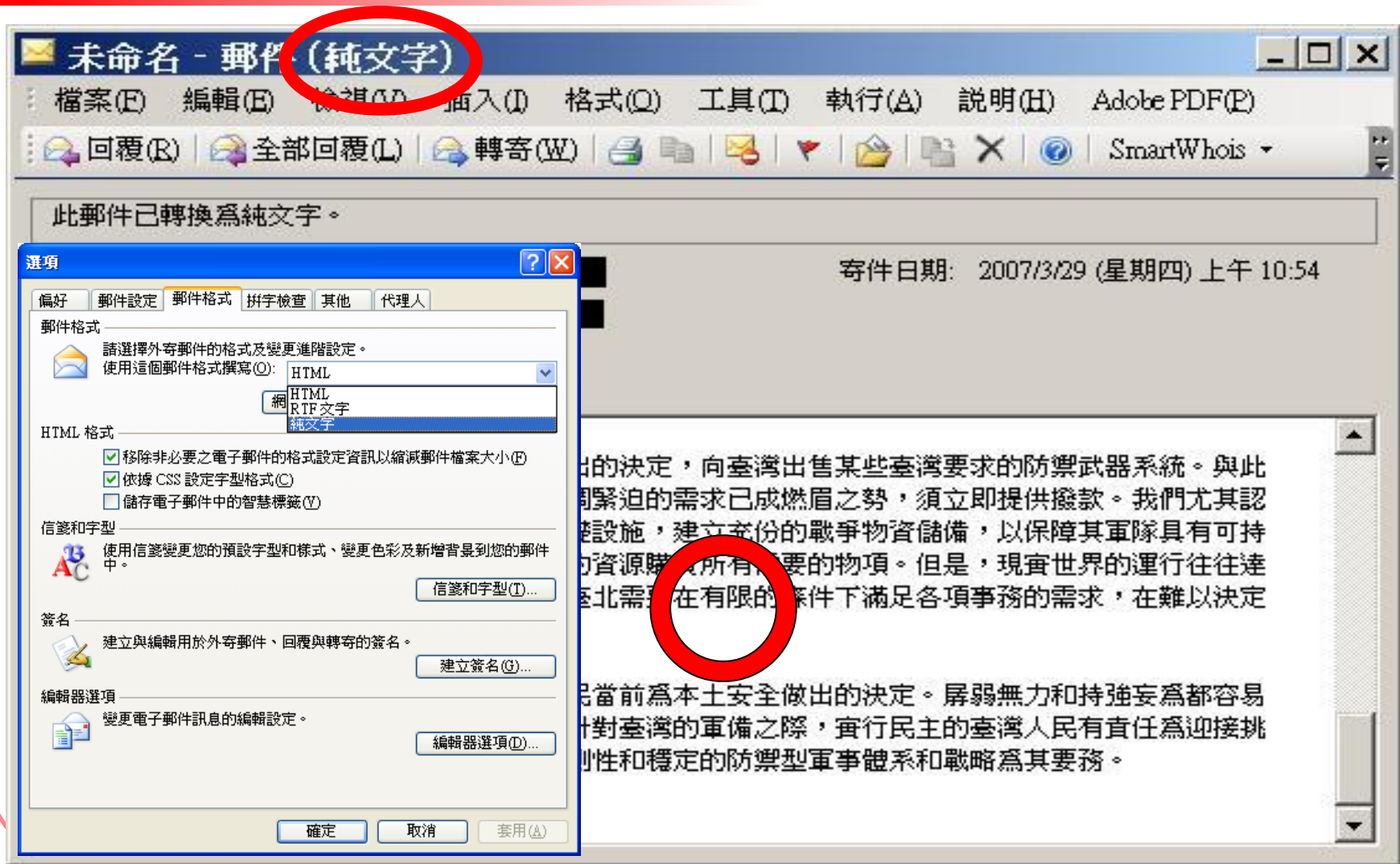
關閉自動下載圖檔

- Windows Live Mail
 - 選取【工具】／【安全性選項】／【安全性】
 - 勾選【阻擋HTML電子郵件中的圖片和其他外部內容】
- Outlook express
 - 選取【工具】／【選項】／【安全性】
 - 勾選【阻擋HTML電子郵件中的圖片和其他外部內容】
- Outlook 2010
 - 選取【檔案】／【選項】／【信任中心】／【信任中心設定】／【自動下載】
 - 勾選【不自動下載HTML電子郵件訊息或RSS項目中的圖片】
- Outlook 2007
 - 選取【工具】／【信任中心】／【信任中心設定】／【自動下載】
 - 勾選【不自動下載HTML電子郵件訊息或RSS項目中的圖片】

不以HTML模式開啟郵件



以純文字模式開啟郵件



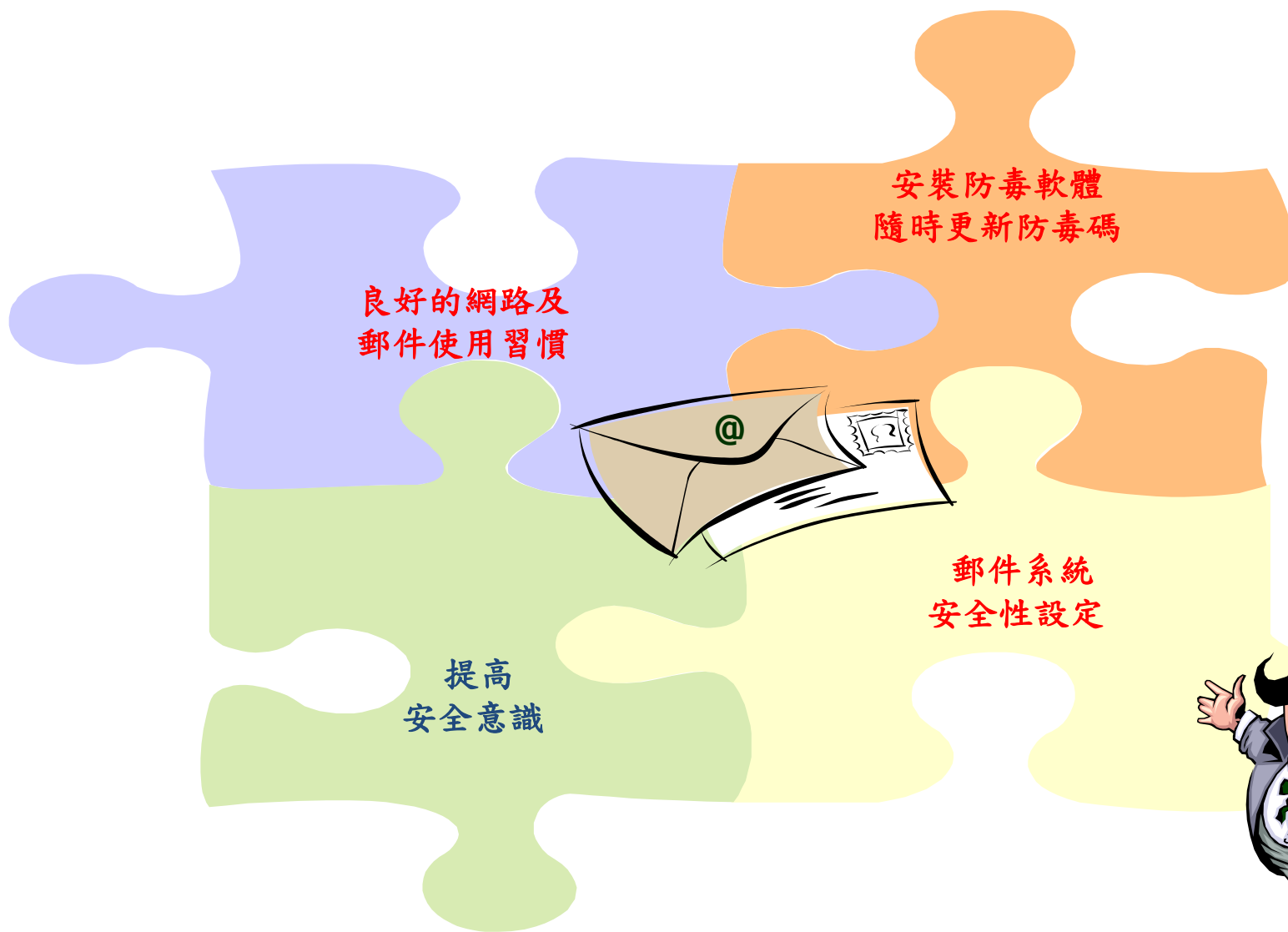
以純文字開啟信件

- Windows Live Mail
 - 選取【工具】／【選項】／【讀取】
 - 勾選【在純文字中讀取所有郵件】
- Outlook express
 - 選取【工具】／【選項】／【讀取】
 - 勾選【在純文字中讀取所有郵件】
- Outlook 2010
 - 選取【檔案】／【選項】／【信任中心】／【信任中心設定】
／【電子郵件安全性】
 - 勾選【以純文字讀取所有標準郵件】
- Outlook 2007
 - 選取【工具】／【信任中心】／【電子郵件安全性】
 - 勾選【以純文字讀取所有標準郵件】

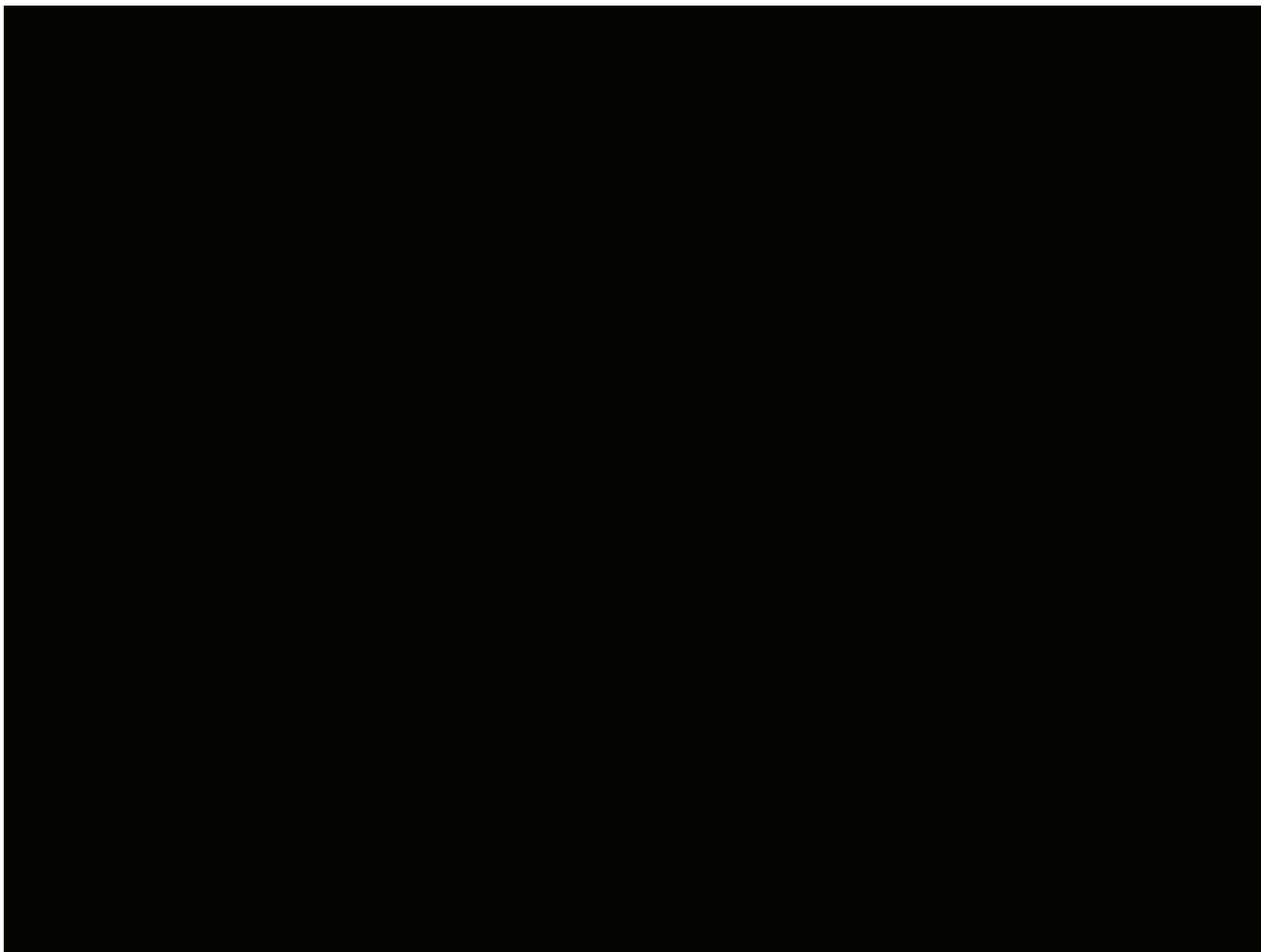
使用者防護停看聽(2)

- 看 – 收到郵件後，必須注意
 - 郵件主旨是否與本身業務相關
 - 其餘郵件不建議開啟，如需開啟應確認郵件來源
- 聽 – 若懷疑郵件來源，必須進行確認
 - 透過電話或電子郵件向寄件人於開啟前確認郵件真偽

使用者端郵件安全管理



蝴蝶效應



總結

- 網路安全必須是一種習慣與文化，而不能只是一種技術與專業。

Thank You

感謝聆聽 敬請指教