tsc 德欣 TSC CAPITAL GROUP
The Bridge to the Asia Pacific Region

屏東縣政府

一般人員資訊安全講習

資安顧問：賴東熙

時間：5月23日 09:00~12:00

德欣寰宇科技股份有限公司 TSC TECHNOLOGIES, INC.
台北公司：台北市10059新生南路一段50號5樓500室 TEL: 886 2 2358 2775 · FAX:886 2 2358 3775
新竹公司：新竹市30046四維路130號2樓之2 TEL: 886 3 522 9570 · FAX:886 3 524 750

目錄

- 資訊安全基本概念介紹
- 資安事件案例分享
- 社交工程
- 惡意電子郵件防範宣導
- USB儲存媒體使用安全

目錄

- 資訊安全基本概念介紹

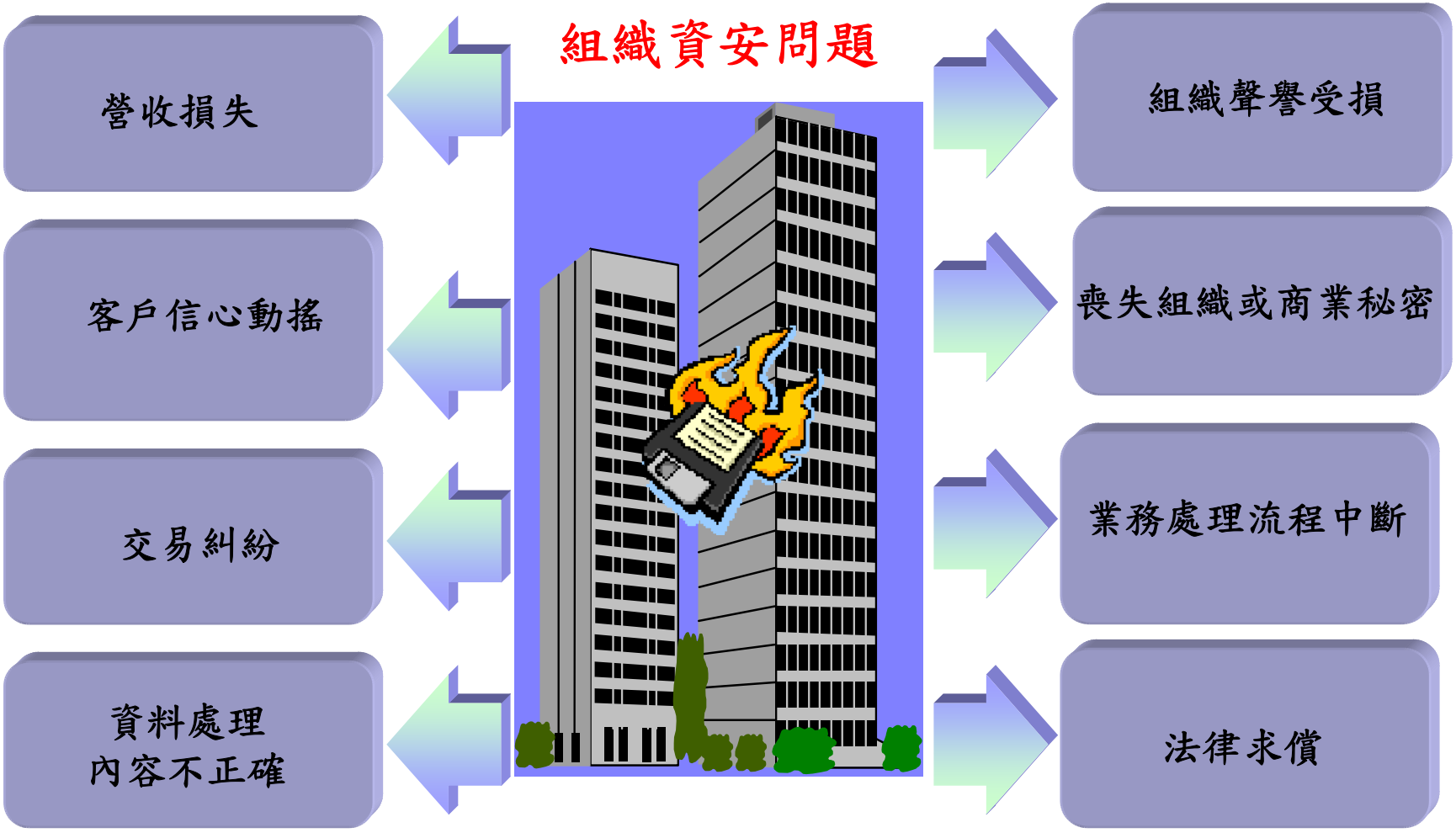
資訊安全基本概念介紹

- 資安影片
- 由上述影片中， 您看到那些重點？
  - 總經理走出來為何大家的螢幕都變色？ 玩小遊戲種田
  - 軟體使用方面？ 禁止使用即時通、P2P、盜版軟體
  - 硬體方面？ 限制使用光碟、行動碟、照相手機、行動碟、筆電
  - 備份如何作？利用硬碟每天備份，送總經理室隔離放置
  - 資料銷毀如何作？用過光碟繳回銷毀內部資料，廢棄文書資料使用碎紙機處理
  - 資料殺手誰最危險？員工比駭客更危險
  - 影片中那個資安漏洞沒講到？ 人員門禁管理

資訊安全基本概念介紹

- 由上述影片內容所描述之各項資安控管措施，主要保護的東西是甚麼— 資訊資產（如：客戶資料、公司機密資訊...），也就是說在高度倚賴資訊及網路科技的今日，資訊資產已是組織或個人的一項非常重要的資產，就像其它重要的營運或個人資產一樣，具有相當之價值因此需要適當保護，尤其是高度依賴資訊化服務的組織及個人更形重要。
- 尤其在現今網際網路高度發展及應用，這些資訊資產也更有機會暴露於日益多樣的威脅與脆弱性中，其對組織或個人所帶來的風險及損失也日益擴大，資訊安全已成為不可忽視之重要課題。

資訊安全問題對組織可能造成的影響



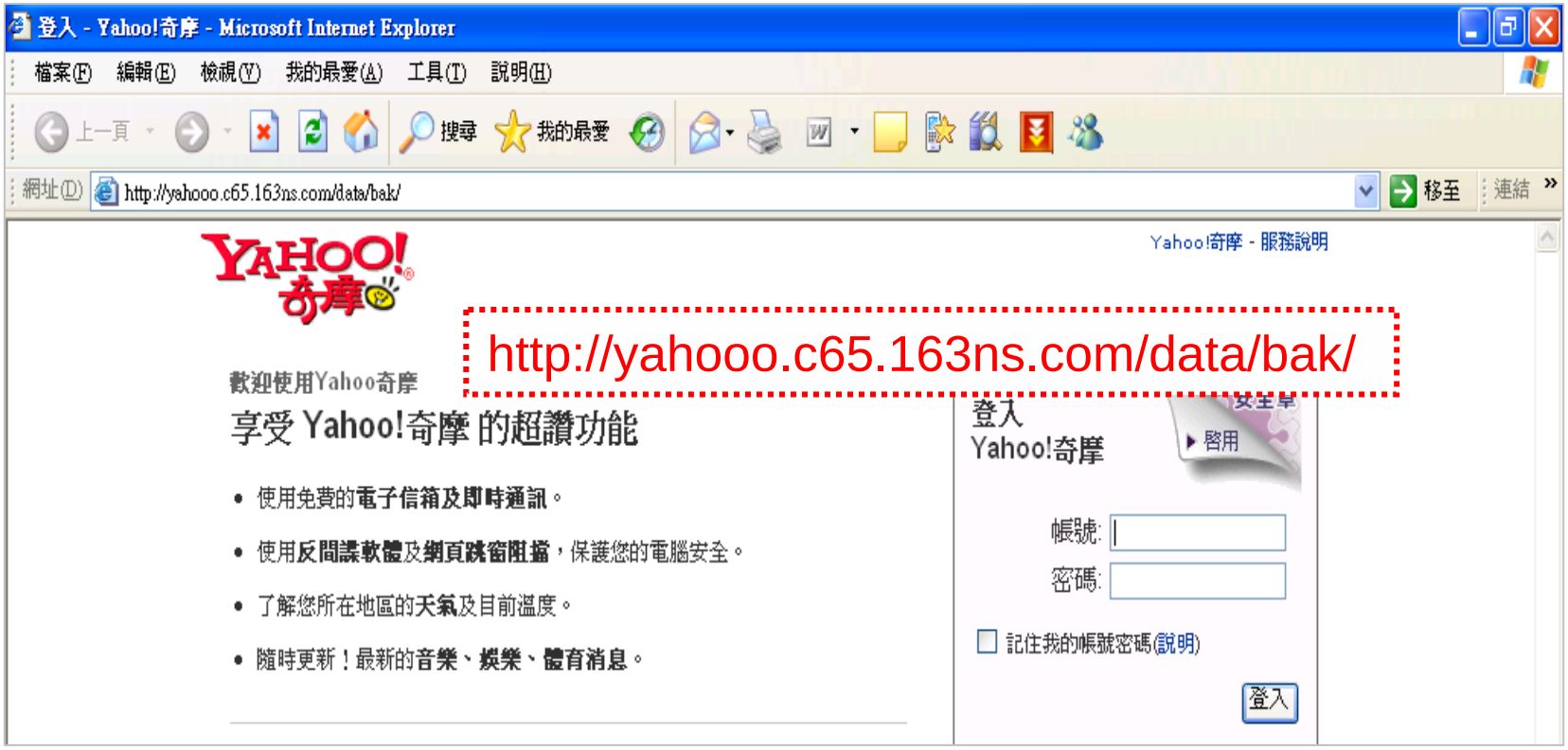
資訊安全常見之威脅

- 網路釣魚
- 垃圾郵件
- 社交工程攻擊、惡意電子郵件
- 惡意程式碼、窺視或間諜軟體(Spyware)
- 可攜式裝置(如USB隨身碟、 無線AP…)
- 設備故障
- 人員差錯
- 天災
- 資訊安全最大的威脅就是不知道威脅或未能正確評估威脅

資訊安全常見之威脅-釣魚網頁

您可能不曉得...

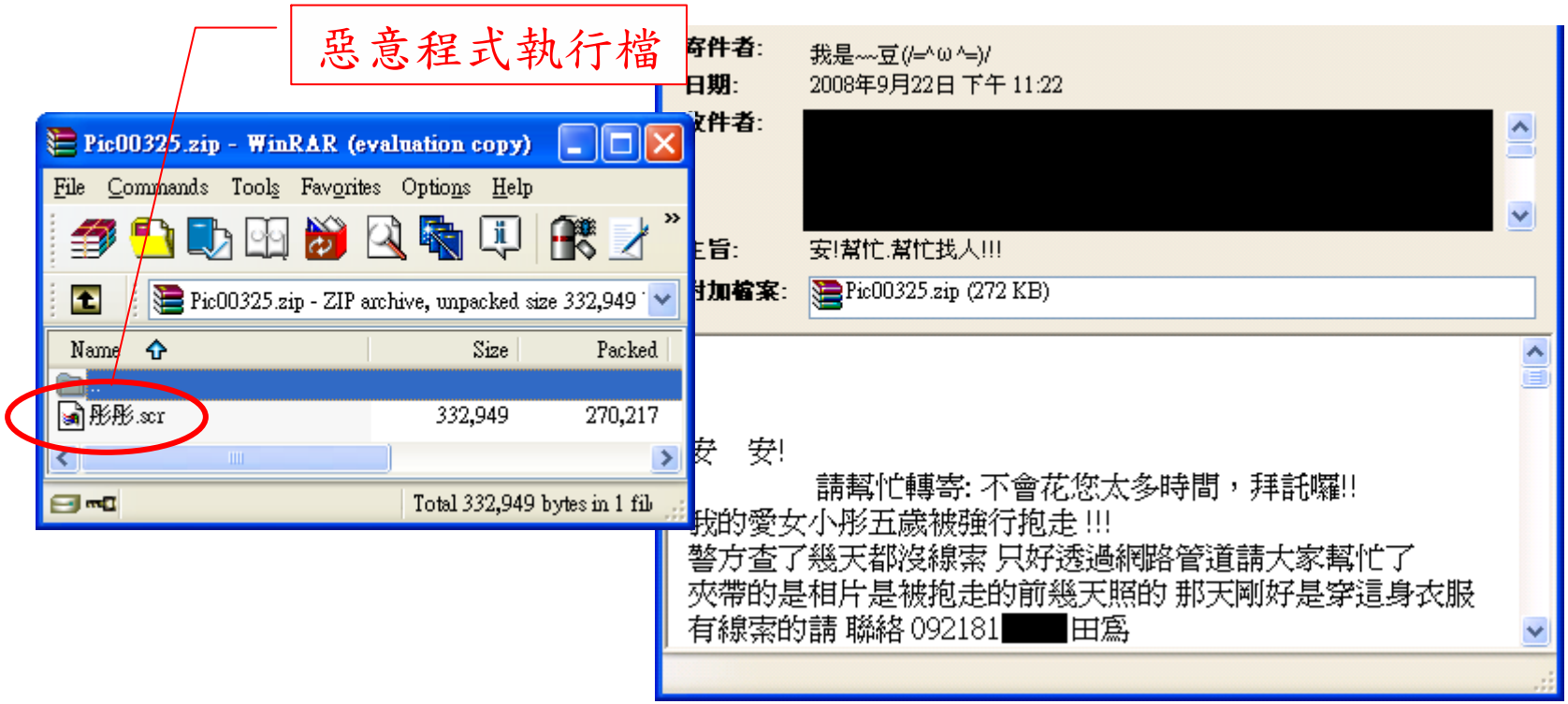
您接到詐騙電話或是個資外洩，是因為您自己在釣魚網站洩露了帳號密碼！



資訊安全常見之威脅-社交工程攻擊

您可能不曉得...

您早就淪為社交工程攻擊受害者！



資訊安全常見之威脅-木馬程式的威脅

- 您不能依賴防毒軟體能幫您阻擋掉所有的木馬程式，因為這些惡意程式可能利用「加殼免殺」技術避過防毒軟體的偵測！

資訊安全常見之威脅-利用漏洞進行入侵

利用尚未更新修補程式的漏洞

網路上有各種利用系統漏洞 / 軟體漏洞進行攻擊的惡意程式

若您沒有即時更新修補程式，您就可能成為這些惡意程式的受害者

資訊安全常見之威脅-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

為何要推動資訊安全

- 組織的資訊安全目標與期望
  - 客戶要求
  - 長官的期望
  - 核心服務
  - 形象與聲譽
- 資訊安全推動的範圍是否符合組織的期望
- 資訊安全的措施是否適切

資通安全三要素

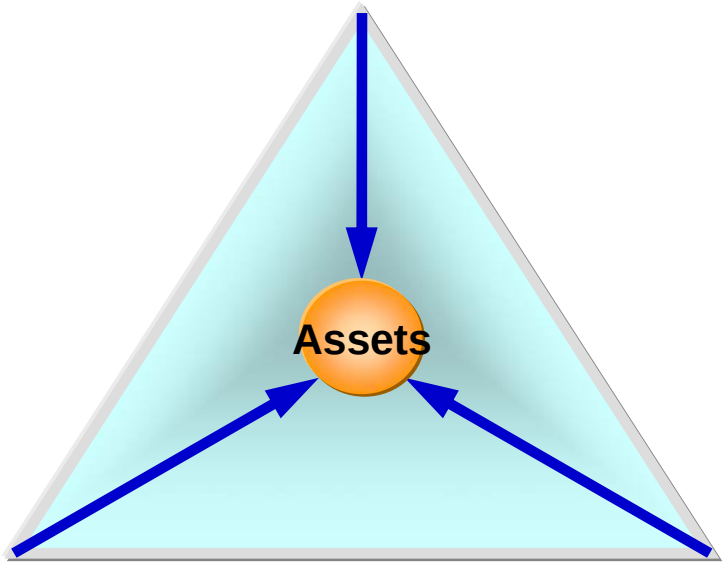
- 安全認知
- 權責分工
- 人員取存管制
- 人員安全

People

Keep Going and Improving

- 政策與流程
- 文件與標準流程
- 營運持續規劃
- 遵循法令規章
- 授權管理
- 安全稽核

Process



- 實體安全
- 系統取存控制
- 電腦與網路安全
- 身分驗證技術
- 系統開發與維護
- 備援管理

Technology

目錄

- 資安事件案例分享

(新聞1)無線溢波始祖盜刷逾百萬 (新聞2)洩露個資1.6萬筆 玉山銀罰4百萬

手機竊臉書帳號 FaceNiff一指搞定

作者：廖珮君整理 -07/04/2011

智慧型手機不僅是現代人的社交工具，也是駭客竊取資料的好幫手，6月初發表的Android應用程式FaceNiff，可以任意取得同一個無線網路中，Facebook使用者的帳號密碼，當然，除了臉書以外，FaceNiff還可以竊取Twitter、YouTube、Amazon等網站的使用者登入資訊。

2010年10月問市的Firefox套件Firesheep，同樣也是透過無線網路竊取資訊，Firesheep讓人可以輕易存取同一個無線網路環境裡，其他使用者的cookie及登入資訊。FaceNiff則是Firesheep行動版，其與Firesheep目的一樣，但做法更簡單也更厲害，只要按一個鍵就可以，就算無線網路已經使用WEP、WPA、WPA2加密機制，FaceNiff還是可以監聽手機所在Wi-Fi網路環境並取得正在使用的帳戶資訊。

然而，FaceNiff並不是完全無敵，它無法取得經由SSL加密傳輸的帳號密碼，因此，在公用無線網路環境裡，如果要使用網路服務，最好事先更改成SSL設定，包括Facebook、Twitter等網站皆已內建「強制https加密連線」的功能，但若該網站不支援SSL模式，建議在VPN連線模式下再使用。

當紅炸子雞 臉書賣個資賺錢

自由時報 – 2012年2月13日 上午4:24 編譯楊芙宜／特譯

全球社群網站龍頭臉書（Facebook）提交公開募股（IPO）申請文件一週以來，在私募股票交易市場的股價已飆漲10%，使公司市值突破1000億美元。然而，不像其他高價股公司，通常有零件、小工具、汽車或手機等財產登錄，臉書持有的財產清單，其實是你我在內的使用者所貢獻。

臉書有8億4500萬用戶，去年的廣告收入達32億美元，佔它總營收的85%。它的賺錢方式是靠販賣網頁空間，給那些想登廣告影響特定用戶群的公司。臉書提供廣告商選擇關鍵字，或感情狀態、居住地方、興趣活動、喜愛書籍、職業等資料，然後，臉書會針對這些被鎖定的用戶群顯示廣告。

例如，你在臉書上寫喜歡杯子蛋糕、住在特定社區、曾經邀請朋友到家裡玩，可以預期住家附近的麵包店廣告就會顯示在你的臉書網頁。

這些臉書從每位用戶取得的資訊，可被廣告商用作開發特定市場，影響力之大，令人驚訝。歐洲法律就規定，民眾有權利知道網路公司從他們身上取得何種資料，美國卻沒有此種規範。許多網路公司聲稱擁有民眾的上網資料，其實是在個人電腦、瀏覽器植入如cookies的軟體或其他追蹤工具，藉以取得。

如果你曾在電子郵件裡寫過很焦慮，在Google網頁搜尋過「壓力」，或利用線上健康日誌記載你的情緒變化，那麼可以預期，與焦慮相關的醫療服務廣告，就會顯示在你的電腦網頁上。

或許，你認為，這些跳出來的顯示廣告可能有用，或令人討厭，還是無所謂，但嚴重的是，這些關於你生活點點滴滴的記載，很容易就被用來對付你自己。當找工作、決定信用額度、買保險時被拒絕，你可能不知道，這些跟你極為相似的個體資料被用來作為參考，甚至是影響最後決定的重要因素。

專門提供法律研究檢索線上服務的LexisNexis公司，一項稱作Accurint for Law Enforcement 的產品，提供政府機關有關民眾在社群網站言行所為的資訊。美國國稅局以臉書與另一社群網站MySpace的搜尋結果，作為逃稅者收入與行蹤的證據。美國移民局也被獲知，藉由檢視這些張貼於網站的照片、訊息確認親屬關係或淘汰假結婚案例。

網友不希望被追蹤

根據2008年一項對2000位消費者抽樣的調查顯示，高達93%受訪者認為網路公司在使用個人資料前應徵求同意，72%更希望能選擇在線上不被追蹤。當美國民間團體力促立法保護網路隱私權之際，也許臉書創辦人與執行長祖克柏（Mark Zuckerberg）可認真思考，什麼樣的經營方式能不侵犯使用者隱私權，又能永續發展。

(新聞)誤點臉書不明連結 帳號信用卡遭盜用

汰換硬碟再銷售 機密個資恐外洩

- 有不少業者在網路上販賣二手硬碟，不過現在傳出有消費者在買來的二手硬碟裡,發現有某家商業銀行內部關於客戶的貸款或個資，大量的民眾隱私外流，目前金管會已經對此開始調查，如有違反銀行法內控相關規定，將會對這家銀行開罰2百萬到1千萬。

千筆中信局客戶個資丟馬路

- 銀行竟將民眾重要個資丟棄在路邊，真是太離譜！北縣八里鄉西濱快速道路一處路段，前天被人發現上千張前中央信託局開戶申請的文件散落一地，部分還掉落下方涵洞，單據上除了姓名、電話，還有身分證號及銀行帳戶等重要個資，《蘋果》依文件資料的電話號碼聯繫到數名開戶人，一名開戶者驚呼：「若被壞人拿去，後果不堪設想！」

投訴市長信箱個資遭洩

- 台中市一名大樓保全人員，遭到都發局稽查大樓電梯，之後他投信到了市長信箱反應這名市府人員態度不好，問題來了，市長信箱明定民眾個資一定保密，結果他卻收到了被他投訴的市府官員電話，電話中還要求跟他對質，進一步了解胡志強在五月才發公文下令，公務員謹守民眾個資保密一事，基層卻是陽奉陰違。
- 新聞報導影片

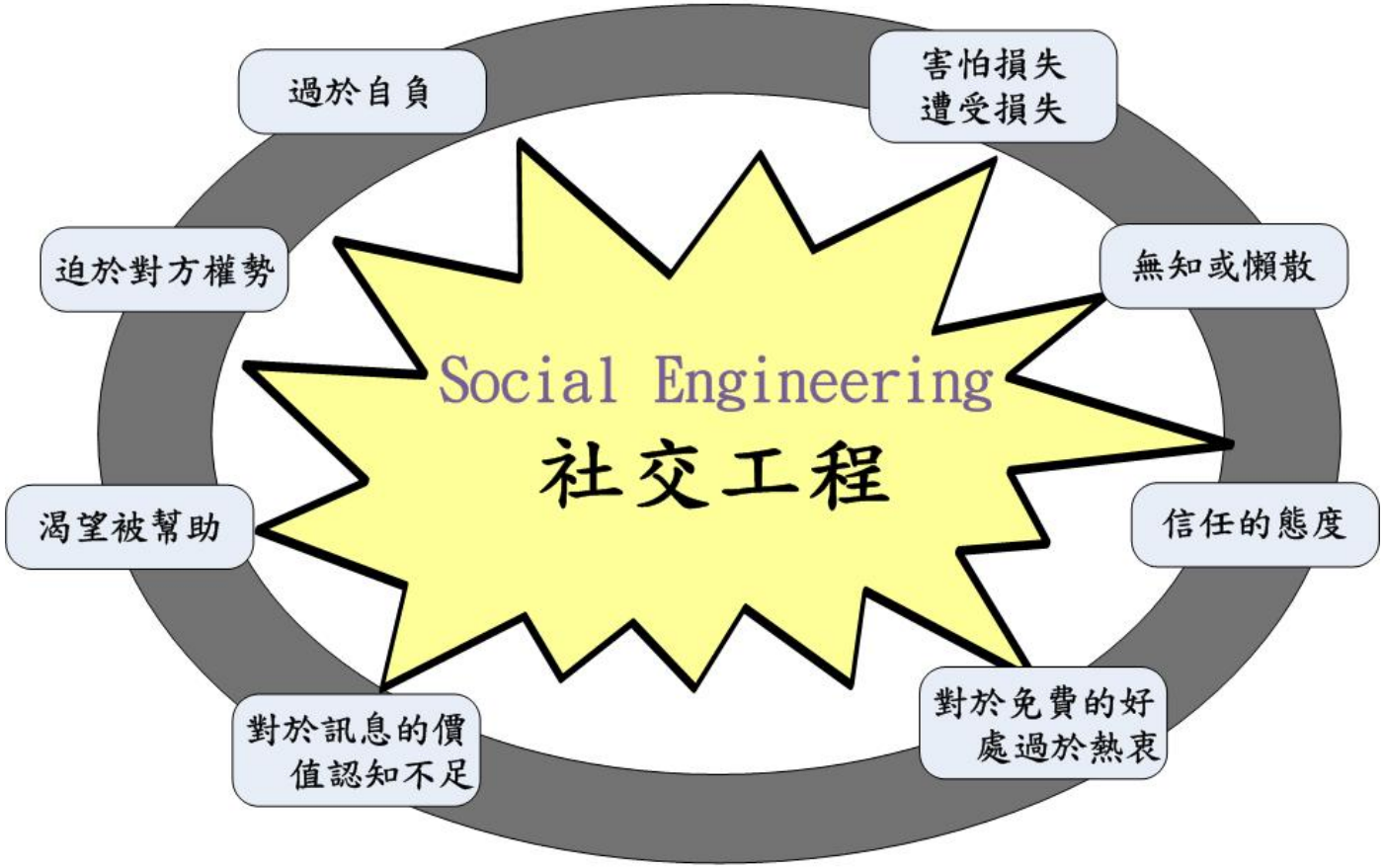
目錄

- 社交工程

社交工程介紹

- 社交工程是一種利用人類天性，透過嚴密的手段或騙局來得到敏感的資訊。通常利用人性的弱點不外乎下列幾種：
  - 對人的信任(人性本善)
  - 恐懼的心態
  - 渴望被幫助的需求
- 社交工程通常想獲取下列的資訊
  - 敏感的資料(帳號密碼、個人資料、公司機密資料...)
  - 金錢或實質上的利益

人性的弱點



社交工程宣導影片

「社交工程」攻擊手法

- 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、社群或交友網頁來進行攻擊
- 釣魚網站
- 網頁隱藏式惡意連結
- 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、時事相關或令人感興趣的郵件內容
  - ✓含有惡意程式的附件
  - ✓利用應用程式之弱點(包括所謂零時差攻擊)

社交工程-惡意郵件

- 駭客最常利用的弱點
  - 文書處理軟體(Microsoft Office)
  - 常見應用程式(WinRAR、Adobe Reader、Flash player、Real player)
  - P2P軟體
- 駭客最常運用的社交工程手法
  - 生活議題
  - 政治新關
  - 假冒公務或個人名義

社交工程的類型

- 將社交工程的攻擊進行分類，大致上可歸為以下兩種類型：
  - **非技術性(人性為基礎)**
    - ✓ 藉由與受害者互動得到敏感資料
    - ✓ 藉由組織管理的漏洞或人為疏失取得敏感資料

    例如：利用欺騙/愚弄、模仿、暗中監視/偷聽、命令式口吻、假裝工作人員、假扮技術專家與翻垃圾
  - **技術性(電腦為基礎)**
    - ✓ 此類的社交工程攻擊是藉由電腦來實行資料收集/竊取

    例如： Phishing、Vishing、跳出的視窗、有趣的軟體、垃圾郵件

以人為基礎的社交工程攻擊

- 冒充合法的使用者
  - 提出識別並詢問一些敏感的資訊。
    - ✓ Hi!我是XX部門的John，我忘掉密碼了，你能夠幫助我嗎？
- 冒充重要的使用者
  - 假裝目標公司的VIP、有價值的客戶、、、等。
    - ✓ Hi!我是財務長的助理Kevin。我現在有一個重要的事要做，不過我忘記了系統密碼，你可以幫我嗎？
- 假裝技術支援者
  - 聲稱自己是公司的技術支援者，需要你提供帳號與密碼來重新取得資料。
    - ✓ 您好!我是XX的技術支援，我發現你們的系統故障，您可以提供你的帳號和密碼讓我把貴公司的重要資料救回？

以人為基礎的社交工程攻擊

- 透過利用委外的授權
  - 利用與組織的重要人物交談獲取更高的權限與嘗試搜集資料冒充重要的使用者
- 偷聽/偷看(Eavesdropping)
  - 偷聽或未經授權的竊聽或閱讀訊息，包括：聲音、影像與書寫的資料
- 肩窺(Shoulder Surfing)
  - 由您的後面偷看你輸入的帳號、密碼、身分證號碼、、、等資訊)
  - 通常他們都會由你的背後透過高於你肩膀的高度，用他的雙眼來的到想獲取的資訊

以人為基礎的社交工程攻擊

- 翻垃圾車(Dumpster Diving)
  - 由目標的公司要搜尋敏感資料，可以由：
    - ✓ 垃圾桶。
    - ✓ 印表後廢棄的紙張。
    - ✓ 使用者的桌面上的便條紙、便利貼、、、等。
  - 可以搜集到：
    - ✓ 電話/手機號碼。
    - ✓ 聯絡的資訊。
    - ✓ 財務的資訊。
    - ✓ 有關操作的資訊(如密碼、重要的文件存放位置、、、等)。

案例

- 某平面媒體記者花了40元，買到這兩大袋廢紙條，發現內容不是一般的廢紙板或紙箱這麼簡單，經過拼湊，赫然發現廢紙條上的文字依舊清晰可見，其內容涵蓋六大機密，包含了我國監控共軍戰報，空軍演習計畫和美軍動態等內容。
- 為了防止軍機外洩，軍方才花了八億元增購監控電腦裝備，如今機密卻因為小兵最傳統的文件銷毀疏失外流，實在相當諷刺。

資訊安全的問題不是只有電腦的問題!

資料來源：96/10/02 台視新聞

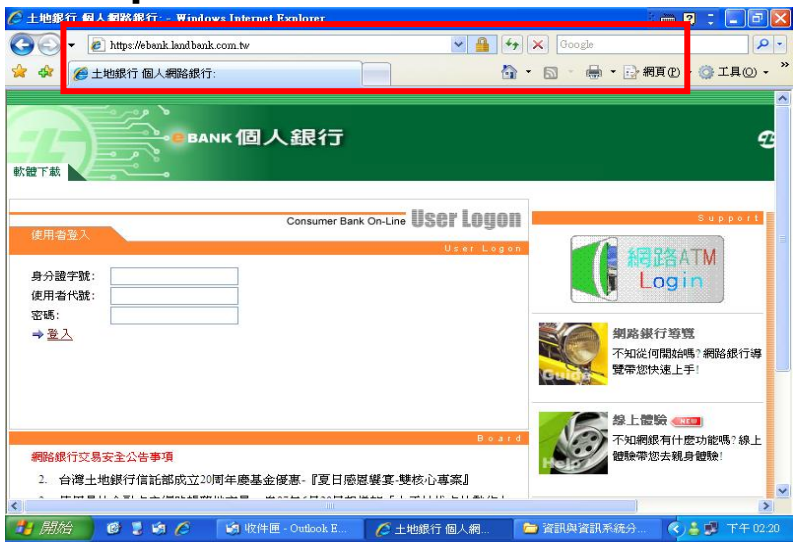
以電腦為基礎的社交工程攻擊

- 我們可以將它分為下列六類：
  - 惡意掛馬網頁/社群交友網站or 有趣的軟體
  - 垃圾郵件
  - 郵件的連結(Phishing) /即時通訊的連結(MSN 、Facebook …)
  - Vishing(釣魚網站)
  - 彈出的視窗
  - War Driving(使用無線網路設備探測目標是否有開放的無線網路設備)
  - P2P軟體

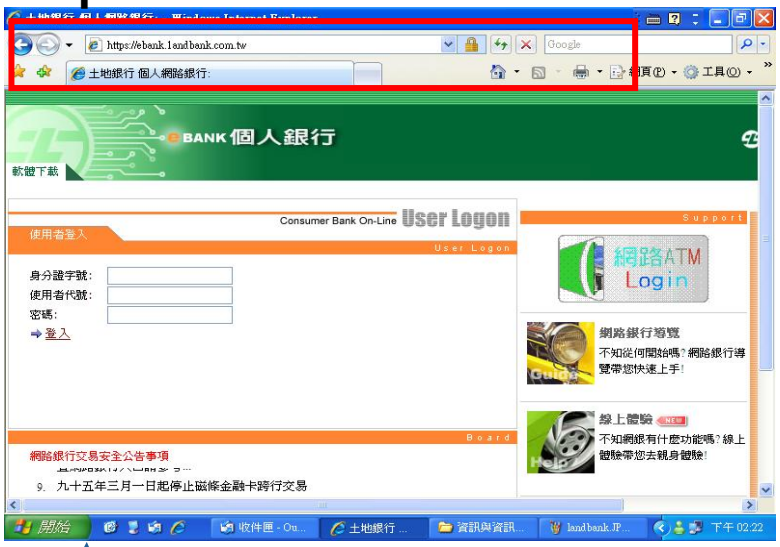
案例一：利用假網頁騙取匯款

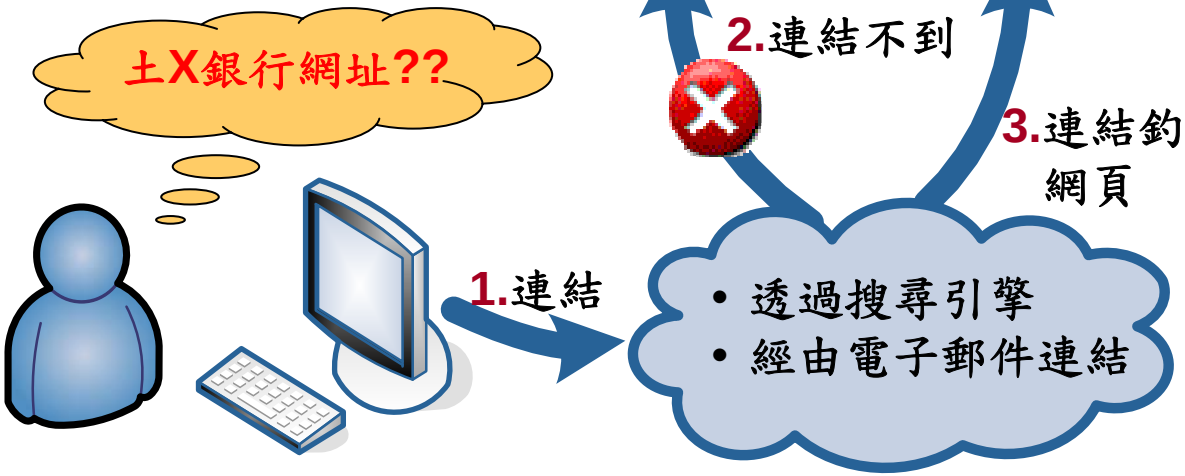
案例二：釣魚網頁

http://www.landbank.com.tw



http://www.1andbank.com.tw





例如：

遊戲X子

http://tw.gamania.com

vs. http://tw.gamannia.com

聯X銀行

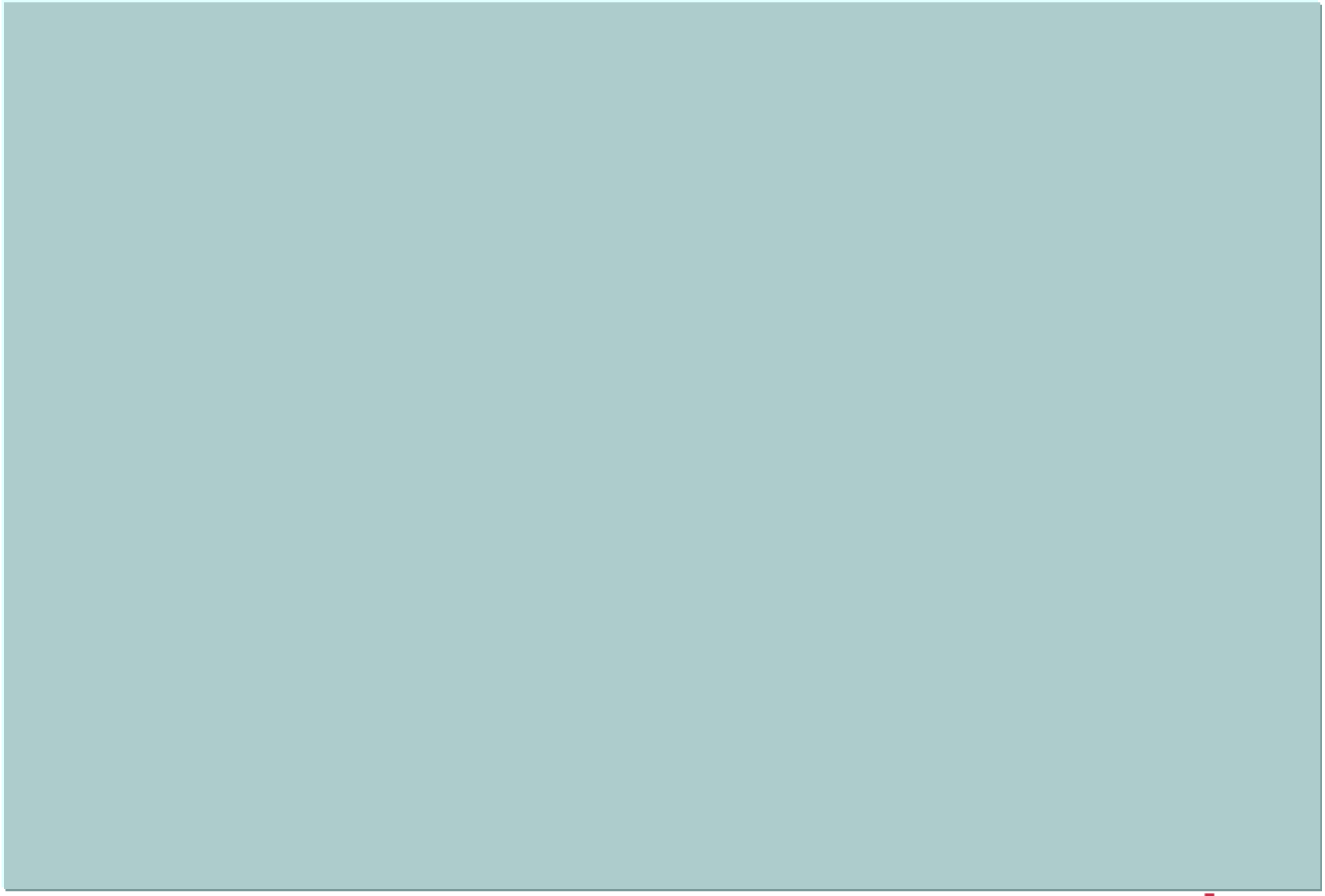
http://www.ubot.com.tw

vs. http://www.obot.com.tw

如何避免釣魚網站

- 釣魚網站防範
  - 網路釣魚篩選工具
  - 不直接點選任何來自即時通訊聯絡人所傳來的超連結。
  - 不開啟所有來路不明的電子郵件。
  - 連結任何交易網站，都必須確認有通過SSL的相關安全認證。
  - 儘量避免經由網路連線來完成金錢交易。
  - 安裝防毒軟體並更新病毒碼。
  - 啟用個人防火牆。

釣魚網站通報-台灣電腦網路危機處理暨協調中心
http://www.apnow.tw/index.cgi

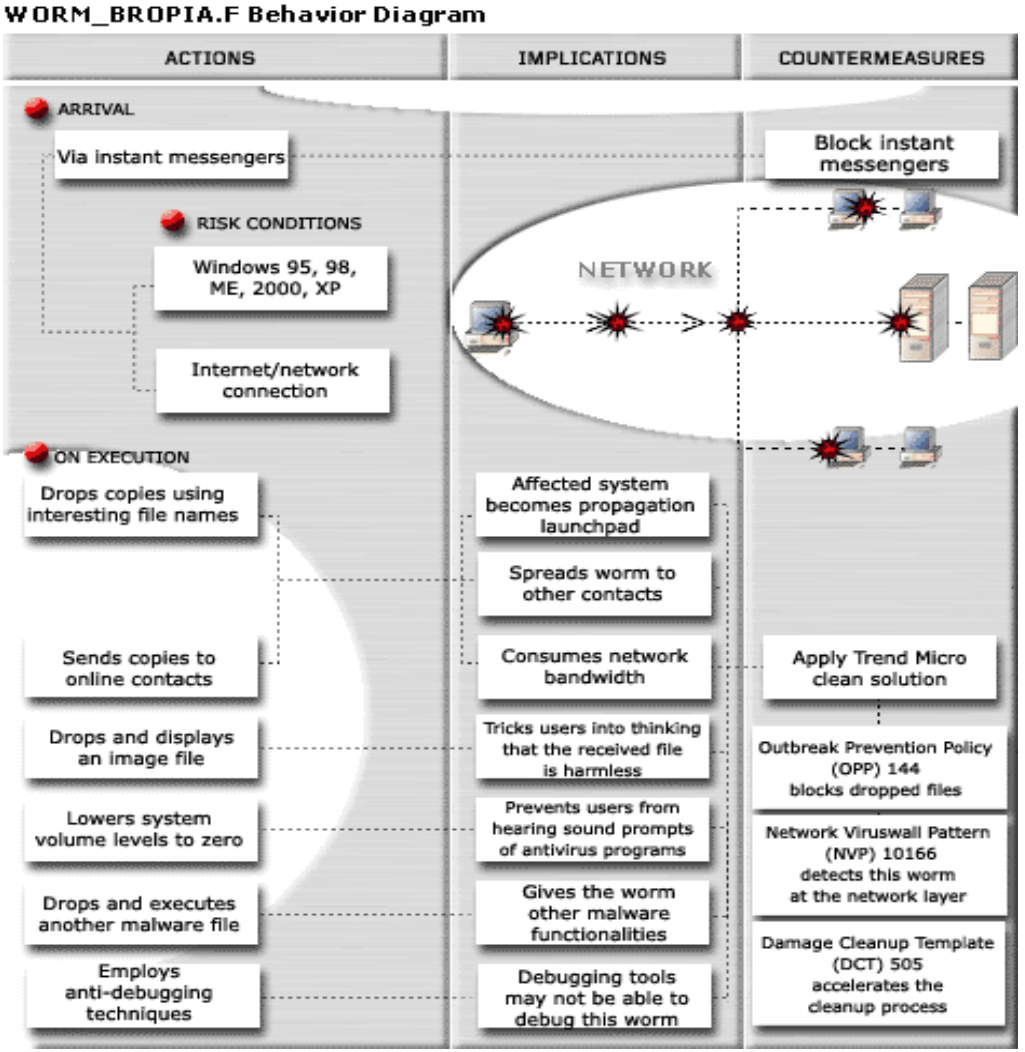


案例三：利用P2P軟體獲取個資

即時通軟體的安全隱憂

台灣常見的即時通軟體

- MSN Messenger
- YAHOO! 奇摩 即時通訊 免費網路電話
- Yam 蕃薯藤
- icq
- facebook



案例四：Facebook傳來的聯結

不直接點選任何來自即時通訊聯絡人所傳來的超連結

陳[redacted]被標記在海派小甜心的相片中。

蜜糖★甜心3

❤[redacted]❤ 每日舉辦火辣派對,讓你體驗超刺激感官享受
【 http://26best99.weebly.com/ 】 日系美眉全天候線上為您服務^O^ ►
http://26best99.weebly.com/ ◄寂寞的夜晚有我陪你聊天，上千位台灣美眉真人視訊聊天室!!
http://14avgirl.weebly.com/

15 小時前

陳[redacted]被標記在林文鈞的相簿中。

您利用零碎的時間,用電腦建立一份穩定的收入!

大愛(燦爛星空)拍攝點滴./您可以利用零碎的時間,在家用電腦建立一份穩定的收入! 它就像您在網路上開一家店! 當您的店上軌道之後,您就會有一份持續而穩定的收入! 當您在上班時您的店不會休息,它還在幫您賺錢! 當您無法工作時您的店不會休息,它還在幫您賺錢! 當您在旅行時您的店不會休息,它還在幫您賺錢! 當您在睡覺時您的店不會休息,它還在幫您賺錢! 免費註冊報名,90天免費在家了解! http://wenchunlin.weebly.com/

昨天 14:49

網路詐騙的因應之道

- 人身安全優先原則
- 避免個人資料外漏或被冒用
- 維護個人帳號密碼的安全
- 確認信用記錄且盡量當面交易

39

被入侵了怎麼辦

- 電腦、網路帳號(MAIL信箱、網路銀行、MSN /Yahoo)遭入侵或成為跳板主機該怎麼辦？
  - 電腦遭入侵立即離線(拔除網路線或關閉網路設備)
  - 帳號遭入侵在乾淨的電腦立即更改可能被偷竊的帳號 MAIL信箱、網路銀行、MSN/Yahoo…
  - 向服務廠商檢舉(ISP 、信箱、銀行、MSN/Yahoo..,)
  - 電腦實施掃毒掃駭及修補作業，或重新安裝 (如有損失或被利用侵犯他人宜報案並保留硬碟資料)
  - 換掉該電腦的帳號與密碼
  - 通知朋友要注意避免因帳號遭盜用導致親友受害

被入侵了怎麼辦

- 報警留記錄
  - ✓ 網路連線記錄、資安設備(如防火牆、入侵偵測)軌跡紀錄。
  - ✓ 電腦本身的軌跡紀錄
  - ✓ E-Mail帳號的收件、發送及登錄記錄(ISP)
  - ✓ 被竊帳號的使用記錄
  - ✓ 立即封存電腦不要再開機/重灌之前保留原始硬碟備案作為木馬入侵 / 被當成跳板轉發MAIL 或入侵他人之抗辯依據。

41

警察大人我要報案

- 報案：要準備甚麼?
  - 網路遊戲寶物被偷? 網路銀行存款不翼而飛?
  - 人、事、時、地、物、紀錄
- 報案機構
  - 科技犯罪中心已成立，各地分局亦有專責網路犯罪承辦人。
  - 調查局可接受報案。

42

報案管道

- 各地區警察局110
- 內政部刑事警察局-線上檢舉信箱

  http://www.cib.gov.tw/mail/Mail_Report.aspx

  電話：(02) 2766-1919 、 (02) 2766-8989
- 法務部調查局-陳情檢舉信箱

  http://www.mjib.gov.tw

  檢舉電話：(02)2917-7777 、 (02)2918-8888
- 國家通訊傳播委員會

  http://www.ncc.gov.tw/

  檢舉電話： 0800177177

社交工程攻擊之防範

- 建立社交工程防範技術措施*(Engineering)*
- 辦理相關宣導及法治認知*(Enforcement)*
- 加強資安訓練與演練*(Education)*

目錄

- 惡意電子郵件防範宣導

電子郵件的隱憂


等你喔..... - 郵件 (RTF 文字)
傳送(S)
選項(P)...
檔案(F) 編輯(E) 檢視(V) 插入(I) 格式(O) 工具(T) 執行(A)
說明(H)
Arial
12
收件者...
Hsu, Magic
副本(C):
密件副本(B)...
主旨(J):
等你喔.....
Hi Magic,
我什麼都會，只看你敢不敢打，等你喔!!!
視訊聊天室... http://www.sex-come.com
明日世界生活購物網
http://www.tomorrow.com.tw
acer
M35
LINUX/XP-HOME
AMD Sempron 2800+
256MB DDR400
80GB/7200RPM
光碟機COMBO機
超值推薦價
$9800/$12255
宏基桌上型電腦
本日最HOT
(平)CASIO Z750
(平)PanasonicFX9
(平)NIKON CP5600

惡意郵件攻擊手法

- 偽裝熟悉或可信任的寄件者
- 郵件主旨與內文與收件者相關或吸引興趣
- 附加檔案都包裝有惡意程式
- 郵件內的網路連結導向惡意網站
- 攻擊主要利用使用者系統應用程式的弱點

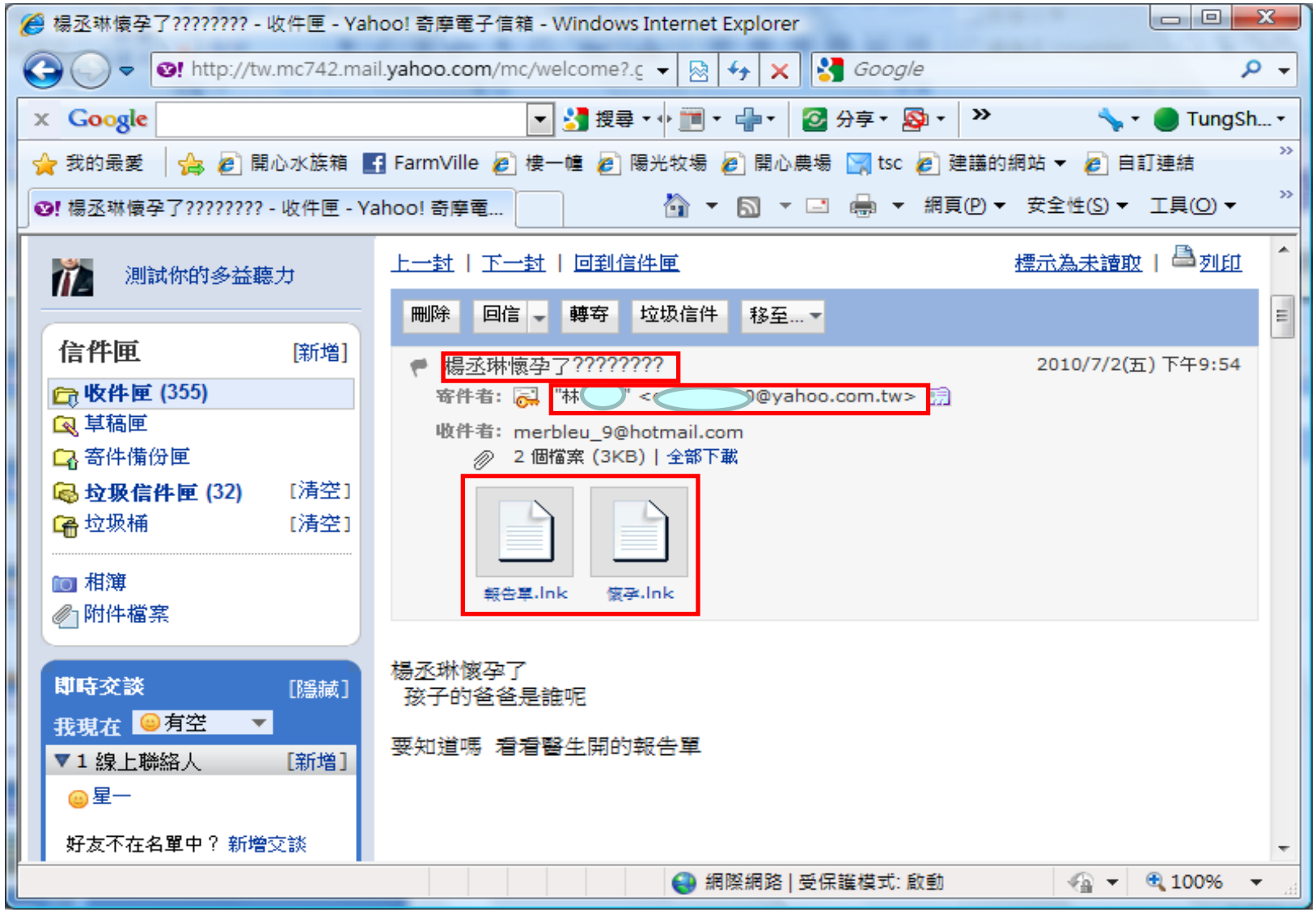
電子郵件社交工程郵件類型

- 八卦影視
- 休閒娛樂
- 保健養生
- 財經資訊
- 情色內容
- 新奇資訊
- 郵件內容包含圖片、連結、*Word*附檔及*PowerPoint*附檔

惡意電子郵件範例一


玉山銀行電子對帳單 - 郵件 (HTML)
檔案(F) 編輯(E) 檢視(V) 插入(I) 格式(O) PGP 工具(T) 執行(A) 說明(H)
回覆(R) 全部回覆(L) 轉寄(W)
寄件者: 玉山銀行 [esuntrust@email.esunbank.com.tw]
副本:
主旨: 玉山銀行電子對帳單
附件: 電子對帳單.xls (62 KB)
您好！本行預設電子對帳單爲加密信件，開啓檔案的解壓縮密碼爲您的身分證字號，英文請輸入大寫。
若您不需對帳單加密服務，煩請登入本行網路銀行->帳單服務->電子帳單加密功能，選擇「不加密」即可。
網站連結：https://netbank.esunbank.com.tw/nbsvr2001/

惡意電子郵件範例二


楊丞琳懷孕了???????? - 收件匣 - Yahoo! 奇摩電子信箱 - Windows Internet Explorer
http://tw.mc742.mail.yahoo.com/mc/welcome?c
Google
測試你的多益聽力
上一封 | 下一封 | 回到信件匣
標示為未讀取 | 列印
刪除 回信 轉寄 垃圾信件 移至...
信件匣 [新增]
收件匣 (355)
草稿匣
寄件備份匣
垃圾信件匣 (32) [清空]
垃圾桶 [清空]
相簿
附件檔案
即時交談 [隱藏]
我現在 有空
1 線上聯絡人 [新增]
星一
好友不在名單中？ 新增交談
楊丞琳懷孕了????????
2010/7/2(五) 下午9:54
寄件者: "林 <@yahoo.com.tw>
收件者: merbleu_9@hotmail.com
2 個檔案 (3KB) | 全部下載
報告單.lnk
懷孕.lnk
楊丞琳懷孕了
孩子的爸爸是誰呢
要知道嗎 看看醫生開的報告單
網際網路 | 受保護模式: 啟動
100%

惡意郵件防範停看聽(1)

- 惡意電子郵件防範宣導影片

- 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(推動電子識別證)

惡意郵件防範停看聽(2)

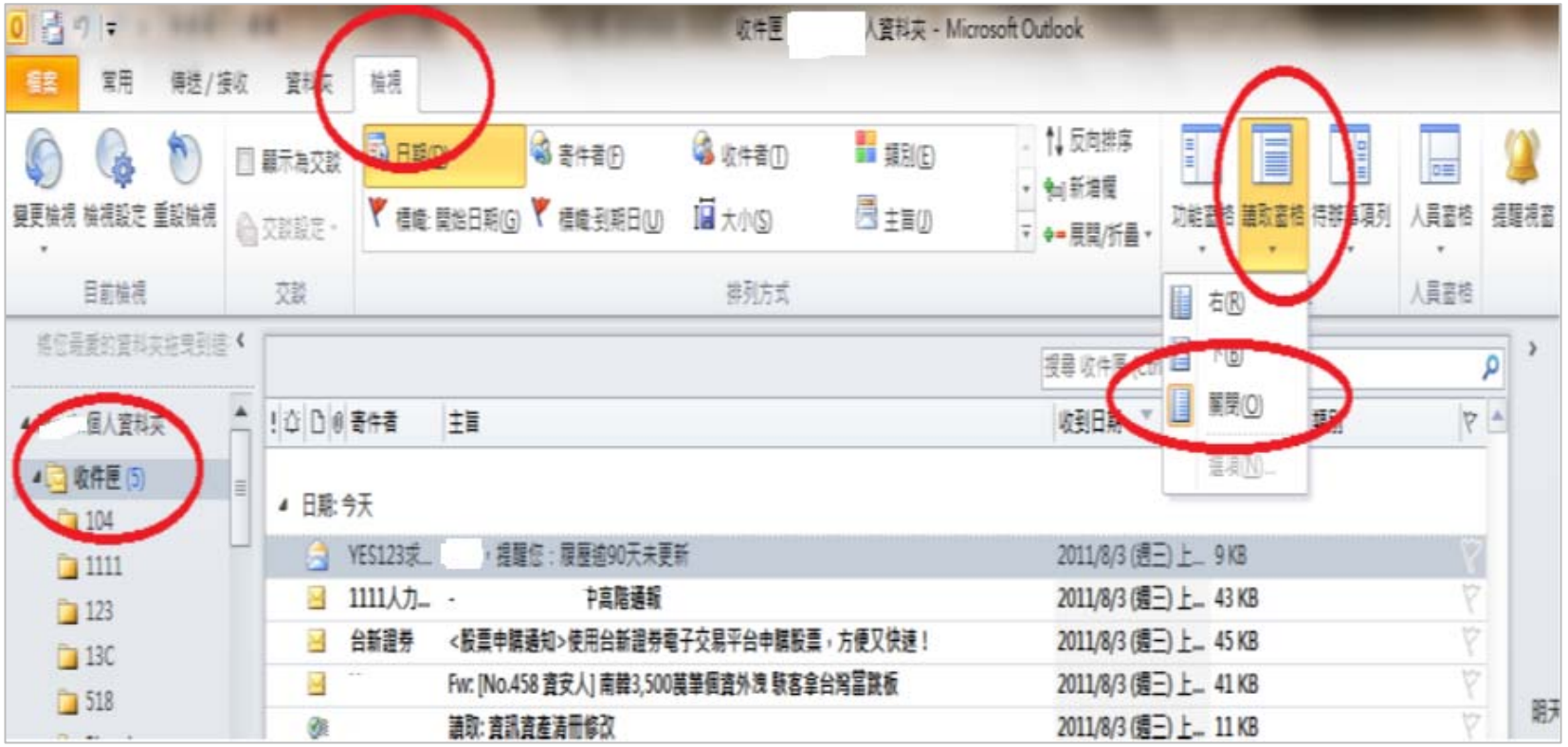
- **看** — 收到郵件後，必須注意
  - 郵件主旨是否與本身業務相關
  - 其餘郵件不建議開啟，如需開啟應確認郵件來源
- 開啟電子郵件前應先依序檢視：
  (1)【寄件者】
  (2)【郵件主旨】
  (3)【附加檔案】等郵件訊息
- 【寄件者】或【郵件主旨】與公務無關者，建議應立即刪除不要開啟郵件

惡意郵件防範停看聽(3)

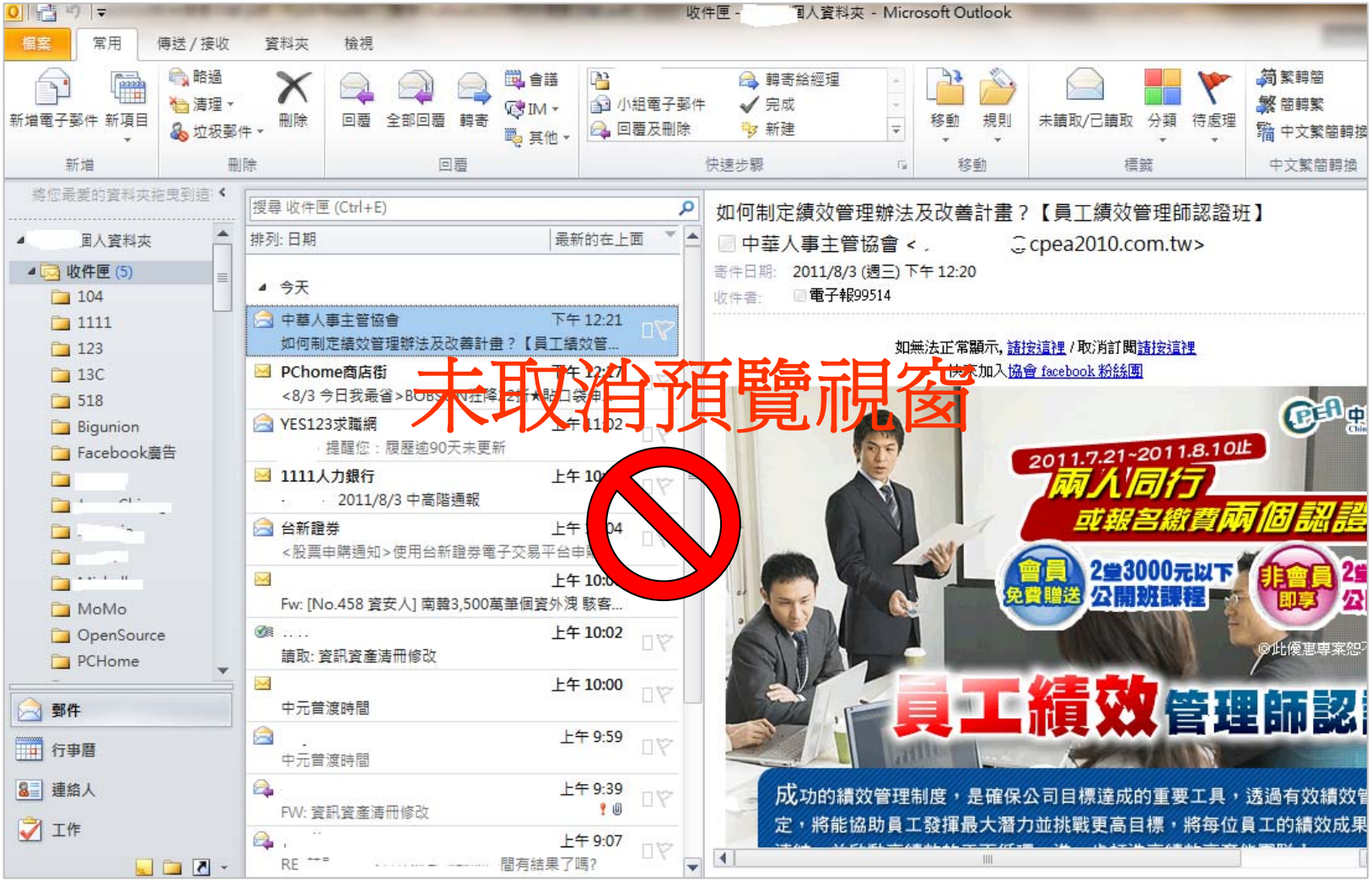
- 聽 — 若懷疑郵件來源，必須進行確認
  - 透過電話或電子郵件向寄件人於開啟前確認郵件真偽

Outlook 2010取消讀取窗格功能

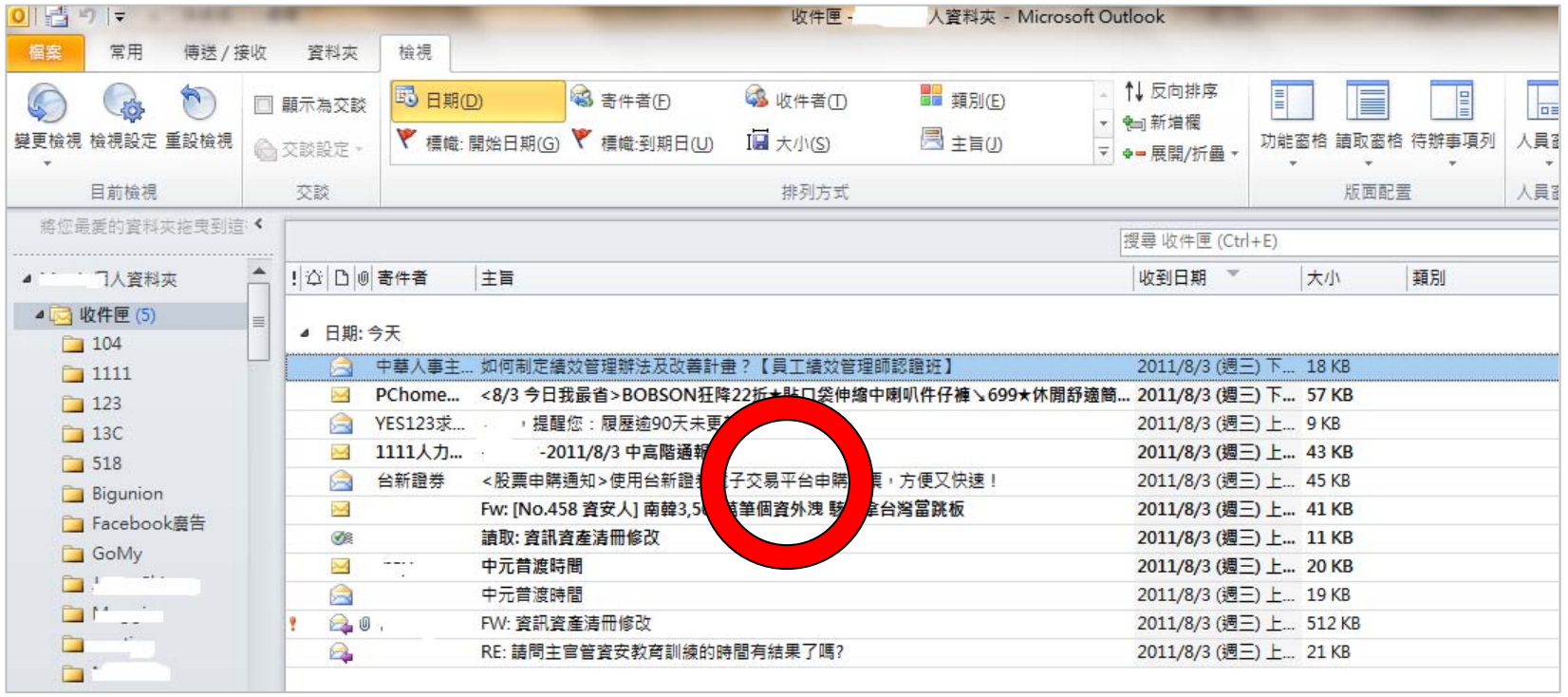
- 【檢視】>【收件夾】>【讀取窗格】>【關閉】
  (每個資料夾皆須各自設定成關閉)



預覽視窗範例(1/2)

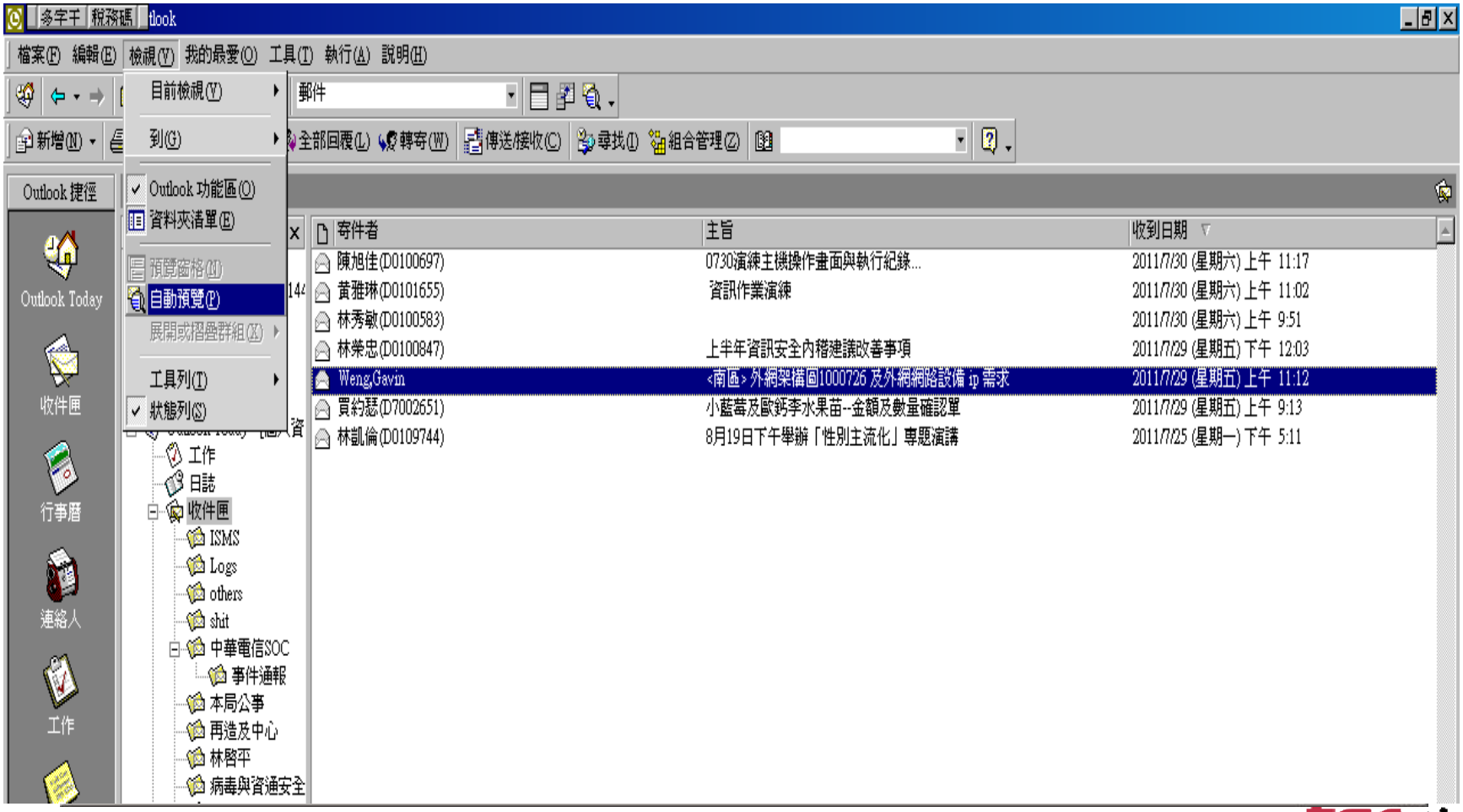

收件匣 - 個人資料夾 - Microsoft Outlook
檔案
常用
傳送 / 接收
資料夾
檢視
新增電子郵件
新項目
刪除
回覆
全部回覆
轉寄
會議
IM
其他
小組電子郵件
回覆及刪除
轉寄給經理
完成
新建
移動
規則
未讀取/已讀取
分類
待處理
繁轉簡
簡轉繁
中文繁簡轉換
新增
刪除
回覆
快速步驟
移動
標籤
中文繁簡轉換
將您最愛的資料夾拖曳到這
個人資料夾
收件匣 (5)
104
1111
123
13C
518
Bigunion
Facebook廣告
MoMo
OpenSource
PCHome
郵件
行事曆
連絡人
工作
搜尋 收件匣 (Ctrl+E)
排列: 日期
最新的在上面
今天
中華人事主管協會 下午 12:21
如何制定績效管理辦法及改善計畫？【員工績效管...
PChome商店街
<8/3 今日我最省>
YES123求職網
提醒您：履歷逾90天未更新
1111人力銀行
2011/8/3 中高階通報
台新證券
<股票申購通知>使用台新證券電子交易平台申
Fw: [No.458 資安人] 南韓3,500萬筆個資外洩 駭客...
上午 10:02
讀取: 資訊資產清冊修改
上午 10:00
中元普渡時間
上午 9:59
中元普渡時間
上午 9:39
FW: 資訊資產清冊修改
上午 9:07
RE
間有結果了嗎?
如何制定績效管理辦法及改善計畫？【員工績效管理師認證班】
中華人事主管協會 < cpea2010.com.tw>
寄件日期: 2011/8/3 (週三) 下午 12:20
收件者: 電子報99514
如無法正常顯示, 請按這裡 / 取消訂閱請按這裡
快來加入協會 facebook 粉絲團
未取消預覽視窗
2011.7.21~2011.8.10止
兩人同行
或報名繳費兩個認證
會員免費贈送
2堂3000元以下公開班課程
非會員即享
員工績效管理師認
成功的績效管理制度，是確保公司目標達成的重要工具，透過有效績效管
定，將能協助員工發揮最大潛力並挑戰更高目標，將每位員工的績效成果

預覽視窗範例(2/2)


收件匣 - 人資料夾 - Microsoft Outlook
檔案
常用
傳送 / 接收
資料夾
檢視
變更檢視
檢視設定
重設檢視
目前檢視
顯示為交談
交談設定
交談
日期(D)
寄件者(F)
收件者(T)
類別(E)
標幟: 開始日期(G)
標幟:到期日(U)
大小(S)
主旨(J)
反向排序
新增欄
展開/折疊
排列方式
功能窗格
讀取窗格
待辦事項列
版面配置
將您最愛的資料夾拖曳到這
人資料夾
收件匣 (5)
104
1111
123
13C
518
Bigunion
Facebook廣告
GoMy
搜尋 收件匣 (Ctrl+E)
寄件者
主旨
收到日期
大小
類別
日期: 今天
中華人事主... 如何制定績效管理辦法及改善計畫？【員工績效管理師認證班】 2011/8/3 (週三) 下... 18 KB
PChome... <8/3 今日我最省>BOBSON狂降22折★貼口袋伸縮中喇叭件仔褲↘699★休閒舒適簡... 2011/8/3 (週三) 下... 57 KB
YES123求... 提醒您：履歷逾90天未更 2011/8/3 (週三) 上... 9 KB
1111人力... -2011/8/3 中高階通 2011/8/3 (週三) 上... 43 KB
台新證券 <股票申購通知>使用台新證 子交易平台申購 ，方便又快速！ 2011/8/3 (週三) 上... 45 KB
Fw: [No.458 資安人] 南韓3,5 筆個資外洩 駭 台灣當跳板 2011/8/3 (週三) 上... 41 KB
讀取: 資訊資產清冊修改 2011/8/3 (週三) 上... 11 KB
中元普渡時間 2011/8/3 (週三) 上... 20 KB
中元普渡時間 2011/8/3 (週三) 上... 19 KB
FW: 資訊資產清冊修改 2011/8/3 (週三) 上... 512 KB
RE: 請問主官管資安教育訓練的時間有結果了嗎? 2011/8/3 (週三) 上... 21 KB

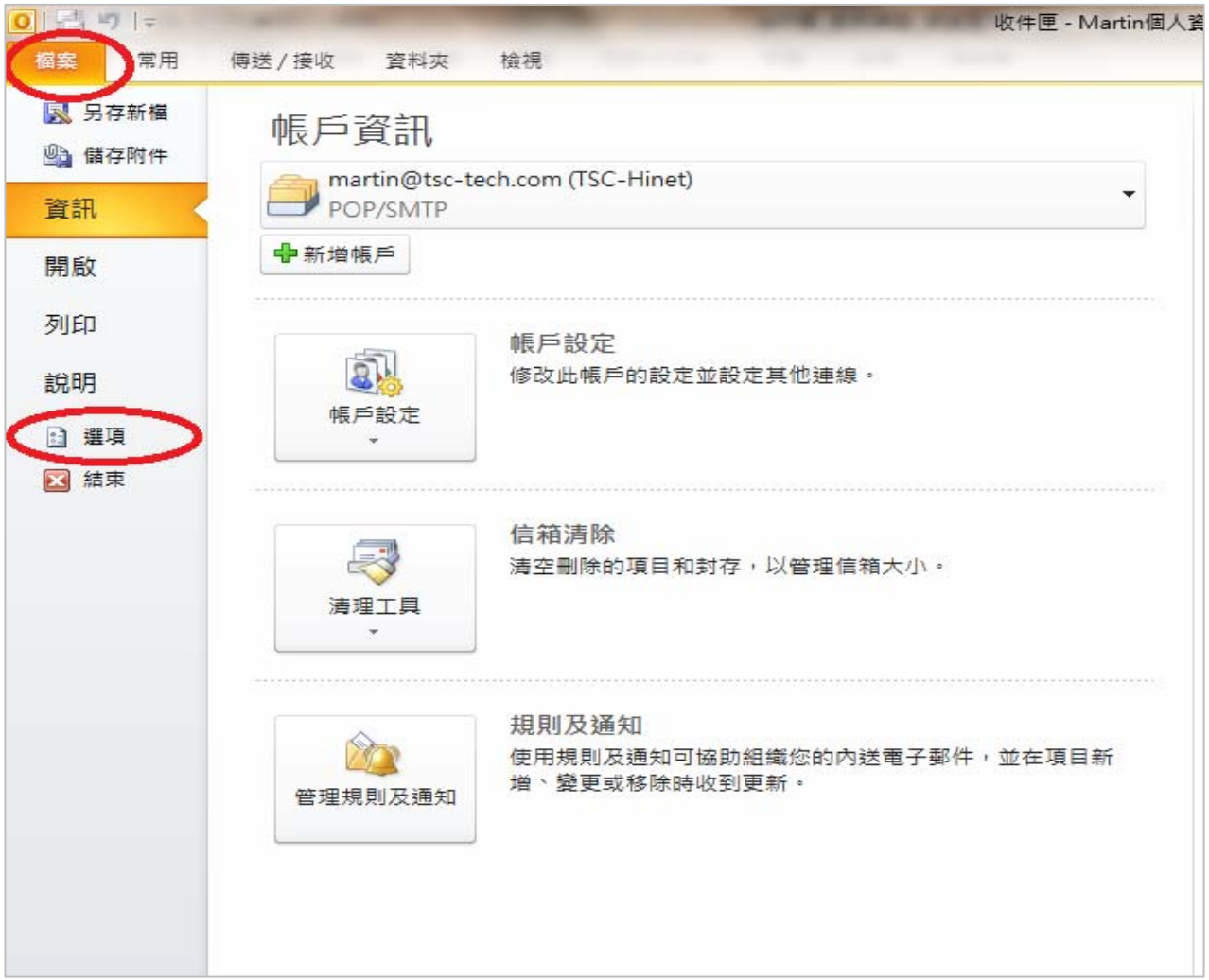
惡意電子郵件社交工程演練因應措施

- 關閉自動預覽功能(outlook 2003版以前)
  - 每個資料匣均需關閉



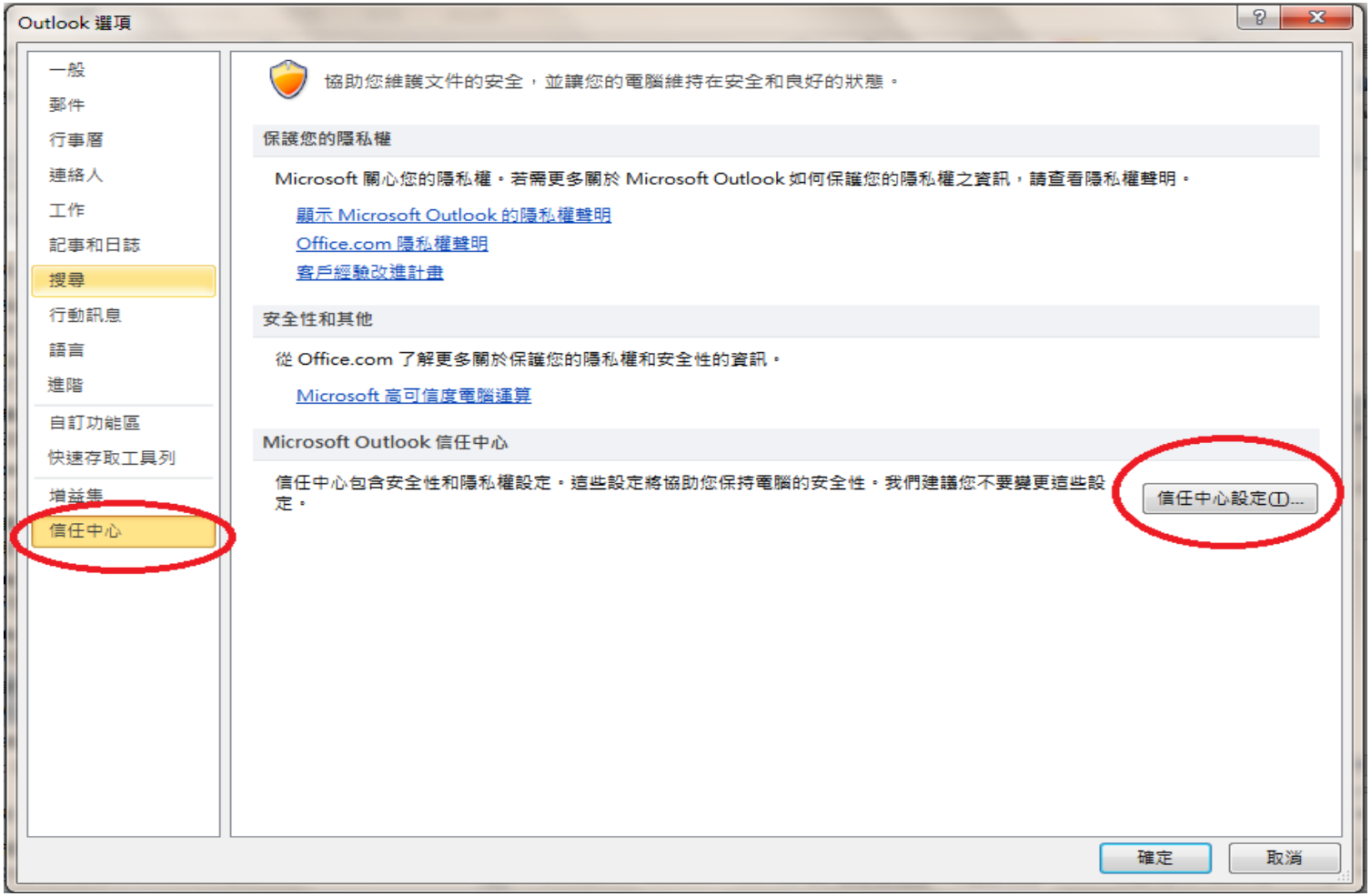
關閉Outlook 2010附件預覽功能(1/3)

- 點選【檔案】>【選項】



關閉Outlook 2010附件預覽功能(2/3)

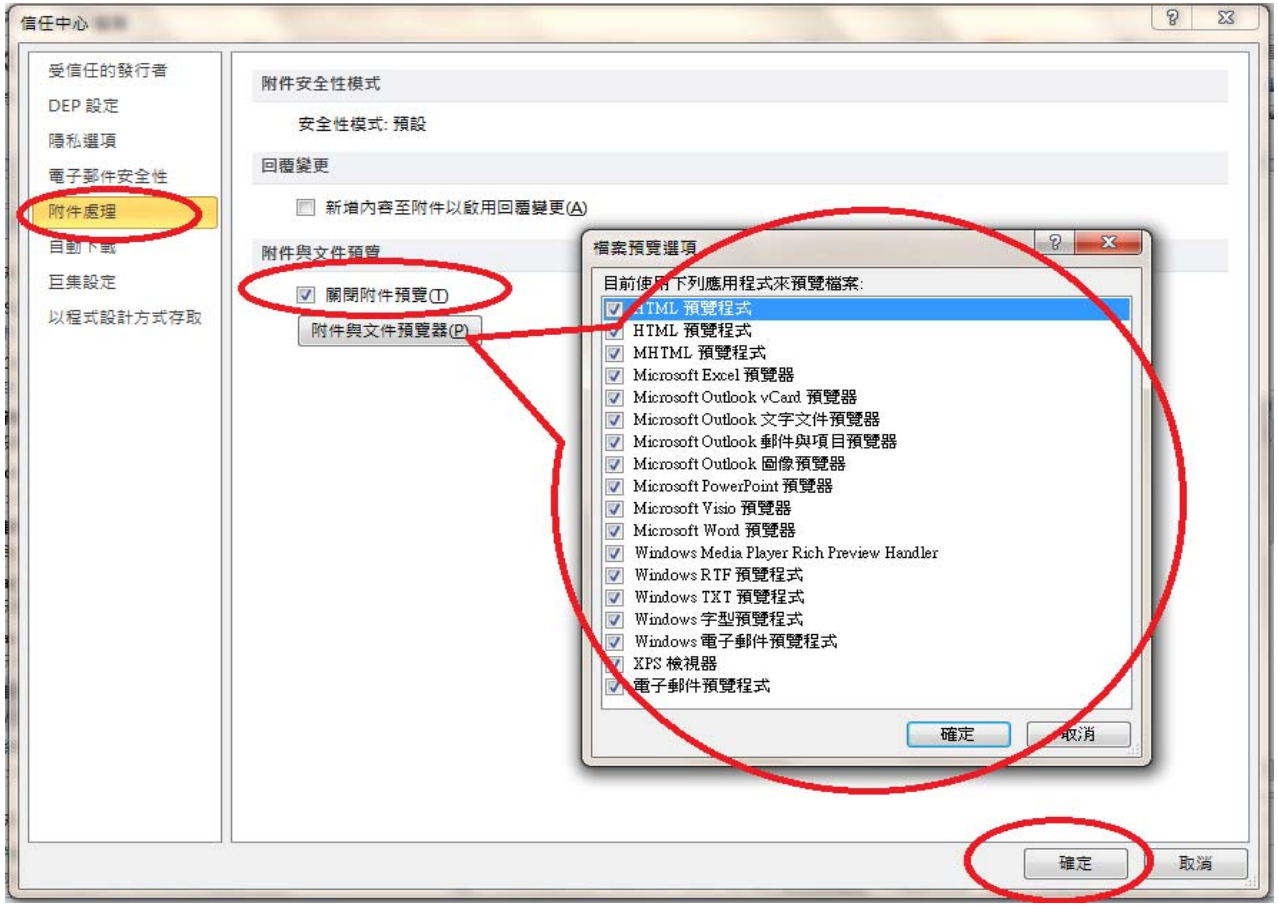
- 點取【信任中心】 > 右邊的【信任中心設定】



關閉Outlook 2010附件預覽功能(3/3)

- 【附件處理】 >勾選右邊的【關閉附件預覽】

(記得按【確定】後離開，並關閉Outlook後重新開啟outlook，設定才會生效)

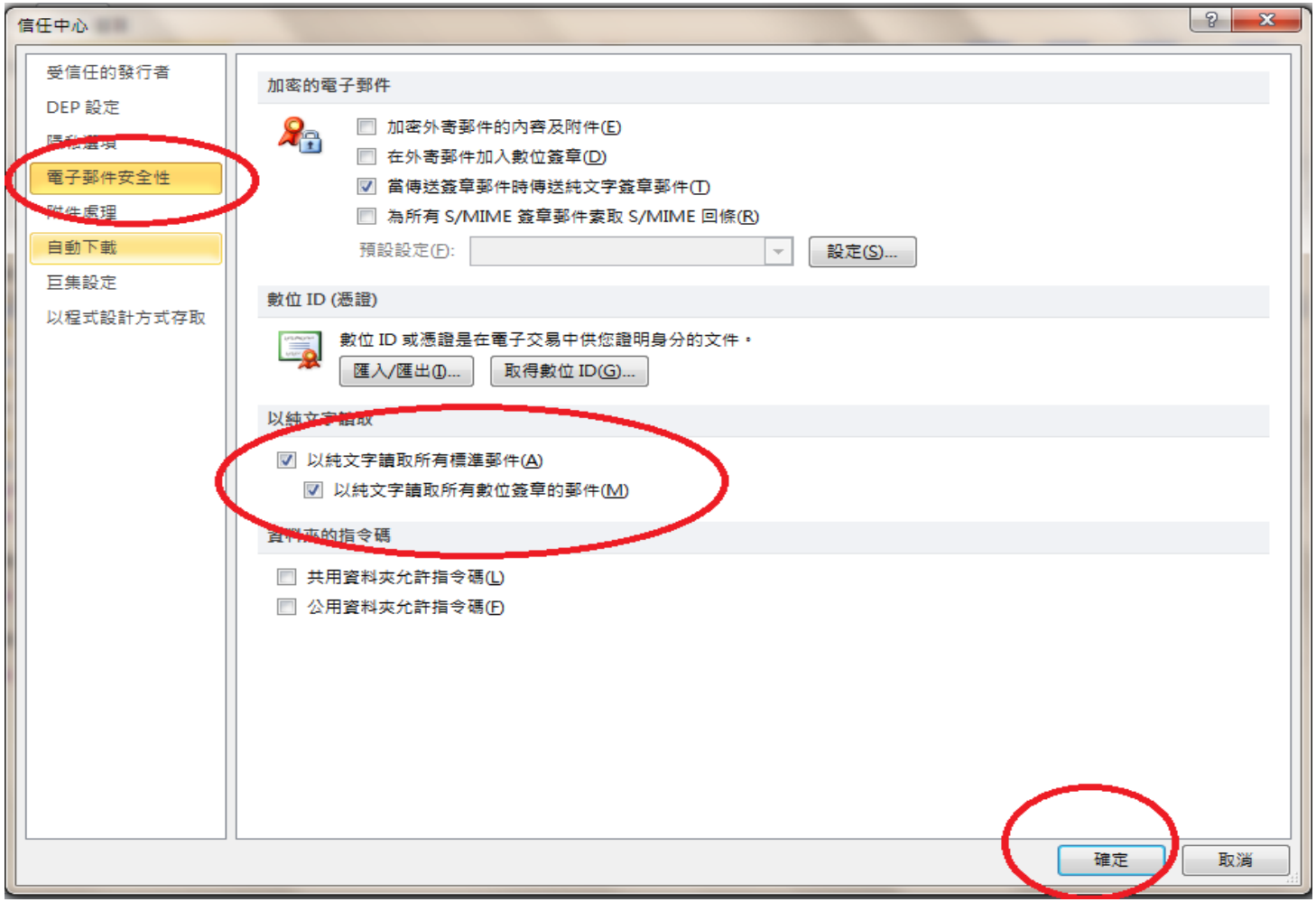


附件預覽範例


附件工具
FW: 資訊資產清冊修改 - 郵件 (HTML)
檔案
郵件
附件
開啟
快速列印
另存新檔
儲存所有附件
移除附件
全選
複製
簡繁轉簡
繁簡轉繁
中文繁簡轉換
顯示郵件
動作
選取項目
中文繁簡轉換
郵件
檔案名稱: ISMS-04-01風險評鑑報告v1.5_20110802.doc
大小: 487 KB
作者: r
2011年8月2日星期二
訊息
ISMS-04-01風險評鑑報告v1.5_20110802.doc (487 KB)
未關閉附件預覽功能
臺北市
局
資訊安全管理制度（ISMS）導入建置案

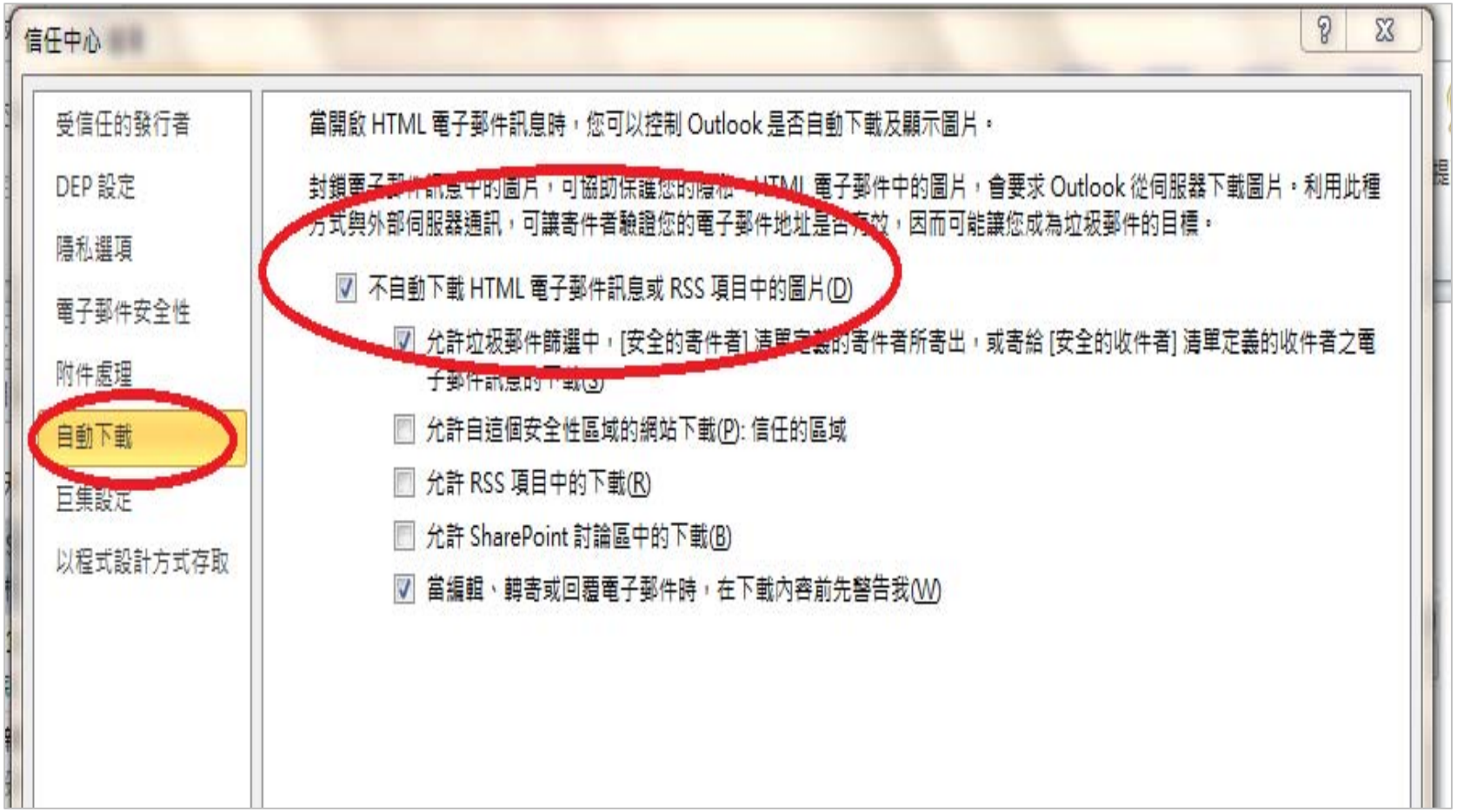
Outlook 2010以純文字讀取電子郵件

- 【電子郵件安全性】>勾選【以純文字讀取所有標準郵件】



Outlook不自動下載HTML中的圖片

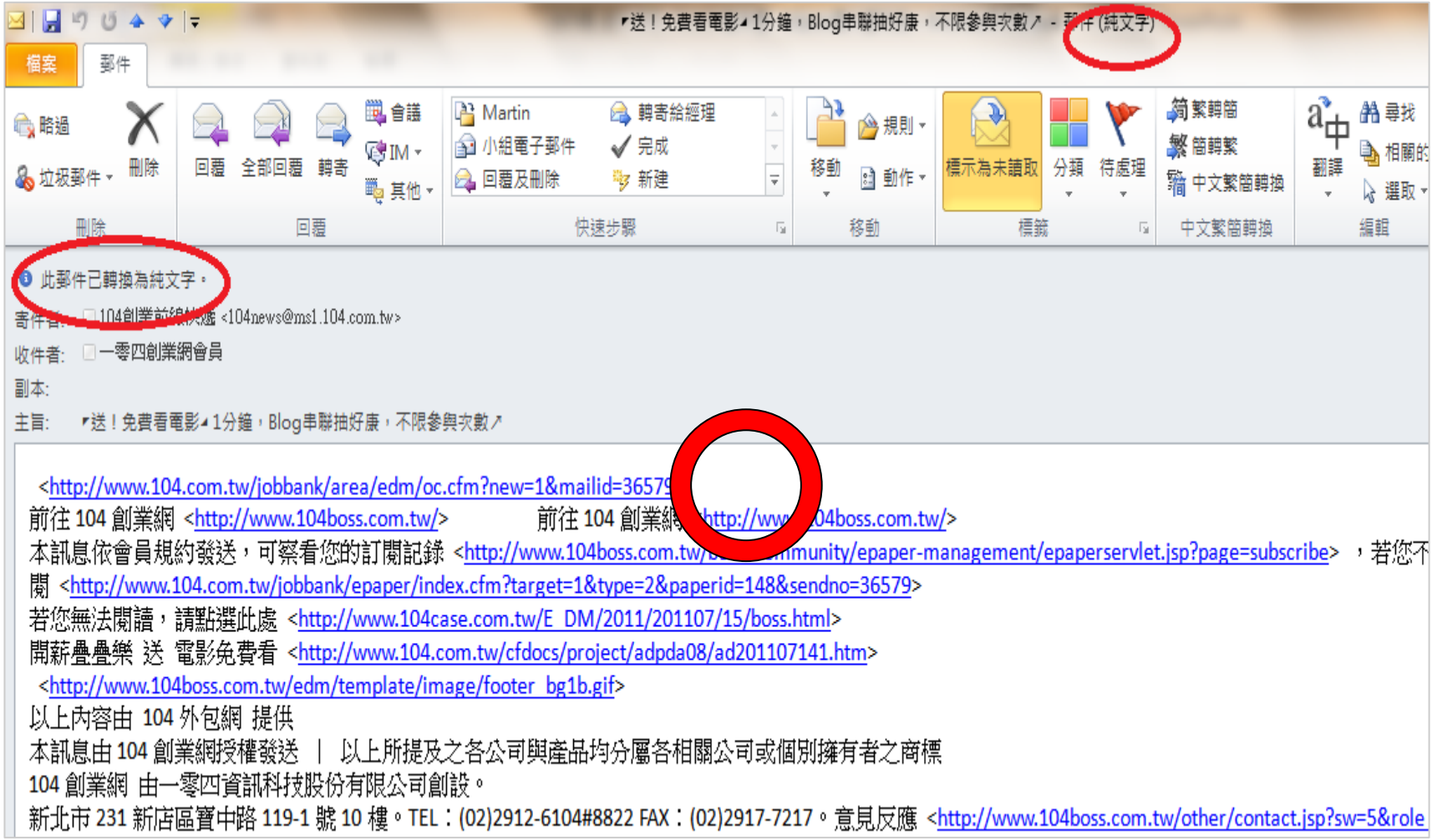
- 【自動下載】>勾選【不自動下載HTML電子郵件訊息或RSS項目中的圖片】



未以純文字及關閉圖片讀取範例(1/2)

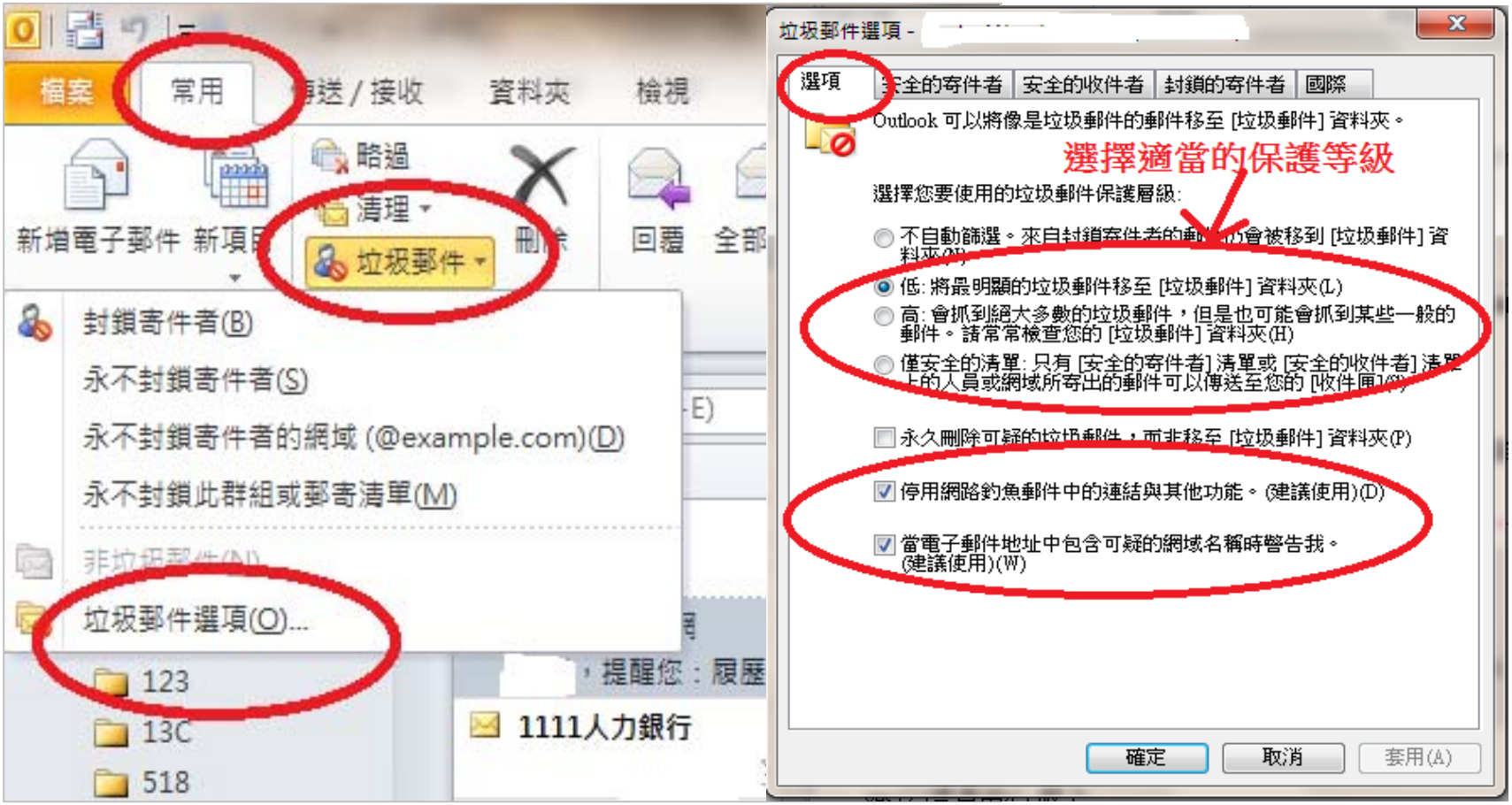
未取消圖片預覽及以純文字讀取

以純文字及關閉圖片讀取郵件範例(2/2)



Outlook 2010選用垃圾郵件功能

- 【常用】>【垃圾郵件】>【垃圾郵件選項】>【選項】>選擇適當的保護等級與保護



使用者端郵件安全管理

目錄

- USB儲存媒體使用安全

USB隨身碟的風險

- 因為其便利性，易於毀損、遺失或遭竊。
- 外型設計多樣化，不易被偵測。
- 功能多樣化，實務作業上不易杜絕使用。
- 設備周邊及通訊功能設計安全性的保護不足，在公共場合使用時，易被有心人士竊取資料或進行破壞。
- 大多數USB隨身碟無法產生事件記錄，故無法追蹤其使用過程。

USB隨身碟的風險

- 保存重要或機密資料，容易成為有心人士竊取的目標。
- 常被共享使用，讓病毒擴散情形更為嚴重，甚至進入內部網路進行擴散。

USB隨身碟的威脅

- 病毒—容易將病毒由家中電腦或其他地方帶進辦公室之電腦，造成內部網路中斷。
- 惡意程式—使用USB隨身碟，易將後門程式帶進辦公室內電腦，導致機密外洩。
- 公司內部不滿員工或有心人士—因對公司不滿或是人員離職，透過USB隨身碟，複製重要資料。

USB隨身碟的威脅

- 資料遺失—容易造成資料遺失。
- 非法軟體—任意在公司內部使用非法軟體會讓機關面臨侵權風險。

USB隨身碟病毒特性

- 常見的病毒檔案為kavo.exe、ntdelect.com、kavo1.dll 、ubs.exe。
- 在各磁碟機下產生autorun.inf檔案，而autorun.inf通常為隱藏檔 ，並利用autorun.inf的特性啟動指定的惡意程式，造成感染。
- 感染病毒後系統無法勾選顯示隱藏檔的選項，藉以避免使用者發現病毒檔案。

案例一：遺失USB個資外洩

香港醫院遺失USB 47名病人個資涉其中

作者：何依玟 -03/30/2009

香港聯合醫院一名女眼科醫師日前將存有47名病人個人資料的USB隨身碟遺失，裡頭包括病患姓名、身分證號碼、及曾接受的手術名稱等資料。

有消息指出，該名醫生為進修需要，自行下載病人病歷等個人資料，並儲存入自己的USB隨身碟內，該名醫生在自行搜索下，並未尋獲遺失的USB，故向醫院通報該事件。而醫院方面，除了要進一步釐清她抄下病人資料的目的，也已向33名的受害者進行通知，院方表示，所幸至今未傳出有接獲病人資料外洩的查詢和記錄。

初步調查，院方認為該名員工未遵守資料安全保護守則，即使用可攜式媒體前須向醫院申請。香港食物及衛生局表示，醫院建立制度來保障病人隱私，這些資料應先刪除病患姓名及身分證號碼後，才可下載。這次的事件，相關部門的主管必須為此負責。

資料來源： 資安人雜誌網頁2009/03/30

案例二：公務家辦

- 一名簡姓中尉飛行官以USB硬碟將公務資料從營區複製後帶回家處理，但因個人電腦遭木馬程式感染，導致包括國軍年度重要演訓「○○二十三號」資料、飛行前任務提示等十多種機密文件，甚至連機密等級相當高的電戰機資料外洩。
- 空軍已責由該基地成立緊急應變小組，逐一清查單位內所有公務電腦，以避免遭感染植入惡意程式。

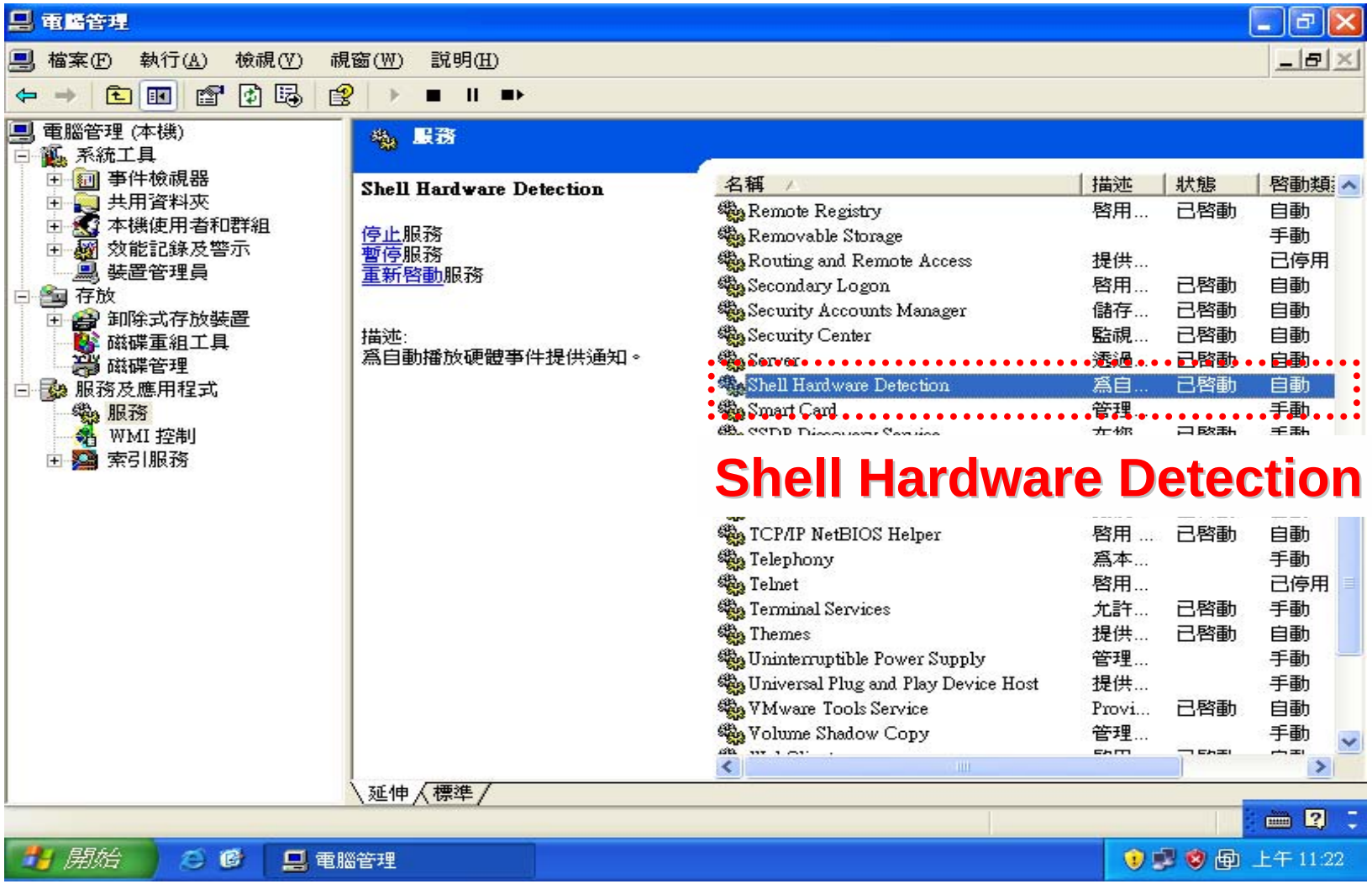
案例三：公務家辦

- 根據媒體報導，國防大學某上校教官違反資安管制規定，將漢光演習機密資料藉由隨身碟帶回家「辦公」，雖無洩露軍機目的，但卻因家中電腦遭中國網軍入侵植入木馬，造成漢光23號演習「攻擊軍」的機密資料外洩，內容包括各軍種簡報內容與演習動次表等引起高度重視。

防範USB隨身碟的威脅

- 使用隨身碟前需先行掃毒。
- 避免將未經加密之機密資料存放於USB隨身碟。
- 避免將私人的USB隨身碟到處使用。
- 選用具有硬體防寫功能的USB 隨身碟，沒有寫入必要時，設定為防寫狀態。
- 定期格式化隨身碟，尤其曾經在其他電腦使用後。
- 關閉作業系統上 USB 自動執行功能。

關閉USB隨身碟自動執行



USB埠封鎖的11種方法

USB埠封鎖可分3大類-11種方式

- 第1大類---實體封鎖
  - 黏上易碎貼紙
    - 優點：從肉眼就可以分辨電腦的USB埠有無使用過的跡象
    - 缺點：貼紙不小心破裂時，容易引起誤會
  - 用熱熔膠堵住
    - 優點：可確實封鎖USB埠
    - 缺點：USB埠硬體隨之損壞，無法使用
  - 移除主機板上的跳接器
    - 優點：使USB埠功能達到真正的完全失效
    - 缺點：管理欠缺彈性，重新啟用USB埠功能時，需開機殼插回跳接器
  - 插上專用介面卡或硬體鎖
    - 優點：重新啟用時，不需要拆掉細部硬體，或者重新開機，原本的操作方式不會因此中斷或改變
    - 缺點：每台電腦均需安裝

USB埠封鎖的11種方法

- 第2大類---修改系統設定
  - 停用BIOS的相關設定
    - 優點：設定容易，做法簡單
    - 缺點： BIOS的管理密碼可能被破解
  - 利用群組原則集中控管(AD)
    - 優點：適用於大量電腦環境，可批次強制實施，統一設定
    - 缺點：僅windows系統及加入AD之電腦適用
  - 修改電腦內的特定登錄機碼
    - 優點：設定簡單
    - 缺點：對於了解電腦操作的人來說，效果有限
  - 刪除USB儲存裝置的驅動程式
    - 優點：可針對不同USB裝置個別控管
    - 缺點：僅能針對先前未曾連接USB儲存裝置的電腦

USB埠封鎖的11種方法

- 第3大類---利用專屬的周邊控管解決方案
  - 建置USB管理系統
    - 優點：可視需求開放一部分的功能，具備良好的管理彈性
    - 缺點： 建置成本高
  - 將重要檔案予以加密
    - 優點：可讓員工正常使用USB埠，並能防止裝置遺失
    - 缺點：檔案密碼管理不易一旦金鑰遺失，就無法開啟隨身碟裡的檔案
  - 建置DLP解決方案
    - 優點：可以有效防止機密資料透過各種途徑外流，同時無需封鎖USB埠功能
    - 缺點：建置成本高

Thank you