電子郵件社交工程介紹與資安防範

- 資 訊 科 技 與 競 爭 優 勢 -

李政峰 (James Lee)
經濟部工業局-能源管理系統輔導顧問
E-mail：jameslee1858@gmail.com

- ISO 27001 主導稽核員
- ISO 20000 主導稽核員
- BS 25999 主導稽核員
- BS 10012 主導稽核員

簡報大綱

0. 前言
1. 什麼是電子郵件社交工程
2. 如何防止Email受駭
3. 行動裝置安全防範
4. 物聯網與安全威脅
5. 網路安全事件分享
6. 課後評量

張善政：中國將台灣當網攻試驗場

「自己的資安自己救」

- 〔自由時報記者鍾麗華／台北報導2015.01.22〕行政院召開資安會報，會報召集人、行政院副院長張善政在會後記者會指出，政府機關每年有三百多件資安事件通報，而且資安攻擊時間點多發生在節慶、選舉等政經事件時，他強調，「**中國把台灣當作網路資訊攻擊試驗場**」，很多手法是全球首見。

歐盟美國指定與我資安交流

2014 是資料外洩年

- 2014 年的網路犯罪主要動機以個資盜竊為主，佔所有資料外洩 54%，超過其他任何外洩事故類別。
- 個資盜竊外洩事故亦佔最嚴重資料外洩事故的三分之一，外洩事故於去年也變得更加嚴重，根據外洩水平指數評分，50宗最嚴重的外洩事故有三分之二於 2014 年發生，涉及 1 億多受影響數據紀錄，是 2013 年數字的一倍。

資料來源：數碼保安供應商 Gemalto 發表最新的外洩水平指數(Breach Level Index；BLI)

0.前言-電子郵件社交工程演練計畫

- 教育部每年實行2次電子郵件社交工程演練
- 由技術小組以偽冒公務、個人或公司行號等名義發送惡意郵件給演練對象，統計惡意郵件**開啟率**及**連結**或檔案**點閱率**，並記錄**開啟**及**點閱**狀況 。
- 演練作業不會植入後門程式及讀取個人電腦資料，不會影響正常公務執行。

- **電子郵件社交工程的主旨類型有：**
  - **政治新聞、公務相關、科技新知 、保健養生、休閒娛樂、影劇八掛、情色內容、體育新聞等類型，郵件內容包含連結網址或word附檔。**

0.前言-獎懲規定

- 各單位之惡意郵件開啟率應低於10%以下；
- 惡意連結(或檔案)點擊率應低於6%以下。
- 預定於每年10月底前，針對電子郵件社交工程演練(6月、10月)結果，選取績優單位、持續改善單位、加強改善單位及未依本執行方案辦理單位，辦理敘獎作業。

★教育部(資訊及科技教育司)會函告知演練結果(開啟名單)：

內容：誰、幾點幾分，做了什麼行為

教育部實施電子郵件社交工程演練類型

編號	信件類別	信件標題
Letter 1	生活類	【必看瘋傳】一個高階主管在台積電【賣命癌症過世後給大家的啟示】
Letter 2	知識類	改變孩子一生的5個習慣
Letter 3	科技類	關於蚊子的一些事
Letter 4	美女類	瑜珈女神性感誘惑　史上最辣開球沒有之一
Letter 5	美容類	呼吸就能瘦　美女中醫示範腹式呼吸法
Letter 6	旅遊類	【驚奇景點】聽說最近台灣很紅！最受國際矚目的台灣旅遊奇觀登場
Letter 7	財經類	央行打房下一波？　專家：桃園、新竹恐遭殃
Letter 8	時事類	提早規劃財務 年初退休最省稅
Letter 9	健康類	看清這10點，讓你果汁喝得更安心！
Letter 10	新奇類	智利政府認證：確有UFO！詭異飛行器不是戰機！

教育部實施電子郵件社交工程演練類型

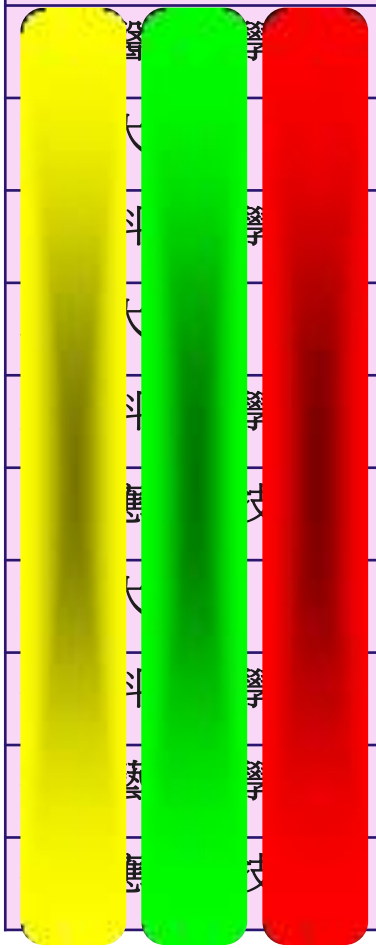
編號	信件類別	信件標題
Letter 1	生活類	台電烏龍帳單頻傳！你有注意過你家的電
		費是否合理嗎?
Letter 2	知識類	到底是先有雞還是先有蛋！？答案公佈了！
Letter 3	美女類	世足正妹比一比！你最喜歡哪位！
Letter 4	美容類	女生不可不知的夏日四大困擾
Letter 5	健康類	炎炎夏日，喝杯清涼的飲料最爽快！但是你知道什麼飲料會讓你越喝越肥嗎?
Letter 6	教育類	明年指考 單選題可望取消倒扣
Letter 7	趣味類	睡要有睡相！你沒看過的精采睡相....
Letter 8	時事類	公務員退休八五新制 明年元月上路
Letter 9	旅遊類	鐵道迷的參加！ 國定古蹟一下淡水溪鐵橋
Letter 10	科技類	全世界第一支全透明手機！未來的新趨勢~
Letter 11	旅遊圖片類	【HiNet 旅遊網】開學旅遊團 超低價好康!

教育部實施電子郵件社交工程演練結果

教育機構社交工程演練成果

單位	人數	測試信件	總測試信件	項目	開啟信件	點選連結人數
A級單位	262	11	2882	點選人數	12	1
				人數比例	4.58%	0.38%
B級單位	13346	11	146806	點選人數	1521	613
				人數比例	11.40%	4.59%

單位名稱	第1次演練開啟信件(%)	第1次演練點選連結(%)	第2次演練開啟信件(%)	第2次演練點選連結(%)
	0%	0%	0.00%	0.00%
	0%	0%	0.00%	0.00%
	0%	0%	0.00%	0.00%
	0%	0%	0.00%	0.00%
	0%	0%	0.00%	0.00%
	0%	0%	0.00%	0.00%
	1.11%	0%	0.00%	0.00%
	1.23%	0%	0.60%	0.00%
	1.46%	0%	0.70%	0.70%
	0%	0%	0.00%	0.00%



教育部實施電子郵件社交工程演練結果-部分

（2）B級單位(公私立大專校院)

學校名稱	Total		Average
	開啟信件	點選連結	
	34.62%	42.31%	38.47%
	50.00%	17.65%	33.83%
學	47.12%	19.23%	33.18%
	35.79%	27.37%	31.58%
	50.00%	8.72%	29.36%
	31.67%	25.00%	28.34%
	52.17%	4.35%	28.26%
	43.33%	11.11%	27.22%
	32.14%	21.43%	26.79%
	45.45%	6.82%	26.14%
	36.07%	11.48%	23.78%
	35.71%	8.04%	21.88%
	34.85%	7.58%	21.22%
	30%	12.00%	21.15%

教育部實施電子郵件社交工程演練結果–部分

代號	第1次演練開啟信件(%)	第1次演練點選連結(%)	第2次演練開啟信件(%)	第2次演練點選連結(%)
015	45.56%	4.44%	22.20%	5.60%
032	17.5%	12.5%	15.00%	2.50%
031	13.33%	1.64%	15.20%	1.90%
038	11.78%	2.78%	11.60%	3.90%
043	14.81%	0%	11.10%	5.60%
039	19.83%	12.4%	11.60%	3.30%
006	23.96%	22.78%	32.30%	6.20%
034	20.72%	5.41%	12.60%	1.80%
026	17.09%	9.4%	17.10%	8.50%
046	93.1%	13.79%	10.30%	0.00%

教育部實施電子郵件社交工程演練結果–部分

代號	第 1 次演練開啟信件(%)	第 1 次演練點選連結(%)	第 2 次演練開啟信件(%)	第 2 次演練點選連結(%)
018	18.33%	1.67%	21.70%	3.30%
027	22.34%	6.38%	16.00%	5.30%
044	29%	2%	11.00%	2.00%
033	25.96%	9.62%	13.50%	4.80%
035	10.58%	0.96%	12.00%	0.00%
029	29.46%	9.3%	15.50%	4.70%
011	34.51%	11.2%	24.70%	6.80%
134	50%	0%	25.00%	0.00%
013	48.48%	6.06%	22.70%	2.30%
009	64.18%	0%	27.30%	0.00%
135	42.86%	0%	14.30%	0.00%
003	65.59%	12.9%	67.70%	19.40%
041	22.22%	12.61%	11.40%	7.20%
047	62.56%	22.05%	10.30%	1.00%

什麼是電子郵件社交工程

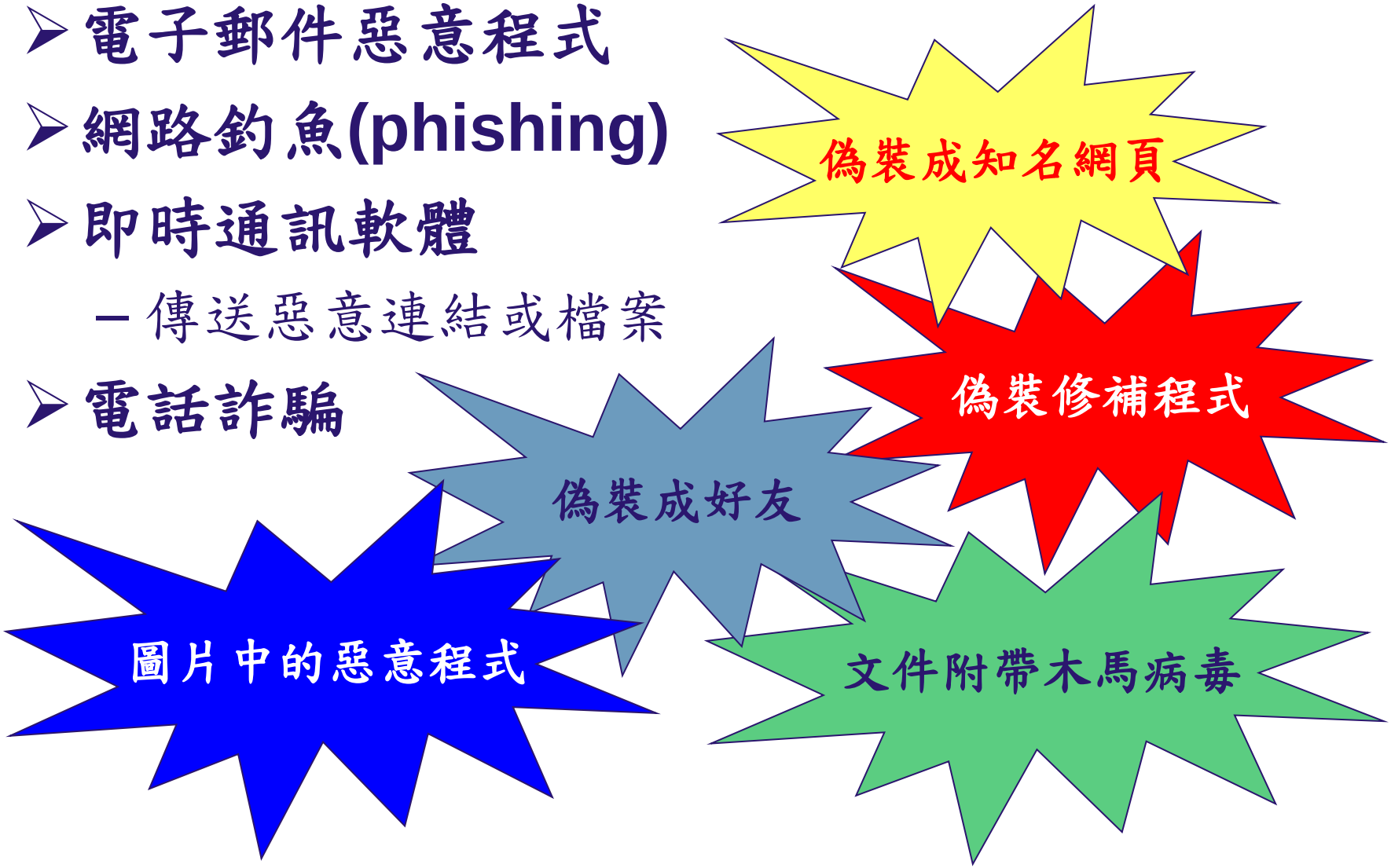
- 資 訊 科 技 與 競 爭 優 勢 -

何謂社交工程(social engineering)?

- 利用人性弱點的詐騙技術
- 以影響力、說服力或誘惑力來欺騙他人以獲得有用的資訊。

常見社交工程手法

- 電子郵件惡意程式
- 網路釣魚(phishing)
- 即時通訊軟體
  - 傳送惡意連結或檔案
- 電話詐騙



駭客詐騙目標

- 信用卡／金融卡號碼，包含卡片上的姓名、使用期限， 以及驗證號碼
- 個人身份資料，包含身分證號、姓名、地址、生日、電話號碼
- 電子郵件帳號密碼
- 網路銀行用來驗證身份提問的相關問題與答案

電子郵件惡意程式

- 附檔含有木馬程式
- 利用”社交工程”結合用戶端軟體漏洞
  - 網頁瀏覽器、Office軟體、E-mail軟體
  - 多媒體播放器、Adobe Reader。
- 電子郵件社交工程的危害
  - 電腦中毒、個人隱私資訊洩漏
  - 殭屍電腦(讓中毒的電腦任由駭客操控，成為犯罪工具，這種病毒散佈快不易追查)或駭客跳板、DoS攻擊(拒絕服務攻擊：在一段期間內透過大量且密集的封包傳送，達到使被攻擊的網站無法處理)
  - 發送廣告信、成為詐騙集團人頭、遭竊取遊戲寶物。

電子郵件惡意程式


女網友愛點選「折扣」男網友愛點選「火辣」小心上當！-Yahoo!奇摩新聞 - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁 搜尋 我的最愛
網址(D) http://tw.news.yahoo.com/article/url/d/a/090331/35/1h0km.html
移至
Google 搜尋 書籤 尋找 登入
會員登出 帳號資料
新聞首頁 政治 社會 地方 國際 財經 科技 運動 健康 教育 藝文 影劇 旅遊 生活
資訊3C 科學發展 自然環境 照片故事 專輯 領袖專訪 民調中心 雜誌 6行動愛地球 冷氣選購指南
新聞首頁 > 科技 > 資訊3C > Yahoo!奇摩
寄給朋友 友善列印 字級設定:
女網友愛點選「折扣」男網友愛點選「火辣」小心上當！
YAHOO! 奇摩
更新日期：2009/03/31 17:16 特約記者 薛怡青 台北報導
現在的網路環境簡直可以用「危機四伏」來形容，不但隨時都可能被駭，
再不然就是帳號被盜用，甚至有人還可以透過遠端搖控來控制自己的電腦
完成
網際網路

電子郵件惡意程式


女網友愛點選「折扣」男網友愛點選「火辣」小心上當！-Yahoo!奇摩新聞 - Microsoft Internet Explorer

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

上一頁 搜尋 我的最愛

網址(D) http://tw.news.yahoo.com/article/url/d/a/090331/35/1h0km.html 移至

Google 搜尋 書籤 尋找 登入

嚴重提醒，要民眾與企業多注意個人電腦的健康狀況，以免因被駭造成個資外洩而衍生治安問題。

而Yahoo！奇摩也針對六千多位網友進行「網路安全危機」調查發現，有五成以上的網友因被誘惑而主動點選或下載有毒的檔案。其中，又以「下載有毒的音樂或影音檔案」的網友占最多，達到27.6%；此外也有24.2%的網友會因「收到夾帶有毒檔案和連結的電子郵件」因素而點選連結或開啓附件檔，而導致木馬或惡程式植入自己的電腦。

另外，駭客們也會利用社交工程與心理戰的因素來誘騙網友點選連結，其中最容易讓網友身陷其害的就是，有42.3%的網友因誤點「跟搜尋結果相關的網站」而誤入釣魚網站，另外有29%的網友會因「好友寄的信件或訊息」而誤點連結。

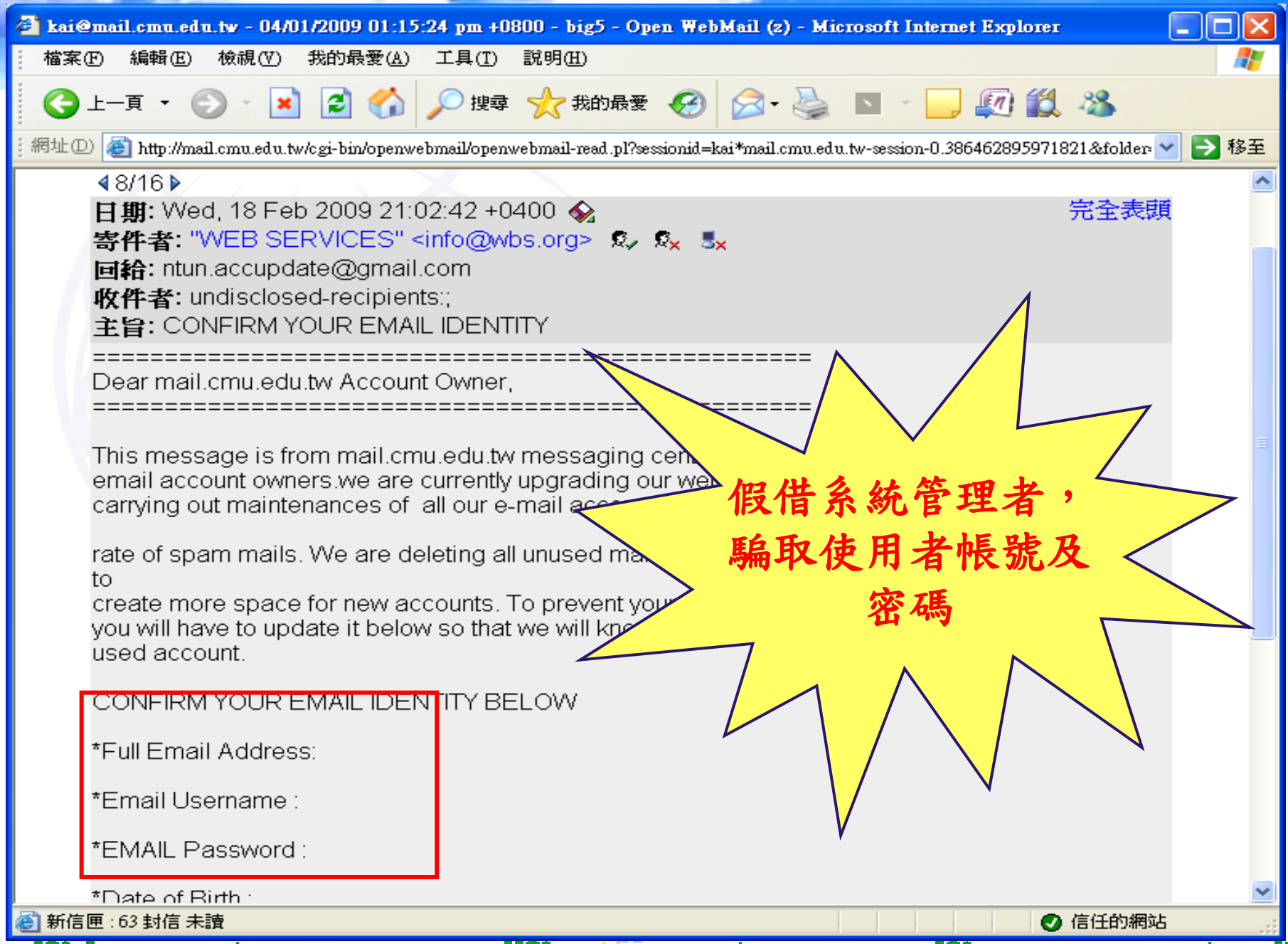
例如許多網友的電腦中毒後，其MSN會自動散布惡意的釣魚網站連結給

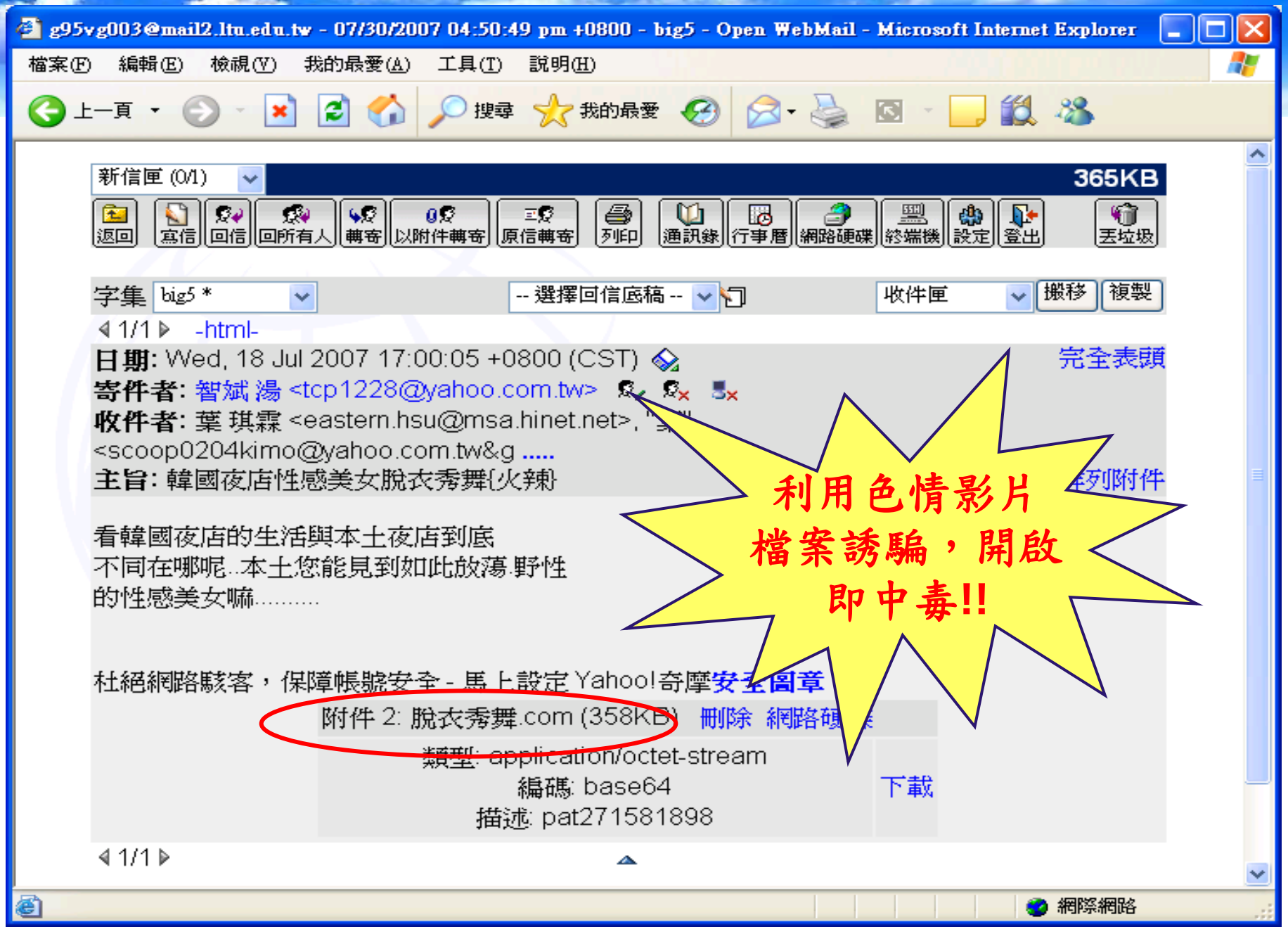
請問 裡繳 (投票

» 前

» 看

完成 網際網路


kai@mail.cmu.edu.tw - 04/01/2009 01:15:24 pm +0800 - big5 - Open WebMail (z) - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁 搜尋 我的最愛
網址(D) http://mail.cmu.edu.tw/cgi-bin/openwebmail/openwebmail-read.pl?sessionid=kai*mail.cmu.edu.tw-session-0.386462895971821&folder=
移至
8/16
日期: Wed, 18 Feb 2009 21:02:42 +0400
完全表頭
寄件者: "WEB SERVICES" <info@wbs.org>
回給: ntun.accupdate@gmail.com
收件者: undisclosed-recipients:;
主旨: CONFIRM YOUR EMAIL IDENTITY
==========
Dear mail.cmu.edu.tw Account Owner,
==========
This message is from mail.cmu.edu.tw messaging cen
email account owners.we are currently upgrading our we
carrying out maintenances of all our e-mail acc
rate of spam mails. We are deleting all unused ma
to
create more space for new accounts. To prevent you
you will have to update it below so that we will kn
used account.
CONFIRM YOUR EMAIL IDEN TITY BELOW
*Full Email Address:
*Email Username :
*EMAIL Password :
*Date of Birth :
新信匣 : 63 封信 未讀
信任的網站
假借系統管理者，
騙取使用者帳號及
密碼


g95vg003@mail2.ltu.edu.tw - 07/30/2007 04:50:49 pm +0800 - big5 - Open WebMail - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁 搜尋 我的最愛
新信匣 (0/1)
365KB
返回 寫信 回信 回所有人 轉寄 以附件轉寄 原信轉寄 列印 通訊錄 行事曆 網路硬碟 終端機 設定 登出 丟垃圾
字集 big5 * -- 選擇回信底稿 -- 收件匣 搬移 複製
1/1 -html-
日期: Wed, 18 Jul 2007 17:00:05 +0800 (CST)
完全表頭
寄件者: 智斌 湯 <tcp1228@yahoo.com.tw>
收件者: 葉 琪霖 <eastern.hsu@msa.hinet.net>,
<scoop0204kimo@yahoo.com.tw&g .....
主旨: 韓國夜店性感美女脫衣秀舞{火辣}
列附件
看韓國夜店的生活與本土夜店到底
不同在哪呢..本土您能見到如此放蕩.野性
的性感美女嘛.....
杜絕網路駭客，保障帳號安全 - 馬上設定 Yahoo!奇摩安全圖章
附件 2: 脫衣秀舞.com (358KB) 刪除 網路硬
類型: application/octet-stream
編碼: base64
描述: pat271581898
下載
1/1
網際網路
利用色情影片
檔案誘騙，開啟
即中毒!!

帶你的兒子來享受一下，蠻好玩的哦! - 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(W) SmartWhois

寄件者: [redacted]
收件者: [redacted]
副本:
主旨: 帶你的兒子來享受一下，蠻好玩的哦!
寄件日期: 2007/7/3 (星期二) 下午 04:33

附件: 宣傳手冊.chm (77 KB)

台糖高雄漆彈場配套一日遊,簡單說明

一:漆彈全配備100發500元,不限時間,要續彈可自行添加
二:烤肉或土窯一爐1200至2500元(價格自己選)
三:戀戀五分小火車一人80元(可參觀糖廠百年古蹟)
四:攀岩(可登峰造極)一人200元
五:小型賽車250元
六:農庭花卉DIY選擇性消費
七:養蜂館(蜂蜜勿來源)
八:台糖勿(吱丫冰)10元
以上提供參考消費自選,如有不明之處即可來電查詢

假借宣傳文件，
開啟即中毒

定案的人事薪獎資料！！

李 政峰

收件者: James Lee;

101年度人評會資料.rar

有力人士提供的定案資料，請勿傳閱！！

Best regards,

James.

ISO 27001 LA
ISO 20000 LA
BS 25999 LA
BS 10012 LA
CISSP 訓練合格

李政峰(James Lee) 祝您
喜 福 充 滿 吉 運 年 年

最近最夯的照片，自己看就好，請勿傳閱！

李 政峰

收件者: James Lee;

富二代李oo偷拍精彩照.rar

FYR.

James Bon.

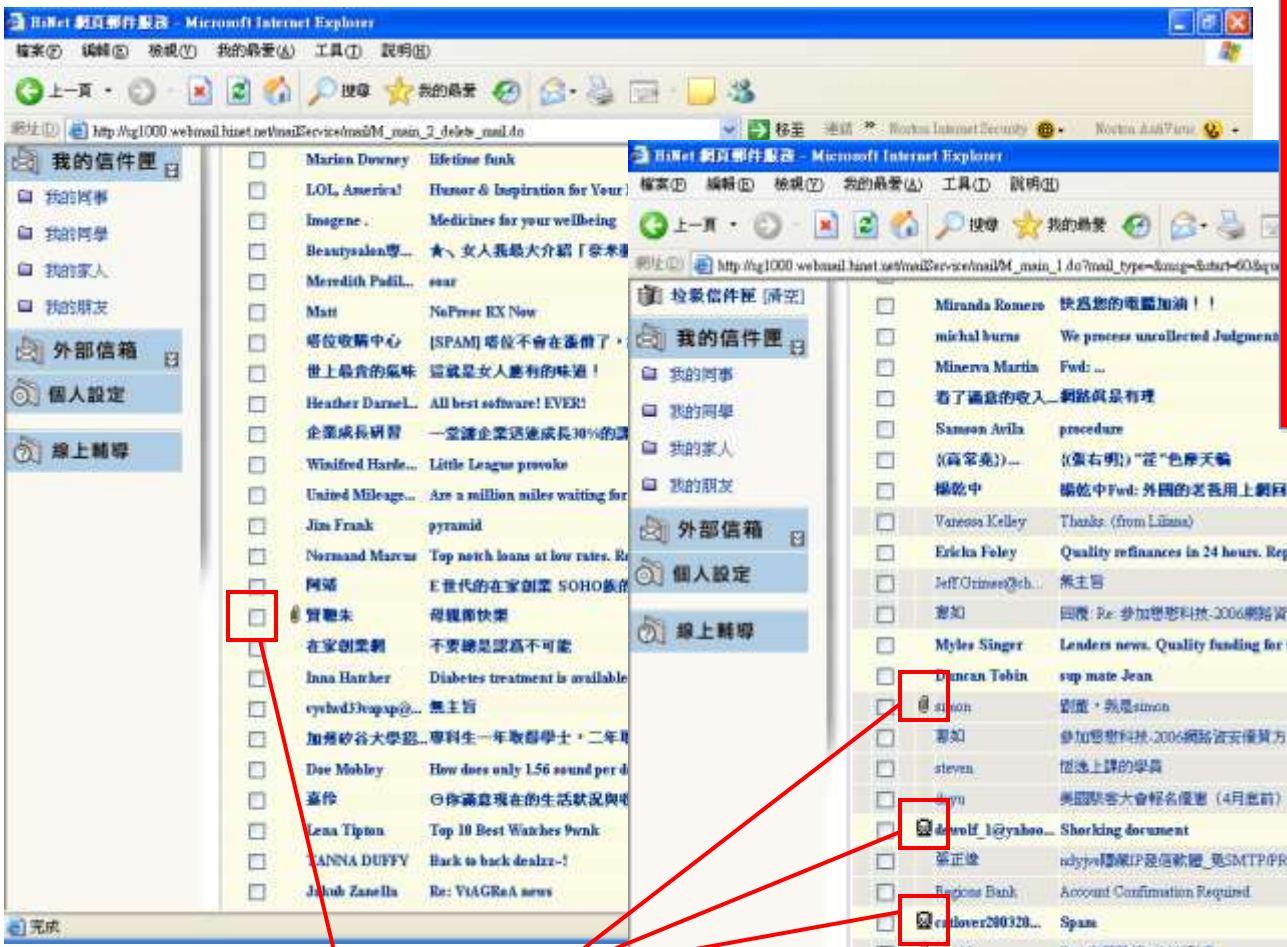
ISO 27001 LA
ISO 20000 LA
BS 25
BS 10012 LA
CISSP 訓練合格

李政峰(James Lee) 祝您
喜 福 充 滿 吉 運 年 年

文件檔案，包含有病毒的壓縮檔案

如何檢查郵件是否夾帶木馬後門程式？

- 請您檢查電子郵件是否夾帶檔案？檔名尾碼是否為異常名稱？如果有異常名稱，請勿直接開啟執行。



高危險檔案類型名稱

.exe	.com	.scr
.pif	.bat	.cmd
..reg	.lnk	.hta

中危險檔案類型名稱

.zip	.rar	.swf

電子郵件的附件檔案

網路釣魚(Phishing)

- 結合“Phone”和“Fishing”
- 姜太公釣魚，願者上鉤
- 駭客偽造電子郵件與網站作為”誘餌”，寄發電子郵件要求使用者輸入帳號、密碼，來偷取使用者的身分資料及金融帳號等機密資料。
- 電腦可能會被植入木馬程式，重要資訊遭竊

網路釣魚(Phishing)-案例

網路釣魚(Phishing)-案例

假銀行網站 竊個資盜存款

Focus

鎮代開淫窟 逼越女賣淫

掌握多名中國可疑共犯

竊取數十萬筆個資行騙

網站偽冒金融機構

網路下餌釣魚

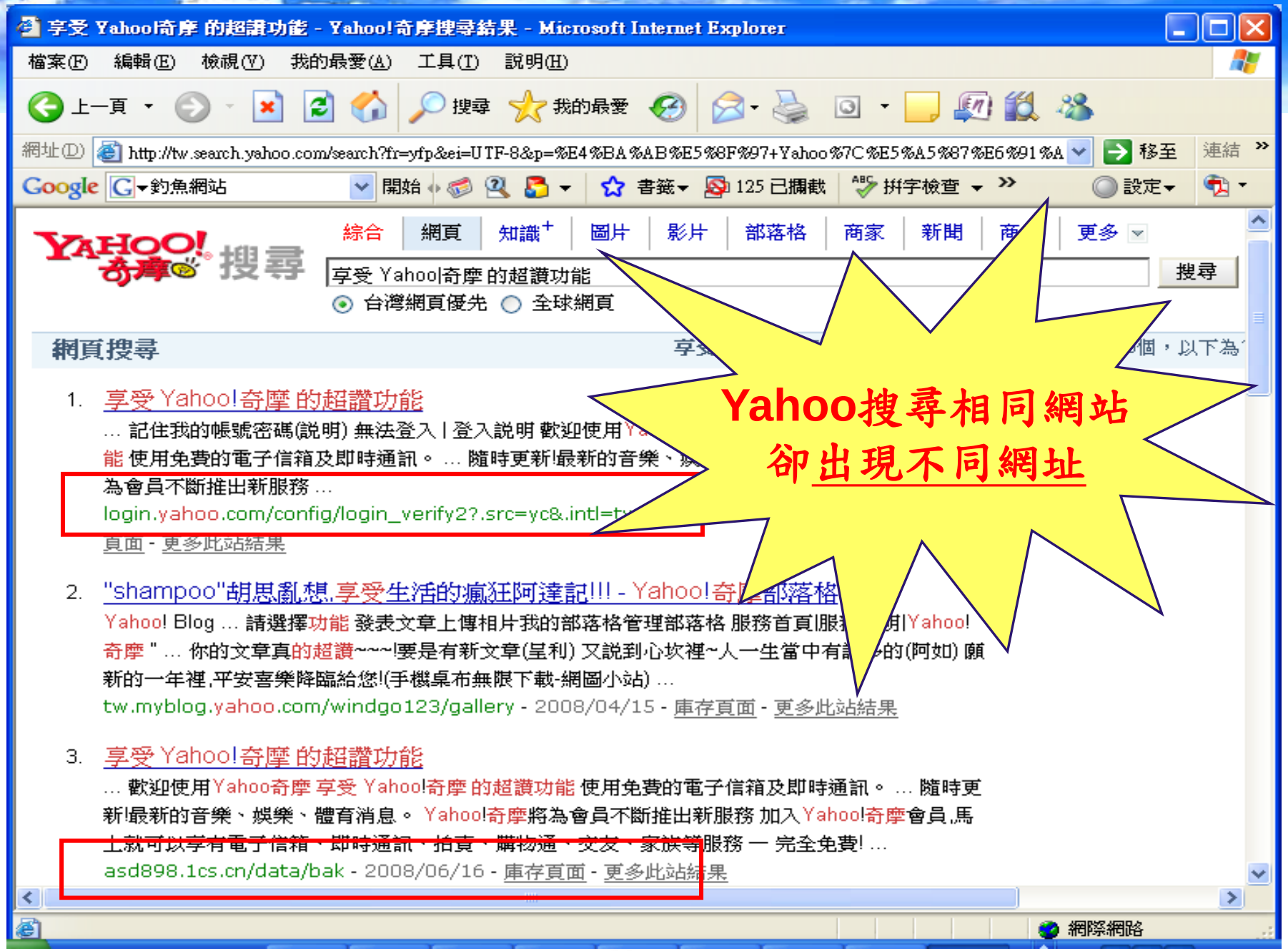

Yahoo!奇摩搜尋結果有關土地銀行 - Microsoft Internet Explorer
假網頁的網址連接
http://www.landbank.com.tw
http://www.1andbank.com.tw
土地銀行landbank
提供基金、信用卡、金融資訊相關連結服務。 www.1andbank.com.tw
快速捷國際 - 全方位貸款專家
提供土地銀行代辦信貸、信用卡業務，整合您的負債，首創
Easyloan - 汽車貸款
土地銀行汽車貸款，專業熱誠的服務，利率低，額度高，輕鬆貸，
汽車貸款
土地銀行汽車貸款，提供您資金週轉及購車需求，額度高、利率低、貸
在Yahoo!奇摩生活+查土地銀行的電話地址和
Yahoo!奇摩捷徑 - 說明
1. 土地銀行
土銀簡介、網路銀行、業務簡介、便民資訊、理財天地、帳務資料等服務。 ... 臺灣土地銀行標售本行所有臺中市中區仁愛段六小段8-3、9-14地號等2筆土地及地上1棟房屋。 ... 臺灣土地銀行標售行有嘉義市東區北門段二小段44-1及44-2地號土地。 ...
分類: 銀行
www.landbank.com.tw - 52k - 2006/12/25 - 庫存頁面 - 更多此站結果 - 儲存 - 封鎖
贊助網站
AutoLoan - 汽車貸款
有車讓您貸款更容易，土地銀行汽車貸款，額度高、利率低、省時方便又安全。
www.autoloan.com.tw
My Bank線上諮詢網
提供土地銀行貸款諮詢服務，0%免諮詢費！
www.1bank.com.tw
全程免收費 - 銀行貸款
免費提供多家銀行各類貸款、信貸、整合負債、房屋、企業貸款諮詢，省息專案實施。

網路釣魚(Phishing)-案例

假網頁的網址連接

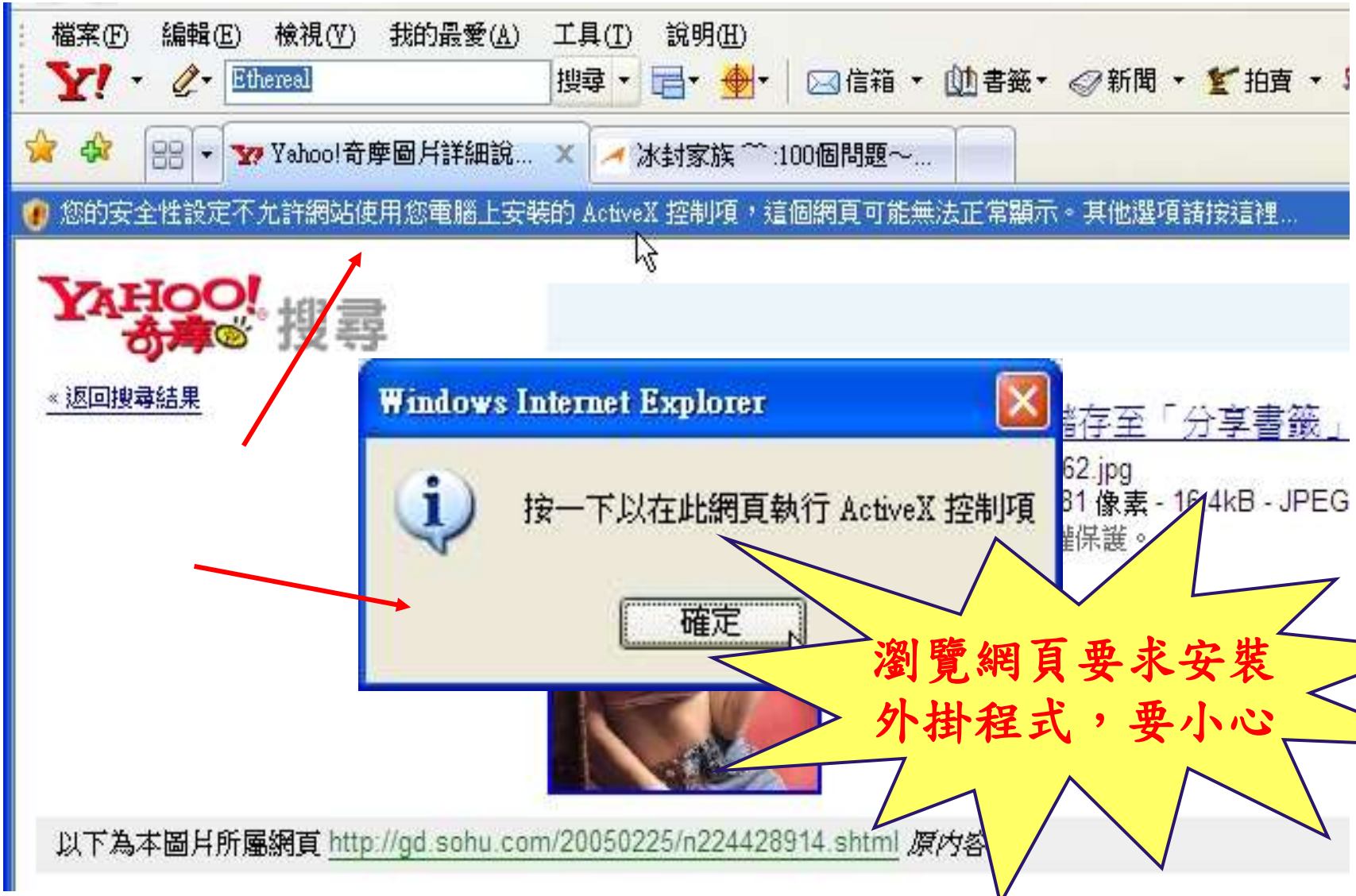

國際機票 休閒旅遊票券 旅遊住宿 比價購物最便宜,種類多元,優質商
檔案(F) 編輯(E) 檢視(V) 瀏覽(G) 書籤(B) Yahoo! 工具(T)
http://72.14.235.104/sear
Google china-airlines
搜尋 檢查 選項 china-airlines
YAHOO! 奇摩 購物通
會員登入
新使用者？立即註冊
搜尋網頁
服務首頁 | 服務說明 | Yahoo!奇摩
手機 相機 筆電 年終慶 資訊月 保養 名牌包 女鞋 彩妝 飾品 手錶 牛爾 Kevin 聖誕假期 特賣會
電腦資 分類
http://www.china-airlines.com.tw
熱門搜尋： 澳洲紐西蘭 青藏鐵路之旅 泡湯賞楓 住宿券 迪士尼 宜蘭賞鯨 雙人 法國普羅旺斯
八大館聯合跨年慶★免消費送
購物通首頁 > 旅遊住宿 > 休閒旅遊票券 > 國際機票
精準搜尋
搜尋結果：共有9項商品，顯示1 - 9項
檢視方式： 清單瀏覽 | 圖片瀏覽
比較商品 加入追蹤清單
排序方式： 依相關度 | 依價格
相關分類
行李箱拉桿包
旅遊觀光書籍
數位相機
旅行背包背袋
其他戶外休閒用品
上海計劃旅遊票5日(兩人成行、保証出團)NX
搭乘航班：NX+NX兩地機場稅+兵險安檢燃油費外加
NT 8,999 起
商店名稱：發現之旅 商店評比：
贊助網站
中華航空公司
NRT-東京，YVR-溫哥華，VIE-維也納，SHA-上海，提供網上定位。
www.china-airlines.com.tw
升達旅遊美加專業機票行程規劃
專營洛杉磯、舊金山、紐約、溫哥華國際機票及美國加拿大各城市之國內機票及飯店。
www.gogousa.com.tw
ZUJI足跡 - 提供特惠機票
國際機票促銷熱賣中，各大
縮小金額從
搜尋商品 重設
http:// www.china-airlines.com.tw
香港優惠票 讓您輕鬆飛往香港 免擔心價錢
尋找: li
往後尋找(N) 往前尋找(P) 高亮度變色標記(A) 符合大小寫(C) 找不到指定文字
完成

網路釣魚(Phishing)-案例

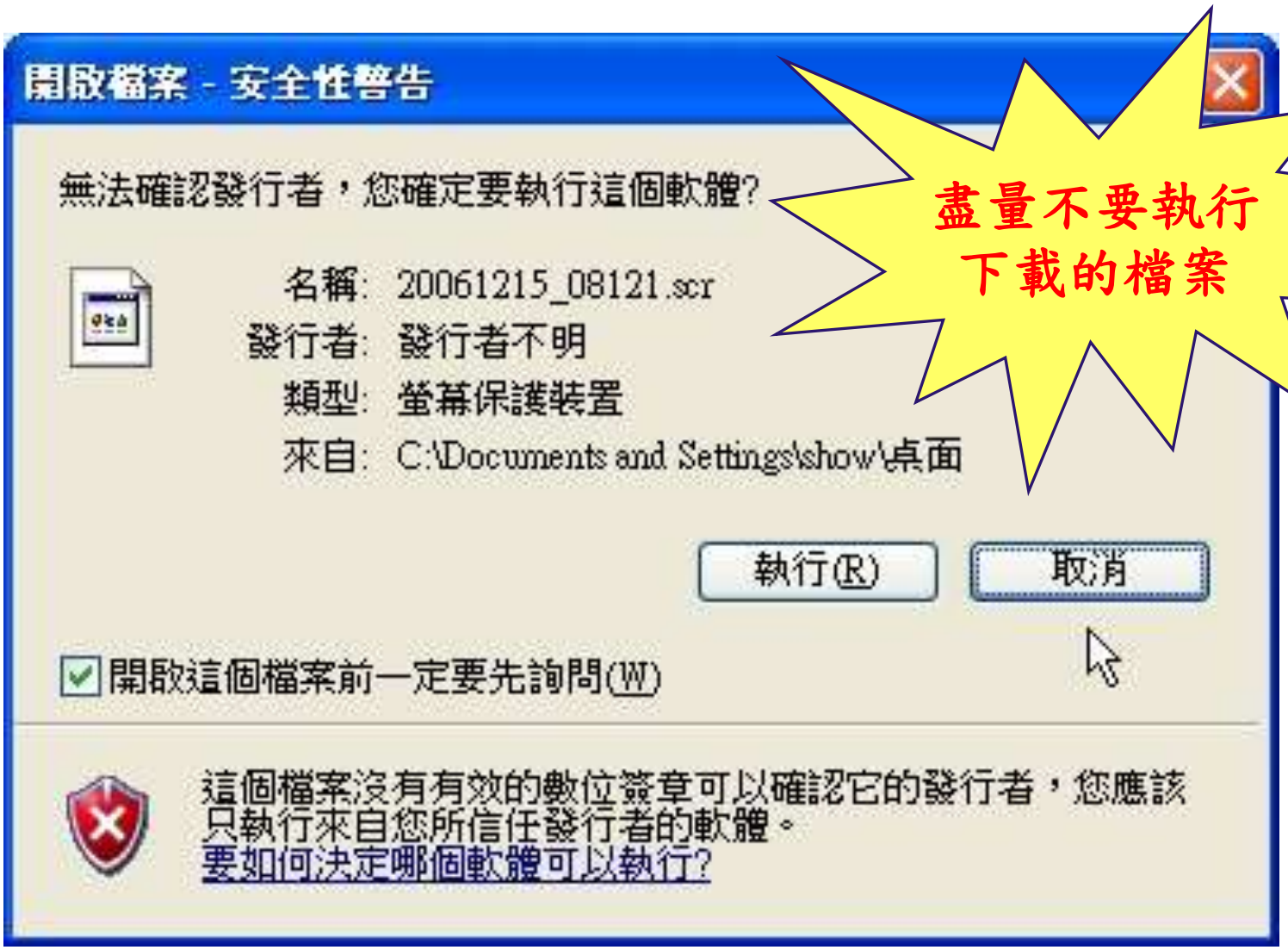

享受 Yahoo!奇摩 的超讚功能 - Yahoo!奇摩搜尋結果 - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁 搜尋 我的最愛
網址(D) http://tw.search.yahoo.com/search?fr=yfp&ei=UTF-8&p=%E4%BA%AB%E5%8F%97+Yahoo%7C%E5%A5%87%E6%91%A
移至 連結
Google 釣魚網站 開始 書籤 125 已攔截 拼字檢查 設定
YAHOO! 奇摩 搜尋
綜合 網頁 知識+ 圖片 影片 部落格 商家 新聞 商 更多
享受 Yahoo!奇摩 的超讚功能
搜尋
台灣網頁優先 全球網頁
網頁搜尋
1. 享受 Yahoo!奇摩 的超讚功能
... 記住我的帳號密碼(說明) 無法登入 | 登入說明 歡迎使用Ya
能 使用免費的電子信箱及即時通訊。 ... 隨時更新!最新的音樂、
為會員不斷推出新服務 ...
login.yahoo.com/config/login_verify2?.src=yc&.intl=t
頁面 - 更多此站結果
2. "shampoo"胡思亂想,享受生活的瘋狂阿達記!!! - Yahoo!奇摩部落格
Yahoo! Blog ... 請選擇功能 發表文章上傳相片我的部落格管理部落格 服務首頁|服
明|Yahoo!
奇摩 " ... 你的文章真的超讚~~~!要是有新文章(呈利) 又說到心坎裡~人一生當中有
的(阿如) 願
新的一年裡,平安喜樂降臨給您!(手機桌布無限下載-網圖小站) ...
tw.myblog.yahoo.com/windgo123/gallery - 2008/04/15 - 庫存頁面 - 更多此站結果
3. 享受 Yahoo!奇摩 的超讚功能
... 歡迎使用Yahoo奇摩 享受 Yahoo!奇摩 的超讚功能 使用免費的電子信箱及即時通訊。 ... 隨時更
新!最新的音樂、娛樂、體育消息。 Yahoo!奇摩將為會員不斷推出新服務 加入Yahoo!奇摩會員,馬
上就可以享有電子信箱、即時通訊、拍賣、購物通、交友、家族等服務 一 完全免費! ...
asd898.1cs.cn/data/bak - 2008/06/16 - 庫存頁面 - 更多此站結果
網際網路
Yahoo搜尋相同網站
卻出現不同網址

網路釣魚(Phishing)-案例

瀏覽網頁時被要求安裝軟體

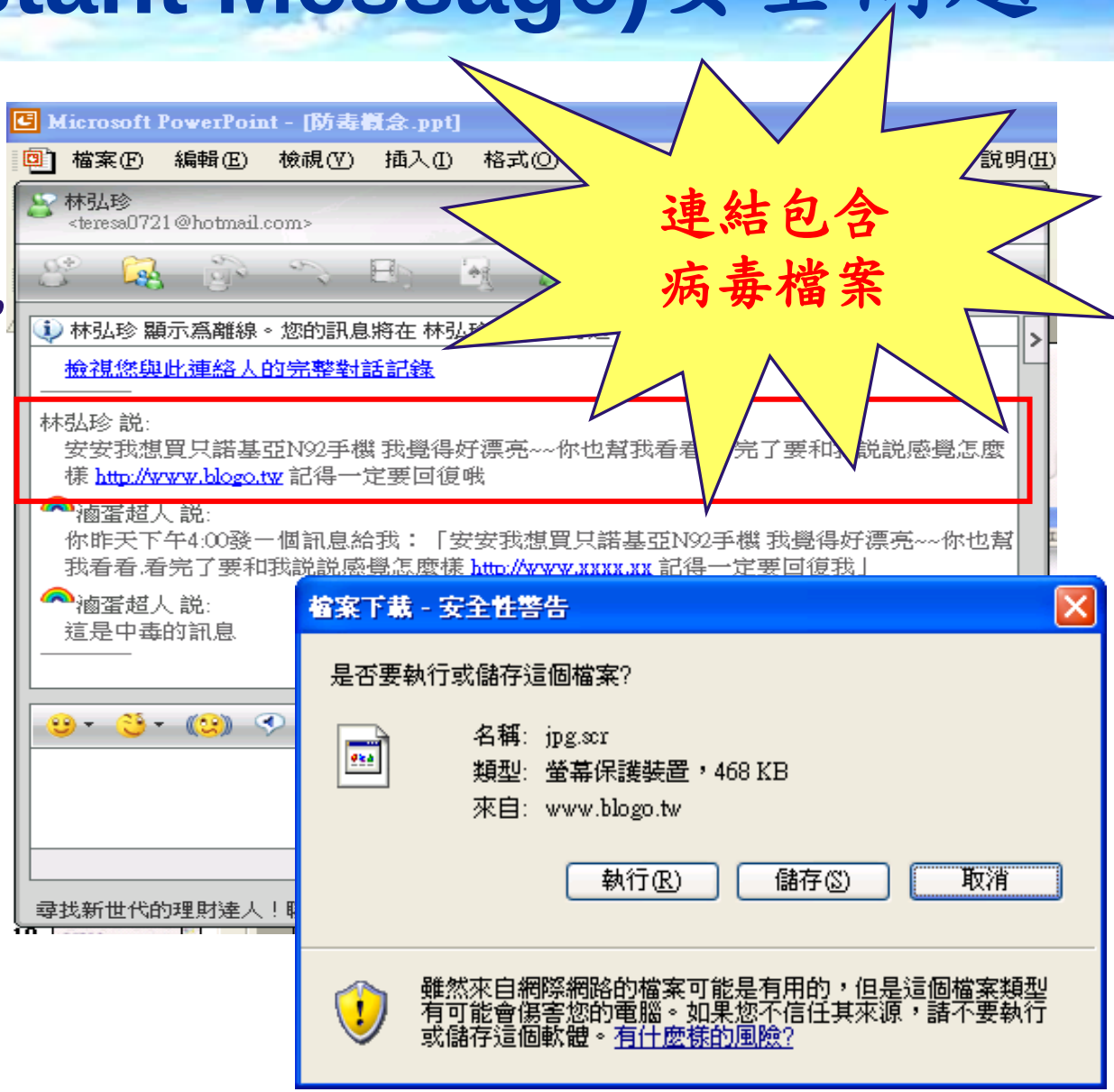


瀏覽網頁時被要求執行軟體



即時通(Instant Message)安全問題

- 當 你 使 用 Line/Skype 發現有以下幾種狀況，可能要小心..
  - 發現一直有人傳檔案給你。
  - 或是別人傳附檔名為“.pif”檔案給你。
  - 無法關閉，一直顯示正在與連絡人傳輸。



電子郵件社交工程攻擊類型

- 假冒寄件者
- 使用讓人感興趣的主旨與內文
- 含有惡意程式的附件檔案
- 利用0_DAY(零時差)攻擊

案例1. 政治新聞

中共十七大即將召開，民主開放將成爲共產黨存亡的大難題.. - 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)

寄件者: 兩岸觀察站 [Montague@applepie.serveblog.net]

寄件日期: 2007

收件者: [redacted]

副本:

主旨: 中共十七大即將召開，民主開放將成爲共產黨存亡的大難題..

龍應台於台北市文化局長任內的貪污自白!! - 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)

按這裡下載圖片。爲了協助保護您的隱私，Outlook 不會自動下載郵件中的某些圖片。

寄件者: 政治評不平 [Halbert@applepie.serveblog.net]

寄件日期: 2007/7/17 (星期二) 上午 10:5

收件者: [redacted]

副本:

主旨: 龍應台於台北市文化局長任內的貪污自白!!

附件: 龍應台對馬市長任內的貪污自首告白.doc (58 KB)

龍應台於台北市文化局長任內的貪污自白!! 信件內容: 曾經在馬英九市長下擔任文化局局長的龍應台, 在公務首長特別費爭議中的貪污自首告白! 連龍應台這樣高道德標準的人也貪污了嗎?

案例2.房市稅務相關

提早規劃財務 年初退休最省稅

當職涯告一段落，進入退休的新人生，可開始盡情享受人生，但每個月已不再有穩定的薪水收入，相關稅務問題也要及早考量、規劃，在可節稅範圍內，選擇最佳的退休時間點及財務規劃。

勤業眾信會計師莊琦惠表示，退休金等退職所得要納入年度綜所稅計算，若可以選擇，年初退休會比在年中或年底退休省稅，勞保及國民年金的老年給付或老人年金，則屬免稅所得。

個人領取的退休金、資遣費、退職金、離職金、終身俸及非屬保險給付的養老金等所得均屬退職所得。

退職所得還可選擇一次領、分期領或兼採一次領及分期領，課稅的計算方式也不一樣。

央行打房下一波？ 專家：桃園、新竹恐遭殃

央行日前一連祭出4大打房措施，除了再擴大「限貸很無感」之外，也降低了對家戶認定標準，堪稱是過去以來動作最大、下手最重的一次。外界也猜測，在這次打房過後，央行還會不會再祭出下一波打房手段？對此專家認為，如果以央行「房價再漲降就出手」的打房標準來看，桃園八德、新竹和竹北恐怕都將成為下一波新房的限貸管制區。

案例3. 科技新知

十大新物種 一個比一個怪

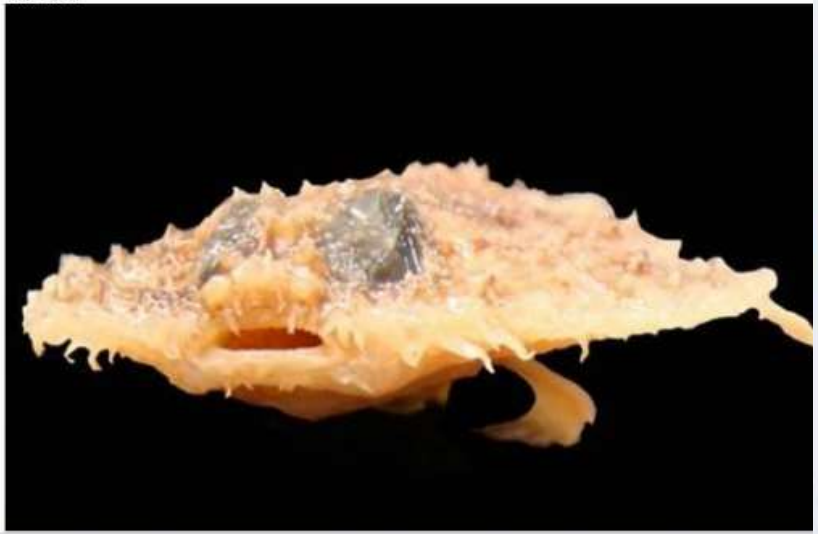
寄送信件 (nuke_chein@facebook-linked.com) 新增連絡人

收件者 ust.edu.tw;

十大新物種圖片.doc

每年美國亞利桑那州立大學國際物種勘測協會都會編撰十大新發現的物種名等特點。

蝙蝠魚



寄件者: 新知報你知 <nchuews@yahoo.com.tw>

寄件日期: 2014/7/15 (週二) 下午 06:27

收件者: [redacted]

副本:

主旨: 關於蚊子的一些事

附加 防蚊大作戰.doc (3 KB)

關於蚊子的一些事

為什麼喜歡叮我

想必大家都有這樣子的經驗，一群人坐在一起閒話家常，有的人被叮的滿身包，有的人卻毫髮無損。有人說，這和體質有關，體質偏酸性的人容易吸引蚊子，體質偏鹼性的比較不容易被蚊子叮咬，真的是這樣子嗎？

案例4. 保健養生

「瘦肉精」知多少

猶擾信件 (steven1689@my-google-apps.com) 新增連

收件者: [redacted]st.edu.tw;

10個拒絕拒絕瘦肉精的理由.doc

資料來源：藥物食品安全週報第318期
上稿日期：2011/11/11

最近媒體不時報導行政院衛生署執行進口肉精的消息，用的肉品

瘦肉精是種類交感神 Terbutaline 合成的功能潤，所以

由於瘦肉精在禽、畜肉品生產上，具提高飼一、二種「瘦肉精」使用為動物用藥，並訂與可使用的動物）與殘留標準並不一致。其絕大多數是萊克多巴胺。

餿水油、飼料油…

寄件者: 必看瘋傳 <pgocircle@mm.com>
寄件日期: 2014/7/15 (週二) 下午 06:27
收件者: [redacted]
副本:
主旨: 【必看瘋傳】一個高階主管在台積電【賣命癌症過世後給大家的啟示】
新增 一個高階主管在台積電【賣命癌症過世後給大家的啟示】.doc (2 KB)

【必看瘋傳】一個高階主管在台積電【賣命癌症過世後給大家的啟示】

案例5. 休閒娛樂


深坑老街「大團圓」，週休二日好去處 - 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)
寄件者:
收件者:
副本:
主旨:
附件:
2007宜蘭童玩節來了!! - 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)
寄件者: 童玩大使 [Felix@extremefun.servebeer.com]
寄件日期: 2007/7/17
收件者: [redacted]
副本:
主旨: 2007宜蘭童玩節來了!!
2007
宜蘭童玩節
7.7-8.26
8:30-20:30
1212童玩最快樂
童玩節 12 歲囉！
讓我們大手牽小手 邁開腳步
1 2 1 2 齊步走 ～一起向充滿歡笑希望的兒童夢土出發！
今年在冬山河畔，用最快樂的節奏 最熱情的步伐，享受夏日水舞的沁涼，隨著海洋之歌的音符起舞，
7月7日 讓我們跟著小雨和童玩娃娃兵團，展開童玩國度51天的夏日冒險！
[更多活動資訊]
演出
【野外劇場】 來自全世界五大洲民俗音樂舞蹈團隊的精采演出
【蔚藍舞台】 海洋之歌的曼妙樂符 悠揚於冬山河畔!
展覽
【七彩陀螺館】 感受陀螺七彩旋風的魅力!
【童玩童食回味屋】 回味兒時童玩童食的時光之旅!
【飛行船劇場】 全國首座的球體型可移動式3D立體劇場
飄浮在半空中的【水母瀑布】，突如其來的多樣水幕瀑布，傾瀉而出，彷彿水母的觸足沖
大團圓鄰近深坑老街，
境舒服，吃飽飯可在
(圖 / 王以瑾攝影)

案例6. 影劇新聞

小S如何追求自己的幸福，值得共勉的好文章喔~ - 郵件 (HTML)

檔案(F) 編輯(E) 檢視(V) 插入(I)

回覆(R) 全部回覆(L) 轉寄(

按這裡下載圖片。為了協助保護您的隱私

寄件者: 小劉 [Tyler@easylife.servegame

收件者: [redacted]

副本:

主旨: 小S如何追求自己的幸福，值

附件: 小S如何追求自己的幸福.d

看看小S如何追求自己的幸福~~

寄件者: DONG棒球 <dongbaseball@ms.hinet.net>

寄件日期: 2014/7/15 (週二) 下午 06:26

收件者: [redacted]

副本:

主旨: 瑜珈女神性感誘惑 史上最辣開球沒有之一

附件: 史上最辣開球沒有之一.doc (987 B)

瑜珈女神抖 G 奶誘惑　史上最辣開球沒有之一

開球沒有極限！！Lamigo 桃猿豹紋趴「豹力五連發」第三發，請來擁有 G 奶加上 19 腰的瑜珈女神房妍擔任開球嘉賓，他在場上秀了一段瑜珈後，直接脫下上衣露出 G 奶，誠意十足，開球後還跟林智勝來了一段貼身「濕背秀」，球迷直呼這是「史上最有誠意的開球」。

脫下上衣：

案例7. 飲食

寄件者: Gaston_Wu <gaston@gmail.com>
寄件日期: 2014/7/15 (週二) 下午 06:25
收件者: [redacted]
副本:
主旨: 看清這10點，讓你果汁喝得更安心！
訊息 果汁喝得更安心.doc (2 KB)

看清這 10 點，讓你果汁喝得更安心！

台灣的夏天，氣溫常接近、甚至高過人的體溫，許多民眾為了迅速的消暑解渴，尤其不習慣純水口感的族群（特別是年輕的一代），常會用各式果汁或者其他替代飲料，當作水份的補充來源，所以，果汁的選擇也成為一門重要的常識。

案例7. 旅遊與勵志

【驚奇景點】聽說最近台灣很紅！最受國際矚目的台灣旅遊奇觀登場

【驚奇景點特段】今年暑假又再規劃要出國？其實不必舟近求遠，台灣許多「特色奇觀」你都去過了嗎？像是 CNN 日前選出 15 大世界

改變孩子一生的 5 個習慣

哪些好習慣最重要!

習慣百百種，《康健》綜合專家意見，就點生活、學習、愛 3 個領域整理 5 個習慣影響孩子一輩子，建議父母一定要從小幫孩子建立。

●生活：維持健康的習慣，包括飲食與運動，懂得處理的習慣和正面思考與自己對話。

●學習：終身主動學習的習慣。

●愛：感恩的習慣。

第一好習慣-健康

在學齡期，是孩子在規範與限制的階段，在這階段向孩子示範健康飲食的選擇極為關鍵，比其他階段更重要。

日本文部科學省（同台灣教育部）建議幫小孩從小建立的習慣，前三項就是睡眠、吃早餐和排便的習慣。

《康健》曾針對台灣國小學生調查發現，超過一半的小學生 10 點以後才上床睡覺，超過四成的孩子沒有規律排便的習慣，有三成的家長一星期內幾乎沒有帶過小孩外出運動。

台積電董事長張忠謀曾對台下上千名大學新生演講，大學生應該要花心思的 11 件事裡，第一件事就是養成一個終身、健康的生活習慣，不見得是要當個運動家或校隊選手，而是養成習慣，把運動當成健康生活的一部份，「沒有健康，一切都不用說，」81 歲仍在領航大企業的張忠謀，說來更具說服力。

第二好習慣-正向思考

長庚生技董事長高一生認為，正向思考的習慣影響人最深，一定要從小養成。

當人有正面的念頭，做什麼事都正面，成為人生的指南針，自己面對問題困難就會很積極，別人也會對你相信，而且不會消極被動，遇到問題就能想。

案例8. 太空科幻

寄件者: 東森新聞雲 <ettoday@gmail.com>　　寄件日期: 2014/7/15 (週二) 下午 06:26

收件者: [redacted]

副本:

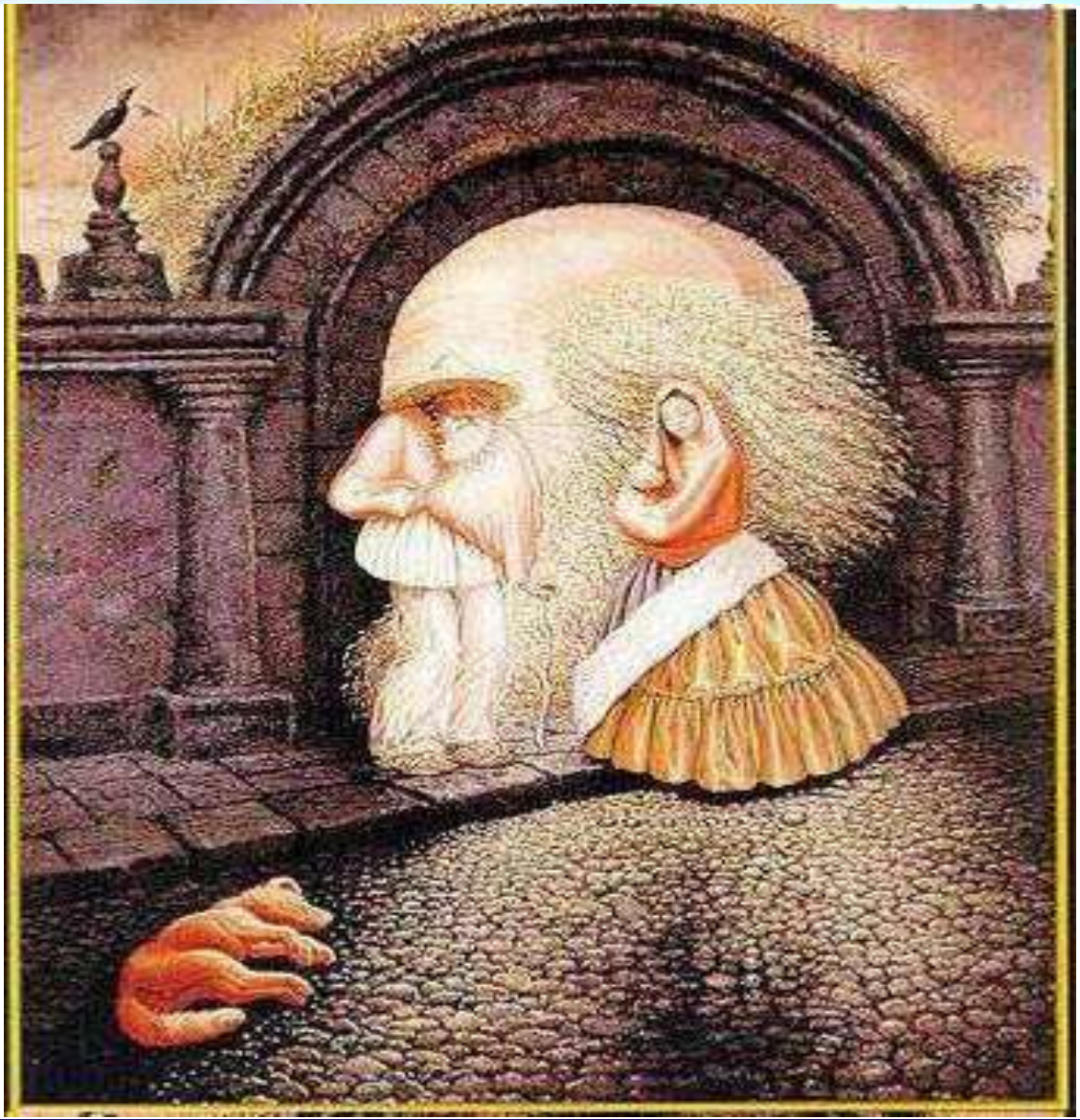
主旨: 智利政府認證：確有UFO！詭異飛行器不是戰機！

訊息　智利政府認證：確有UFO！.doc (2 KB)

智利政府認證：確有 UFO！　詭異飛行器不是戰機！

最近許多國家的官方機構，似乎都開始釋放外星文明確有其事的訊號，最新英國《每日郵報》刊載，智利政府公佈一張照片，而經過多重查證後，確定照片上的生物不是地球上的生物，也不是新研發的飛行器，而是確確實實的 UFO。這照片是在去年 4 月拍攝的，4 名礦區工程師在開採過程中看見礦區上空出現不明飛行物，該物體為平坦碟狀物，顏色燦亮，直徑長 5 到 10 公尺，在很短的距離內進行升降及水平移動，離地約 600 公尺。CEFAA 著手調查後，已排除任何大氣現象的可能性，如透鏡狀雲朵，或者是實驗性質戰機、飛機、氣象

聽說有9個人像



如何防止Email受駭

- 資 訊 科 技 與 競 爭 優 勢 -

誤點率高的網路釣魚主旨

- 黑心食品一覽表
- 武媚娘傳奇有胸版
- 你的FB 帳號即將被鎖定
- 我的應徵履歷
- 二代健保補充保險費扣繳辦法


郵件主旨是什麼??
寄件者是誰??
郵件內容是什麼??

點閱前思考一下

Q:為何我會收到這封郵件??
A:應確認寄件來源及寄件者

Q:我是否應該收到這封郵件?
A:應確認郵件主旨及郵件內容

Q:我是否應該開啟這封郵件??
A:是否與業務工作相關。
不點選連結是否有影響。
審慎查證（寄件者）。

大多數e-mail受到攻擊的主要因素

- 郵件軟體設定問題
- 使用者的疏忽
- 系統未更新
- 防毒軟體未更新

如何防止Email受駭？你可以做得到

- **技術層面**
  - 定期掃描及修補系統之漏洞
  - 安裝”防毒軟體”及”間諜程式”檢查軟體
  - 關閉信件預覽及html功能。
- **行為層面**
  - 不隨意打開有害的郵件附檔
  - 不隨意點選郵件內容的超連結(URL)，網域名稱(Domain Name)是否足以識別？若為數字IP之網址勿輕易開啟。
  - 重要公務用Email不隨意外洩
  - 只在官網登入帳號密碼(不在Email中輸入帳號密碼來登入網站)，並定期更換密碼。
- **系統面**
  - Email軟體安全性設定
  - 更新用戶端軟體、檢查webmail 設定。

如何防止Email受駭？你可以做得到

- 時時更新病毒定義檔
- 密碼不可太過簡單
- 不連線至未知網站
- 不隨意開啟陌生的電子郵件
- 下載、開啟時三思而後行
- 關閉網路芳鄰

如何防止Email受駭？你可以做得到

- 個人資料不放於網路
- 避免使用非法軟體或破解軟體
- 別讓好奇心害了你
- 養成資料備份習慣
- 有狀況即時通報資訊單位
- 避免使用點對點傳輸軟體(例如：fox、edonkey、Kuro、Bit-torrent…等等)

不隨意打開有害的郵件附檔
- 辨識可疑電子郵件之特徵

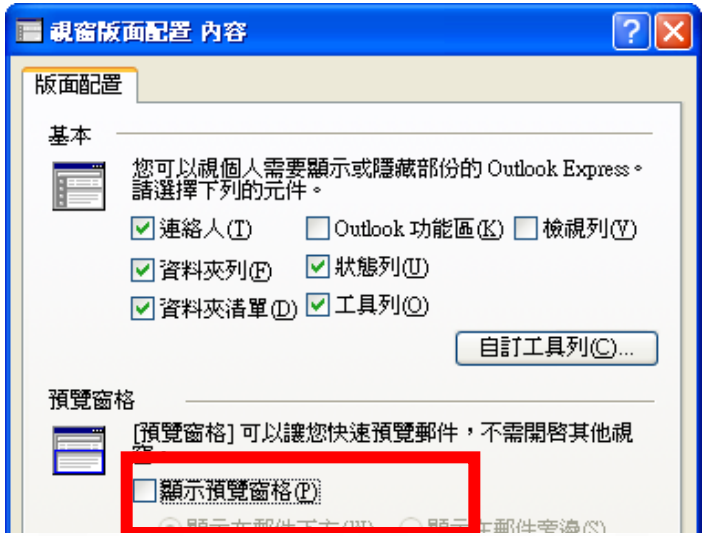
- 陌生人或少交流對象來信
- 聳動的主旨與緊急要求語氣信件
- 不正常的發信時間
- 認識的人來信但主旨或內容與本身業務無關或非預期會收到信件
- 要求輸入私密資料送出
- ……

Email軟體安全設定

- 版面設定
  - 關閉預覽窗格
- 選項設定
  - 附件有可能有病毒時不允許儲存或開啟
  - 阻擋HTML電子郵件中的圖片和其他外部內容
  - 將郵件設定為無法預覽
  - 設定純文字讀取模式
  - 關閉自動下載郵件設定

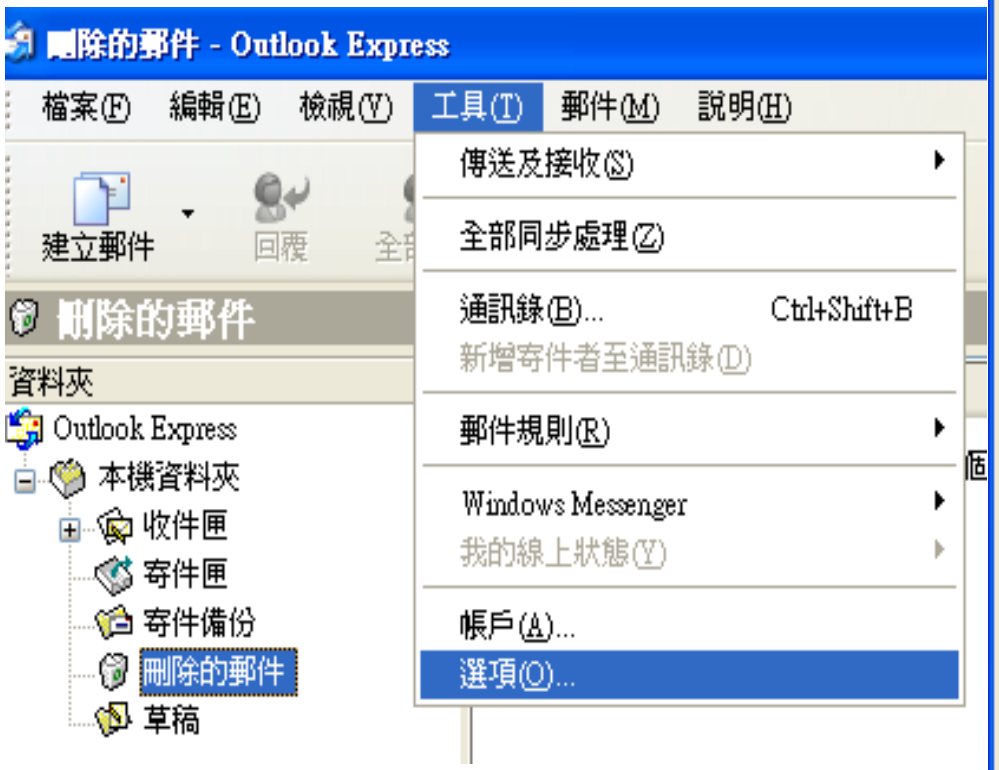
Email軟體安全設定(續)

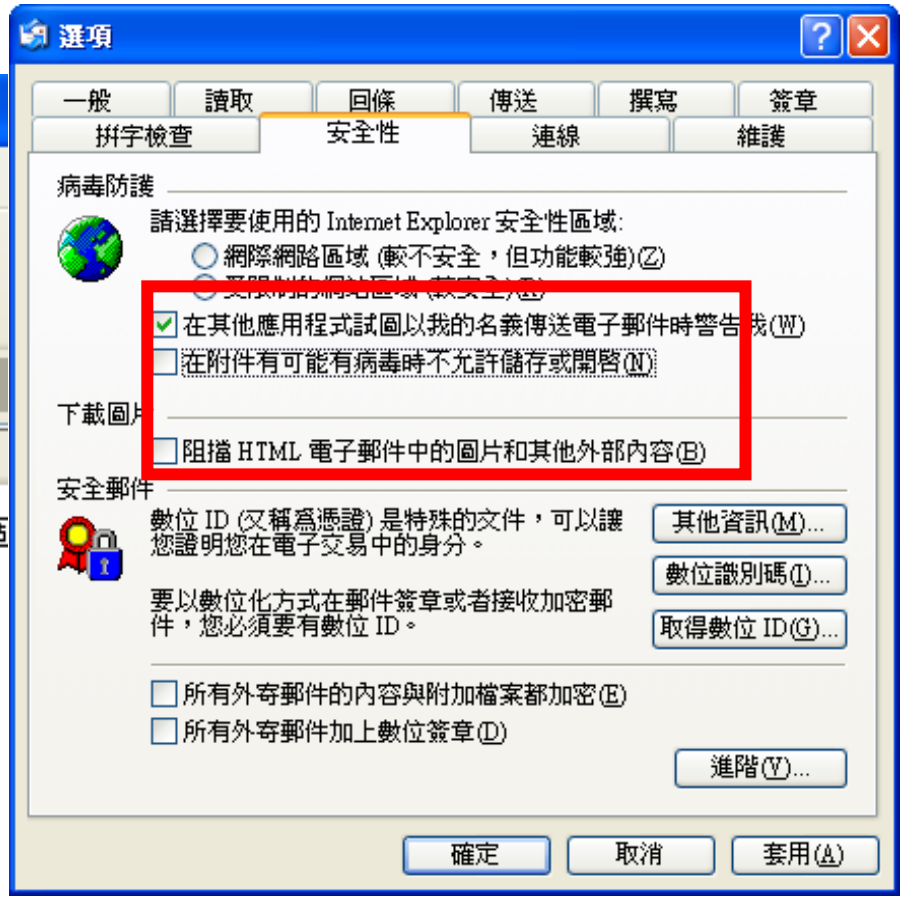
➢關閉預覽窗格



Email軟體安全設定(續)

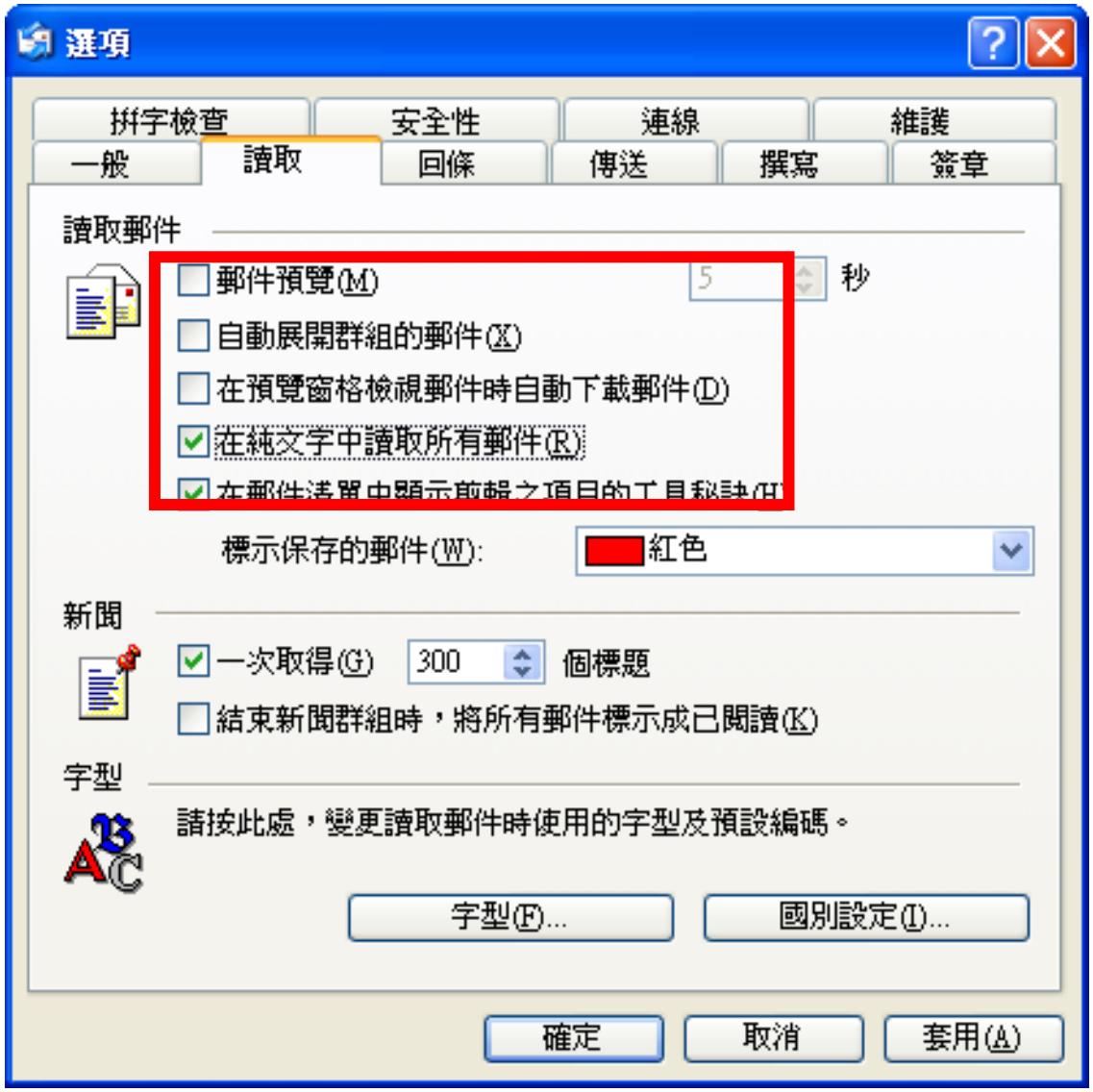
- 附件有可能有病毒時不允許儲存或開啟
- 阻擋HTML電子郵件中的圖片和其他外部內容。

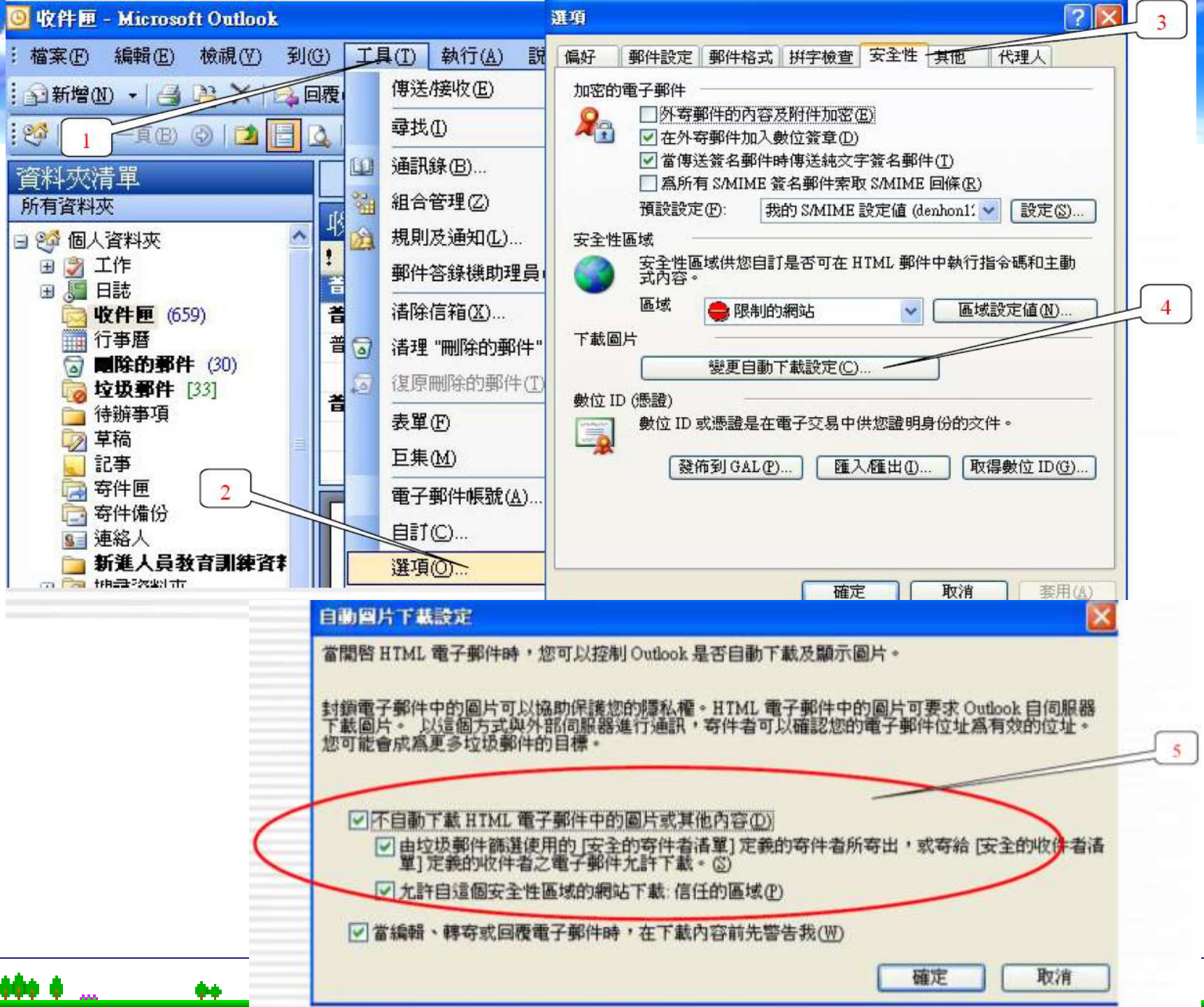


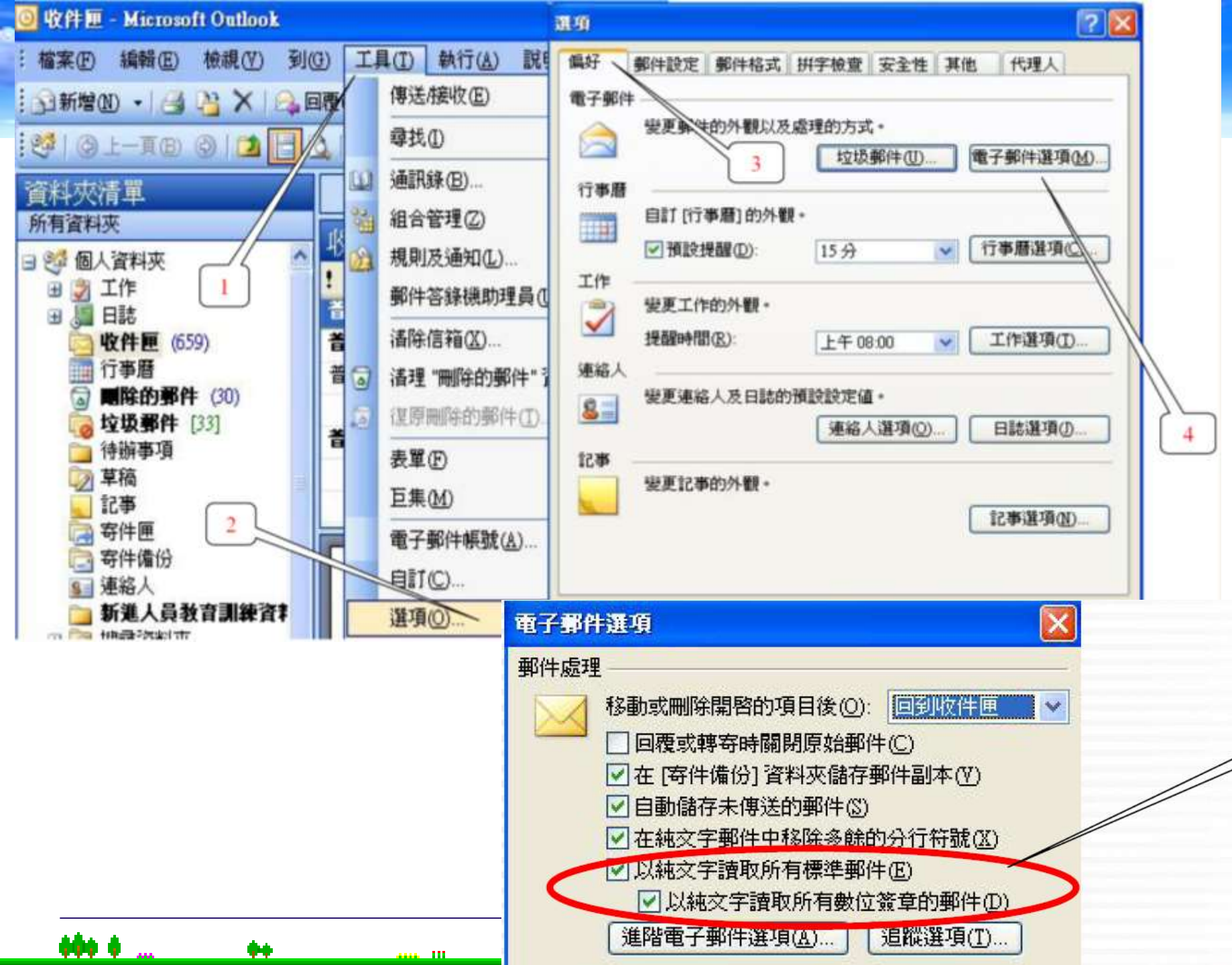


Email軟體安全設定(續)

- 關閉郵件預覽
- 關閉自動下載郵件設定
- 設定在純文字中讀取所有郵件。

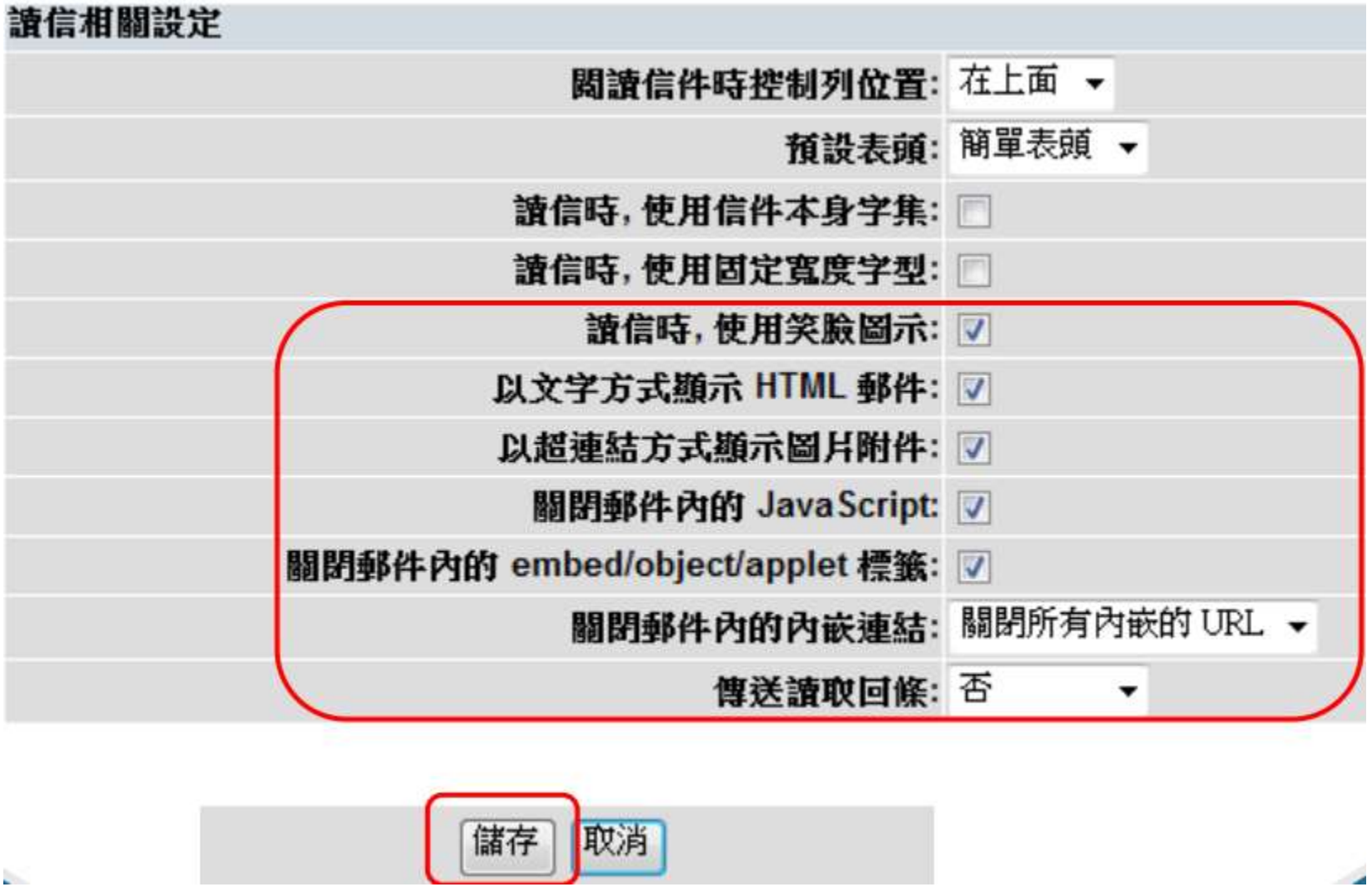



收件匣 - Microsoft Outlook
檔案(F) 編輯(E) 檢視(V) 到(G) 工具(T) 執行(A)
新增(N)
資料夾清單
所有資料夾
個人資料夾
工作
日誌
收件匣 (659)
行事曆
刪除的郵件 (30)
垃圾郵件 [33]
待辦事項
草稿
記事
寄件匣
寄件備份
連絡人
新進人員教育訓練資料
傳送/接收(E)
尋找(I)
通訊錄(B)...
組合管理(Z)
規則及通知(L)...
郵件答錄機助理員
清除信箱(X)...
清理 "刪除的郵件"
復原刪除的郵件(T)
表單(F)
巨集(M)
電子郵件帳號(A)...
自訂(C)...
選項(O)...
1
2
選項
偏好 郵件設定 郵件格式 拼字檢查 安全性 其他 代理人
加密的電子郵件
外寄郵件的內容及附件加密(E)
在外寄郵件加入數位簽章(D)
當傳送簽名郵件時傳送純文字簽名郵件(T)
為所有 S/MIME 簽名郵件索取 S/MIME 回條(R)
預設設定(F): 我的 S/MIME 設定值 (denhon1
設定(S)...
安全性區域
安全性區域供您自訂是否可在 HTML 郵件中執行指令碼和主動式內容。
區域 限制的網站
區域設定值(N)...
下載圖片
變更自動下載設定(C)...
數位 ID (憑證)
數位 ID 或憑證是在電子交易中供您證明身份的文件。
發佈到 GAL(P)...
匯入/匯出(I)...
取得數位 ID(G)...
確定 取消 套用(A)
3
4
自動圖片下載設定
當閱啓 HTML 電子郵件時，您可以控制 Outlook 是否自動下載及顯示圖片。
封鎖電子郵件中的圖片可以協助保護您的隱私權。HTML 電子郵件中的圖片可要求 Outlook 自伺服器下載圖片。 以這個方式與外部伺服器進行通訊，寄件者可以確認您的電子郵件位址為有效的位址。您可能會成為更多垃圾郵件的目標。
不自動下載 HTML 電子郵件中的圖片或其他內容(D)
由垃圾郵件篩選使用的 [安全的寄件者清單] 定義的寄件者所寄出，或寄給 [安全的收件者清單] 定義的收件者之電子郵件允許下載。(S)
允許自這個安全性區域的網站下載: 信任的區域(P)
當編輯、轉寄或回覆電子郵件時，在下載內容前先警告我(W)
確定 取消
5


收件匣 - Microsoft Outlook
檔案(F) 編輯(E) 檢視(V) 到(G) 工具(T) 執行(A)
新增(N)
上一頁(B)
資料夾清單
所有資料夾
個人資料夾
工作
日誌
收件匣 (659)
行事曆
刪除的郵件 (30)
垃圾郵件 [33]
待辦事項
草稿
記事
寄件匣
寄件備份
連絡人
傳送/接收(E)
尋找(I)
通訊錄(B)...
組合管理(Z)
規則及通知(L)...
郵件答錄機助理員(I)
清除信箱(X)...
清理 "刪除的郵件"
復原刪除的郵件(I)...
表單(F)
巨集(M)
電子郵件帳號(A)...
自訂(C)...
選項(O)...
1
2
3
4
選項
偏好
郵件設定
郵件格式
拼字檢查
安全性
其他
代理人
電子郵件
變更郵件的外觀以及處理的方式。
垃圾郵件(U)...
電子郵件選項(M)...
行事曆
自訂 [行事曆] 的外觀。
預設提醒(D):
15 分
行事曆選項(C)...
工作
變更工作的外觀。
提醒時間(R):
上午 08:00
工作選項(T)...
連絡人
變更連絡人及日誌的預設設定值。
連絡人選項(O)...
日誌選項(J)...
記事
變更記事的外觀。
記事選項(N)...
電子郵件選項
郵件處理
移動或刪除開啓的項目後(O):
回到收件匣
回覆或轉寄時關閉原始郵件(C)
在 [寄件備份] 資料夾儲存郵件副本(V)
自動儲存未傳送的郵件(S)
在純文字郵件中移除多餘的分行符號(X)
以純文字讀取所有標準郵件(E)
以純文字讀取所有數位簽章的郵件(D)
進階電子郵件選項(A)...
追蹤選項(T)...
5

WebMail的設定

WebMail的設定


讀信相關設定
閱讀信件時控制列位置: 在上面
預設表頭: 簡單表頭
讀信時，使用信件本身字集:
讀信時，使用固定寬度字型:
讀信時，使用笑臉圖示:
以文字方式顯示 HTML 郵件:
以超連結方式顯示圖片附件:
關閉郵件內的 JavaScript:
關閉郵件內的 embed/object/applet 標籤:
關閉郵件內的內嵌連結: 關閉所有內嵌的 URL
傳送讀取回條: 否
儲存
取消

GMail的設定

不要自動顯示外部內容

系統面其他設定

- 更新相關用戶端軟體
  - OS、瀏覽器、Office、收件軟體、多媒體播放器、Adobe等。

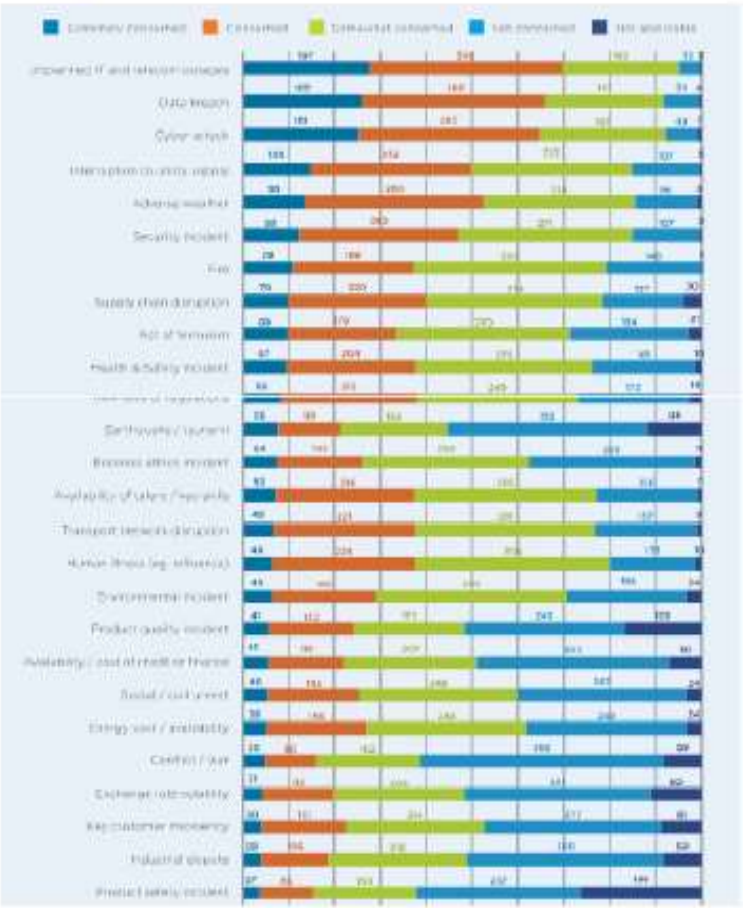
- Webmail
  - 檢查是否有設定可疑自動轉寄帳號
  - 關閉Webmail執行javascript功能。

行動裝置安全防範

- 資 訊 科 技 與 競 爭 優 勢 -

行動裝置安全防護

Top threats in 2013



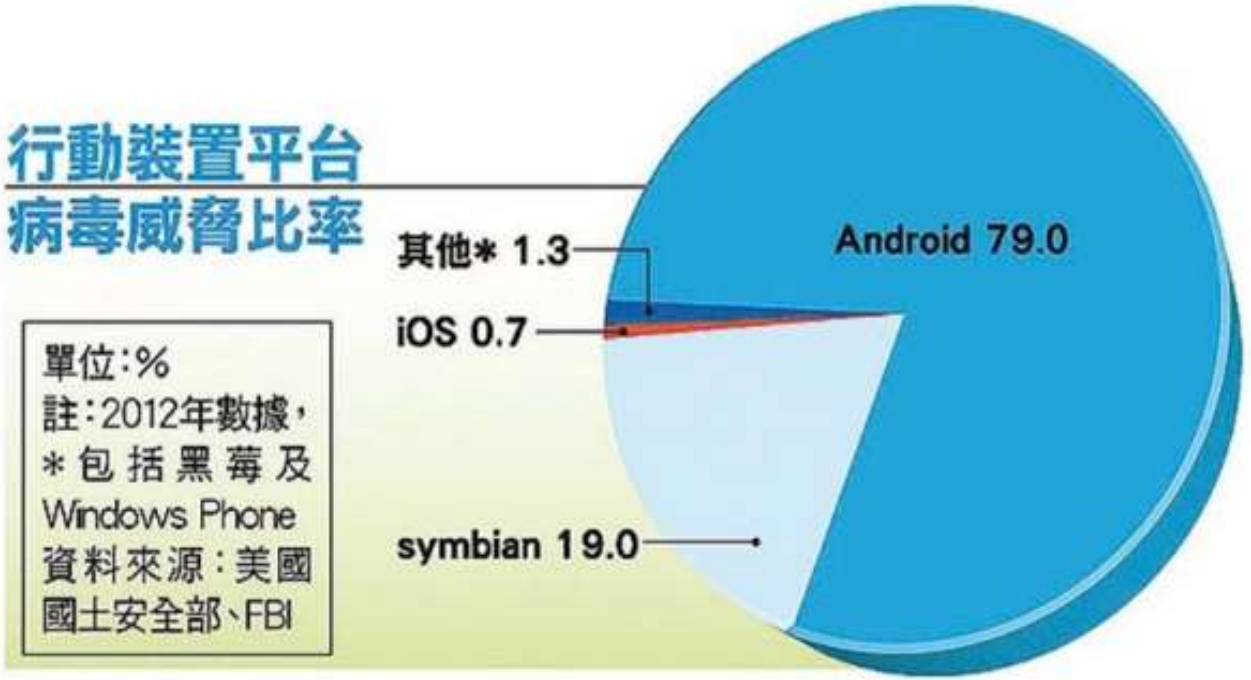
1. Unplanned IT and telecom outages(70%)

2. Data breach (66%)

3. Cyber attack (65%)

Source:
Horizon Scan 2013 Survey Report (BCI & bsi)

行動裝置安全防護


行動裝置平台
病毒威脅比率
單位:%
註:2012年數據,
*包括黑莓及
Windows Phone
資料來源:美國
國土安全部、FBI
其他* 1.3
iOS 0.7
symbian 19.0
Android 79.0

行動裝置安全防護

- 行動裝置存在資安威脅徵兆：
  - 電池壽命變短
  - 通話經常不尋常中斷
  - 電信費用異常
  - 自動下載軟體
  - 手機效能變差

行動裝置安全防護

- ［國際］Cisco年度安全報告：Java與Android為兩大惡意程式目標(2014/1/22)

Cisco於2014年1月公布年度安全報告，內容指出Java與Android為惡意程式的兩大目標。該報告並披露，全球短缺近百萬名安全專家，導致整體的漏洞與威脅程度達到自2000年以來的新高。截至2013年10月的累計漏洞與威脅警告數量比2012年同期增加了14%，其警告數量創下該報告自2000年5月展開追蹤以來的新高。此外，隨著駭客技術愈來愈精密，且攻擊次數不斷升高，已經超出目前資安專家解決威脅的能量負荷，大多數的組織並沒有足夠的系統或人力，持續監控網路或偵測是否遭到入侵，以採取即時且有效的保護措施。

從各種網路威脅來看，Java持續成為最常被駭客利用的程式語言，在感染指標(Indicators of Compromise)中，Java攻擊程式就佔了91%。多種目的之木馬程式則是最常在網路上遇到的惡意程式，佔了網路惡意程式的27%，惡意script則佔了23%，專門竊取資料的木馬程式佔了22%。有99%的行動惡意程式都是鎖定Android裝置。其中，Andr/Qdplugin-A是最常見的行動惡意程式，佔了43.8%，多半是附著在合法的Android程式中，並藉由非官方的應用程式商店遞送。另外，阻斷式服務攻擊的數量與嚴重度皆大增，而且這類攻擊的目的部分是為了分散注意力來掩蓋其他的不法行動。

行動裝置安全防護

- 【愈智慧，愈危險！】 手機也要防毒 防詐騙

自由時報 - 2014年3月5日 上午6:14

智慧型手機盛行，詐騙戰場轉移至手機，社群軟體如LINE廣告訊息多，詐騙集團常以「XX裸照外流」等聳動標題，引誘民眾點擊連結不明網站，進而掉入小額詐款的陷阱，或竊取個資。使得手機防毒的議題益加被重視。

台灣民眾手機防毒認知不成熟，趨勢科技行銷經理朱芳薇表示：「民眾多有電腦必須安裝防毒軟體的認知，但對於手機，卻顯得輕忽。台灣手機使用者安裝防毒軟體，遠遠不到1成，少得驚人。而多數民眾喜愛下載免費程式，高達6成的病毒卻來自免費程式，手機若無防護機制，危險度高。」

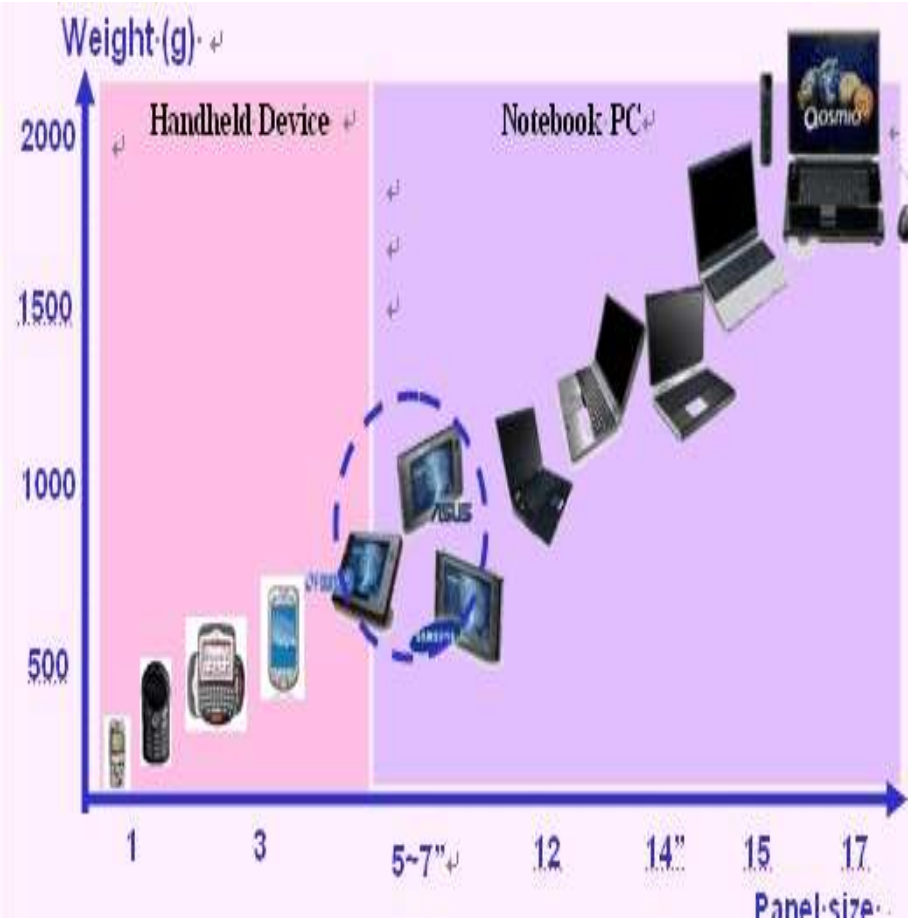
Android自由度高，危險性高，希悅資訊總經理蕭伊婷也說：「Android平台因為給予軟體開發者高度自由，加上全球市占高，使得Android平台上的惡意程式暴增，遠多於相較封閉的iPhone系統，儘管Google已採取相關措施，成效有待加強。」此外，根據卡巴斯基調查，近98.05%惡意程式鎖定Android平台。

行動裝置安全防護

- 智慧型手機驚傳安全漏洞
- 智慧型手機驚傳安全漏洞，用戶個人資料已在不知不覺中被駭客盜取。美國研究員進行7款應用程式的安全性測試，其中Google電子郵件Gmail被成功入侵的機率高達9成以上，主要原因是應用程式共享手機記憶體所導致。

行動裝置使用安全(定義與特徵)

行動裝置(Mobile Device)，也被稱為移動設備、手持裝置（handheld device）等可隨身攜帶，隨開即用的小型電子隨身設備，是一種口袋大小的計算裝置，通常有一個小的顯示螢幕，觸控輸入，或是小型的鍵盤。因為透過它可以隨時隨地存取獲得各種訊息。



行動裝置使用安全(案例分享1)

- 低頭族注意！LINE.APP聊天恐遭監看-壹電視

行動裝置使用安全(案例分享2)

➢ 手機植入程式 簡訊通話位置全曝光－民視新聞

行動裝置使用安全(案例分享3)

- 小心！假充電APP 盜手機個資通訊錄-中視新聞

行動裝置安全防護建議

行動裝置安全防護建議

軟體下載與使用

- 僅安裝可信任來源之軟體
- 注意軟體安裝時所要求之權限是否合理
- 定期進行軟體更新或修補作業
- 安裝資安防護軟體

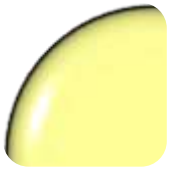
行動裝置安全防護建議

資料保護

- 注意資料備份與加密防護
- 安裝具「可遠端定位並進行資料清除」功能的資安軟體
- 注意廢棄行動裝置之資料處理

行動裝置安全防護建議

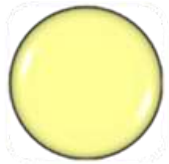
連線功能設定



小心使用公開的無線 wi-fi 網路

小心使用藍芽（Bluetooth）功能

小心使全球定位（GPS）功能



小心使用近場通訊（Near Field Communication, NFC）功能

行動裝置安全防護建議

- WIFI與藍芽接收、傳送檔案要謹慎，以免收到病毒檔案。
- 中毒時暫時關閉行動裝置上的WIFI與藍芽接收功能，以免繼續搜尋感染目標。

  ＝＞惡意程式可以側錄按鍵資訊，記錄到電話語音密碼來做銀行轉帳，或是只要找到電腦的遠端弱點，透過行動裝置的3G、3.5G、4G或是藍芽當作跳板入侵其他電腦。

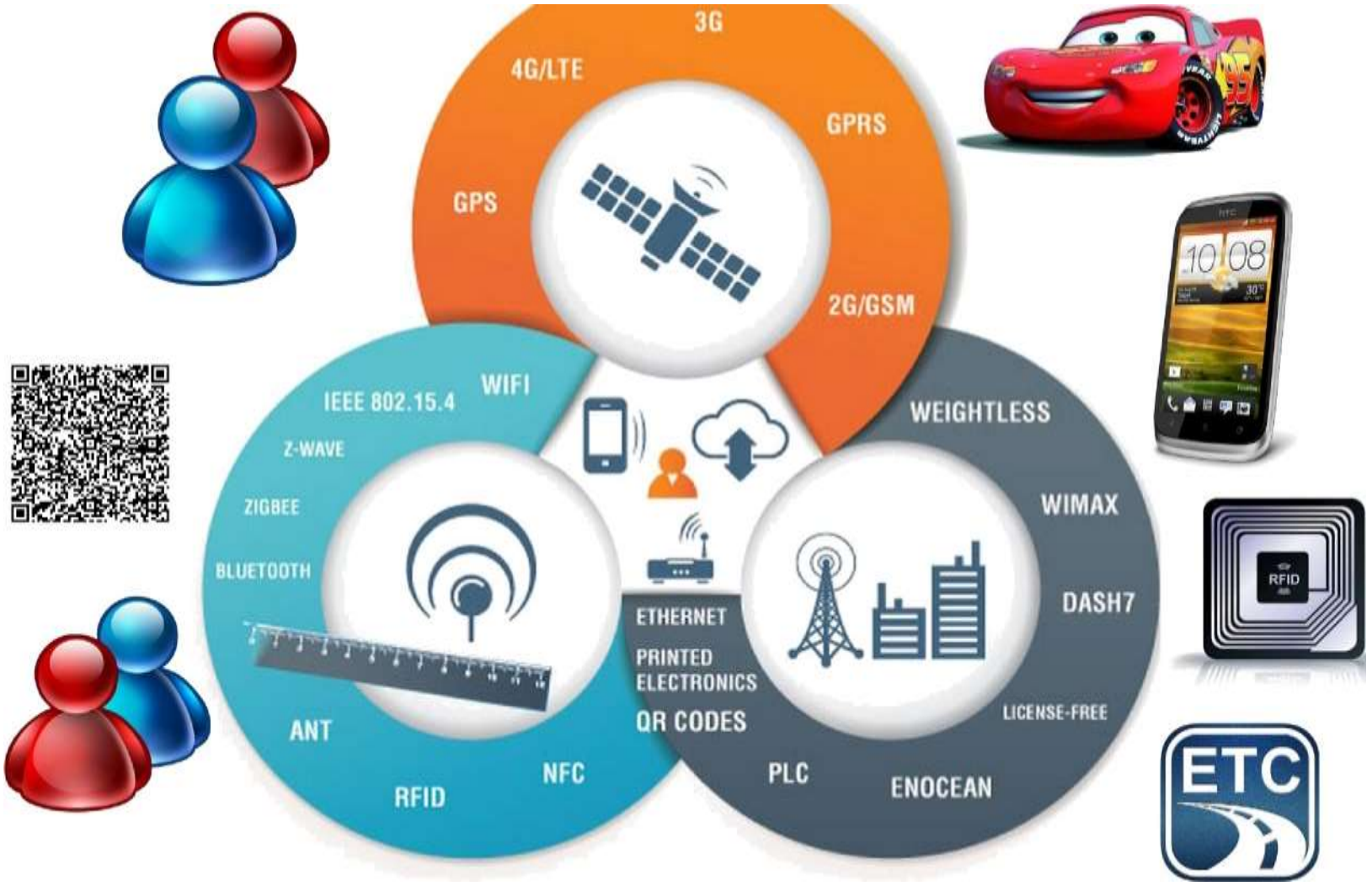
物聯網與安全威脅

- 資 訊 科 技 與 競 爭 優 勢 -

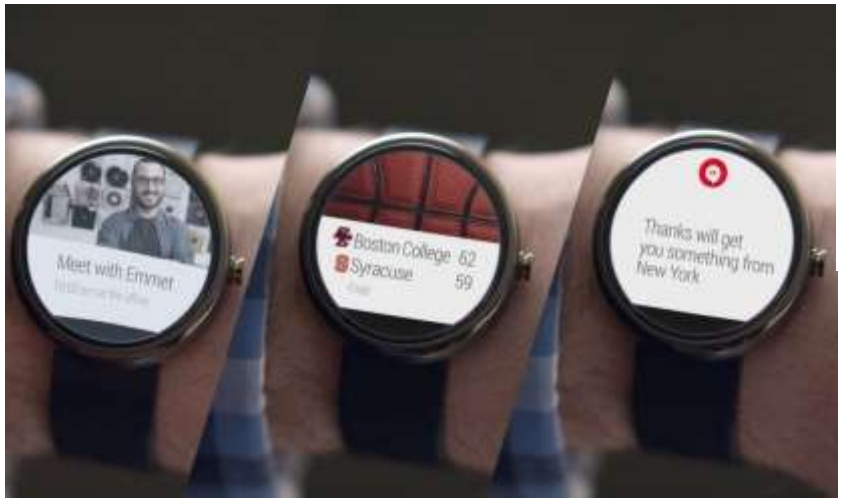
什麼是物聯網(IOT)

- 物聯網(IOT, Internet of Things)
  - Internet：網路提供資訊傳遞的平台
  - Things：人、物、通訊、資料…等
- 資通訊的環境以行動通訊為主
  - 行動裝置的時代、無線通訊為主
- 資訊交換時間的縮短
- 高速運算能力的需求
- 巨量資料的加值與應用
- 下一代的網路(NGN)
  - 資訊交換的方式改變
  - 資訊交換的對象多樣化

物聯網示意圖


3G
4G/LTE
GPRS
GPS
2G/GSM
WIFI
IEEE 802.15.4
Z-WAVE
ZIGBEE
BLUETOOTH
ANT
RFID
NFC
WEIGHTLESS
WIMAX
DASH7
LICENSE-FREE
ETHERNET
PRINTED ELECTRONICS
QR CODES
PLC
ENOCEAN
RFID
ETC

穿戴與可攜裝置


Meet with Emmet
Boston College 62
Syracuse 59
Thanks will get you something from New York


7'27"
2.96
00:05:11
1.04
BIKE


10:08

網路成為資訊傳播的主要管道

- 社群網路成為人類社交的主要管道
- 網路的連結提供需求雙方資訊的交換
- 終端裝置的多樣化，提供即時的資訊
- 人是物聯網主要的使用者，並與行動裝置緊密結合
- 數位化的智慧城市時代

行動裝置的資安威脅

- 資料遺失(Data loss)
  設備遺失、退休的設備等
- 惡意程式(Mobile Malware)的資訊竊取
- 應用程式的資安威脅
  寫的不好，造成資訊處理風險
- 設備的弱點
  作業系統、應用程式、裝置設計
- 通訊的資安威脅
  不安全的WiFi通訊、暱名(不合法)的AP存取點
- 管理功能不足
  身份管理、功能限制
- NFC與近場通訊的安全
  NFC通訊的風險、駭客就在你身邊

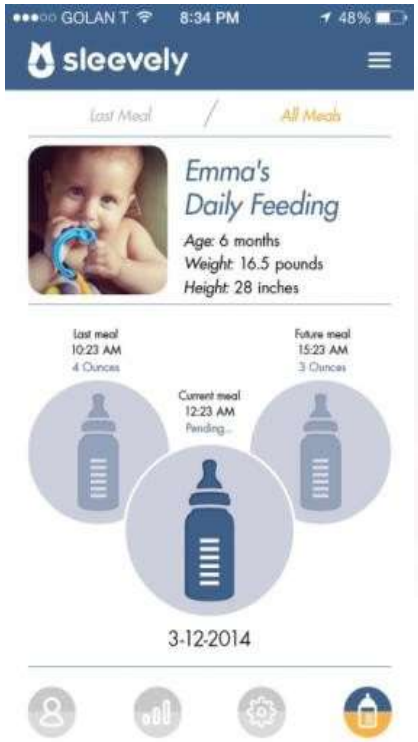
NFC成為資料竊取的管道…

NFC只有在螢幕開啟時才有作用，所以…

智慧城市

- 提供人類活動需要的資訊
  - 食、衣、住、行、育、樂
  - 資訊取得的便利
    - 網際網路、數位媒體
  - 建置預警的機制與環境
- 處理人類活動過程產生的資訊
  - 商務活動中的金流、物流
  - 生活資訊的產生
    - 消費、活動、位置等

智慧奶瓶



- 紀錄嬰兒的的食量
- 餵食的日期、時間
- 長時間紀錄飲食曲線

太陽能轉成電能


Solar panels
Suction plate
The absorber is easily attachable and removable from the window by the air pressure.
On.Off

生理狀況資訊

- 即時掌握生理狀態
- 具備通訊能力
- 運用網路社群資源

五種物聯網上可能的威脅攻擊及防範

- 2015年3月初世界行動通訊大會在巴賽隆納舉行，趨勢科技的執行長陳怡樺以傑出的技術領導者身分出席此會議。來自世界各地的專家和從業人員齊聚一堂討論市場上最新及未來的行動創新，不過重要的是記住網路風險也隨之而來，及如何去對抗常見威脅以保護你的行動裝置和寶貴的資料。五種網路犯罪分子可能對物聯網（IoE, Internet of Everything）進行的威脅攻擊，以及你可以做些什麼防範來減輕風險。

五大威脅攻擊

- **監聽攻擊**。這種攻擊會用到監聽程式（sniffer），竊聽任何透過網路傳送的未加密資訊再加以竊取。
- **阻斷服務攻擊**。網路犯罪分子利用這種攻擊來封鎖或癱瘓對某些網路或設備的使用。
- **金鑰淪陷攻擊**。在此類攻擊中，用來加密通訊的金鑰被竊，被用於解譯加密過的資料。
- **基於密碼的攻擊**。網路犯罪分子利用這類攻擊來入侵網路或連到特定網路的設備。主要是經由猜測或竊取密碼。
- **中間人攻擊**。在此種攻擊中，第三者會竊走雙方或設備間傳輸的資料。

安全防範

- 啟用智慧型設備上所有的安全功能
- 定期更新產品韌體
- 正確地加密其韌體更新和網路通訊
- 使用安全的密碼
- 了解製造商如何管理他們設備的漏洞

- **萬物聯網（IoE，Internet of Everything）**呈現出令人興奮的時代，具備更多的**方便性、行動性和創新科技**。今日市場上許多的智慧型設備都是種革新，讓我們一窺可能的未來。然而，增加的易用性和連通性也帶來隱私的安全威脅。這些設備收集和傳輸更多的**個人資料**，就讓網路犯罪分子有更多機會來加以攔截並用在犯罪用途上。

現在進行式的資安威脅情境1、2

影音資料來源：下載自趨勢科技po於youTube

網路安全事件分享

- 資 訊 科 技 與 競 爭 優 勢 -

資訊資料存在哪邊？

- 電腦相關資訊
- 正式文件
- 文件草稿
- 信手塗鴉
- 內部通訊
- 正式及非正式會議
- 媒體及公開來源
- 閒聊八卦
- 社群

網安事件分享

世界經濟論壇(WEF) Global Risks 2015 Report

Top 10 risks in terms of Likelihood	Top 10 risks in terms of Impact
1 Interstate conflict	1 Water crises
2 Extreme weather events	2 Spread of infectious diseases
3 Failure of national governance	3 Weapons of mass destruction
4 State collapse or crisis	4 Interstate conflict
5 Unemployment or underemployment	5 Failure of climate-change adaptation
6 Natural catastrophes	6 Energy price shock
7 Failure of climate-change adaptation	7 Critical information infrastructure breakdown
8 Water crises	8 Fiscal crises
9 Data fraud or theft	9 Unemployment or underemployment
10 Cyber attacks	10 Biodiversity loss and ecosystem collapse

bsi.

資料來源：BSI

網安事件分享

《IoE 萬物聯網安全趨勢 》

智慧型燈泡遭駭使得 Wi-Fi 密碼遭竊

這款「可變換顏色的省電 LED 燈泡」會經由標準的「6LoWPAN 」網狀網路（mesh network）廣播 Wi-Fi 密碼，這種網路是最適合低功率無線裝置（如燈泡）的一項通訊標準。

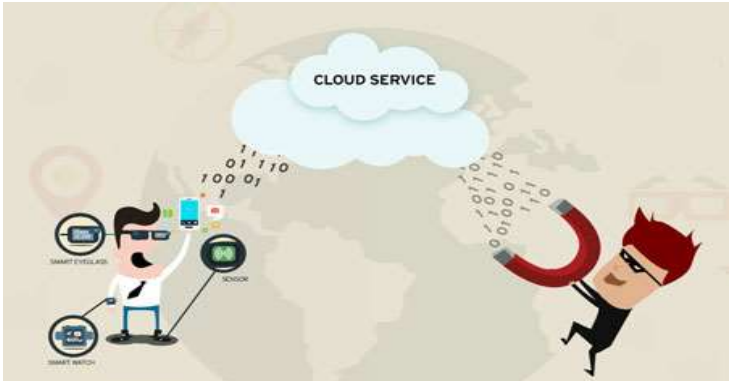
駭客發現了一個可讓其進入主燈泡以及其他相連燈泡的漏洞。駭客接著又在屋主不知情的狀況下，向網路業者索取該 Wi-Fi 網路的詳細資料。透過這個方法，駭客就能在離其中一個燈泡 30 公尺的距離內取得其加密後的密碼。

網安事件分享

《IoE 萬物聯網安全趨勢 》

穿戴式裝置攻擊

Apple Watch 引發了各種隱私權和資訊安全的問題。尤其是 Apple Watch 新的健康追蹤功能讓人們對這類敏感資訊安全性感到質疑。



駭客入侵雲端服務業者來竊取資料

駭客控制了穿戴式裝置。

網安事件分享

《IoE 萬物聯網安全趨勢 》

付款終端機在交易中如何處理你的信用卡資料？

2014年的付款終端機（PoS）惡意軟體攻擊呈現大幅度的上升，不管是數量上、金額上或危害的範圍。經常有著數以千萬計的支付用卡片資料被竊，有時是一次攻擊行動就能造成。這些卡片資料接著會賣往地下世界的卡片論壇，它們在那被用來進行詐騙性購物、轉帳或提款。

這不只是出現在單一產業的現象而已，在這整年中，攻擊涵蓋了零售業（當然）、郵政、停車場、餐廳、旅館和美容產業。

圖片來源：趨勢科技

網安事件分享

《IoE 萬物聯網安全趨勢 》

飛機、火車與汽車 － 有哪裡可以逃過PoS惡意軟體的威脅？

網路犯罪分子在PoS(付款終端機)惡意軟體中加入遠端管理功能。因為遠端存取工具加上RDP/VNC功能讓他們可以進入自動付款或電子服務系統。

任何具備網路連線的處理支付卡資料設備都該被視為潛在目標，不管其位在何處。使用者永遠不該假設位在機場、火車站甚或是停車場的自助服務機都具備跟其他自助服務機相同或正確的安全等級。

Image source: commons.wikimedia.org

網安事件分享

卡巴斯基：發現世界上最狡猾的APT攻擊，病毒暗中傳播已有7年！

資安業者卡巴斯基實驗室（Kaspersky Lab）周一（2014/2/10）揭發一個名為The Mask（Careto）的APT攻擊行動，自2007年起就涉及全球的間諜行動，迄今才被發現。

The Mask主要鎖定政府機關、外交辦公室、大使館、能源或石油企業、研究單位，特別是政府機關和能源企業，而且都是透過精密的工具進行攻擊。攻擊目的是竊取機密資料，諸如辦公室文件、加密金鑰、VPN配置、SSH金鑰，或是可用來開啟遠端電腦連結的RDF檔案。卡巴斯基並以「世界上最狡猾的進階持續性滲透攻擊（APT）行動」來形容它。受害者遍布全球31個國家，從中東、歐洲、非洲到美洲，所使用的工具涵蓋極為複雜的惡意程式、rootkit、bootkit，鎖定平台除了Mac OS X與Linux外，還可能包括Android與iOS。

資料來源：
iThome
文/陳曉莉2014-02-12發表

網安事件分享

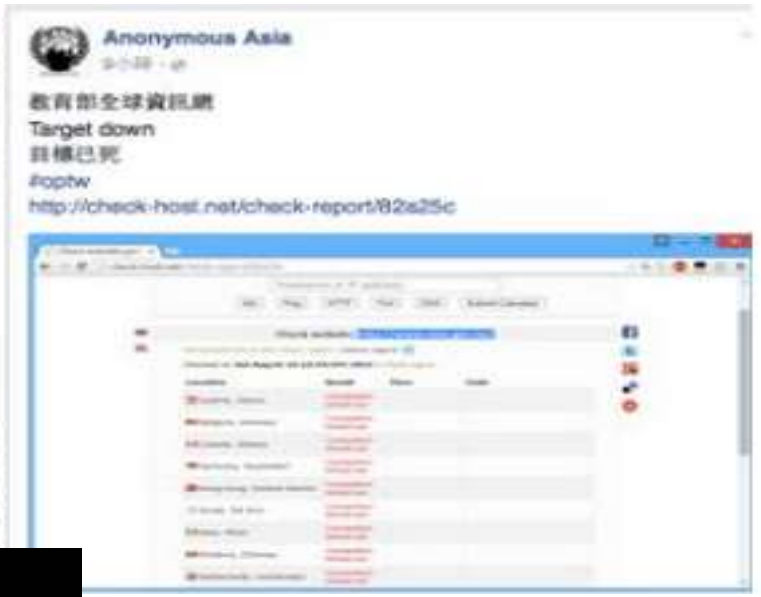
歐洲遭遇史上最大DDOS攻擊

內容遞送網路(Content Delivery Network, CDN)服務供應商CloudFlare於2014/2/10受到大規模的分散式阻斷服務攻擊(Distributed Denial-of-Service Attacks, DDoS)，並宣稱這次規模大過歐洲反垃圾郵件組織Spamhaus在2013年3月所受到的攻擊，創下DDoS攻擊的新紀錄。在2013年遭受阻斷式服務攻擊的Spamhaus也是CloudFlare的客戶，當時攻擊的尖峰流量為300Gbps，差點癱瘓歐洲網路。CloudFlare執行長Matthew Prince於2/10在其Twitter上指出，他們正遭受網路校時協定(Network Time Protocol, NTP)類型的阻斷式服務攻擊，規模大過於上次針對Spamhaus的攻擊。根據Mr. Prince的貼文，這次攻擊流量約400Gbps以上，且影響最大的地區在歐洲。

資料來源：行政院國家資通安全會報技術服務中心

網安事件分享

「匿名者」三度攻擊 癱瘓國民黨、新黨、經濟部、國民黨台北市黨部網站(2015.8.3)



網安事件分享

- **ANDROID 惡意程式數量已突破100萬門檻**
- 資安業者趨勢科技(Trend Micro)在8月公布的第二季行動安全報告(TrendLabs 2Q 2013 Security Roundup)中指出，過去3年鎖定Android的惡意程式數量為35萬個，但今年上半年的惡意程式數量已增長至71.8萬，當時趨勢根據此一成長速度估計今年底Android平台上的惡意程式數量便會超過**100萬個**，但此一預測已於9月提前到達。現在市場上已有100萬種行動惡意程式，其中約有**75%屬於真正的惡意程式**，另有25%則是包含廣告程式在內的高風險程式。
- 趨勢表示，在惡意程式的類別中，佔最大比例的是Fakeinst(34%)與Opfake(30%)家族，Fakeinst會**偽裝成合法程式，然後傳遞簡訊到高費率的號碼或是訂閱昂貴的服務**。Opfake與Fakeinst的手法類似，另**還會要求使用者下載其他的惡意程式。**
- 趨勢科技建議使用者，對待自身行動裝置要像對待個人電腦一樣，特別是在**安全**議題上，應對所下載的程式保持警覺，並閱讀程式的評論與開發人員資訊等。另外，如非必要，**不要在Google官方Play以外的網站下載應用程式。**

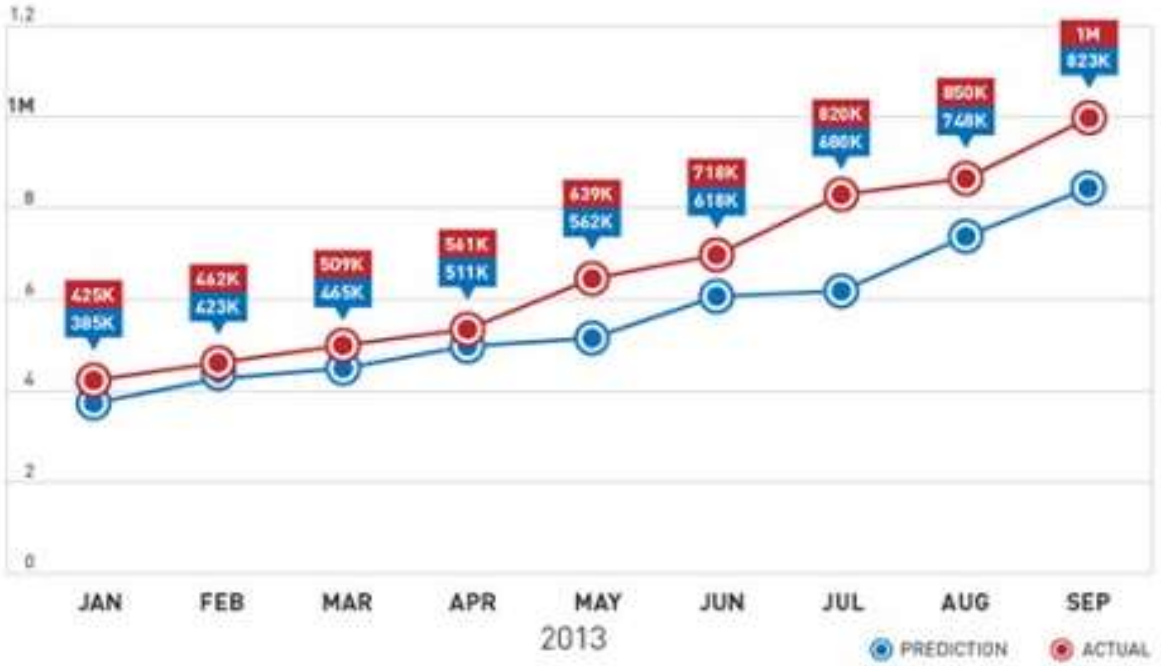
資料來源：http://blog.trendmicro.com/trendlabs-security-intelligence/mobile-malware-high-risk-apps-hit-1m-mark/

網安事件分享

➢Android惡意程式數量已突破100萬門檻

資料來源： iThome 文/陳曉莉（編譯）2013-10-07

現在市場上已有100萬種行動惡意程式，其中約有75%屬於真正的惡意程式，另有25%則是包含廣告程式在內的高風險程式。



網安事件分享

➢Android惡意程式數量已突破200萬門檻

資料來源：趨勢科技全球技術支援與研發中心 2014-04-10

就在惡意及高風險的行動裝置 App 程式突破100萬關卡後的半年內，該數字又翻了一倍、突破200萬支的大關！

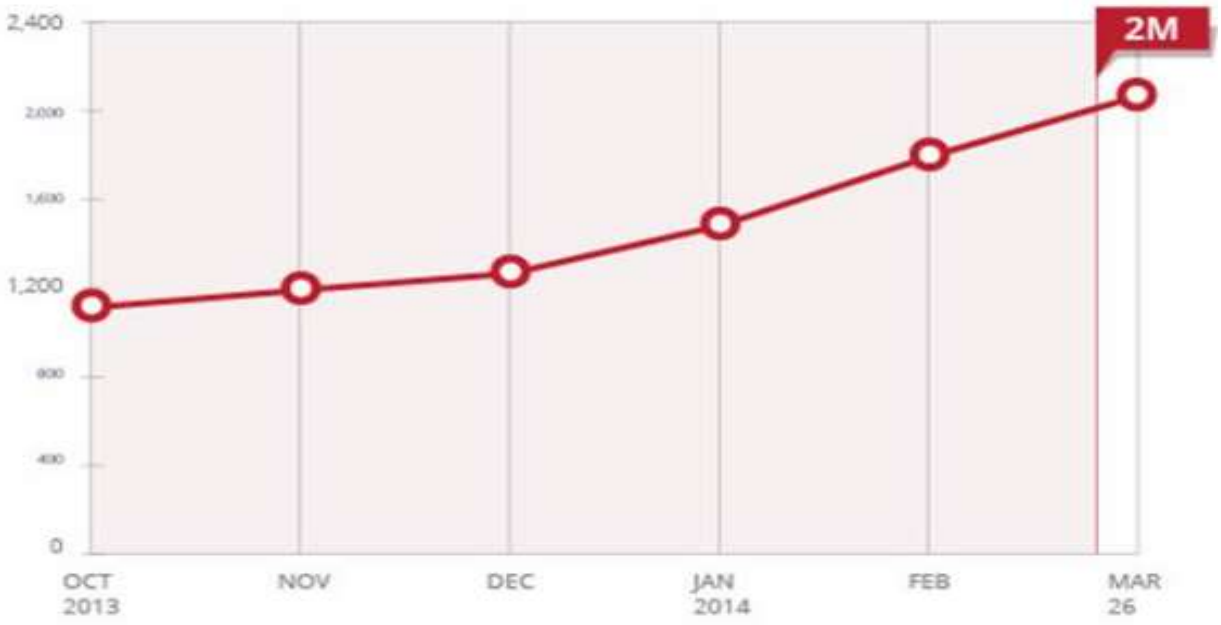


圖1：惡意及高風險的App程式數量，已突破二百萬關卡

網安事件分享

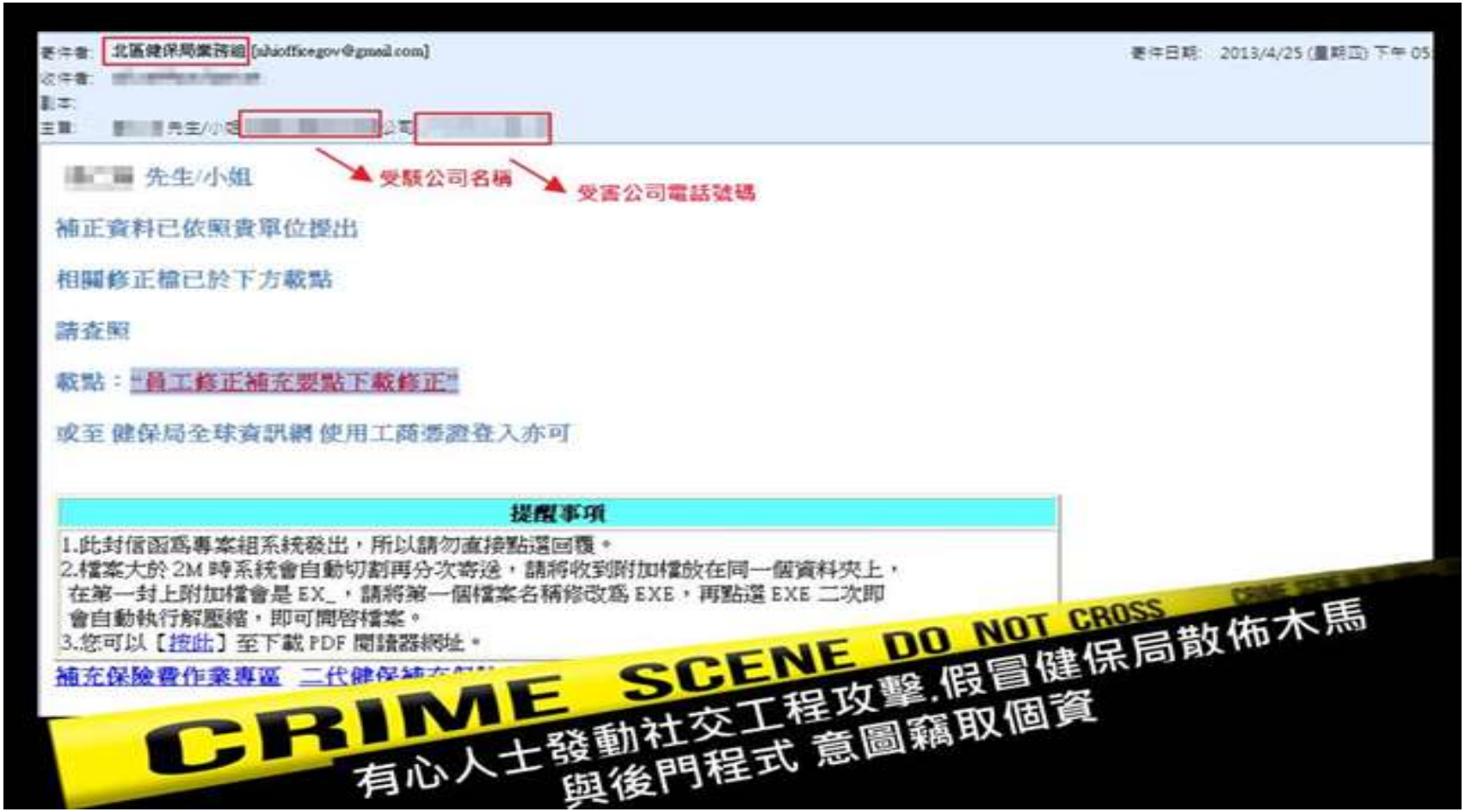
連上網站會執行惡意程式

- 警政署刑事局偵破駭客假冒健保局竊取個資案件

  2013年5月26日 台北訊】刑事局今日宣佈偵破駭客四月底冒用健保局北區業務組名義進行目標性攻擊竊取個資一案，駭客係假冒健保局名義發動客製化的社交工程陷阱(Social Engineering)攻擊，首先透過發送大量以健保局北區業務組為名寄送的郵件，其中內含「員工修正補充要點下載修正」的連結，一旦點選此連結將被轉址至另一個網址並自動下載一個名為「二代健保補充保險費扣繳辦法說明」的RAR壓縮檔。

網安事件分享

連上網站會執行惡意程式



資料來源：趨勢科技

網安事件分享

➢小心！史上最狠毒勒索軟體肆虐臺灣

資料來源：iThome 文/張景皓 2013-10-16

近日，有一支名為CryptoLocker的勒索軟體（Ransomware）現蹤臺灣，企業陸續傳出受害災情，該軟體透過釣魚郵件入侵，會將受害者電腦的檔案全數加密，導致檔案無法存取，而且駭客採用高超的加密技術，讓受害者無法自行復原，並限期3天支付9,000元(台幣)贖金，否則將毀損解密金鑰，受害者苦不堪言。

網安事件分享

- 國際執法單位也致力打擊去年(2013)9月出現的Cryptolocker電腦病毒。
- Cryptolocker病毒將受害者電腦加密，再胡亂開價要使用者付錢換解鎖密碼，金額經常高達700美元以上。
- 疑為駭客組織首腦的30歲俄羅斯籍鮑加契夫（Evgeniy Mikhailovich Bogachev）依14項罪名於美國賓州匹茲堡（Pittsburgh）起訴，包含利用玩完宙斯和Cryptolocker病毒犯下共謀罪、電腦駭客行為、銀行詐欺和洗錢。

（資料來源：譯者-中央社張詠晴）

網安事件分享

- 加密勒索軟體感染翻兩倍-行動惡意威脅App突破500萬大關！

  資料來源：2015 年 06 月 01 日 BY TREND LABS 趨勢科技全球技術支援與研發中心

- 趨勢科技於最新發表的「2015年第一季資安報告」指出，醫療產業、iOS裝置與PoS(銷售櫃台系統)為新興惡意攻擊目標，2015年惡意威脅數量也再創新高，第一季平均每月攔截到的惡意威脅數量高達47億，較去年同期增加15億，且第一季每秒平均攔截到1800個惡意威脅，比去年同期每秒增加600個！
- 而伴隨著行動裝置盛行，行動裝置惡意威脅的成長幅度更是以驚人速度大幅攀升，已於2015年第一季突破500萬大關。
- 2015年第一季全球共有800萬用戶曾造訪惡意網站，而台灣更名列最常造訪惡意網站的第四大國家。

網安事件分享

資料庫被駭

- 南韓1.04億筆信用卡個資外洩

南韓於2014/1爆發了高達1.04億筆的信用卡個資外洩案，估計影響當地2000萬人，大約是南韓總人口數的2/5，甚至連南韓總統朴槿惠的個資都遭竊，此一堪稱是全球最大的個資外洩案引起了各地的關注。竊取大量個資的是南韓信用評價組織(Korea Credit Bureau)所聘請的39歲朴姓電腦工程師，他負責開發可辨識偽卡的軟體，並擁有存取南韓三大發卡公司KB Kookmin Card、Lotte Card與NH Nonghyup Card資料庫的權限。朴姓工程師自2002/5到2013/12間，多次趁機將資料庫中的信用卡個資複製到私人的USB裝置內，最終在2014/1被發現並遭到警方逮捕。

資料來源：行政院國家資通安全會報技術服務中心

網安事件分享

資料庫被駭

- **美國 TARGET 遭駭客入侵**

  美國僅次於Walmart的第二大折扣連鎖零售商Target於12/19在官網對外證實遭到駭客入侵，估計約有4000萬筆的信用卡或簽帳卡資料被竊。在美國擁有1800家商店的Target在12/19發出郵件通知客戶，表示該公司的付款資料遭到駭客非法存取，可能影響從2013/11/27至12/15於該公司美國商店消費的顧客，這些被竊取的資料涵蓋顧客的姓名、信用卡或簽帳卡號碼、卡片到期日與卡片驗證碼。這是美國歷史上規模第二大的信用卡資料外洩事件。

資料來源：行政院國家資通安全會報技術服務中心

網安事件分享

資料庫被駭

美破超級駭客 竊個資1.6億筆

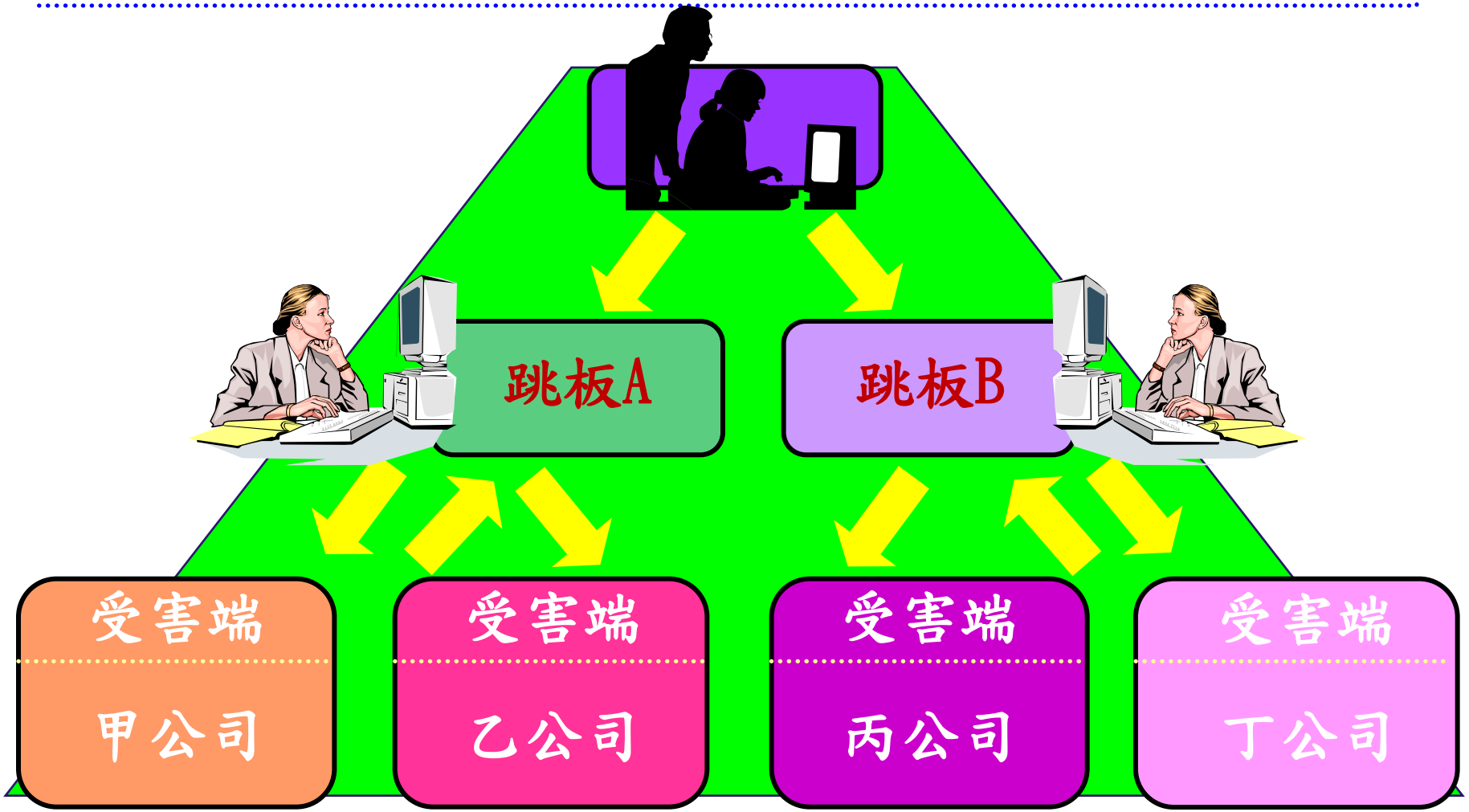
2013-07-27 01:55 | 中國時報 | 【謎悠文、實習編譯易晉羽／綜合報導】

美國新澤西州檢方廿五日起訴五名外國男子，指控他們在全球進行駭客行動，竊取至少一億六千萬筆信用卡和金融卡帳號資料，轉賣牟利，保守估計企業損失超過三億美元，這也是美國歷年來破獲的最大規模駭客入侵及竊取資料的案子。

根據新澤西州紐瓦克檢方的起訴書，四名俄羅斯和一名烏克蘭男子組成的駭客集團，涉嫌在七年間侵入十多家美國和國際企業電腦網路竊取個資，世界各地付款處理商、零售業者和金融機構是他們的主要目標。美國那斯達克股市（Nasdaq）電腦遭到攻擊，威士卡（Visa）的相關業者以及法國零售業者家樂福集團也受害。

網安事件分享

殭屍病毒攻擊



網安事件分享

- 發送惡意郵件之中繼站

  中部某○○醫院網站遭入侵(變成跳板、殭屍電腦)，發送惡意電子郵件，經過濾２萬餘封電子郵件，發現內含8種不同木馬之郵件有1791件，其中政府部門有642封分屬28單位，學校、法人及個人有1149封。

  經過調查局查明後，以公函分別通知各受駭單位或法人，建請其更改帳戶密碼以維資安。

網安事件分享

- 資安漏洞 Android手機恐靠簡訊就能駭

  資料來源：中央社 - 2015年7月28日 下午1:58

- （中央社舊金山27日綜合外電報導）網路安全公司Zimperium今天警告，全球最熱門智慧型手機作業系統Android存在漏洞，能讓駭客透過文字訊息入侵操控。
- 根據法新社，Zimperium行動安全（ZimperiumMobile Security）在部落格中說：「攻擊者只需要利用你的手機號碼，就能透過MMS（多媒體訊息）發送特製媒體檔案遠端操作。」
- 「一項完全武器化的成功攻擊，甚至可以在你查看訊息前就先刪除。你只會看到訊息通知。」

網安事件分享

➢駭客扮文青 經典小說淪電腦入侵工具

資料來源：法新社 - 2015年7月29日 上午12:05

- （法新社華盛頓28日電） 在21世紀的今天，駭客居然會想到盜用19世紀經典小說「理性與感性」（Sense and Sensibility）的文句來散播惡意軟體，作者珍・奧斯汀和書中角色若知道此事，肯定驚訝無比。
- 資安防護服務業者思科安全（Cisco Security）的研究人員在今天公布的一份報告指出，文學作品的詞句成為隱藏惡意指令的新途徑，讓駭客得以非法侵入電腦與網路。
- 在這份年中資安報告中，研究人員表示：「和傳統使用隨機文字的手法相比，將經典文句加入漏洞攻擊包登陸頁面，是更有效的隱匿技術。」

網安事件分享

➢ 美國防部關閉電子郵件

資料來源：路透社 - 2015年7月29日 上午8:58

- （中央社華盛頓28日路透電）美國國防部發言人今天表示，因發生可疑狀況，由陸軍上將鄧普西（MartinDempsey）與美國軍方聯合幕僚單位成員使用的非機密電子郵件網絡已遭下線。
- 陸軍中校韓德森（Valerie Henderson）指出，上週末時，由於發現可疑活動，國防部將聯合幕僚單位所有成員共同使用的非機密電子郵件網絡關閉，現階段已完全下線。
- 韓德森說，「我們一直持續留意與降低自身網絡的安全危機」，「基於這個嚴記在心的準則，我們先關閉聯合幕僚單位網絡，也會持續進行調查」。
- 韓德森未特別說明何謂網絡的可疑活動，但她表示，網絡是被國防部主動關閉，不是遭可疑活動或外部單位所影響。

中央社（翻譯）

網安事件分享

➢ 美國國防部電子郵件系統疑遭俄國駭客入侵，已停擺超過11天

資料來源：iThome - 2015年8月7日 編譯/陳曉莉

➢ 根據報導，美國五角大廈辦公室（Pentagon）的非機密（unclassified）電子郵件系統在上個月遭到駭客入侵，於7月25日緊急關閉聯合參謀總部的相關系統，迄今尚未回復正常運作，起因可能是參謀長辦公室員工遭受**網釣郵件攻擊**，致使五角大廈伺服器受到感染。之後駭客採用自動系統以迅速蒐集五角大廈伺服器的大量資料並傳送到網路上的數千個帳號，不過，駭客僅存取了非機密郵件伺服器上的資料，並未取得機密資料。

網安事件分享

- 全球知名偷情網站Ashley Madison被駭，3700萬用戶資料恐曝光

  資料來源：中央社 - 2013年8月27日 下午7:58

- 專門提供婚外情及一夜情交友平台的Ashley Madison傳出遭到駭客入侵，駭客集團The Impact Team要求其母公司Avid Life Media永遠關閉Ashley Madison與Established Men網站，否則就要公布公司機密與客戶資料。
- The Impact Team指稱，該網站提供19美元個人資料刪除服務，一年帶來170萬美元的收益，但卻無法實際刪除所有資料，還留有使用者的交易資訊，包含實際姓名與地址，而這卻是使用者真正想刪除的內容。

網安事件分享

- 台中市議長狂發色情圖片…臉書中毒了！

資料來源：聯合新聞網 - 2015年6月11日 上午3:16

- 台中的政治人物擅用臉書宣傳，點閱率也高，但這兩天卻不約而同「中毒」；立委何欣純和議員張廖萬堅等人臉書被植入色情圖片，粉絲點進去「嚇一跳」；議長林士昌臉書則瘋狂轉發色情影片給好友，病毒隨之散發。
- 林士昌議長已向警方報案；其他人則採取更改密碼、或暫時關閉臉書因應。
- 台中市警局刑警大隊科偵組長張承瑞表示，經過調查應非駭客入侵或帳號盜用，研判是臉書中毒。

網安事件分享

➢《兩則瘋傳的病毒》 “被偷拍的是你麼"手機簡訊 / facebook 流傳的長髮美胸女孩圖

資料來源： 2013.08.19由 Trend Labs 趨勢科技全球技術支援與研發中心

看到這張圖不要點

http://shareaza2.fr/A3xszi5GQ5Nbk1zu4p.jpg?d=NmfPMvuccmTP
shareaza2.fr

“被偷拍的是你麼“收到這簡訊不要點連結(夾帶手機病毒)

網安事件分享

➢ 假宅急便:「您的快遞簽收通知單」

➢ 資料來源： 2014.03.17由 Trend Labs 趨勢科技全球技術支援與研發中心

上周出現「我的手機送修，麻煩替我收個簡訊好嗎？」的小額詐騙後,今天又出現一則上面寫著「您的快遞簽收通知單，收件電子憑證 http://goo.gl/0000」，有位網友購買空氣清淨機後，接獲自稱黑貓宅寄便送貨員發送簡訊:「您的快遞簽收通知單，收件電子憑證」並附上短網址,受害網友點選網址後，卻被要求下載軟體才能觀看，下載後竟收到電信業者「小額付款」授權碼，根據警方表示,3月至今已發生四起類似案例，被騙的金額都是1000元。

網安事件分享

LINE簡訊詐騙 逾2月19起

資料來源： 記者王燕華／宜蘭報導 | 聯合新聞網 - 2013年11月6日 上午3:44

「看著這些照片，好懷念以前的日子喔」、「朋友家狗狗參加人氣比拼，幫忙讚一下」，

民眾如果最近接到手機或LINE的簡訊，有類似字樣並附上網路連結時，千萬別馬上按下去，否則手機很可能被植入木馬程式，遭到詐騙。(按連結後，向中華電信調帳單明細，發現**被扣1千元行動電話費用**。)

類似詐騙方式**從9月起**在宜蘭出現，縣警局刑警大隊表示，9月至今受理19件，其中9月2件，10月14件，這個月迄今有3件，詐騙總金額6萬3800元，受害者最多被騙走7千元，少則1千元。

網安事件分享

網路銀行資料遭竊取

資料來源：教育部資訊及科技教育司 (轉載自刑事警察局)

據科技犯罪防制中心指出：有犯罪集團利用假資料註冊與國內知名網路銀行、航空公司等極為類似之網址，再於各大搜尋引擎公司購買關鍵字廣告，誘使民眾連結至藏有木馬程式網頁，俟民眾電腦遭植入木馬後再導向正常網站，此時木馬程式已開始進行鍵盤側錄與竊取檔案，竊取民眾網路銀行帳號密碼，其後再進行轉帳盜取，此類損失達已數千萬元。

網安事件分享

- 全台近千網站植入惡意程式

資料來源：教育部資訊及科技教育司

據媒體報導：平均每 10 個網頁，就有 1 個植入惡意程式碼，「拒絕壞程式基金會」(http://stopbadware.org) 發布「全台近千網站植入惡意程式」訊息，顯示目前網站內含惡意程式碼問題嚴重。

網安事件分享

➢ 電子郵件帳號遭駭客竊取

資料來源：教育部資訊及科技教育司

國內 4 所大學之郵件伺服器與駭客中繼站建立連線，且特定電子郵件帳號遭登入下載郵件查看，疑似洩漏重要資訊內容。

✓ 如果您必須要離開公用電腦一段時間，登出所有的程式並關閉所有可能含有機密資訊的視窗。

網安事件分享

➢ 學生駭客竊取帳號修改網站

資料來源：教育部資訊及科技教育司

北區某知名高中之學生於駭客教學網站習得駭客入侵技巧，練習入侵多所學校網站，並於某小學網站發布『學校寒假延長訊息』假消息，另刪除多所學校網站重要資料。

- ✓ 如果您必須要離開公用電腦一段時間，登出所有的程式並關閉所有可能含有機密資訊的視窗。
- ✓ 校園應加強宣導駭客行為必須擔負法律責任。

安全事件案例分享

駭客疑狂猜密碼-A咖裸照被看光

資料來源：中央社 - 2014年9月2日 下午1:47

（中央社洛杉磯1日綜合外電報導）網路論壇昨天出現珍妮佛勞倫斯等百位A咖名流裸照，部分報導起初說，蘋果公司雲端硬碟被攻擊，致照片外流，但駭客也可能是不厭其煩狂試密碼，讓女星私密照全都露。

駭客用蘋果最常認可的500組密碼試圖登入使用者帳號。如果成功的話，駭客便可直搗iCloud帳號，要取得用戶照片當然不是問題。The Next Web科技新聞網站威廉斯（OwenWilliams）說：「如果駭客成功猜到Find my iPhone密碼，理論上也可藉此登入iCloud，並可在使用者渾然不知情況下，數分鐘內同步Mac或iPhone照片。」

圖片來源：中時電子報

網安事件分享

17歲駭客破譯帳戶19萬筆 盜75億元被抓

資料來源：中央社 - 2015年2月8日 下午4:35

（中央社台北8日電）廣東省公安廳最近宣布特大駭客信用卡詐騙案，抓獲17歲葉姓少年等11名嫌犯。這名17歲少年駭得19萬筆銀行卡帳戶資料，盜刷涉案金額人民幣近15億元（約新台幣75億元）。

廣東省公安廳表示，上述集團先由葉嫌利用自己編寫的駭客軟體攻擊銀行網銀系統，大批提取客戶銀行卡、信用卡的資料，再由網路仲介人員層層轉賣葉嫌盜取的大量銀行信用卡資料。

省公安廳指，最後，不法分子在網路上尋找銀行網路支付、第三方快捷支付漏洞，將葉嫌竊取的銀行卡資料在網路大肆盜刷或轉帳牟利。

網安事件分享

2014年-4000多家公司成為網絡攻擊目標

資料來源：2015.04 卡巴斯基實驗室報告

- 在2014年，安裝Android的設備受到攻擊的次數，和去年相比，上升了四倍。
- 安全事故中，那些最容易受到駭客攻擊的應用程式，包括安裝在移動設備上的程式，首當其沖的是Oracle Java，接下來是瀏覽器，包括IE瀏覽器、谷歌瀏覽器和火狐瀏覽器，排在第三位的則是Adobe閱讀器，尤其是PDF閱讀器。
- 在2014年連續發起的網路攻擊運動（APT），全球至少55個國家4400多家公司受到影響，比2013年增加了2.4倍，2013年受到網絡攻擊的公司大約是1800家。
- 根據英特爾網絡安全和國際研究與戰略中心發佈的一份報告，網路犯罪給全世界帶來高達大約5750億美元的損失。

網安事件分享

私密影片勒贖新手法-以惡意App竊取個資

資料來源：2015.04 趨勢科技報告

- 不法集團利用社交交友管道發動愛情攻勢，誘騙被害者拍攝分享個人私密影片進行側錄，再誘騙安裝惡意App竊取個資勒贖，目前已在日本、韓國出現受害案例，該犯罪手法可能蔓延到台灣。
- 犯罪集團製作20款以上的惡意App，偽裝成LINE或是消費者熟悉的圖案如Android機器人、QR-Code等等，以降低被害者的警覺心。

網安事件分享

強化資安-國防部擬製無照相智慧手機

資料來源：2015年04月11日 15:45 中天記者報導

- TSMC台積電手機，配發給工程師，只能打電話、發簡訊，就是不能拍照。宏達電則是用自家手機，要關掉照相功能。鴻海明文規定，一律禁帶手機入廠區，就是要杜絕機密外流。
- 阿帕契觀光團拍照打卡，讓軍紀破功。國防部仿效科技大廠，想研發無拍照功能智慧手機保密防諜。

Android 指紋辨識的資安危機

資料來源：科技新報 作者　發布日期 2015 年 08 月 08 日

- 指紋辨識技術開始運用於智慧手機上的時候，許多人都提出了一個問題：密碼被盜了，可以改掉；指紋被盜了，你總不能換掉手指吧？。
- 由於許多 Android 手機並沒有完全鎖死指紋感測器，透過遠端遙控，駭客們可以竊取到使用者儲存在受影響手機中的指紋圖像。而如果你 Root 了你的 Android 手機 ，你的指紋被竊取的風險將會更大。

指紋資訊被竊取後，駭客可以用這些資訊來解鎖你的手機，甚至完成行動支付的身分驗證，指紋資訊被人盜用於移民身分驗證、犯罪紀錄等領域的時候，事情的嚴重性就提升到了新的層級！

課後評量

- 資 訊 科 技 與 競 爭 優 勢 -

李政峰 (James Lee)
經濟部工業局-能源管理系統輔導顧問
E-mail：jameslee1858@gmail.com

- ISO 27001 主導稽核員
- ISO 20000 主導稽核員
- BS 25999 主導稽核員
- BS 10012 主導稽核員