電腦入侵手法
社交工程篇

漢昕科技
資安顧問　K2

課程大綱

- 郵件社交工程的定義
  - 社交工程是什麼？
  - E-mail社交工程演練方法及流程
  - 社交工程信件的類型
  - 電子郵件社交工程要求標準
- 傳送接收郵件的考量
- 使用WebMail的考量
- 郵件社交工程防護停看聽
  - 1. 信件攻擊手法
  - 2. 社交攻擊手法
  - 3.注意可疑電子郵件的特徵
  - 4. 社交工程信件的防範措施

郵件社交工程的定義

- 社交工程是什麼？
- E-mail社交工程演練方法及流程
- 社交工程信件的類型
- 電子郵件社交工程要求標準

郵件社交工程的定義

- 社交工程是什麼？
  - 社交工程的定義利用**人性的弱點**或利用**人際之信任關**係來進行詐騙，是技術與人性之間的攻擊方式，藉由人際關係的互動進行犯罪行為。

郵件社交工程的定義

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

E-mail社交工程演練方法及流程

駭客

網際網路

郵件伺服器

紀錄伺服器

使用者

使用者點閱信件及紀錄(四週)

- 使用者開啟郵件紀錄
- 使用者點選連結或附件紀錄
- 轉寄信件紀錄歸屬轉寄者

- 以Hinet、Google、Yahoo等偽造發出
- 是否偽造受測單位寄件者名稱
- 是否以受測單位業務資訊為信件標題

電子郵件社交工程執行目的及依據

- 目的：為提升電子郵件使用者警覺性意識，避免使用者因瀏覽垃圾及惡意電子郵件進而影響網路安全及發生個人資訊洩漏事件
- 依據**行政院國家資通安全會報**96年05月18日資安發字第0960100539號函96年政府機關(構)資安演練評審辦法規定：
- (一)中央A級機關
- 惡意郵件開啟率需為**16%**以下，超連結點閱率需為**9%**以下。
- (二)其餘主管機關
- 惡意郵件開啟率需為**26%**以下，超連結點閱率需為**15%**以下。

人數百分比/信件數百分比

執行細項及結果

- 執行期間：9X年X月X日~ 9X年X月X日
- 發送測試信件
  - *免費送巧連誌影音教材*、*民代可以蒐集個資嗎*、*茂德增資*、*殺OnLine線上遊戲桌布*、*豬哥亮準備復出*、*男人誌線上閱讀網*、*座位靠窗邊*、*2009台北國際花卉展開始囉*
- 會開啟社交工程信件之
- 次數**24**次，佔該項發信量**1272**封信中的**1.9%**
- 會點選社交工程信件中超連結之
- 次數**6**次，佔該項發信量**1272**封信中的**0.5%**

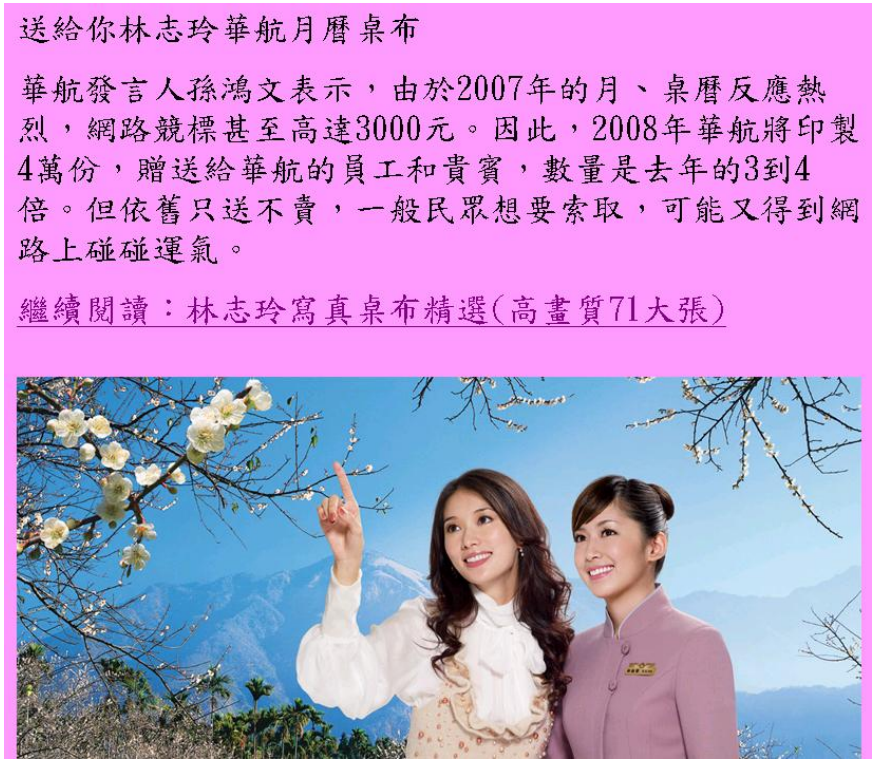
標準16%

標準9%

（模擬數據）

信件範本-01-林志玲華航月曆桌布

- 包含*明星或寫真圖片的電子郵件*點閱率始終居高不下；本封電子郵件利用民眾對於明星相關訊息具有高度興趣的習慣下，發送明星相關活動新聞並於內容提及明星桌布取得不易以及本郵件具有*高畫質寫真桌布*，誘使使用者繼續點選電子郵件中的連結



- 對於明星所代言之活動，*官方並不會以電子郵件方式宣傳且提供下載*，而是應於*官方網站中以網頁方式呈現*，因此只要收到此類信件大多為有心人士於網路上找尋大眾所感興趣之話題所製成的社交工程詐騙信件

信件範本-02-人生就是跟自己賽跑

人生就是跟自己賽跑，用這樣的態度去面對人生，你會產生推動自己不斷學習、進步的能量，而且你眼中會看到一個更遠、更高的目標。每天醒來，你都會因此而感到生氣勃勃。--馬英九

- 社交工程就是一種利用人性弱點的詐騙技術，藉由與人之間的互動而形成的犯罪行為；本封電子郵件為*模擬駭客針對剛當選總統的馬英九為議題*，以垃圾信件的大量發送手法發送測試信件於使用者

下一篇：馬英九(妙語如珠)

23【閱讀，可漫遊、可發光】

四、五十年代的台灣，小小的租書店裡，架子上擺滿了各式各樣的武俠小說。

幾個男孩等不及，手上抓著一本小說，坐在小板凳，就津津有味地看了起來。

- 對於名人的事蹟、名言等內容的電子郵件，*大多數人認為這是好文章因此轉寄給他人*，孰不知這是垃圾郵件的常見手法，無形轉寄中已幫了惡意人士的大忙。*對於此種電子郵件應盡量做到不開啟、不轉寄*

信件範本-03-限制級精彩古代漫畫

限制級精彩古代漫畫(要看完喔!)

- *情色類電子郵件由於點閱率高*，在垃圾信件中一直佔有一定的比例，更是*有心人士慣用的手法*；本封電子郵件模擬駭客針對使用者寄發一封具有情色相關內容的電子郵件，引誘使用者閱讀電子郵件甚至點擊內文中的超連結

- 對於情色類的電子郵件，應於*辦公室環境中明令禁止使用者開啟瀏覽及點閱*，電子郵件主旨中包含*隱喻*、*影射*、*寫真*等字眼皆為情色類的電子郵件類型

信件範本-04-麥當勞也悄悄漲價了

- 該封電子郵件為行政類電子郵件，利用*陳舊的新聞事件*並結合近期民眾關心的*民生物資漲價議題*，模擬駭客手法，大量發送電子郵件於使用者

麥當勞也悄悄漲價了　台北都會區售價最多比別區貴20元(2008/07/31 17:18)

生活中心／綜合報導

去年12月才調漲過早餐價格的台灣麥當勞，宣布明天起又要漲價，調漲金額從4元至20元不等。而首開連全國將採分三區調漲，北部都會區以及交通樞紐區漲幅最高。

想吃麥當勞，得先看看你身處何處，因為販售價錢可會有所不同了。從八月一號起，麥當勞不只要調漲台灣分成3個區域，雲林縣、南投縣、花蓮縣、台東縣、台南縣、嘉義縣、屏東縣是第一區，販賣價格將不及娛樂交通樞紐區劃分為第二、三區，價格最高比第一區貴了20元。

針對麥當勞這種「突破性」的調漲，民眾反應不一。一位反對的民眾說：「當然會覺得有點不公平，同樣什麼價錢會不一樣。」；另外一位贊成的民眾則說：「因為台北的消費本來就比較高。店租也相對比較高合理的。」

改價後的麥當勞新的商品價格，6塊麥脆雞餐有賣199元，也有賣209元，第三區最貴賣到219元，最高跟最元。6塊麥克雞餐也一樣，分成105元、109元跟115元3種價格，第一區跟第三區售價就差了10塊錢，就連也有45元跟49元兩種價格。

同樣的商品，從北到南麥當勞售價大不同，民眾抱怨，以後除了少吃麥當勞外，好像也沒什麼辦法了。一說：「（調整售價）會覺得不舒服，可是如果你喜歡吃的話，還是會多花那10到20塊吧。」

麥當勞發出聲明稿表示，考慮到原物料漲幅以及全台各地家庭可支配收入，而分區訂定價格，也才會出現三制的售價。只是看在生活負擔已經很重的都會區消費者眼中，麥當勞這一漲真的讓他們的痛苦指數也跟

麥當勞漲價新聞

- 防範此種電子郵件的方式應該宣導使用者做到[不開啟]、[不轉寄]，由於*一般正常的公務內容的電子郵件皆為一般純文字文件*，所以也可以在電子郵件軟體中設定(以outlook express 為例)，[工具/選項/讀取/*以純文字方式讀取所有郵件*]，即可避免此類社交工程電子郵件的攻擊

信件範本-05-市長不見了？

- 該封電子郵件為政治類電子郵件，利用*聳動的政治標題*並選擇政治人物新聞為內容的社交工程電子郵件。本封電子郵件模擬駭客手法利用公務人員上司新聞，誘使使用者開啟該電子郵件

胡志強今上班-線營要給他好看〔記者唐在馨／台中報導〕

市長胡志強昨天返國，民進黨市議會黨團將於今天上午9點到市府前「迎接台中市府兼外交部長胡志強回國」，表達對「颱風來，市長落跑」最大的不滿及抗議。

民進黨議員陳淑華、蕭杰、鄭功進及賴佳徵昨天偕妥布條，預備今天號召黨團成員一起到市府前廣場舉辦「歡迎式」。陳淑華表示，雖然胡志強昨天回國，對自己的決策表示「兩難」及「歉意」，但市長為何執意要以外交為重，以及「市長的心在哪裡」？身為中市民意代表，不能不追究。

議員鄭功進、賴佳徵說，胡志強說，「研判颱風不會造成太大的傷害」，所以才出國，胡志強那麼會研判氣象，乾脆去當「氣象局長」好了，還諷刺胡的「預測神功」怎麼沒有發揮在卡玫基颱風來臨時，太晚宣佈停班停課，且中市還出現百年難得一見的大淹水？

蕭杰則表示，市長說「要給市府團隊一個表現的機會」，市長還有一年半的任期，就急著要「給別人表現的機會」，不如快點去中央任職，讓市府團隊「好好表現」就好了；至於胡志強去中央做什麼？蕭杰說，外交部、社會福利部都可以，因為他這次選擇颱風來仍出國，只是為了送腳踏車給馬紹爾。

- *任何媒體並不會主動寄發新聞消息*，除非*使用者有明確的訂閱電子郵件*的動作，否則主動寄發的新聞、政治類電子郵件，大多為社交工程惡意郵件

信件範本-06-情人節專屬玫瑰花桌布

- 電子郵件社交工程手法越來越多樣化，除了利用時事吸引使用者點擊之外，同時也會利用*美麗的版面*與大量的圖片來降低使用者的緊戒心；本封電子郵件模擬駭客針對*七夕情人節議題*對使用者寄發一封具有大量情人節專屬玫瑰花桌布為內容的電子郵件

- 對於*來路不明的電子郵件*，即使內容或標題多吸引人，也*不應該開啟或點擊郵件內的任何連結*，隨時保持接收電子郵件及上網的警覺心，是保護個人電腦資訊的最佳法門

信件範本-07- 2008花旗銀行網路辦卡

- 選擇美商花旗銀行夏季網路辦卡服務的原因為：近來*使用信用卡消費的人數越來越多*，基於信用卡帶來的便捷性以及該活動具有優惠方案，故模擬駭客以社交工程手法利用美商花旗銀行夏季網路辦卡服務電子廣告信件，誘使電腦使用者瀏覽並點選該電子郵件超連結

- 正確辦理信用卡服務的方式，應該是由*洽辦者親自前往該銀行辦理*，凡是網路上的電子郵件，*只要聲稱與任何銀行有洽辦關係*，*大部分皆為詐騙行為*，如果該電子郵件為正式花旗銀行所發出之電子郵件，電子郵件標頭網域名稱應該是*[@citibank.com*]

信件範本-08-擺脫菸癮 1通電話專人協助

- *行政類電子郵件*其主要為*一般政府機關對外公告知途徑*，但由於網路新聞媒體的氾濫，常見由一般使用者於閱覽之後轉寄他人以共同閱覽，本封電子郵件模擬駭客以*真實網路新聞事件*內容，大量轉寄於其他使用者

擺脫菸癮 1通電話專人協助

〔記者李信宏／苗栗報導〕

修正後的菸害防制法從明年1月施行，抽菸場所的限制更趨嚴格，苗栗縣衛生局呼籲癮君子趕快戒菸，提供戒菸專線0800-636363的免付費電話，有專人輔導，為癮君子量身打造專屬戒菸計畫，擺脫尼古丁的糾纏。

圖片由董氏基金會提供

衛生局表示，根據統計，約有70%的癮君子曾嘗試戒菸，但因為毅志力不足、誘因太多及缺乏醫療專業指導，以致多數人的戒菸計畫功敗垂成。

戒菸專線 量身打造

衛生局說，1通電話就能開始戒菸，戒菸專線有專業的醫療人員1對1電話訪談，依個人菸齡、吸菸量及健康條件，量身打造個人專屬的戒菸計畫，這可提高戒菸的成功率。

- 對於電子郵件的轉寄，經常是駭客入侵以及病毒傳播的一大途徑，應於辦公室環境中宣導[*勿轉寄非公務用途的電子郵件*]

測試帳號相關資料

- 測試對象: **159**個聯絡人(信箱)
- 總發信量: **1272**封。(159信箱x 8封信)

單位分類	人數(信箱數)	單位分類	人數(信箱數)
A	13	H	4
B	22	I	3
C	11	J	13
D	11		
E	14	L	11
F	13	M	19
G	22		

（模擬數據）

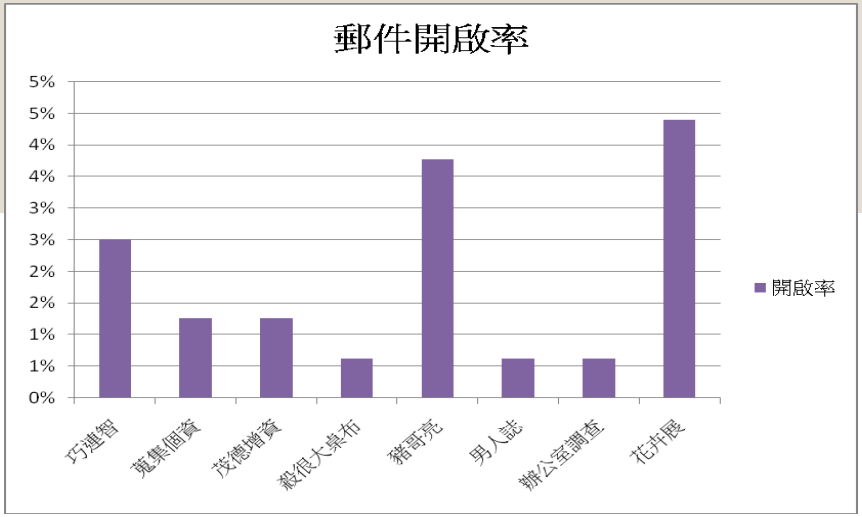
測試人數影響百分比/隨機抽樣

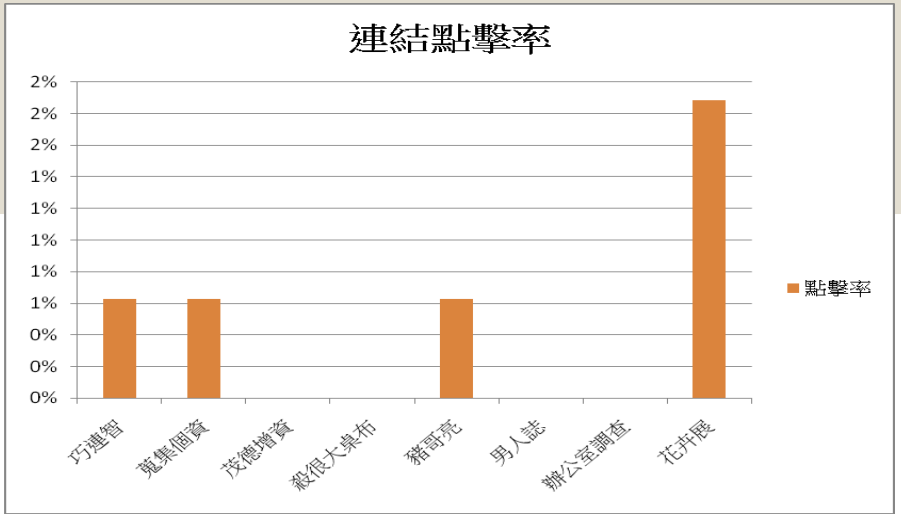
測試結果概要

單位分類	受測人數	郵件開啟數	郵件開啟率	超連結點擊數	超連結點擊率
A	13	6	5.8%	1	1.0%
B	22	2	1.1%	1	0.6%
C	11	1	1.1%	0	0.0%
D	11	1	1.1%	0	0.0%
E	14	1	0.9%	2	1.8%
F	13	0	0.0%	0	0.0%
G	22				1.1%
H	4				0.0%
I	3	0	0.0%	0	0.0%
J	13	2	1.9%	0	0.0%
M	19	6	3.9%	0	0.0%
各項目總計	159	24	1.9%	6	0.5%

（模擬數據）

測試人數影響百分比/隨機抽樣





類別	巧連智	個資	茂德	殺很大	豬哥亮	男人誌	調查	花卉展	合計
開啟次數	4	2	2	1	[illegible]	1	1	[illegible]	24
點擊次數	1	1	0	0	1	0	0	[illegible]	6
發信數					[illegible]		159	159	1272
開啟率	2.5%	1.3%	1.3%	0.6%	3.8%	0.6%	0.6%	4.4%	1.9%
點擊率	0.6%	0.6%	0.0%	0.0%	0.6%	0.0%	0.0%	1.9%	0.5%

（模擬數據）

測試年齡層影響測試數據

演練結果說明

（模擬數據）

- 98年政府機關(構)資安演練評審辦法規定：
- (一)中央A級機關
- 惡意郵件開啟率為**16%**，附件點閱率為**9%**。
- (二)其餘主管機關
- 惡意郵件開啟率為**26%**，附件點閱率為**15%**。
- (開啟社交工程信件之)
- 次數**24**次，佔該項發信量**1272**封信中的 **1.9%**
- 下載社交工程信件中附件(指點選超連結)之點閱率
- 次數**6**次，佔該項發信量**1272**封信中的 **0.5%**

演練結果明細表

（模擬數據）

單位	姓名	巧連智	收集個資	茂德增資	遊戲桌布	豬哥亮	男人誌	座位靠窗	花卉展	統計
A	加菲貓				1	1	1	1		4
B	米妮	1	1	1						3
C	皮卡丘					2			1	3
D	哆啦A夢		2			1				3
E	柯南								2	2
F	蠟筆小新	2								2
G	小熊維尼	1							1	2
H	米其					1				1
I	櫻木花道								1	1
J	史奴比								1	1

傳送接收郵件的考量

- 傳送與接收E-mail建議使用純文字模式
  - 優點
    - 在安全性的考量來說可以減少被信件攻擊的風險！
  - 缺點
    - 只有文字，所以若是有做漂漂的信件，將會看不到！

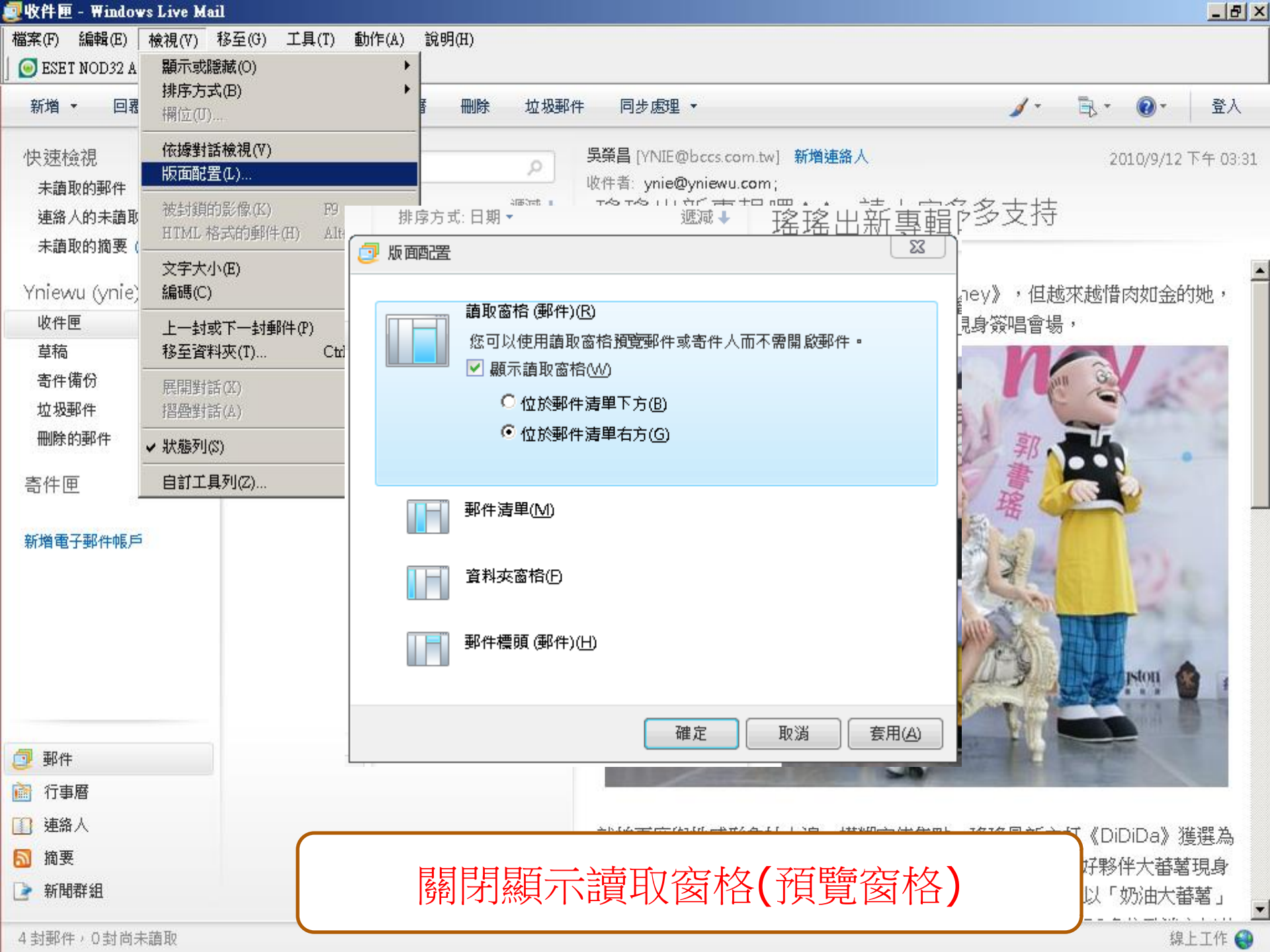
吳榮昌 [YNIE@bccs.com.tw] 新增連絡人 2010/9/12 下午 03:31

收件者: ynie@yniewu.com;

瑤瑤出新專輯囉^^~請大家多多支持

郭書瑤（瑤瑤）簽唱會帶領歌迷一同跳《honey》，但越來越惜肉如金的她，以一身包很緊的洋裝造型現身簽唱會場，

就怕再度與性感形象扯上邊，模糊宣傳焦點。瑤瑤最新主打《DiDiDa》獲選為「2011老夫子動畫電影」片尾曲，特別來賓老夫子與他的好夥伴大蕃薯現身相當搶鏡，在歌迷群中引起騷動，大蕃薯還特地穿上蓬蓬裙以「奶油大蕃薯」



關閉顯示讀取窗格(預覽窗格)

苗栗大峽谷一日遊

檔案(F) 編輯(E) 檢視(V) 工具(T) 郵件(M) 說明(H)

回覆 全部回覆 轉寄

寄件者: bjliu <bjliu@cier.edu.tw>;

日期: 2008年9月8日 下午 03:23

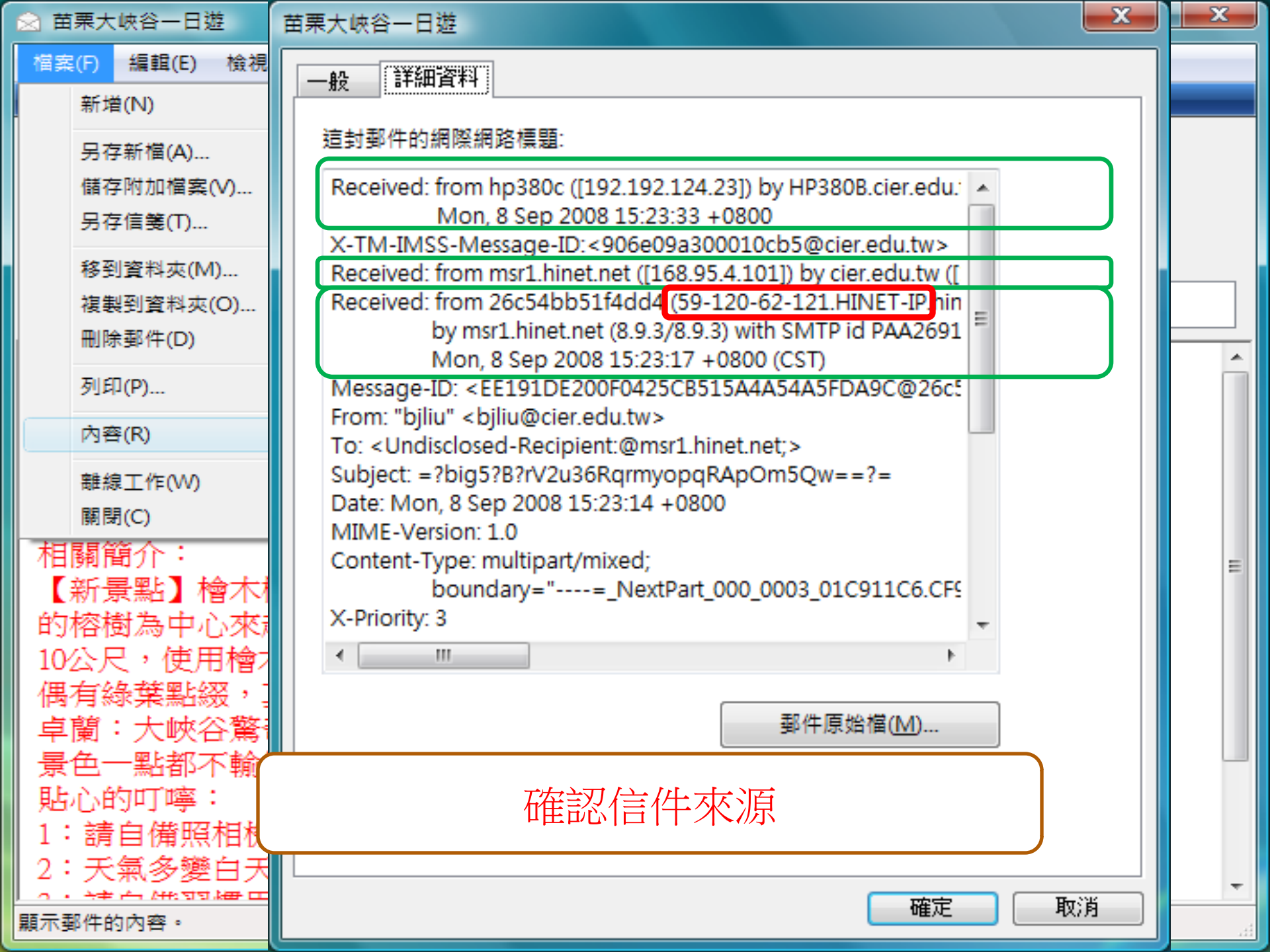
收件者: Undisclosed-Recipient:@msr1.hinet.net; <Undisclosed-Recipient:@msr1.hinet.net;>;

主旨: 苗栗大峽谷一日遊

附加檔案: 苗栗大峽谷一日遊文宣.doc (113 KB)

出發日期 ：97.9.18（星期六）。集合地點：教師會館（南海路）。
集合時間：上午7：30集合。7：45準時出發（逾時不侯）。
預計行程如下：（行程視情況增減變更）
教師會館 → 檜木樹屋 → 午餐 → 大峽谷驚奇 → 卓蘭採果 →
薑麻園休閒園區 → 晚餐 → 教師會館。
相關簡介：
【新景點】檜木樹屋～（是一棟真實的樹屋，以一棵逾200年
的榕樹為中心來起造，呈正方形，高度及邊長皆為
10公尺，使用檜木及檀香木做為建材，樹形優美，
偶有綠葉點綴，真實感覺到大樹的生命力。）
卓蘭：大峽谷驚奇之旅（長300公尺，深達10多公尺，
景色一點都不輸
貼心的叮嚀：
1：請自備照相機
2：天氣多變白天紫外線強，溫差變化大，請攜帶薄外套、帽子或陽傘墨鏡。

非必要閱讀郵件逕行刪除


苗栗大峽谷一日遊
檔案(F)
編輯(E)
檢視
新增(N)
另存新檔(A)...
儲存附加檔案(V)...
另存信箋(T)...
移到資料夾(M)...
複製到資料夾(O)...
刪除郵件(D)
列印(P)...
內容(R)
離線工作(W)
關閉(C)
相關簡介：
【新景點】檜木
的榕樹為中心來
10公尺，使用檜
偶有綠葉點綴，
卓蘭：大峽谷驚
景色一點都不輸
貼心的叮嚀：
1：請自備照相
2：天氣多變白天
顯示郵件的內容。
苗栗大峽谷一日遊
一般
詳細資料
這封郵件的網際網路標題:
Received: from hp380c ([192.192.124.23]) by HP380B.cier.edu.
Mon, 8 Sep 2008 15:23:33 +0800
X-TM-IMSS-Message-ID:<906e09a300010cb5@cier.edu.tw>
Received: from msr1.hinet.net ([168.95.4.101]) by cier.edu.tw ([
Received: from 26c54bb51f4dd4 (59-120-62-121.HINET-IP.hin
by msr1.hinet.net (8.9.3/8.9.3) with SMTP id PAA2691
Mon, 8 Sep 2008 15:23:17 +0800 (CST)
Message-ID: <EE191DE200F0425CB515A4A54A5FDA9C@26c5
From: "bjliu" <bjliu@cier.edu.tw>
To: <Undisclosed-Recipient:@msr1.hinet.net;>
Subject: =?big5?B?rV2u36RqrmyopqRApOm5Qw==?=
Date: Mon, 8 Sep 2008 15:23:14 +0800
MIME-Version: 1.0
Content-Type: multipart/mixed;
boundary="----=_NextPart_000_0003_01C911C6.CF9
X-Priority: 3
郵件原始檔(M)...
確認信件來源
確定
取消

駭客技巧光碟,請勿用於不法用途,否則後果自行負責

檔案(F) 編輯(E) 檢視(V) 工具(T) 郵件(M) 說明(H)

回覆 全部回覆 轉寄 列印 刪除 上一個 下一個 通訊錄

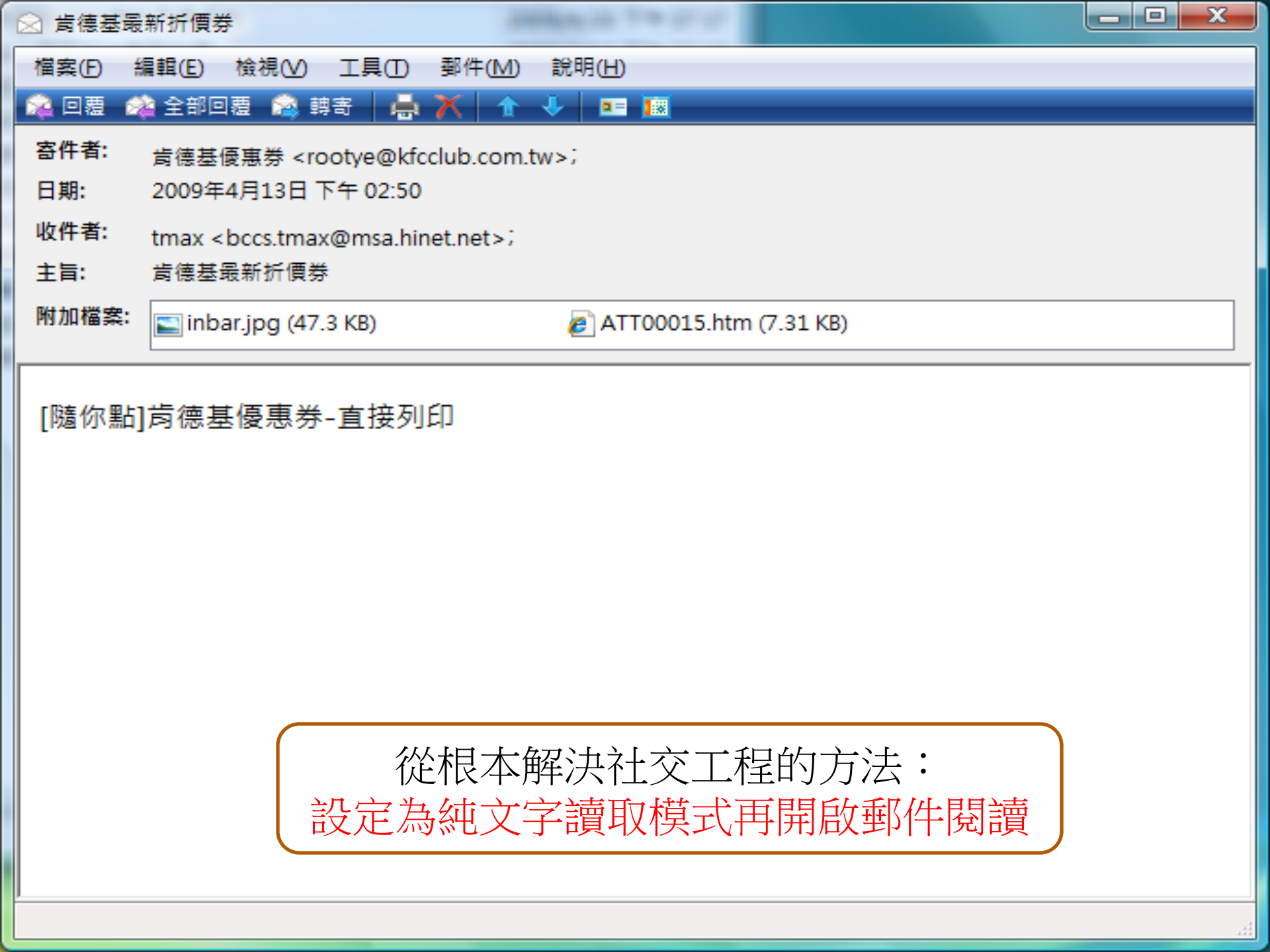
寄件者: 保護自己
日期: 2007年6月11日 上午 08:54
收件者: 無
主旨: 駭客技巧光碟,請勿用於不法用途,否則後果自行負責

避免開啟郵件內的超連結

看不圖請直接上網參觀選購

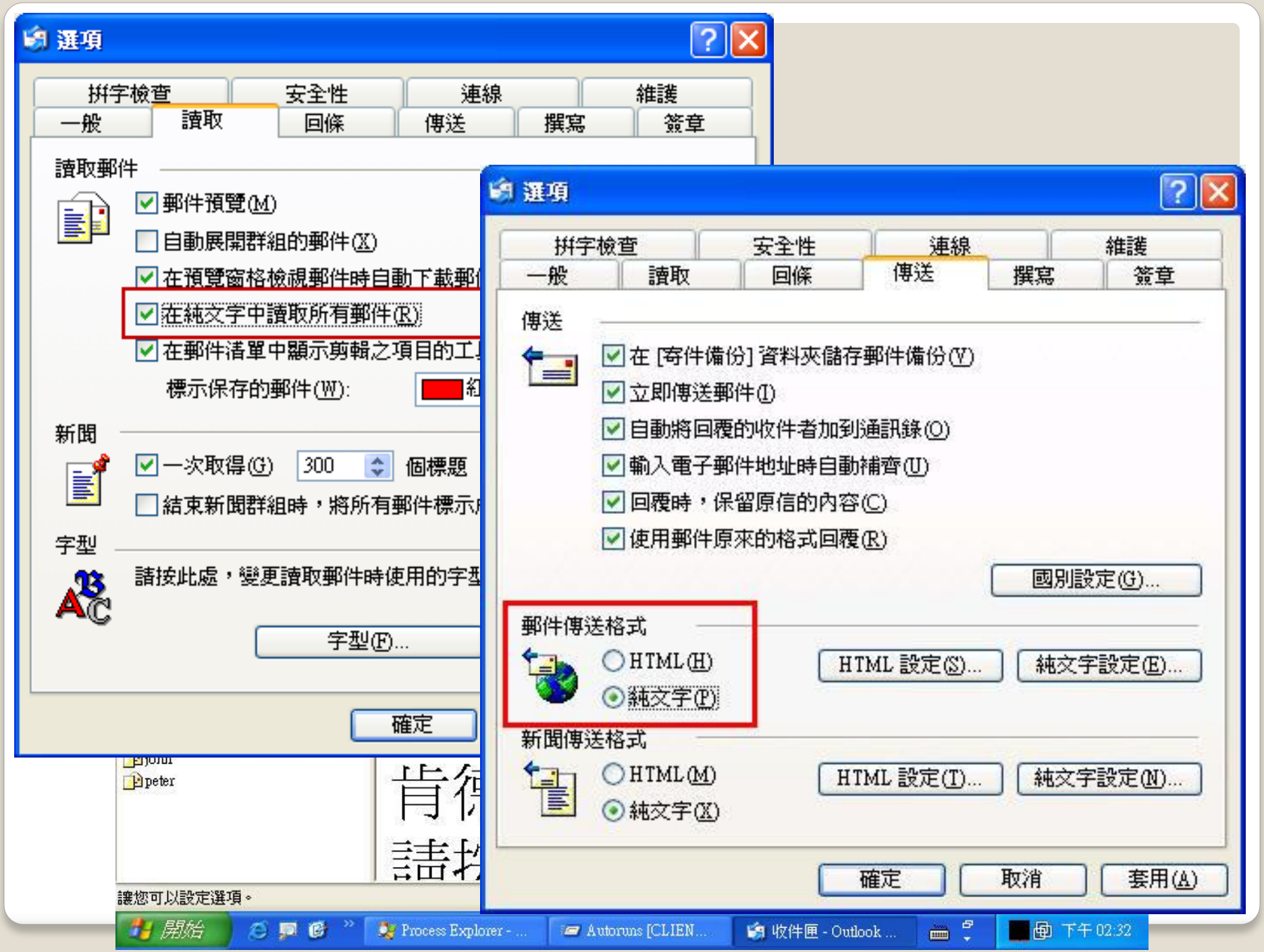
★★★保證市售最強:駭客寶典３ＣＤ★★★

駭客破解


肯德基最新折價券
檔案(F) 編輯(E) 檢視(V) 工具(T) 郵件(M) 說明(H)
回覆 全部回覆 轉寄
寄件者: 肯德基優惠券 <rootye@kfcclub.com.tw>;
日期: 2009年4月13日 下午 02:50
收件者: tmax <bccs.tmax@msa.hinet.net>;
主旨: 肯德基最新折價券
附加檔案: inbar.jpg (47.3 KB) ATT00015.htm (7.31 KB)
[隨你點]肯德基優惠券-直接列印
從根本解決社交工程的方法：
設定為純文字讀取模式再開啟郵件閱讀

傳送郵件的考量

- 可行的話將郵件傳送格式從「HTML」格式改用「純文字txt」格式。(工具→選項→讀取 及 傳送)
- 關閉「啟動時傳送及接收郵件」、「每隔幾分鐘傳送及接收郵件」的功能。
- 公務用 (xxx@mail.xyz.gov.tw) 與個人E-Mail (xxx@yahoo.com)信箱請 分開使用
- 寄件人改用「密件副本」。


選項
拼字檢查
安全性
連線
維護
一般
讀取
回條
傳送
撰寫
簽章
讀取郵件
郵件預覽(M)
自動展開群組的郵件(X)
在預覽窗格檢視郵件時自動下載郵
在純文字中讀取所有郵件(R)
在郵件清單中顯示剪輯之項目的工
標示保存的郵件(W):
新聞
一次取得(G)
300
個標題
結束新聞群組時，將所有郵件標示
字型
請按此處，變更讀取郵件時使用的字型
字型(F)...
確定
選項
拼字檢查
安全性
連線
維護
一般
讀取
回條
傳送
撰寫
簽章
傳送
在 [寄件備份] 資料夾儲存郵件備份(V)
立即傳送郵件(I)
自動將回覆的收件者加到通訊錄(O)
輸入電子郵件地址時自動補齊(U)
回覆時，保留原信的內容(C)
使用郵件原來的格式回覆(R)
國別設定(G)...
郵件傳送格式
HTML(H)
純文字(P)
HTML 設定(S)...
純文字設定(E)...
新聞傳送格式
HTML(M)
純文字(X)
HTML 設定(T)...
純文字設定(N)...
確定
取消
套用(A)
peter
讓您可以設定選項。
開始
Process Explorer - ...
Autoruns [CLIEN...
收件匣 - Outlook ...
下午 02:32

關閉「啟動時傳送及接收郵件」

使用WebMail的考量

- 登入Web mail 信箱
- 點選【設定】
- 在【讀信相關設定】下方
  - 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**


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:
只關閉 CGI
傳送讀取回條:
要求確認

郵件社交工程防護停看聽

- 信件攻擊手法
- 社交攻擊手法

駭客手法-退信攻擊

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

信件-退信攻擊

收件人不存在，退回寄件人
但..寄件人是偽造的

駭客

沒有這個人

郵件伺服器

網際網路

中華電信

使用者

駭客手法-跳板攻擊

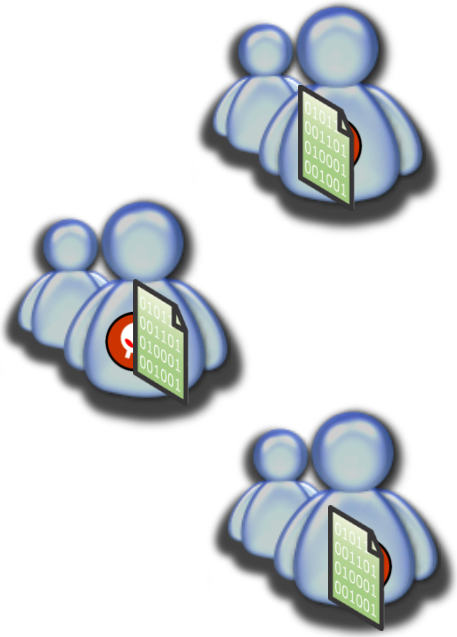
- 當您的*電腦主機本身有啟用SMTP Service* (外寄伺服器服務)，而且*沒有加以防護*時，被有心人士發現，進而不當使用您的網路頻寬及寄信功能，濫寄廣告信件，這就是您的電腦主機被當成廣告信跳板了!!
- 通常受害者不知道自己的電腦安裝了相關服務
- 常見微軟的作業系統，當有*安裝了IIS功能*，*就會一同安裝SMTP(外寄伺服器服務)*，此時若您的網路系統並未安裝防火牆，將 SMTP PORT 25 設為對外阻隔的話 ，基本*上任何人都可以藉由您的 SMTP Service 寄發信件*!! 您的電腦主機，就有可能被有心人士當成廣告信跳板，濫寄廣告信件!!

信件-跳板攻擊

轉寄信件的功能沒有關閉
可以…轉寄垃圾信

駭客

網際網路



駭客手法-密碼猜解(真)

- 要破解密碼絕非易事，被破解的人幾乎有個共同的特性
- 就是*密碼過於簡單*!!
- 只要您是以下的其中一種，就要注意了!!
  - 1.生日組合
  - 2.有意義的英文單字 (Mickey)
  - 3.身分證字號
  - 4.(公事上、私人用)電話號碼，傳真號碼
  - 5.車牌號碼
  - 6.喜好的人事物(興趣)
  - 7.重視的人(包含以上6項)
  - 8.一定要猜的123456
  - 9.鍵盤破解法

最常見也危險的密碼：123456

Awakening 台灣醒報 更新日期：2009/10/10 01:42　李柏勳

【台灣醒報特約記者李柏勳報導】網路時代來臨，動不動就要設密碼。一看，「密碼最少六個字」，隨手就打123456？小心，不只你這麼想，大家都這麼想，連駭客也這麼想！專家呼籲最好每隔90天就更換一次密碼。

日前傳出，有超過一萬筆Hotmail使用者的密碼，遭到釣魚網站竊取並且公佈在網路上。網路安全公司Acunetix的技術長波丹・凱林，在這些敏感資料被移除前，搶先取得內容並進行分析，得到的結果令人吃驚。

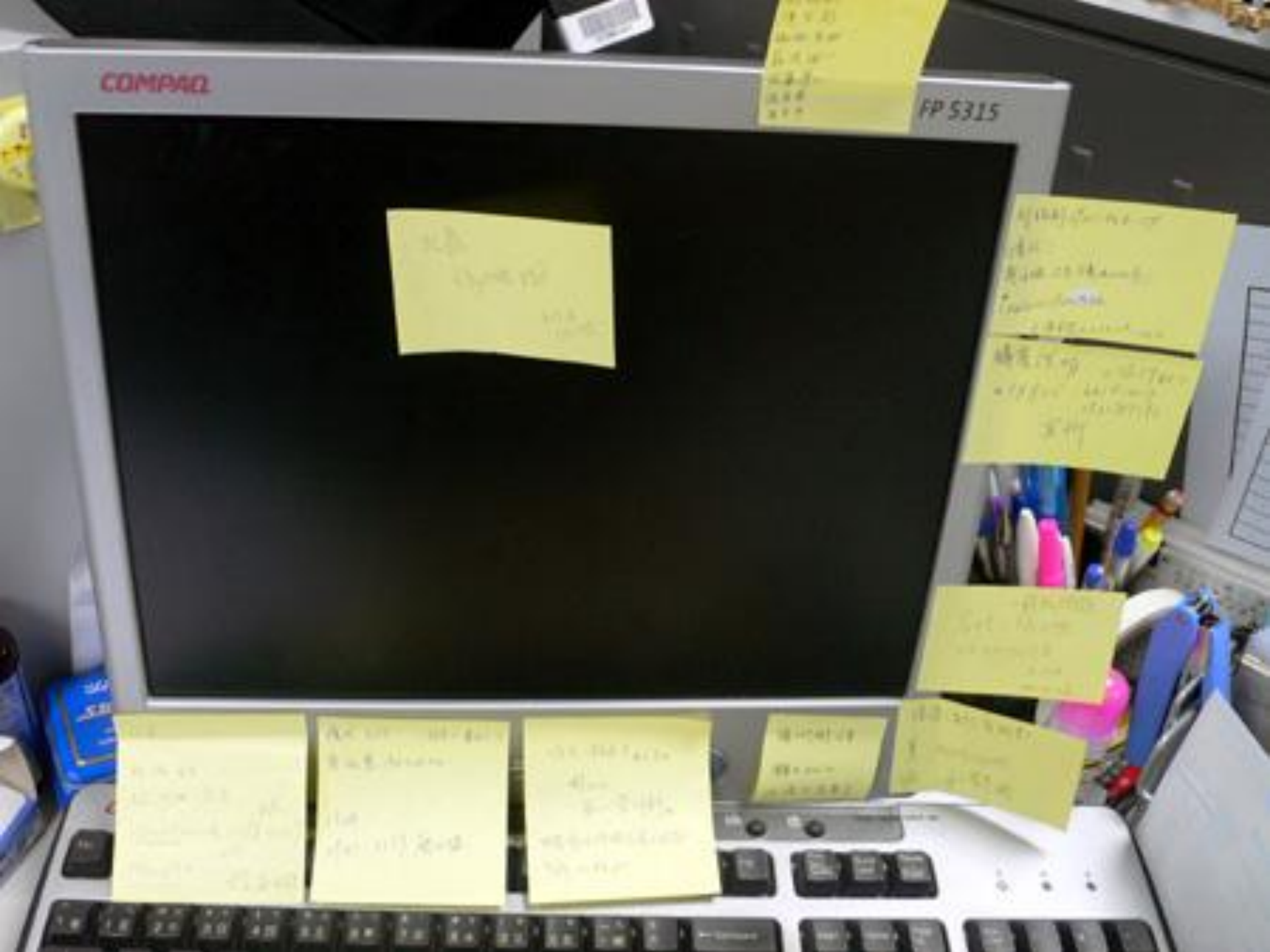
凱林發現，儘管多數網站會建議使用者，要建立具有一定長度的英數混合

章魚哥之我愛猜密碼

- site:wretch.cc password inurl:book 123456

密碼設定的相關事項

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


COMPAQ
FP 5315

密碼背不起來怎麼辦？

- 用鍵盤上　注音符號　的位置。
- J6bj/6t;

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

密碼背不起來怎麼辦？

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

- 某個自己記得起來的語彙，例如：

- Tj;6fu06au/6m,4ej;

駭客手法-偽造攻擊(重點要努力上馬)(假)

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

就是這麼超值-勁辣雞腿堡

檔案(F) 編輯(E) 檢視(V) 工具(T) 郵件(M) 說明(H)

回覆 全部回覆 轉寄

寄件者: 歡樂送兌換券 <rootye@kfcclub.com.tw>;
日期: 2009年4月13日 下午 02:50
收件者: tmax <bccs.tmax@msa.hinet.net>;
主旨: 就是這麼超值-勁辣雞腿堡

偽造攻擊

封鎖了某些圖片以協助防止寄件者辨識您的電腦，請按這裡來下載圖片。

麥當勞[歡樂送]兌換券-馬上列印

http://www.mcdonalds.com.tw/

駭客手法-偽造攻擊

Demo time

新聞影片 -mail零時差

駭客手法-偽造攻擊+附件攻擊(重點要努力上馬)

- 使用郵件社交工程放置木馬
- 只有上馬了~~幾乎全都露囉^^

(what is this ?)

(義大利....維大力...&f2i@1#)

駭客手法-偽造攻擊+附件攻擊(重點要努力上馬)

- 病毒信附件的副檔名常見使用Zip或RAR壓縮檔格式來發送
- 不管是收到認識或不認識的人寄來的信件，請使用加密處理
- 信件的內容大概都是
  - 他去哪裡玩有拍一些照片要分享給你看、他在網路上看到你被偷拍的照片，趕緊寄給你看是不是真的是你。
  - 朋友的小孩離家出走說要見網友，結果都沒有回家，隨信寄了小孩的照片請大家幫忙協尋
- 就是要騙你去開檔來看
- 檔案就是RAR檔，裡面放了一個cmd檔
- 不要好奇去打開裡面的檔案，直接刪除信件信件就好
- 一般常見會讓電腦中毒的副檔名包含：
- .bat、.exe、.com、.scr、.zip、.rar、office、pdf

发送 剪切 复制 粘贴 撤销 检查 拼写检查 附件 优先级

收件人: k1@yniewu.com

抄送:

主题: hi

Times New Roman 12 B I U A

我有好多話想對妳說，但遇到妳又說不出口，但心事都在部落格中，

如果你有時間來逛逛吧~ 部落格在這邊

駭客手法-偽造攻擊(重點要努力上馬)

Demo time

小心狡滑病毒 也會自動更新

醒報新聞網 Awakening News Networks 更新日期：2010/04/12 14:50 林永富

【台灣醒報記者林永富報導】防毒公司病毒碼需要更新，現在連病毒本身都會自行更新！防毒軟體公司賽門鐵克近日發現，一款新的木馬病毒，竟然會透過遠端伺服器下載病毒更新，一旦感染後就很難根除，呼籲電腦使用者要加強安全防護，例如使用雙向防火牆軟體，以免後患無窮。

該公司表示，發現的這款「狡滑病毒」名稱為Backdoor.Dawcun，是一個盜取電腦機密資訊的後門木馬程式，會自己在系統正常啟動或即使進入安全模式啟動時，都會自動載入。

除了蒐集系統資訊，該病毒還會把資訊加密，並植入自動執行檔將蒐集到的資訊發送到遠端伺服器，透過指定伺服器連結並測試連接狀態，若未被防毒程式擋下就可下載病毒更新，成為會自動更新病毒碼的病毒，讓防毒軟體更難查覺。

防毒專家指出，除非在一開始就將這種病毒攔截，否則很難徹底清除，因此用戶要勤於更新病毒碼及使用更強大的防護軟體。

專家也建議，最好使用具雙向防火牆功能的軟體，就算無法在一開始時攔阻，也能夠阻止不明程式竊取使用者資訊並且無法將竊取資訊傳送。

另外，目前也有全球雲端鑑識技術，利用安全智慧型網路即時抵禦最新的威脅，每隔5到15分鐘，就會更新最新病毒檔和下載最新產品更新，可有效保護電腦免受病毒攻擊。

駭客手法-郵件跟蹤

- 電子郵件加入一個圖檔，嵌在信件當中，當收件人打開郵件時，圖檔也同時被下載，這樣寄件人就可以從*圖檔被下載而得知對方已收到郵件*了。
- 加入一段超連結，收件人點選超連結看到網頁時，寄件人就可以從*網頁被下載而得知對方已收到郵件*了。
- 同樣的手法，也可以使用在Word或MSN軟體。

駭客手法-郵件跟蹤

- 若自己懶的架Mail Server..網路是很好用的東西

http://www.spypig.com

駭客手法-郵件跟蹤

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

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

more guessing: "Has he or she read my email yet?"

Sp… opens

It works with virtually all modern email programs: Outlook, Eudora, Yahoo Email, Gmail, Hotmail, AOL Email and m…

… spam, … use it as often as you like, and there's no catch. Just introduce the Pig to all your friends!

Th… e. In ju… e to use it …

To … the si… m on the right.

Enjoy!

Us…

Sp… en you re… h as that on Craigslist (for an employment, for example) and wonder if your email

填寫您自己的E-mail讓spypig可以回信給您

填寫您要寄出掛號信的主旨

選擇您要嵌入信件中的圖案(若有註冊可嵌入自己想加入的圖案)

Spypig回復您的次數

click to read this first!

step 1 **Your email address [?]:**

ynie@yniewu.com

☐ Save [?]

Enter your email address to which we will notify you by email when your message has been read. If you want to save your email address on this computer so you don't have to enter it everytime, check Save.

step 2 **Your message title [?]:**

寄送掛號信喔

Give your email message a unique title such as the recipient's name and/or your message subject (e.g. "Yo Christo Bear. Let's have lunch!") so you can later identify which email message the notification is for.

step 3 **Select your SpyPig tracking image [?]:**

or upload your own image

Select one of the SpyPig tracking images you like best. Choose the blank white image if you wish to make your tracking image "invisible" to the recipient. Or upload your own images to express your creativity.

step 4 **Number of notifications to receive [?]:**

◉ 3 ○ 5 ○ 10 ○ 20 ○ 30 ○ 100

Choose how many times you want to receive the notifications. You will receive a notification every time your email is opened up to the number you select above.

reaches its target.

以上都填完後點選這個按鈕

B

B ust use
a or rich-
text email. Visit the Requirements & Limitations page to learn more about
S

等待60秒之後將此圖案複製並貼到要寄出的信件內容中

D

S . Any
conflict with family or friends that begins with the *I-know-you've-read-my-email* speech must be resolved as humanely as possible without harming the poor Pig in any way. *Oink!*

step

Click to Activate My SpyPig [?]

Click the button above to create and activate your SpyPig tracking image in the box below.

30 seconds t
Copy and paste b

開啟連結(O)
在新索引標籤中開啟連結(W)
在新視窗開啟連結(N)
另存目標(A)...
列印目標(P)
顯示圖片(H)
另存圖片(S)...
用電子郵件傳送圖片(E)...
列印圖片(I)...
到 [我的圖片](G)
設成背景(G)
剪下(T)
複製(C)
複製捷徑(T)
貼上(P)

step 6

**Copy the SpyPig im
paste it into your e
before it is activate**

Copy the SpyPig image
(on a Windows PC), and
into your email message
use an HTML-formatted
or rich-text email.)

You must do this before
the countdown hits 0 seconds. If you do it after,
it may incorrectly think the recipient has opened your email and send you the notification email. To prevent this, simply click the button again to create and activate a new Pig.

Outlook or Firefox users, click to read this first!

step 7

Send your email as usual.
SpyPig will notify you by email when the recipient opens your email. To send another email, repeat the same steps above.

收件者: k3@yniewu.com
副本:
密副:
主旨: 寄送掛號信囉

重要性 普通 回條: 讀取時 傳送時

簽名 通訊錄 存成草稿 傳送 HTML Plain Text

寄給k3@yniewu.com
的掛號信

原始碼

樣式 格式 字體 大小

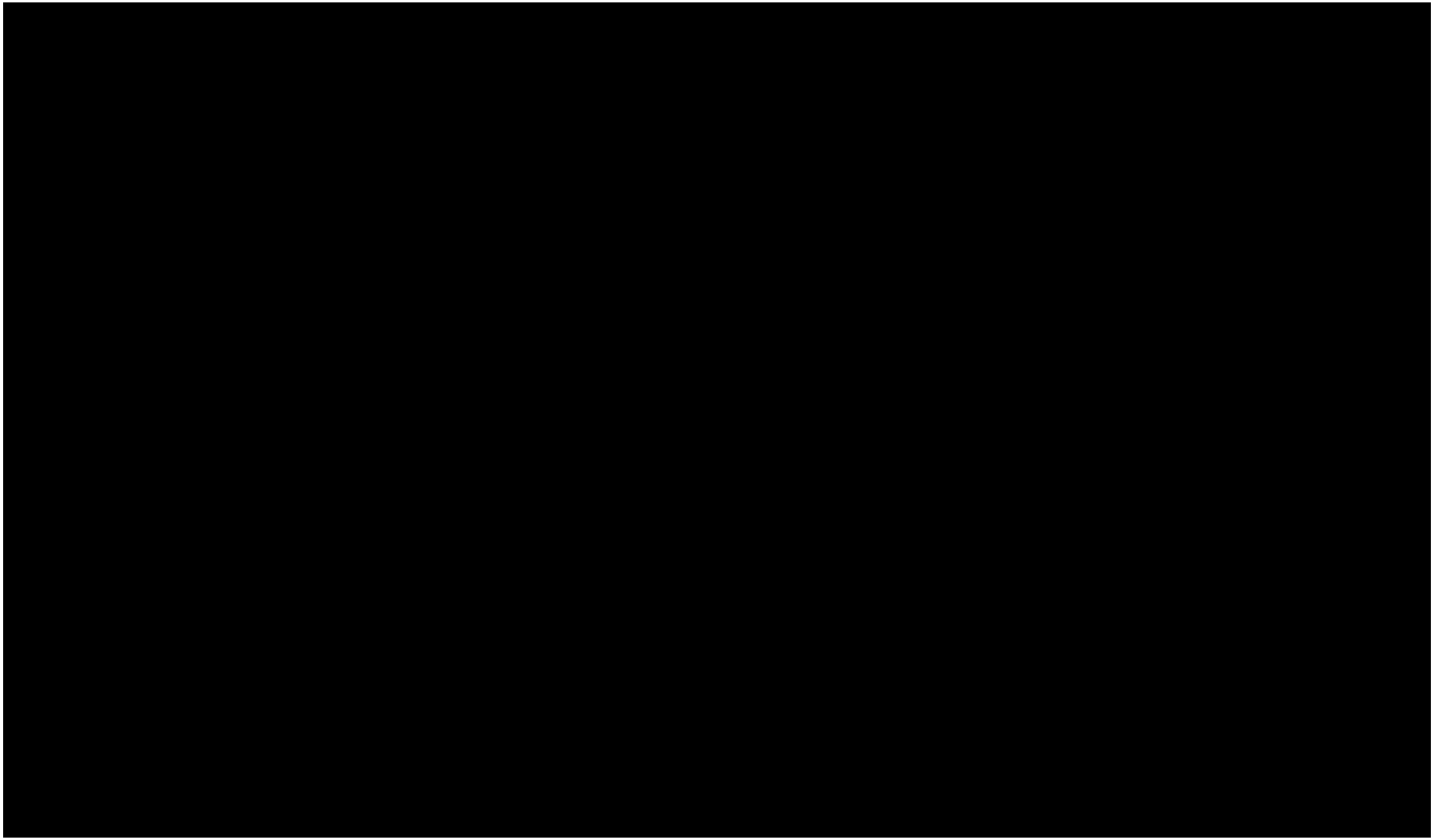
送出掛號信囉，透明的小圖片在下方

嵌在此信件的透明圖片

傳送

對方接收信件後，您會收到這封

新聞影片 -山寨奇摩網頁盜取買家密碼



駭客手法-自己不吃虧

- 特定目標
  - 發簡訊以及發mail
- 非特定目標
  - 亂槍打鳥狂發mal

- 從本月開始提供瑤瑤”幸福不遠”手機來電鈴聲，將自動從下個月手機帳單扣除15元，若不需要此服務，請至XX網站取消此服務~

中華電信

與你生活在一起
台灣大哥大

FAREASTONE
遠傳

yibo
台灣3G-威寶電信

取消手機服務功能

請輸入您的**電子信箱帳戶**的名稱與密碼，才可取消我們提供的手機簡訊服務，謝謝!!

供應商： HiNet 信箱

帳戶名稱：

密碼：

確定

駭客手法-自己不吃虧

Demo time

影分身之術(你看不到我)

影分身之術(你看不到我)

- 註冊新的網路服務
  - 論壇、電子報等等

結果是：

垃圾信都塞爆我信箱

影分身之術(你看不到我)

- 拋棄式電子信箱
  - 打帶跑~用完就丟

http://10minutemail.com

10 Minute Mail

歡迎來到十分鐘電郵

Beat spam with the best disposable e-mail service.

a3971560@bofthew.com 是您的臨時電子郵件地址。

Click here to copy this e-mail address to your clipboard

a3971560@bofthew.com

您的電子郵件地址將會在 10 分鐘後無效。
我需要更多的時間！ 給我 要多十分鐘！

您目前還有 0 封訊息。

訊息:

閱讀	由	主旨	預覽	日期

10 Minute Mail

您的電子郵件地址已經無效。

您的電子郵件地址已經無效。
取得另一個電子郵件地址

Choose Your Language:
Chinese-TW Change

Check out Jasmine Young Editing for quick affordable editing and copywriting!
Share your former glory at HowGoodIWas.com, and reconnect with friends!

影分身之術(你看不到我)

- 拋棄式電子郵件另一面
  - 隱藏發信來源(把自己隱藏起來)
    - 發送黑函
    - 發送含有惡意連結的郵件
      - 雖然沒辦法直接發信給對方(拋棄式無法主動發信，只能回信)，但只要把發送的郵件地址偽造成對方的E-mail信箱，將含有惡意超連結的內容寄到這個可拋棄的電子信箱內，然後加上回信功能，就能把信回(寄)給對方~造成隱匿自己寄信的功效。

三、防範電子郵件社交工程的方法

- 1. 注意可疑電子郵件的特徵
  - 1-1-過於聳動的主旨與緊急要求
  - 1-2-不正常的發信時間
  - 1-3-陌生人或少往來對象來信
  - 1-4-認識的人來信但主旨或內容與其習性不符
  - 1-5-要求輸入私密資料送出
- 2. 社交工程信件的防範措施
  - 2-1-關閉預覽窗格
  - 2-2-非必要閱讀郵件逕行刪除
  - 2-3-確認信件來源
  - 2-4-設定為純文字讀取模式再開啟郵件閱讀
  - 2-5-避免開啟郵件內的超連結

小心！ 假強風特報 真電腦病毒

2009-03-18 | 中國時報 | 【李宗祐／台北報導】

「中央氣象局緊急通知—強風特報」？最近幾天如果接到上述主旨的電子郵件，最好直接刪除掉，千萬不要開啟，以免電腦病毒趁機入侵！氣象局昨日發布通訊安全緊急公告，呼籲民眾提防駭客假冒該局名義發送電子郵件，散播電腦病毒。

氣象局前天發現該局網站設置的民眾意見箱（webqry@cwb.gov.tw）發送出去的電子郵件中，有四、五十封電郵被莫名退回，信件主旨都是「中央氣象局緊急通知—強風特報」。追查發現，原寄信者的ＩＰ位址並非氣象局，且該局最近未傳送電子郵件給這些收件者，懷疑有駭客假冒該局名義發送電子郵件。

氣象局資訊中心為追查冒名信件來源及駭客企圖，逐一打開被退回信件，赫然發現附件檔夾帶電腦病毒。

由於駭客冒用氣象局名義傳送電子郵件，並非針對該局電子報訂戶，而是發送垃圾郵件「散彈打鳥」，不知情民眾看到信件主旨及寄件者電子郵件帳號為代表政府單位的「.gov」，多會不疑有它、打開信件。氣象局為避免無辜民眾慘遭毒手，昨日發布資通安全緊急公告。

過於聳動的主旨與緊急要求

相關新聞

(91 封未讀取的信件。) Yahoo!奇摩電子信箱 2.0, jiangjiunnjye - Windows Internet Explorer

http://tw.mg30.mail.yahoo.com/dc/launch?.gx=0&.rand=64vkkaa6pjia

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

(91 封未讀取的信件。) Yahoo!奇摩電子信箱 2.0,...

網頁(P) 工具(O)

YAHOO!奇摩 電子信箱 2.0

jiangjiunnjye，您好！ 顯示離線

會員登出, 帳號資料, 切換版本

Yahoo!奇摩 | 即時通 | 新聞

搜尋網站... 搜尋

檢查新信 編寫新信

搜尋信件... 搜尋

超人氣開店計畫

- **收件匣** (91)
- 草稿匣
- 寄件備份匣
- 垃圾信件匣 (8) 清空
- 垃圾筒 清空
- 通訊錄 新增
- 行事曆
- 記事本
- 我的信件匣 新增
  - 備份文件

電子信箱首頁 | 垃圾信件匣 8 封信件

手機收信 | 偏好設定 | 服務說明

刪除 | 回覆 | 轉寄 | 這不是垃圾信 | 搬移 | 列印 | 更多選項 | 檢視

	寄件者	主旨	收到日期
	fhjsfbssh巨匠電腦u	[立即了解]告別上班族，自己	2038/1/19(二) 上午11:14
	■社團法人免費服務■	<免費索取最新公職職缺>一	2038/1/19(二) 上午11:14
	漢華國際中文學院	大陸國家護照，普通話水平測	2009/5/8(五) 上午3:34
	麻豆最愛髮型穎	單調的馬尾，讓你想要有所變	2009/4/22(三) 上午11:35
	徵求店家 8aGm	您好,本公司專門進口鹽漬海	2009/4/21(二) 下午7:23
	純銀飾品代製 IGs3P	GOGO88精品批發★精品銀	2009/4/21(二) 下午7:10
	年輕人開店專案 xhO	年輕人免加盟金開店專案起跑	2009/4/21(二) 下午6:51
	Jess Oakley via Ya	Jess Oakley 邀請你建立聯	2009/4/21(二) 下午6:31

不正常的發信時間

今天 4/21 無新增事件。請點選「+」符號新增。

網際網路 | 受保護模式: 啟動 100%

Thinking about you - 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: Alexia [shagarageequ@blackjackforyou.com]

收件者: Hye

副本:

主旨: Thinking about you

寄件日期: 2007/3/27 (星

陌生人或少往來對象來信

寄件人不認識

As well clockville - 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: Camarvon3 boggstown [camarvon3@cluemail.com] 寄件日期:

收件者: jiunn.jye

副本:

主旨: As well clockville

陌生人或少往來對象來信

大部分是英文

these rainless regions all is necessarily silence, desolation, and rears its icy summits to chill and precipitate the vapors again, a death, Egypt fell to one of his generals, cruelty, corruption, and vice which reigned in every branch of the royal

[EXVG] History For Extraordinary Vacations Group inc

Symbol OTC: EXVG.PK
Current Price: $0.10
5 Day Expected: $0.5
Recommendation: Very aggressive buy!!

Before we continue, there is a huge PR campaign under way for EXVG so get in before the move and this price is history

Get in NOW! Watch it like a hawk and get in before the rush!

centers in all those seas. Greek and Roman travelers found now a rain. The water which is taken up by the atmosphere from th beasts, noxious reptiles, and huge and ferocious birds these ends. He invited Greek scholars, philosophers, poets, and artists, generally vicious.--Degradation and vice.--Employment a cure for be very effectually undeceived by reading attentively a full and reflecting, as he reads, that the narrative

can do us no possible harm in the future progress of the war, while to Ptolemies.--Incestuous marriages of the Ptolemy family.--

台視新聞

TTV》新聞》

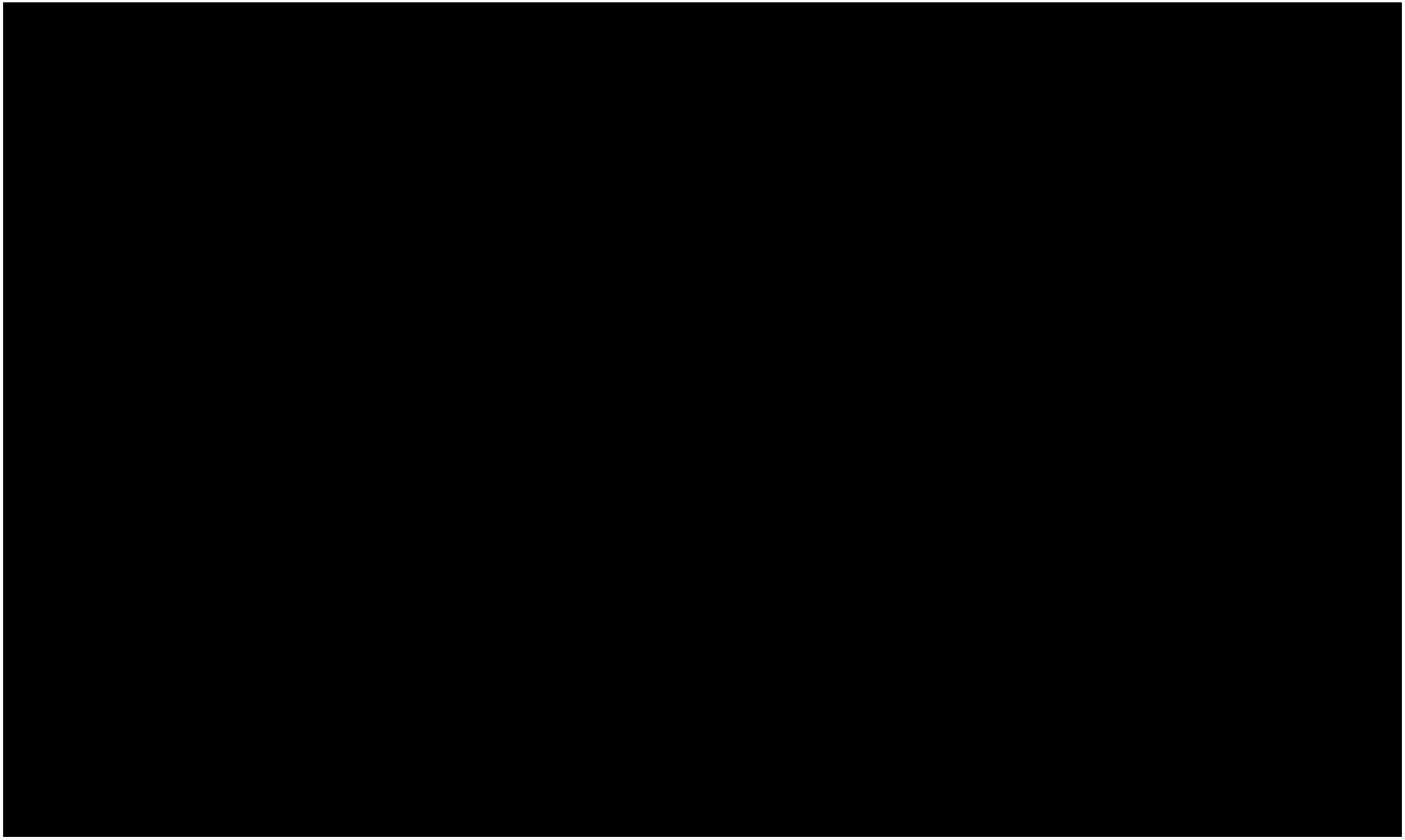
網路劫標客 相仿帳號發信騙錢
數字1小寫L 肉眼難辨成漏洞

報導記者：郭于中 941206

網路拍賣詐騙手法又翻新，一位民眾在網路上向取名flora的賣家購買手機，沒想到，收到的得標信，卻是署名f一ora，由於一跟英文字母小寫的L，實在太過相近，被害人沒發現，就把錢給轉出去，對於類似的詐騙手法，連網路拍賣業者都說還沒聽說過。

網路上琳瑯滿目的拍賣

新聞影片 -在超連結網址動手腳



假冒中華電信 更改帳單騙個資　官網認証方式 無需身分証號碼

2007/11/09 報導記者：陳程振

《更多圖片》

最近不少民眾接到中華電信更改電信帳單的通知，要求確認民眾的身分証號碼，甚至要求更多的隱私資料，但是這可能是詐騙集團的新陷阱.刑事局就表示詐騙集團假冒各種機構騙取民眾資料的情形愈來愈多，民眾得謹慎查証才能避免受騙.

接到電話或者電子郵件主動通知要幫您更改電子帳單可別開心得太早，因爲這可能是詐騙集團設下的陷阱.一位民眾就收到自稱中華電信的電子郵件，要他輸入身分証號碼更改電子帳單，這份電子郵件完全是一場騙局.詳細看一看分辨的方法，認証方法相當多，而且完全不需要身分証號碼，但是詐騙集團的網頁

要求輸入私密資料送出

會員通知手法分析

要求輸入私密資料送出

帳號密碼

遊戲橘子

詐騙者

更改密碼
通知

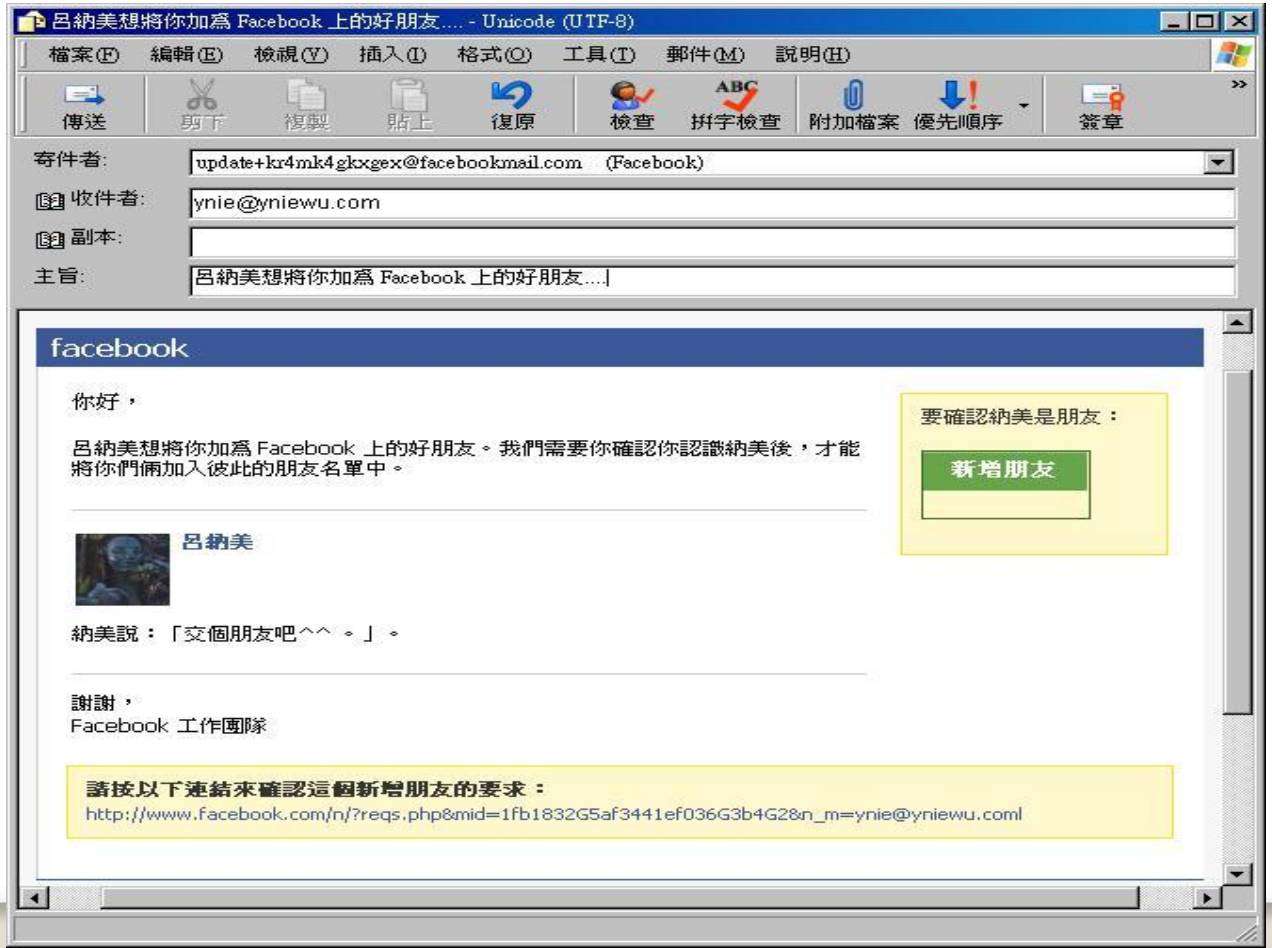
加入會員

小朋友

遊戲檸檬

釣魚社交工程

- 寄出釣魚信件，來吧~你的帳號密碼



釣魚社交工程解

- 收信看看~

釣魚社交工程


登入 | Facebook - Windows Internet Explorer
http://www.facebook.com/login.php
Live Search
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
登入 | Facebook
網頁(P) 工具(O)
facebook
免費註冊
Facebook，讓你和親朋好友保持聯繫，隨時分享生活中的每一刻。
登入 Facebook
電子郵件：
ynie@yniewu.com
密碼：
記住我
將 Facebook 設定為我的首頁
登入
或申請加入 Facebook
忘記密碼？
網際網路
100%

釣魚社交工程解

哈哈~
騙到了

釣魚社交工程

可惡！~如何防禦？~~

防禦陣線：防範社交工程策略

- 收信看看~

避免從E-Mail中點選超連結

防禦陣線：防範社交工程策略

- 我的最愛是個很有用的東西

討厭郵件釣魚

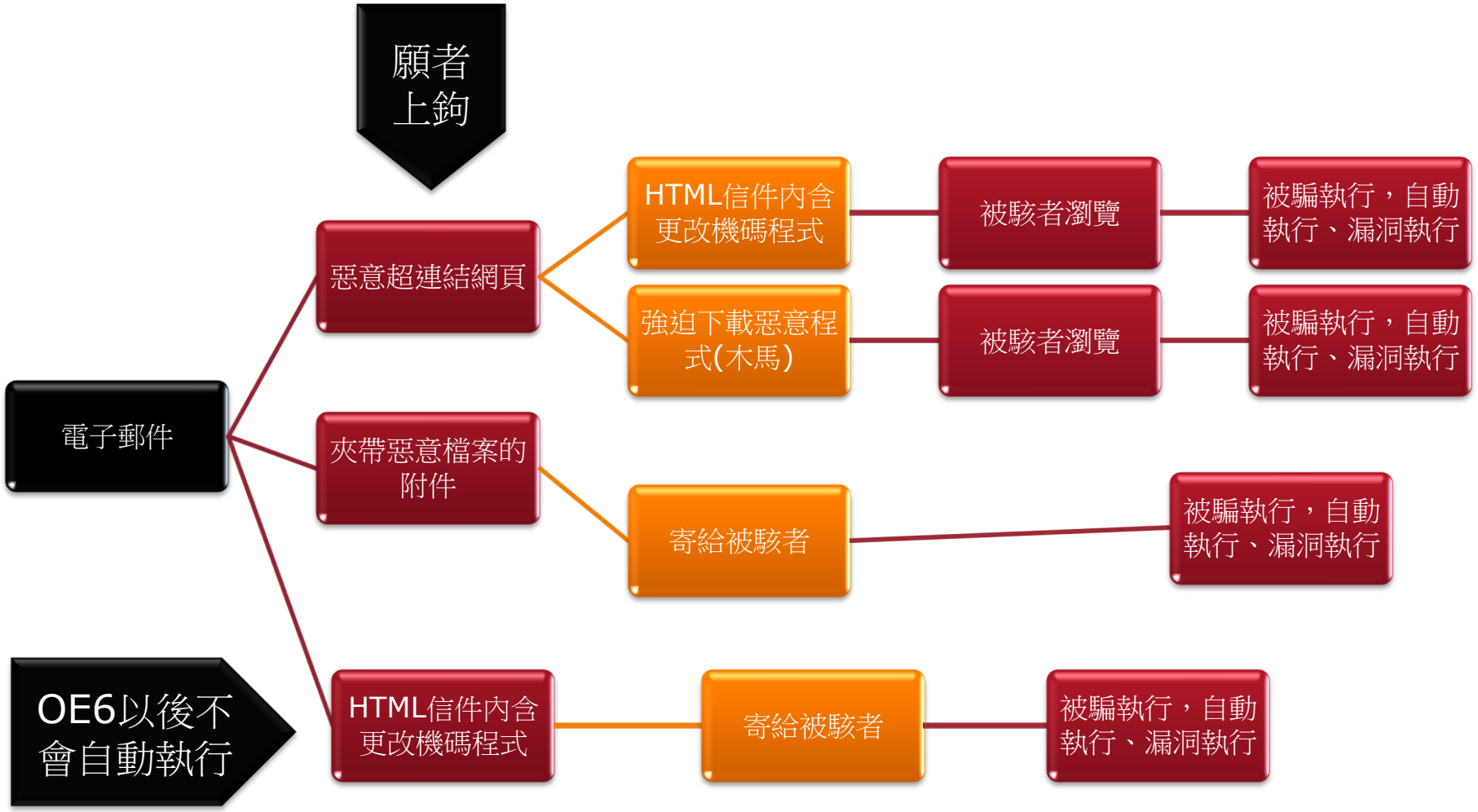
若從郵件下載的附件檔案後

不要立即執行

你的防毒軟體沒有反應不代表

沒問題

討厭郵件釣魚


願者上鉤
電子郵件
惡意超連結網頁
HTML信件內含更改機碼程式
被駭者瀏覽
被騙執行，自動執行、漏洞執行
強迫下載惡意程式(木馬)
被駭者瀏覽
被騙執行，自動執行、漏洞執行
夾帶惡意檔案的附件
寄給被駭者
被騙執行，自動執行、漏洞執行
OE6以後不會自動執行
HTML信件內含更改機碼程式
寄給被駭者
被騙執行，自動執行、漏洞執行

郵件追蹤之術

郵件追蹤之術

追蹤信件從哪裡發出來

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

郵件追蹤之術

- 將信件標頭全部複製下來

網際網路標題(H):

```
X-MS-Has-Attach: yes
X-MS-Exchange-Organization-SCL: -1
X-MS-TNEF-Correlator: <C8789BED.7DB%
jackhwa@bccs.com.tw>
user-agent: Microsoft-Entourage/13.5.0.100510
MIME-Version: 1.0
X-Auto-Response-Suppress: DR, OOF, AutoReply
```

郵件追蹤之術-郵件標頭在哪裡？

- **網頁郵件**
  - Gmail：
    - 登入您的 Gmail 帳戶。
    - 開啟您要檢視標題的郵件。
    - 在郵件窗格的右上方，按一下 **[回覆]** 旁的向下箭頭。
    - 選取 **[顯示原始檔]**。
  - AOL 服務：
    - 登入您的 AOL 帳戶。
    - 開啟您要查看標頭的郵件。
    - 在 [Action] (動作) 選單中選取 [View Message Source] (檢視原始郵件)。
    - 系統會在新視窗中顯示完整的標頭。

郵件追蹤之術-郵件標頭在哪裡？

- Hotmail 使用者：
  - 登入您的 Hotmail 帳戶。
  - 從左側的選單中選取 [收件匣]。
  - 在您想查看標頭的郵件上按一下滑鼠右鍵，然後選取 [檢視郵件來源]。
- Microsoft Internet Mail：
  - 登入您的 Microsoft Internet Mail 帳戶。
  - 開啟您要檢視標題的郵件。
  - 按一下 **[檔案]** 功能表，然後選取 **[內容]**。
  - 選取 **[詳細資料]** 標籤，以顯示完整的標題。

郵件追蹤之術-郵件標頭在哪裡？

- Yahoo!奇摩電子信箱使用者：
  - 登入您的 Yahoo!奇摩電子信箱帳號。
  - 選取您要查看標頭的郵件。
  - 按一下 [更多選項] 下拉式選單，然後選取 [檢視完整標題]。
- Netscape Webmail：
  - 登入您的 Netscape 網頁郵件帳戶。
  - 開啟您要檢視標題的郵件。
  - 按一下灰色標題區段中的黃色的三角形 (在右邊，[**Next >**] (下一個 >) 的下面)。
- Excite 服務：
  - 登入您的 Excite 帳戶。
  - 開啟您要查看標頭的郵件。
  - 按一下「From:」(寄件者：) 行中的 [View Full Headers] (檢視完整標頭) 圖示。

郵件追蹤之術-郵件標頭在哪裡？

- **電子郵件用戶端**
  - Outlook 2007：
    - 開啟 Outlook。
    - 開啟郵件。
    - 在 **[郵件]** 標籤上，於 **[選項]** 群組中，按一下 **[對話方塊啟動器]** 圖示圖片。
    - 在 **[郵件選項]** 對話方塊中，標題會出現在 **[網際網路標題]** 方塊上。
  - 舊版的 Outlook：
    - 開啟 Outlook。
    - 開啟您要檢視標題的郵件。
    - 按一下 **[檢視]** 功能表，然後選取 **[選項...]**。

郵件追蹤之術-郵件標頭在哪裡？

- Outlook Express：
  - 開啟 Outlook Express。
  - 從您的收件匣，找到您要檢視標題的郵件。
  - 在該郵件上按一下滑鼠右鍵，並選取 [**內容**]。
  - 開啟對話方塊中的 **[詳細資料]** 標籤。
- Opera：
  - 開啟 Opera。
  - 按一下您要檢視標題的郵件，這樣它會顯示在您收件匣下面的視窗。
  - 按一下 **[To]** (收件者) 欄位另一端的 **[Display all headers]** (顯示完整的標題)。

- 參考 http://mail.google.com/support/bin/answer.py?hl=b5&answer=22454

郵件追蹤之術-信件從哪裡來

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

Headers:

```
Received: from mail.bccs.com.tw ([192.168.1.11]) by mail.bccs.com.tw
 ([192.168.1.11]) with mapi; Fri, 30 Jul 2010 15:06:17 +0800
Content-Type: application/ms-tnef; name="winmail.dat"
Content-Transfer-Encoding: binary
From: =?big5?B?quGrVLPH?= <jackhwa@bccs.com.tw>
To: =?big5?B?un6p/aX+pL2lcatIvWM=?= <bccs@bccs.com.tw>
Date: Fri, 30 Jul 2010 15:10:36 +0800
Subject: =?big5?B?W7ZnpK2lUqVSuXFdICCnQavnu/K7objcoUGoTal3pOGsT73
Thread-Topic: =?big5?B?W7ZnpK2lUqVSuXFdICCnQavnu/K7objcoUGoTal3pOGsT73W?=
Thread-Index: Acsvtk6iGWfKdMTBmEqOGpYPQpjP5Q==
Message-ID: <C8789BED.7DB%jackhwa@bccs.com.tw>
Accept-Language: zh-TW
Content-Language: en-US
X-MS-Has-Attach: yes
X-MS-Exchange-Organization-SCL: -1
X-MS-TNEF-Correlator: <C8789BED.7DB%jackhwa@bccs.com.tw>
user-agent: Microsoft-Entourage/13.5.0.100510
MIME-Version: 1.0
X-Auto-Response-Suppress: DR, OOF, AutoReply
X-EsetId: DE64072F5B5D7069C162077B550930
```

Get Source

貼上

Get Source

郵件追蹤之術-信件從哪裡來

Source:

The source host name is "web74112.mail.tp2.yahoo.com" and the source IP address is [redacted]4.12.84.

Geo-Location Information

Country	Taiwan
State/Region	03
City	Taipei
Latitude	25.0392
Longitude	121.525
Area Code	

Demo

郵件追蹤之術

別忘了要誰要更新

別忘了要誰要更新

作業系統

Office

應用程式

防毒軟體

好用的進階版工作管理員

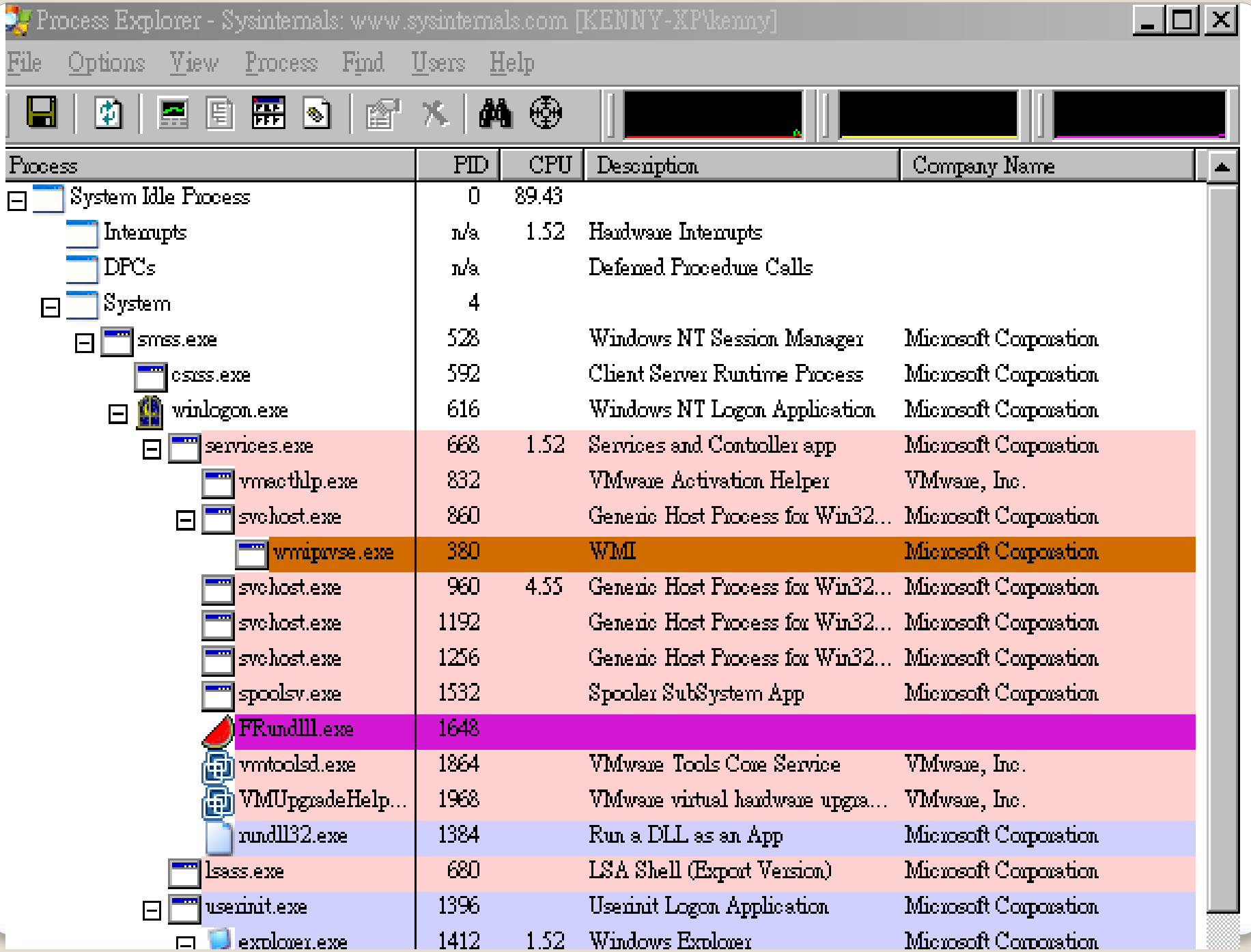
好用的進階版工作管理員

- 下載 Process explorer(進階版工作管理員)
  - http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx

- 找**紫色**的怪東東~~

Process explorer

- 黃色：代表此程式是一個 .NET 的應用程式。例如說我用 Process Explorer 就發現原來 Yahoo!奇摩輸入法就有支程式是用 .NET 寫成的。
- 紫色：代表此程式是一個 Pack (包裝) 過的程式，也就是說這個程式本身又被包了一層程式，意思也就是說該程式是被「修改過」的程式，並非為原本的程式喔！通常這種程式有兩種可能：
  - 中毒的程式：病毒讓你的程式還是可以正常運作，讓你覺得程式沒問題，但是私底下可能「多做了一些事」讓你沒感覺。
  - 壓縮過程式：知名的 UPX (the Ultimate Packer for eXecutables) 工具程式就是專門用來將你製作出來的執行檔壓縮過，讓你的執行檔變小又能正常執行的工具。
- 粉紅色：此程式為一個 Windows 服務。


Process Explorer - Sysinternals: www.sysinternals.com [KENNY-XP\kenny]
File Options View Process Find Users Help
Process PID CPU Description Company Name
System Idle Process 0 89.43
Interrupts n/a 1.52 Hardware Interrupts
DPCs n/a Deferred Procedure Calls
System 4
smss.exe 528 Windows NT Session Manager Microsoft Corporation
csrss.exe 592 Client Server Runtime Process Microsoft Corporation
winlogon.exe 616 Windows NT Logon Application Microsoft Corporation
services.exe 668 1.52 Services and Controller app Microsoft Corporation
vmacthlp.exe 832 VMware Activation Helper VMware, Inc.
svchost.exe 860 Generic Host Process for Win32... Microsoft Corporation
wmiprvse.exe 380 WMI Microsoft Corporation
svchost.exe 960 4.55 Generic Host Process for Win32... Microsoft Corporation
svchost.exe 1192 Generic Host Process for Win32... Microsoft Corporation
svchost.exe 1256 Generic Host Process for Win32... Microsoft Corporation
spoolsv.exe 1532 Spooler SubSystem App Microsoft Corporation
FRundll1.exe 1648
vmtoolsd.exe 1864 VMware Tools Core Service VMware, Inc.
VMUpgradeHelp... 1968 VMware virtual hardware upgra... VMware, Inc.
rundll32.exe 1384 Run a DLL as an App Microsoft Corporation
lsass.exe 680 LSA Shell (Export Version) Microsoft Corporation
userinit.exe 1396 Userinit Logon Application Microsoft Corporation
explorer.exe 1412 1.52 Windows Explorer Microsoft Corporation

免費的社交工程.....

防護軟體

完全免費喔!

免費的網路釣魚防護軟體(家用中文)

- McAfee-網路釣魚軟體
  - www.siteadvisor.com
- 趨勢科技-網路釣魚防護軟體
  - http://www.trendmicro.com.tw/
  - http://www.trendmicro.com.tw/wtp/micro/index.asp

使用者該怎麼做?

McAfee SiteAdvisor - 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://www.siteadvisor.com/download/windows.html 移至 連結

McAfee SECURE

McAfee® | McAfee SiteAdvisor®

支援 關於 McAfee 連絡我們 Taiwan - Chinese)

www.siteadvisor.com

首頁 網站瀏覽安全 如何工作 下載 資源 網站管理員

首頁 / 下載

SiteAdvisor 軟體

安心點選

這項屢獲獎項且免費的保護透過直覺式的圖示，可在您點選有風險之網站前提供安全性與網路釣魚建議。

下載 SiteAdvisor 軟體

SiteAdvisor Plus

保護您珍貴的資產

使用所有 SiteAdvisor 軟體的功能加上即時訊息與電子郵件的「連結檢查」及「保護模式」，可獲得最大、即時、全面的保護，使您遠離危險網站和危害個人身份與個人電腦的網路釣魚攻擊。

購買 SiteAdvisor Plus

系統需求

- Windo
- IE 6 與
- Firefo

要使用 M Firefox 取

請按一下

安裝完畢

網際網路

Yahoo!奇摩 - 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.yahoo.com/ 移至 連結

McAfee SiteAdvisor

設為首頁 網路意見大調查 前3個月房貸優惠利率1.69%起 4月21日星期二 台北

YAHOO! 奇摩

網頁 知識+ 圖片 影片 部落格 商家 字典 商品 綜合

網頁搜尋

熱門：金牛座 優惠券 新遊戲 運勢 暢貨中心 樂透 風之畫師 解夢 彎彎 鞋帶新綁法！ 搜尋板

My» 消費 拍賣 超級商城 購物中心 ATM 社群 部落格 家族 交友

焦點新聞 運動 娛樂 國際 新奇

你家被查封了？新騙術換台詞
「你們家的房子被查封了！」這是詐...

賣藥反攻大陸！地下電台超扯
犯太歲運氣不順，請老師作法喊一喊...

快訊 30歲才學英文二個月變精通

熱門 頭髮天天洗容易禿頭？

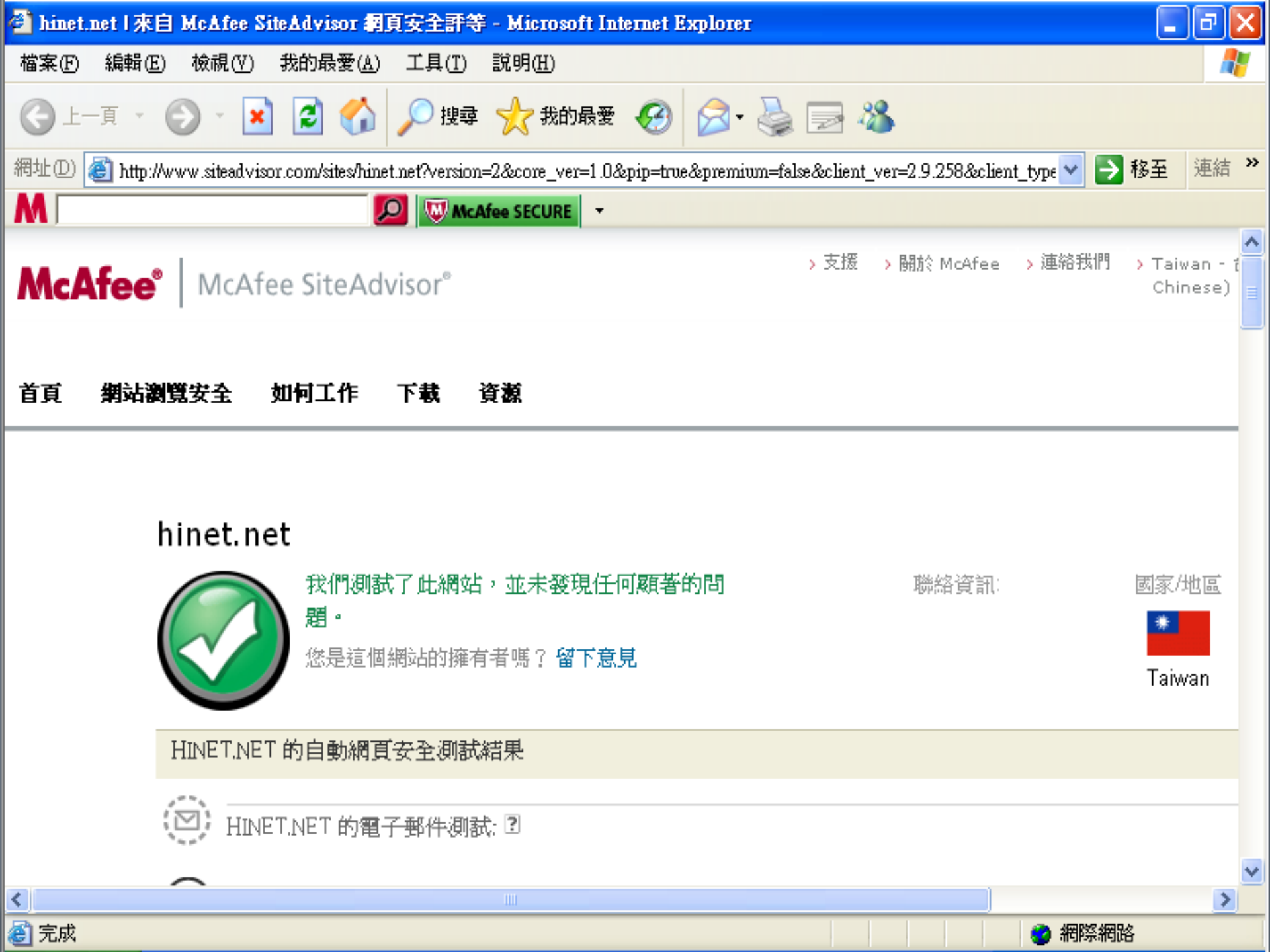
Yahoo! 奇摩會員 登入 | 註冊

信箱 知識+

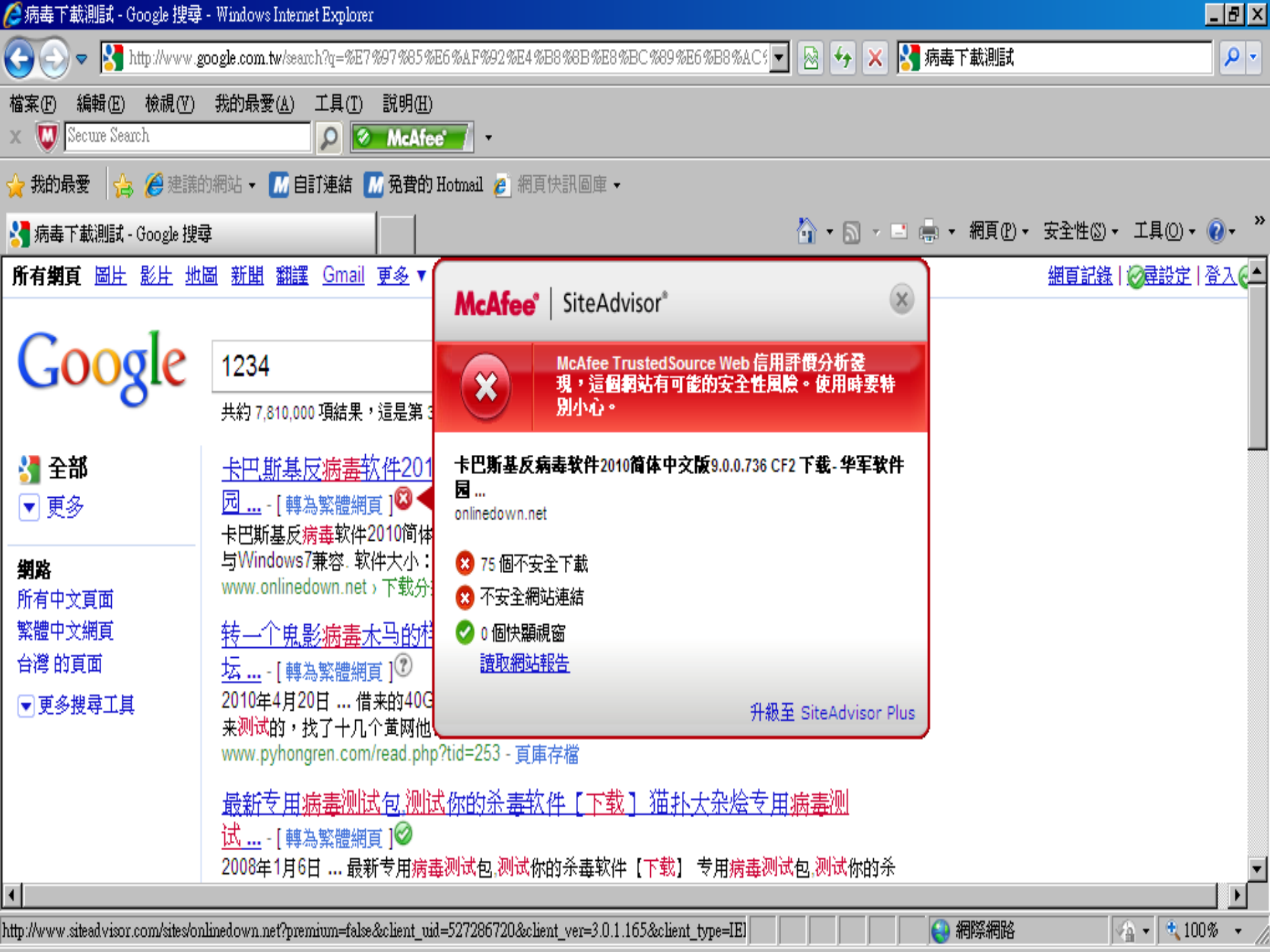
Yahoo! 奇摩購物中心 指定館別36期/全站24期0利率 中信,台新,國泰世華,新光銀行

Yahoo!奇摩超級商城

網際網路


hinet.net | 來自 McAfee SiteAdvisor 網頁安全評等 - 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://www.siteadvisor.com/sites/hinet.net?version=2&core_ver=1.0&pip=true&premium=false&client_ver=2.9.258&client_type
移至
連結
McAfee SECURE
McAfee
McAfee SiteAdvisor
支援
關於 McAfee
連絡我們
Taiwan - Chinese)
首頁
網站瀏覽安全
如何工作
下載
資源
hinet.net
我們測試了此網站，並未發現任何顯著的問題。
您是這個網站的擁有者嗎？ 留下意見
聯絡資訊:
國家/地區
Taiwan
HINET.NET 的自動網頁安全測試結果
HINET.NET 的電子郵件測試:
完成
網際網路


bank site:tw - Google 搜尋 - 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://www.google.com.tw/search?hl=zh-TW&q=bank+site%3Atw&btnG=%E6%90%9C%E5%B0%8B&meta=&aq=f&oq=
移至 連結
McAfee SiteAdvisor
所有網頁 圖片 地圖 新聞 網誌搜尋 Gmail 更多▼ 登入
Google
bank site:tw
搜尋 進階搜尋 | 使用偏好
所有網頁 中文網頁 繁體中文網頁 台灣的網頁
所有網頁 約有1,500,000項符合bank site:tw的查詢結果，以下是第 1-10項。 需時 0.16 秒。
提示： 若要節省時間請按返回鍵來代替「搜尋」。
兆豐國際商業銀行
若您無法看到Flash、PDF 或是匯利率看板，建議您下載Flash Player、Adobe Reader & JAVA
軟體. COPYRIGHT © 2009 Mega International Commercial Bank. ...
https://www.megabank.com.tw/ - 29k - 頁庫存檔 - 類似網頁
歡迎光臨國泰世華銀行
提供個人金融、企業金融服務、信用卡、理財及信託服務。
www.cathaybk.com.tw/ - 55k - 頁庫存檔 - 類似網頁
中國信託商業銀行
提供信用卡、個人金融、基金理財、網路銀行、存款貸款、匯率等服務。
www.chinatrust.com.tw/ - 7k - 頁庫存檔 - 類似網頁
網際網路


病毒下載測試 - Google 搜尋 - Windows Internet Explorer
http://www.google.com.tw/search?q=%E7%97%85%E6%AF%92%E4%B8%8B%E8%BC%89%E6%B8%AC%
病毒下載測試
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
Secure Search
McAfee
我的最愛
建議的網站
自訂連結
免費的 Hotmail
網頁快訊圖庫
病毒下載測試 - Google 搜尋
網頁(P)
安全性(S)
工具(O)
所有網頁 圖片 影片 地圖 新聞 翻譯 Gmail 更多
網頁記錄
登入
Google
1234
共約 7,810,000 項結果，這是第
全部
更多
網路
所有中文頁面
繁體中文網頁
台灣 的頁面
更多搜尋工具
卡巴斯基反病毒软件201
园 ... - [轉為繁體網頁]
卡巴斯基反病毒软件2010简体
与Windows7兼容. 软件大小：
www.onlinedown.net › 下载分
转一个鬼影病毒木马的
坛 ... - [轉為繁體網頁]
2010年4月20日 ... 借来的40G
来测试的，找了十几个黄网他
www.pyhongren.com/read.php?tid=253 - 頁庫存檔
最新专用病毒测试包,测试你的杀毒软件【下载】猫扑大杂烩专用病毒测
试 ... - [轉為繁體網頁]
2008年1月6日 ... 最新专用病毒测试包,测试你的杀毒软件【下载】 专用病毒测试包,测试你的杀
McAfee | SiteAdvisor
McAfee TrustedSource Web 信用評價分析發現，這個網站有可能的安全性風險。使用時要特別小心。
卡巴斯基反病毒软件2010简体中文版9.0.0.736 CF2 下载 - 华军软件园 ...
onlinedown.net
75 個不安全下載
不安全網站連結
0 個快顯視窗
讀取網站報告
升級至 SiteAdvisor Plus
http://www.siteadvisor.com/sites/onlinedown.net?premium=false&client_uid=527286720&client_ver=3.0.1.165&client_type=IE
網際網路
100%


趨勢科技WTP - Windows Internet Explorer
http://www.trendmicro.com.tw/wtp/micro/index.asp
Google
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
趨勢科技WTP
網頁(P) 工具(O)
TREND MICRO 趨勢科技
病毒碼更新再快 也快不過4秒一隻的新病毒
Trend Micro WTP Add-On
TREND MICRO WTP Add-On
WTP Add-On 偵測到
動。
重新整理
時間
2008/8/25 14:22:34
2008/8/25 14:22:34
2008/8/25 14:22:34
2008/8/25 14:21:32
2008/8/25 14:21:31
2008/8/25 14:21:29
意見
記錄
Trend Micro Web Protection Add-On (WTP Add-On) - 網友十大必備免費上網防護工具！有效且主動防護您的電腦免受網頁威脅或遭到僵屍病毒的攻擊，並能偵測秘密控制您的電腦以從事網路犯罪的可疑行為。
您的電腦是安全的！
您的電腦沒有已知的網頁威脅與僵屍病毒。
全球網頁威脅資訊
記錄
設定
與變種病
完成
網際網路 | 受保護模式: 啟動
100%

免費的防毒軟體

- Avira AntiVir-小紅傘防毒軟體—個人與家庭（繁體中文版）
  - http://www.free-av.com/
  - http://g-ray.com.tw/downloads
- Bitdefender-羅馬尼亞防毒軟體
  - http://www.bitdefender.com/world
  - http://download.bitdefender.com/windows/desktop/free/final/en/bitdefender_free_v10.exe

使用者端的防範方式

免費的防毒軟體


Avira AntiVir Personal - Free Antivirus
AVIRA
More Than Security
小紅傘個人免費體驗版 - 僅供非商業使用
請利用這個對話框來解壓縮程式的安裝檔案，並開始實際的安裝程序。
小紅傘個人免費體驗版已包含合法授權金鑰，因此，在安裝過程中，您不需要另外安裝授權檔案。之後，如果您需要更多的防護功能，您可以在我們的網路商店購買小紅傘防毒大師或網路安全大師，以提供系統最完善的防護。
基於安全理由，請確認小紅傘安裝程式是否來自小紅傘網站或吉瑞科技網站。
Copyright © 2000 - 2009 Avira GmbH. All rights reserved.
Continue
Cancel

Download BitDefender - Windows Internet Explorer

http://www.bitdefender.com/world/Downloads/

Google

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

Download BitDefender

網頁(P) 工具(O)

My BitDefender

bitdefender

WorldWide - English

enter query here ...

Go

Company | Home/Home Office | Business | Partners | Downloads | Defense Center | Store

Home/Home Office | Business

Home / Downloads /

Downloads

BitDefender offers you the possibility to download everything from product evaluation versions , white papers, to free virus removal tools, and more. Please use the links below in order to select what you need to download.

Antivirus 2009	Internet Security 2009	Total Security 2009	Free Edition v10	Mobile Security v2
				
download	download	32 64	download	try
product comparison				

Home/Home Office | Business | Enterprise | Online / Partners

網際網路 | 受保護模式: 啟動

100%

線上掃描病毒的方法各家掃毒軟體大評比

VIRUS TOTAL

http://www.virustotal.com/zh-tw

Sophos	4.22.0	2007.09.30	Mal/EncPk-AZ
Sunbelt	2.2.907.0	2007.09.28	-
Symantec	10	2007.09.30	-
TheHacker	6.2.6.074	2007.09.30	-
VBA32	3.12.2.4	2007.09.30	MalwareScope.Worm.Viking.3
VirusBuster	4.3.26:9	2007.09.30	-
Webwasher-Gateway	6.0.1	2007.09.30	Trojan.Crypt.NSPM.Gen

附加訊息

File size: 288476 bytes

MD5: 3d99dd86ba0c7bb8889cdc8ca4a52e5e

SHA1: 595aa493b5c15679cb59e6f5edbeb5091850dd0e

packers: RAR

注意: VirusTotal 是 Hispasec Sistemas 提供的免費服務. 我們不保證任何該服務的可用性和持續性. 儘管使用多種反病毒引擎所提供的偵測率優於使用單一產品, 但**這些結果並不保證檔案無害**. 目前來說, 沒有任何一種解決方案可以提供 100% 的病毒和惡意軟體偵測率. 如果您購買了一款聲稱具有此能力的產品, 那麼您可能已經成為受害者.

掃瞄其它檔案

重點回顧

- 宣導郵件社交工程演練！
  - **與公務非相關的信件，不要開啟！(留意主旨)**
  - **若真的不小心開啟了，千萬不要點選郵件內超連結！**

回顧重點

- 作業系統、應用程式、文書軟體、防毒軟體更新。
- 若是常註冊網路的論壇，不一定要用自己的信箱，免得一天到晚被垃圾信件寄爆了
- 可至http://www.virustotal.com/zh-tw網站掃描不信任的檔案
- 設置密碼記得8碼以上、英文大小寫、特殊符號、可使用輸入法做密碼。
- 郵件追蹤之術可以查出這封信是否是真的。

問題與討論

- E-Mail：ynie@bccs.com.tw
- Blog： http://yniewu.blogspot.com/
- Facebook：
  http://www.facebook.com/ynie.wu