



# 南投縣教育網路中心 資安防護種子教師培訓研習課程

## 防範電子郵件社交工程

蔡和燁

Hoyeh\_tsai@kh.ringline.com.tw

# 大綱

---

- 社交工程
- **社交工程 – 網路篇**
- 如何防範



# 網路社交工程 - 電子郵件

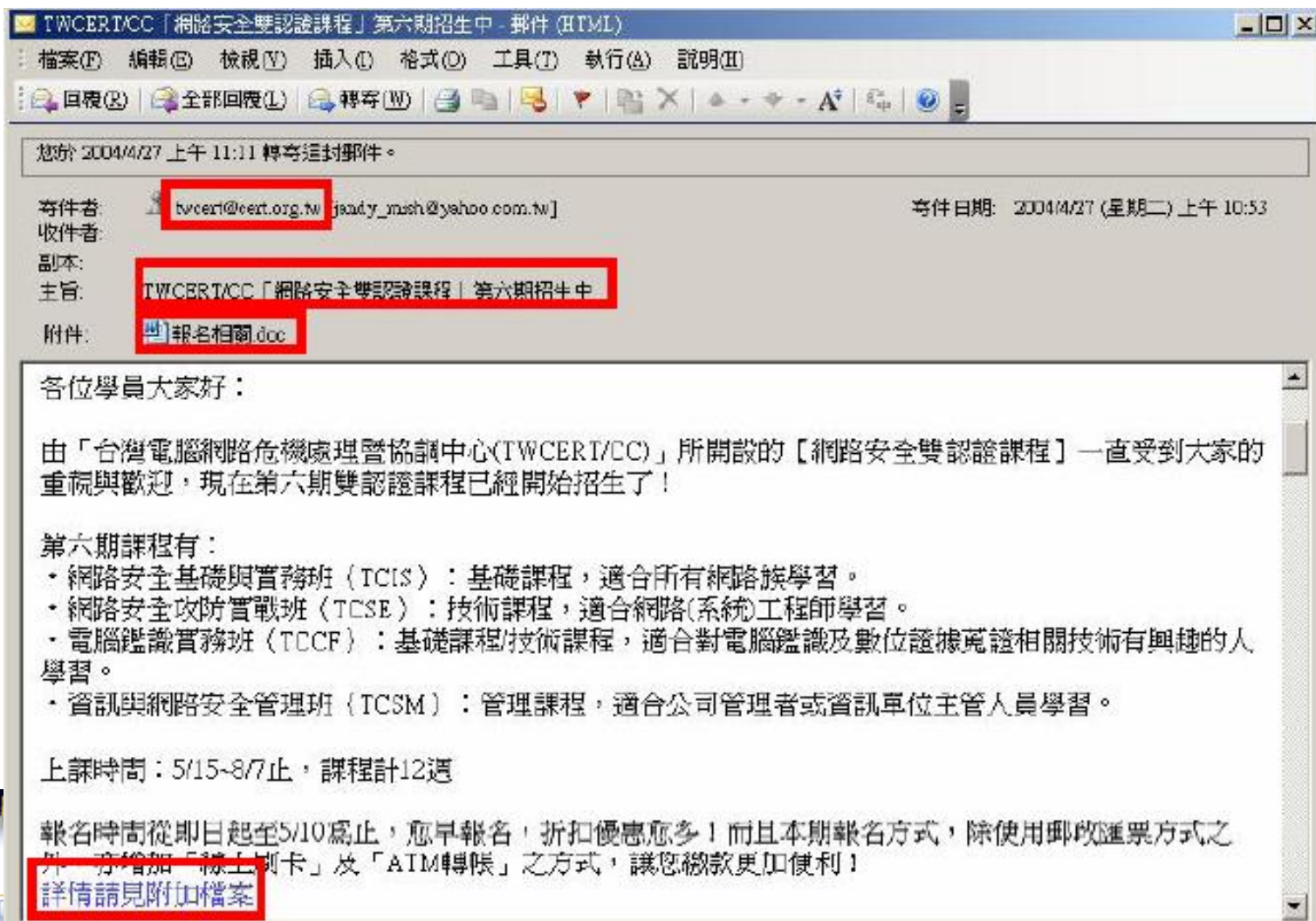
- 電子郵件

- **垃圾郵件**：利用垃圾郵件誇大之形容詞誘使點選郵件中附加之**超連結**或者取消訂閱按鈕，進而植入惡意程式。
- **網路拍賣**：搶在拍賣交易結標後，以偽冒之電子郵件(**截標信**)詐騙買方匯款。
- **會員通知**：以電子郵件(**偽冒信**)通知會員修改密碼，進而竊取會員資料



# 帶有惡意程式的電子郵件

- ◆ 在下面的郵件中，附件的Word 文件含有後門程式，使用者開啟附件後，該後門程式就會被執行且安裝至系統之中。



TWCERT/CC [網路安全雙認證課程] 第六期招生中 - 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)

您於 2004/4/27 上午 11:11 轉寄這封郵件。

寄件者: twcert@cert.org.tw jandy\_msh@yahoo.com.tw 寄件日期: 2004/4/27 (星期二) 上午 10:53  
收件者:  
副本:  
主旨: TWCERT/CC [網路安全雙認證課程] 第六期招生中  
附件: 報名相關.doc

各位學員大家好：

由「台灣電腦網路危機處理暨協調中心(TWCERT/CC)」所開設的【網路安全雙認證課程】一直受到大家的重視與歡迎，現在第六期雙認證課程已經開始招生了！

第六期課程有：

- 網路安全基礎與實務班 (TCIS)：基礎課程，適合所有網路族學習。
- 網路安全攻防實戰班 (TCSE)：技術課程，適合網路(系統)工程師學習。
- 電腦鑑識實務班 (TCCF)：基礎課程/技術課程，適合對電腦鑑識及數位證據蒐證相關技術有興趣的人學習。
- 資訊與網路安全管理班 (TCSM)：管理課程，適合公司管理者或資訊單位主管人員學習。

上課時間：5/15~8/7止，課程計12週

報名時間從即日起至5/10為止，愈早報名，折扣優惠愈多！而且本期報名方式，除使用郵政匯票方式之外，亦增加「線上刷卡」及「ATM轉帳」之方式，讓您繳款更加便利！

詳情請見附加檔案



# 圖片中惡意程式

## 駭客集團 竊上萬網友帳號



更新日期: 2006/08/10 15:14 記者: 記者陳珮琦/台北報導

喜歡在網路上點選色情圖片的網友要注意了! 刑事局偵九隊破獲本土駭客集團將夾帶木馬程式的色情圖片為誘餌，竊取網友入口網站及線上遊戲帳號，再轉手販售給大陸詐欺集團，警方估計該由夫妻檔、姊妹檔所組的本土駭客集團近一年來，計竊取上萬筆網友帳號，光是集團車手就月入20萬元，不法所得合計約近千萬元。

刑事局逮捕該本土駭客集團主嫌李宏文(22歲)和王聲慶(31歲)、溫心燕(女、32歲)夫妻二人，王、李為躲避警方查緝，還不惜遠赴大陸租屋作為上網之用，竊得各式帳號密碼後，在大陸地區分類提供給不同需求的買家。

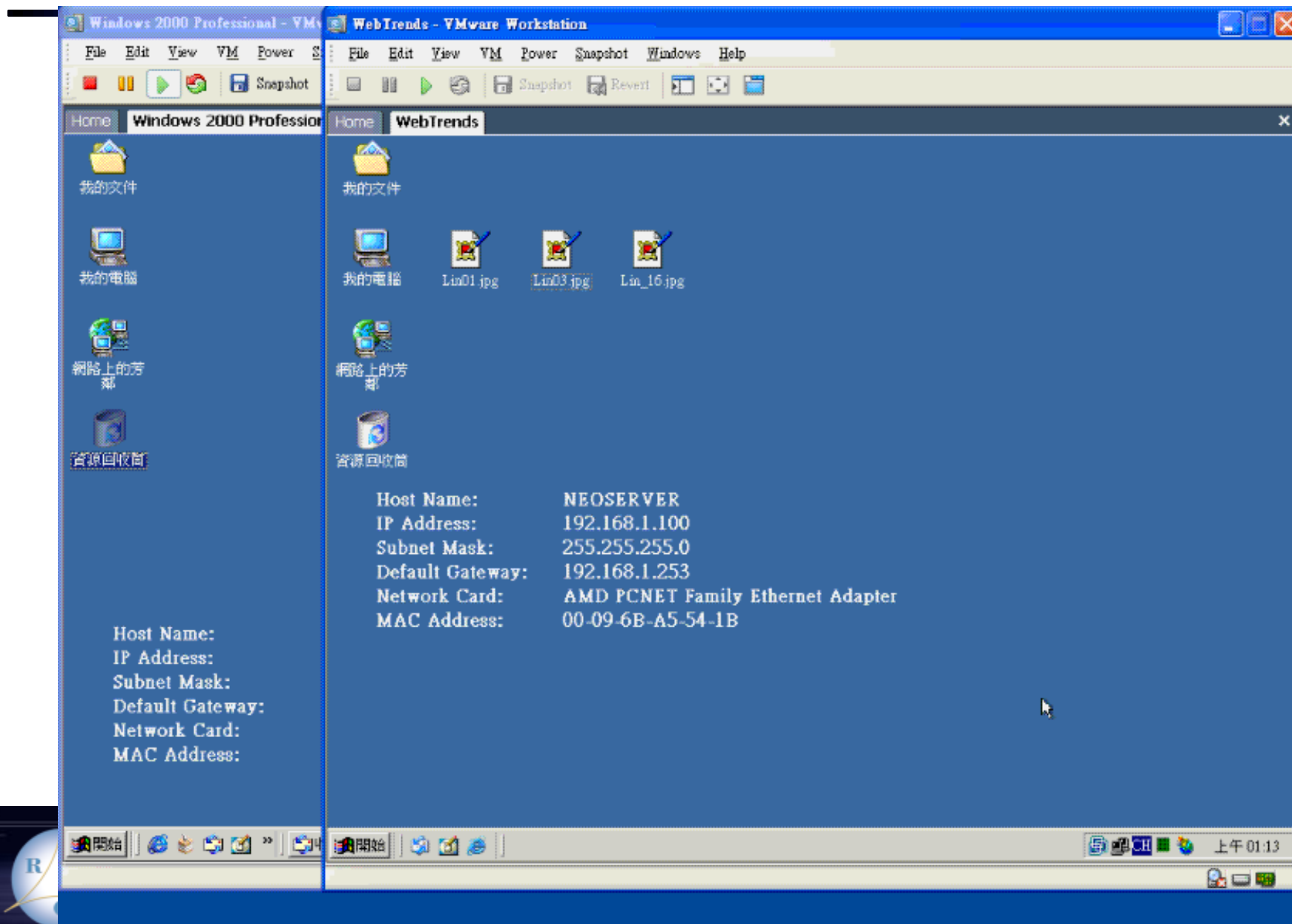
李、王為首的駭客集團以夾帶木馬程式的色情圖片為誘餌，在各網站或依通訊錄、好友名單「大放送」，刻意命名「各國空姐」、「馬子舒琪」或是「台灣山中裸女」等挑逗字眼，勾引喜好瀏覽色情圖片網友點選，網友只要一點選，即渾然不知地掉入陷阱。

近一年來，李、王駭客集團計竊取上萬筆帳號密碼，暴利可觀，王嫌的妻子溫心燕和小姑也都「下海」當起車手，以盜取的帳號密碼登入家族、即時通、電子郵件，將夾帶木馬程式的色情圖片依通訊錄、好友名單主動寄送，讓收件者一開檔就被竊走帳號密碼還不自知。

◆ 明星或色情圖片是許多惡意程式慣用的社會工程技巧之一，利用使用者的好奇心來散佈惡意程式。



# 利用圖片夾帶木馬



# 雅虎拍賣手法分析



下標

查詢拍賣訊息



賣家



詐騙者



劫標信

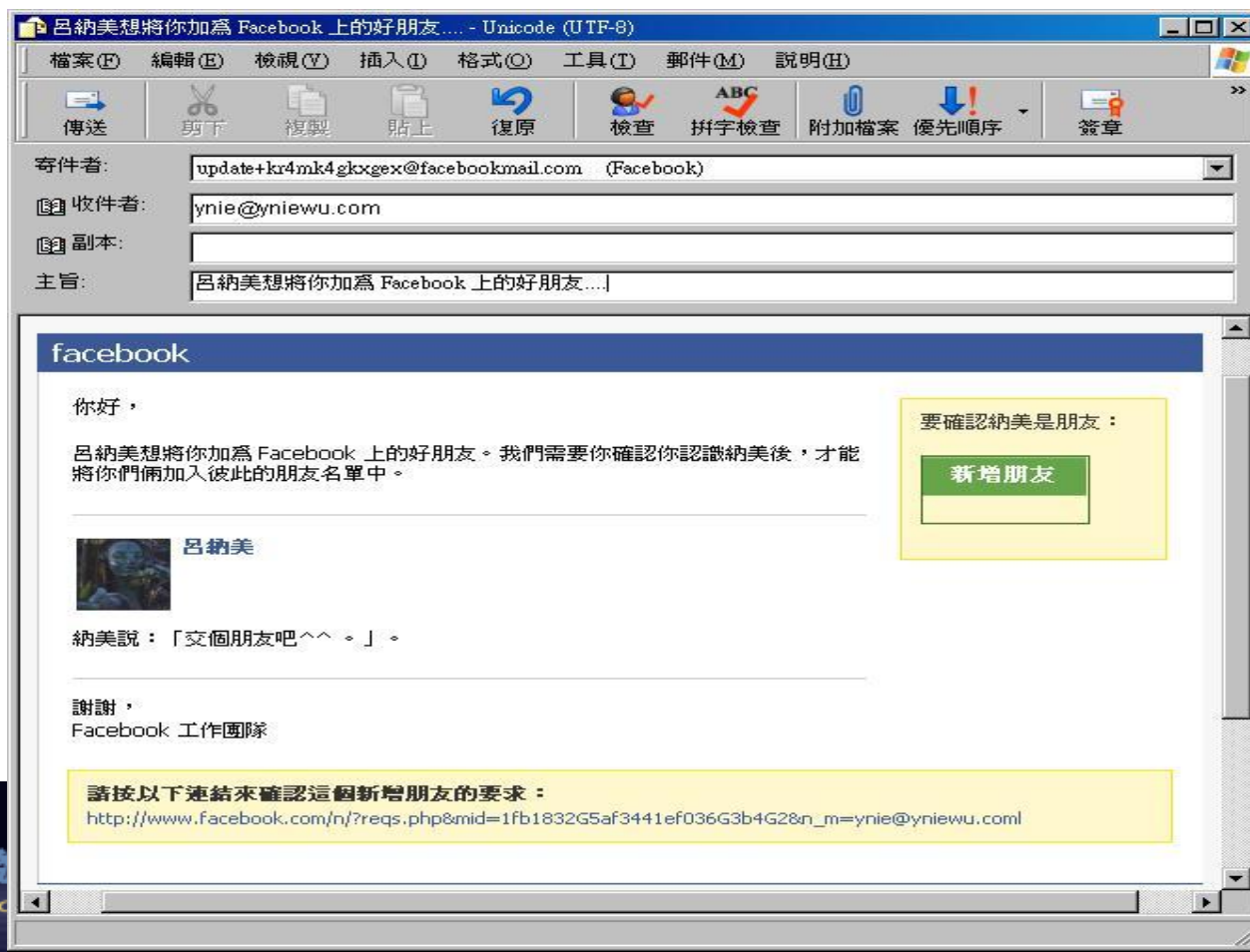
# 會員通知手法分析





# 討厭郵件釣魚

◉ 寄出釣魚信件，來吧~你的帳號密碼



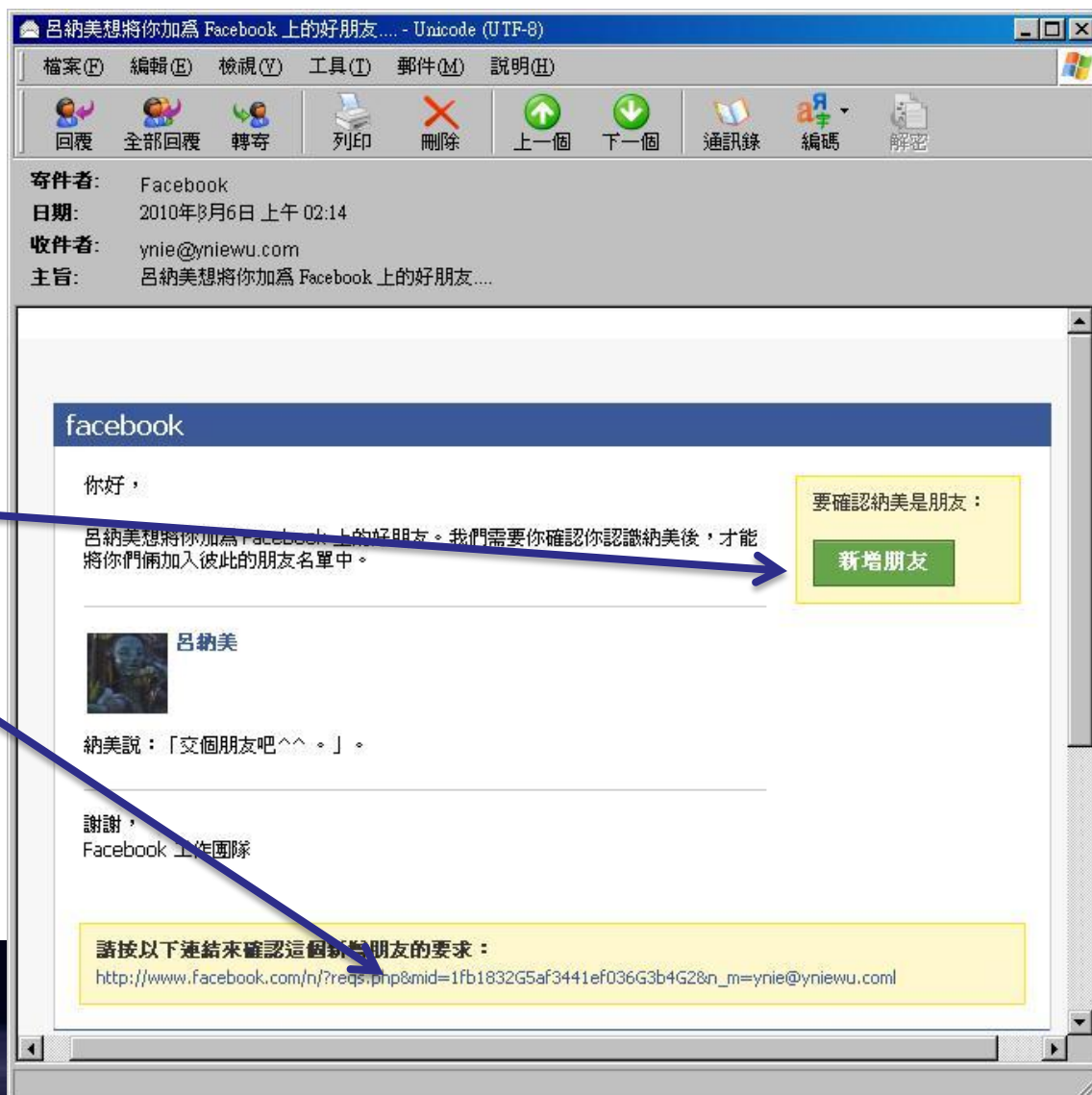
鹿  
RINC



# 討厭郵件釣魚

收信看看~

點選新增  
好友



# 討厭郵件釣魚



# 討厭郵件釣魚

哈哈~  
騙到了



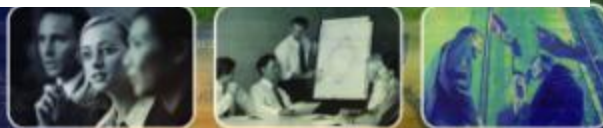
Facebook所回應的帳號密碼

你的E-mail帳號是 : ynie@yniewu.com

你的密碼是 : 123456

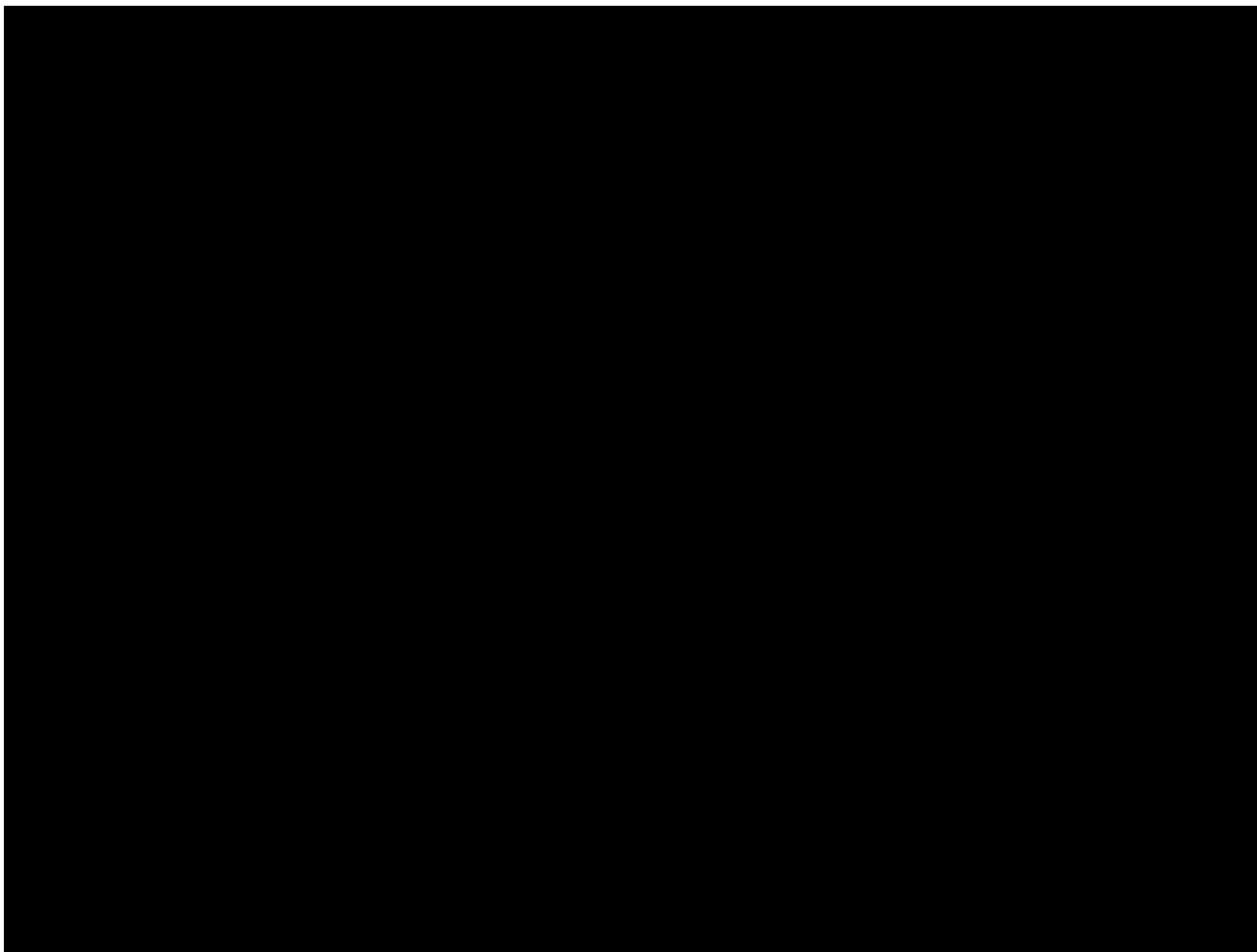


麟瑞科技  
RING LINE CORPORATION



# 偽裝Facebook網站 – 偷取帳號密碼

---



麟瑞科技  
RING LINE CORPORATION





# 看的出問題點嗎？ Facebook 會員通知信



麟瑞科技  
RING LINE CORPORATION



# 匯豐銀行通知信

主旨: HSBC Taiwan warning

HSBC  滙豐 環球金融 地方智慧

## 正式通知

親愛的香港上海滙豐銀行台灣用戶

近來許多不肖之徒大規模的使用木馬程式入侵金融機構客戶的電腦，並竊取帳戶名稱、私人密碼、個人資料及銀行機密等相關資料。為了確保您的網路交易安全和保密，如果您的網路銀行理財戶頭有不正常的提款，滙豐銀行將會立即和您取得絡。滙豐銀行一向重視客戶的個人私隱並謹慎處理客戶的個人及保密資料，為幫助滙豐銀行能更快的通知您，請您點選[此處](#)使用我們的官方網站連結填寫您的連絡方法。

## 滙豐為您提供的保障

貴為香港上海滙豐銀行的個人理財的客戶，在您使用滙豐「[網路銀行理財](#)」服務時，若發生第三方欺騙的情況，您將會獲得全面的保障。未經您授權的帳戶提款，在您沒有欺騙或疏忽的情況下，您將不會蒙受任何損失。

詳情請參閱「[滙豐網路銀行服務](#)」約定條款，或「[信用卡網路服務](#)」約定條款。

[按此處瞭解有關網路安全的「四大重要守則」。](#)

©版權所有 • 不得轉載。  
香港商香港上海滙豐銀行股份有限公司2005

◆ 在上面的郵件中，告訴使用者需要更改帳號密碼，其實當點下連結後會轉至釣魚網站，將使用者個人資料竊取。



麟瑞科技  
RING LINE CORPORATION



# 為什麼政府會有社交電子郵件社交工程？

- ◉ **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10月3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
    - ◉ 惡意郵件開啟率為**26%**，超連結點閱率為**15%**。
  - ◉ (二)其餘主管機關
    - ◉ 惡意郵件開啟率為**40%**，超連結點閱率為**20%**。



# 網路社交工程 - 網站

## ● 網站

- **釣魚網站(偽冒網站)**：駭客註冊網域名稱與「正牌」之真正網域名稱極為相似，利用極為相似之字母或數字，如英文字母小寫l與數字1，n與h等極為相似之符號以假亂真，使上網之民眾難以辨別真偽，而誤觸駭客之網路釣魚陷阱。
- 目前也有是直接註冊與「正牌網站」一模一樣之DNS名稱但只有[上層網域名稱不同的網路蟑螂]。例如：原來是www.abc.com.tw、偽冒成www.abc.com、www.abc.net、www.abc.tw
- **搜尋網站(偽冒網站)**：購買網路關鍵字廣告服務並於各大入口網站搜尋行銷服務刊登「關鍵字廣告」，使用者上網搜尋「網路銀行」等條件時，搜尋結果的最上方即出現犯罪集團之「關鍵字廣告」。一般民眾認為搜尋網站的搜尋結果應該很可靠？進而點選進去。因為這些廣告係駭客精心設計，網站管理者亦無法判別廣告之虛偽，更何況一般民眾，幾乎無法查覺該網站連結係假冒之網站。



# 網路社交工程 - URL欺騙

中國信託	www.chinatrust.com.tw	www.chinatrst.com.tw
淡江大學webmail	webmail.tku.edu.tw	webmail.tku.eud.tw
財政部北區國稅局	www.ntx.com.tw	www.ntx.gov.tw
雅虎拍賣	TW.BID.YAHOO.COM	TW.BID.YAHO0.COM
PCHome	www.pchome.com.tw	www.pchorne.com.tw
無名小站	www.pchome.com.tw	www.pchorne.com.tw





# 網路搜尋

- ◉ 網路搜尋的惡意手法有二：
- ◉ 利用「特殊語法」取得隱藏資訊(Google Hacking)
  - 成功後，利用該資訊取得個人資料，或不公開的文件。
- ◉ 利用「關鍵字廣告」連結惡意網頁
  - 成功後，利用該惡意網頁植入木馬後竊取個人資料。



# 網路社交工程 - 關鍵字廣告

線上繳稅網站 - Google 搜尋 - Windows Internet Explorer

http://www.google.com.tw/search?complete=1&hl=zh-TW&q=%E7%B7%B9%A%E4%B8%8A+%E7%B9%B3%E

Google 線上繳稅網站

搜尋： 所有網頁  中文網頁  繁體中文網頁  台灣的網頁

**http://qa.yesgol.com/index.htm**

**http://paytax.nat.gov.tw/**

創市際市場研究顧問- InsightXplorer Limited  
網路報稅簡化了申報手續，補繳稅費更能透過線上繳稅網站(paytax.nat.gov.tw)來e指完成，它提供報稅民眾以信用卡與電子錢包線上繳稅，便利了民眾繳稅程序，訴求可延後付款與跨越時間限制。配合財政部賦稅署統計，今年採用信用卡刷卡繳稅總筆數五十三萬餘 ...  
www.insightxplorer.com/news/news\_06\_07.html - 32k - 頁庫存檔 - 類似網頁

yam天空-理財-報稅-2007報稅專區-繳稅方式  
線上繳稅一共有四種：... 納稅義務人可利用晶片金融卡透過網際網路繳納稅款(繳稅網站 https://eb.fisc.com.tw/EB/)，自備晶片卡讀卡機，與自然人憑證之讀卡機相同。利用晶片金融卡繳稅需自行負擔手續費10元，繳稅金額無限制。《全文》· 電子錢包： ...  
fn.yam.com/tax/s\_method.html - 11k - 頁庫存檔 - 類似網頁

# 小心關鍵字廣告連結惡意網頁

目前刑事局、TWNIC、金融業以及關鍵字廣告商，都提供相對因應之道

詐騙集團利用關鍵字廣告，誘使網友點擊、連結至惡意網頁的手法層出不窮，而詐騙集團常用的關鍵字更從以往鎖定金融、旅行社等，到隨時事更新，日前最新的詐騙關鍵字為拍賣。

前刑事警察局科技犯罪防制中心主任、現任警政署資訊室主任李相臣表示，針對詐騙集團利用各種關鍵字廣告，誘使網路使用者上當的手法，除了發文給詐騙集團偏好的高風險金融業者，配合提供正確網址外，也委由TWNIC（臺灣網路資訊中心）過濾申請與金融單位雷同的網址。至於關鍵字廣告商也強化人工審查機制，降低關鍵字廣告被利用的潛藏危機。

李相臣表示，隨著每一起關鍵字廣告詐騙手法的曝光，詐騙集團也隨之更換不同的關鍵字。日前最新的發現則是，詐騙集團在Google購買拍賣的關

網頁搜尋

相關詞：台灣土地銀行、土地銀行信用貸款、台灣土地銀行總行、土地銀行法拍屋、土地銀行貸款

www.landbank.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.landbank.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，首創網路指定專人服務。www.aiban.com.tw
- 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，簡單償。www.easyloan.com.tw
- 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，貸款具容易。www.carloan.com.tw

在Yahoo!奇摩生活+查土地銀行的電話地址和評價

分類：銀行  
www.landbank.com.tw - 52k

真的土地銀行網站，網址是www.landbank.com.tw

分類：銀行  
www.landbank.com.tw - 52k - 2006/12/25 - 匯豐頁面 - 更改此站語言 - 備有 - 對帳

刑事局科技犯罪防制中心／提供

鍵字廣告，雖然關鍵字搜尋結果中雅虎拍賣排第一，但該網址卻為惡意網頁。（目前該惡意網頁已清除。）

李相臣說，他日前收到生平第一次，由第一銀行IT同仁寫信告知，網路上有可疑的釣魚網站，請警政單位協助調查的檢舉信函。李相臣對此非常高興，他認為，這也意味著金融業的IT人員願意正視並面對相關的網路威脅。李相臣表示，科技犯罪防

制中心也委由負責臺灣網域申請的TWNIC，過濾疑似金融等高風險單位的網址。

提供關鍵字廣告的廠商，對於關鍵字廣告潛藏危機，連結到惡意網頁的犯罪手法相當重視。被雅虎併購的香港序曲臺灣分公司搜尋行銷事業部業務協理陳婉怡表示，雅虎奇摩針對高風險、高流量的關鍵字，進行更以往嚴謹的人工主動審查的機制。

## 重點

- 詐騙集團的關鍵字廣告會隨時更新，最新受害字眼為拍賣
- TWNIC協助過濾與金融機構雷同網址的申請，杜絕可能詐騙
- 雅虎關鍵字廣告為遏止潛藏惡意連結，強化人工審查機制
- Google設有機制監控特定網站，但關鍵字廣告過濾方式保密

雅虎對於高流量、高風險以及一些違反臺灣法令的關鍵字，有一個專屬資料庫，數量已超過10,000筆，並不斷增加中。陳婉怡指出，只要是高風險資料庫規範內的關鍵字，一旦有人購買類似關鍵字廣告，便會自動進入人工審查系統，由編輯進行審查、篩選是否有疑慮。

另外，詐騙集團都使用偽卡付款，若某關鍵字廣告購買價錢過高，會進行行業別審查以及偽卡驗證。陳婉怡表示，序曲目前也與警政單位積極合作，定期更新近期最熱門的網路犯罪關鍵字。

另一家提供關鍵字廣告服務的廠商Google，同樣重視這樣

的網路犯罪手法。美國Google總部表示，Google已經有一個機制監控受到檢舉的特定網站，若發現該網站有違反Google的廣告政策，將視情節輕重予以不同處置。但Google表示，為了避免防範機制與實例成為詐騙集團的參考，相關細節將予以保密。

李相臣提醒，定期掃毒、採用可辨別安全網站的瀏覽器外掛程式等，都是必要的措施。若登入金融業網址輸入帳號密碼，他建議採用Token、將資料、硬碟加密，使用約定轉帳，都有助於降低被害率，至於銀行則必須做到主動通報被害人的查詢機制，銀行間也必須做到相互通報。文◎黃彥棻



# 網路社交工程 - 即時通訊

- 即時通訊
  - **偽造超連結**：中毒後發送具有惡意程式的**超連結**，誘使好奇使用者點選，進而植入木馬程式或騙取帳號密碼。



# 網路社交工程 - 即時通訊





# 網路社交工程 - 偽裝合法防毒軟體

www.microsoft.com/security/pc-security/antivirus-rogue.aspx

Microsoft®

## Safety & Security Center

Computer Security, Digital Privacy, and Online Safety

United States Change | All Microsoft Sites

Search Microsoft Security



[Home](#) | [Security](#) | [Privacy](#) | [Family Safety](#) | [Resources](#)

[Worldwide](#) | [Get Support](#) | [Sign Up for Newsletter](#)

Home > Security > Watch out for fake virus alerts

### PC Security

Security scanners, tools, and safety guidelines for your PC, laptop, or mobile device.

[Email](#) [Print](#) [Tweet](#) 67

#### How to...

##### + Get a security update, tool, or scan

- [Security updates](#)
- [Free antivirus, antispyware program](#)
- [Free PC safety scan](#)
- [Download Malicious Software Removal Tool](#)

##### Protect my kids from online

## Watch out for fake virus alerts

Rogue security software, also known as "scareware," is software that appears to be beneficial from a security perspective but provides limited or no security, generates erroneous or misleading alerts, or attempts to lure users into participating in fraudulent transactions.

### How does rogue security software get on my computer?

Rogue security software designers create legitimate looking pop-up windows that advertise security update software. These windows might appear on your screen while you surf the web.

The "updates" or "alerts" in the pop-up windows call for you to take some sort of action, such as clicking to install the software, accept recommended updates, or remove unwanted viruses or spyware. When you click, the rogue security software downloads to your computer.

Rogue security software might also appear in the list of search results when you are searching for trustworthy antispyware software, so it is important to protect your computer.



麟瑞科技  
RING LINE CORPORATION



# 網路社交工程 - 偽裝合法防毒軟體

Microsoft Security Essentials Alert

Antivirus	Scan result	Bases update	Removal tool
NOD32	Nothing	1 hours ago	Free Install
Red Cross	Unknown Trojan	6 hours ago	Free Install
IKARUS	Nothing	6 hours ago	Free Install
VirusBuster	Nothing	24 hours ago	Free Install
Dr.Web	Nothing	2 hours ago	Free Install
avast!	Nothing	24 hours ago	Free Install
Peak Protection	Trojan Horse	24 hours ago	Free Install
McAfee	Nothing	1 hours ago	Free Install
bitdefender	Nothing	3 hours ago	Free Install
SOPHOS	Nothing	3 hours ago	Free Install
eTRUST	Nothing	Last bases	Free Install
AVG	Nothing	24 hours ago	Free Install
Clam AV	Nothing	11 hours ago	Free Install
KASPERSKY	Nothing	23 hours ago	Free Install
symantec.	Nothing	24 hours ago	Free Install
VBA32	Nothing	27 hours ago	Free Install
F-PROT antivirus	Nothing	4 hours ago	Free Install
Pest Detector	RootKit	4 hours ago	Free Install

Antivirus	Scan result	Bases update	Removal tool
A-SQUARED	Nothing	8 hours ago	Free Install
TREND MICRO	Nothing	18 hours ago	Free Install
Major Defense Kit	RootKit	3 hours ago	Free Install
F-Secure	Nothing	3 hours ago	Free Install
Windows Live	Nothing	2 hours ago	Free Install
AntiVir	Nothing	14 hours ago	Free Install
ewido	Nothing	Last bases	Free Install
Panda	Nothing	95 hours ago	Free Install
Vexira	Nothing	24 hours ago	Free Install
NORMAN	Nothing	25 hours ago	Free Install
Solo	Nothing	Last bases	Free Install
ArcaVir	Nothing	3 hours ago	Free Install
Webroot	Nothing	3 hours ago	Free Install
TREND MICRO 2010	Nothing	54 hours ago	Free Install
COMODO	Nothing	1 hours ago	Free Install
RISING	Nothing	2 hours ago	Free Install
AntiSpySafeguard	RootKit	2 hours ago	Free Install





# 網路社交工程 - 偽裝合法防毒軟體

The image shows a Windows XP desktop environment. On the left, a window titled "Antivirus XP 2008 demo mode notice" is open. It features the "Antivirus XP 2008" logo and a large red "X" mark over the "Virus Protection" section. The text in this section reads: "Windows did not find any registered Antivirus XP 2008 software on this computer. Antivirus XP 2008 helps protect your computer against viruses and other security threats. Click Recommendations for suggested actions you can take." Below this, there are buttons for "Recommendations..." and "Continue unprotected", and a link to "Click here to switch to the Full Mode".

On the right, the "Windows Security Center" window is open. It displays the "Security essentials" section, which includes:

- Windows Update
- Windows Firewall
- Windows Defender
- Internet Options

The "Security essentials" section is set to "On" for all items. Below this, there are sections for "Virus protection" (Centoso Antivirus reports that it is up to date and virus scanning is on) and "Spyware and other malware protection" (Centoso Antispyware reports that it is turned on). At the bottom, there is a link to "How does anti-malware software help protect my computer?" and an "Other security settings" section set to "OK".



# 大綱

---

- 社交工程
- 社交工程 – 網路篇
- **如何防範**



# 如何防範- 電子郵件社交工程

---

安全意識 + 善用工具



麟瑞科技  
RING LINE CORPORATION





按這裡下載圖片。為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: h (性感魅力專賣) [ptych@ny-lancastr-cadent1-grp4h-a-169.bflony.adelphia.net]

寄件日期: 2007/3/16

收件者: aaa22787455@yahoo.com.tw

副本:

主旨: 『姿勢換5-6種, 只是剛剛開始而已』 For - MAN

6X 美嬌巨乳姬精選合集 OL女秘書精選合集

收件人

✘ 在這裡按一下滑鼠右鍵下載圖片。為了協助保護您的隱私，Outlook 不會自動從網際網路下載此圖片。  
0301

R 激情不敗, 男上持久

不是我

寄件者: Alexia [shagarageequ@blackjackforyou.com]

寄件日期: 2007/3/27 (星)

收件者: Hye







副本:

主旨: Thinking about you

### Discount Pharmacy Online

Do not click, type in your browser:

<http://www.meds4us.org>

	Viagra	100 mg	Only \$1.00 per pill
	Cialis	20 mg	Only \$1.00 per pill
	Ambien	1 mg	Only \$1.00 per pill
	Xanax	1 mg	Only \$2.00 per pill
	Phentermine	37.5 mg	Only \$4.17 per pill
	Valium	1 mg	Only \$1.00 per pill

Savings up to 80%

Do not click, just type <http://www.Meds4Us.org> in address bar of your browser, then press enter key

寄件人  
不認識

寄件者: Camarvon3 boggstown [camarvon3@cluemail.com]

寄件日期:

收件者: jiunn.jye

副本:

主旨: As well clockville

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

[KVG] Histor For Extraordinary Vacations Group inc

Symbol OT KVG.P

Current Price: \$0.00

5 Day Expected: \$0.00

Recommendation: Very aggressive buy!!

Before we continue, there is a huge IPO campaign under way for KVG so get in before the rest of the world. This is history.

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

centers in all those seas. Greek and Roman travelers found a rain. The water which is taken up by the atmosphere from the beasts, noxious reptiles, and frogs, and thus 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.

大部分是英文

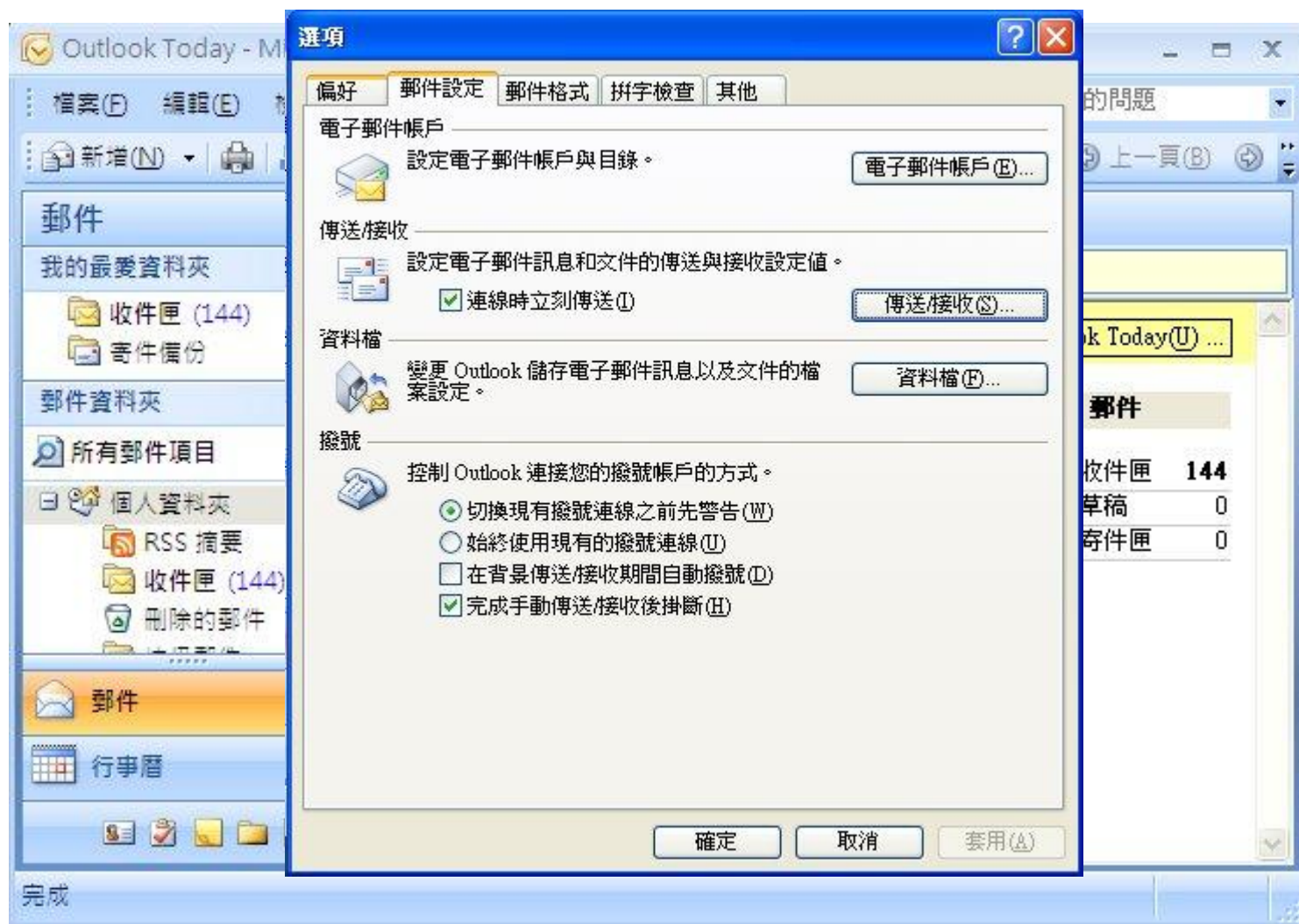
# 垃圾郵件、匿名郵件及偽造郵件攻擊

- ◉ 利用匿名郵件 (例如：要求回信)
- ◉ 利用好康郵件 (例如：程式下載、中獎)
- ◉ 利用連鎖信 (例如：佛像郵件)
- ◉ 利用尋人郵件 (例如：尋找失蹤兒)
- ◉ 利用愛心郵件 (例如：骨髓配對、勵志小故事)
- ◉ 利用銀行郵件
- ◉ 利用廣告郵件 (例如：折價卷)
- ◉ 利用情色郵件



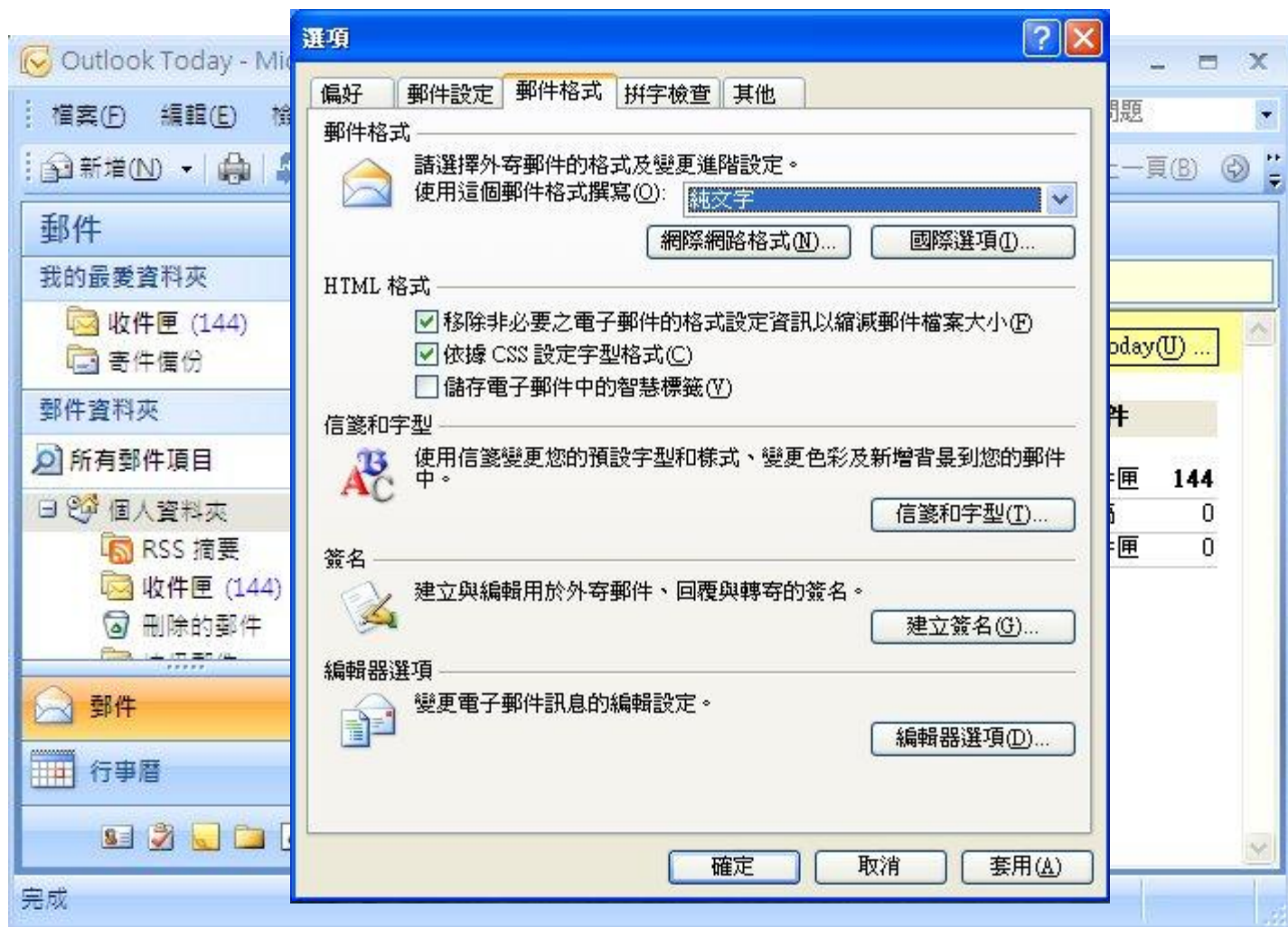


# 關閉「啟動時傳送及接收郵件」





# 以純文字模式 傳送電子郵件



# 關閉自動讀取窗格

收件匣 - Microsoft Outlook

檔案(F) 編輯(E) 檢視(V) 到(G) 工具(T) 動作(A) 說明(H)

鍵入需要解答的問題

新增(N) 回覆(R) 全部回覆(L) 轉寄(W) 傳送/接收(C) 搜尋通訊錄

郵件 收件匣 搜尋收件匣

我的最愛資料夾 按一下這裡啟用「立即搜尋」

收件匣 (144) 郵件備份

郵件資料夾 日期: 星期一

寄件者	主旨	收到日期	大小	類別
z98070...	This is an autoreply...[Re: 機會博之擊賊偵探的辣醬包]	2010/10/...	4 KB	
@ Mail D...	Undelivered Mail Returned to Sender	2010/10/...	16 KB	
@ Mail D...	Delivery Status Notification (Failure)	2010/10/...	15 KB	
@ Mail D...	Delivery Status Notification (Failure)	2010/10/...	15 KB	
@ Mail D...	Delivery Status Notification (Failure)	2010/10/...	17 KB	
@ Mail D...	Delivery Status Notification (Failure)	2010/10/...	15 KB	
@ Mail D...	Delivery Status Notification (Failure)	2010/10/...	17 KB	
@ Mail D...	Delivery Status Notification (Failure)	2010/10/...	17 KB	
@ Mail D...	Delivery Status Notification (Failure)	2010/10/...	17 KB	
@ Mail D...	Delivery Status Notification (Failure)	2010/10/...	17 KB	
@ Mail D...	Delivery Status Notification (Failure)	2010/10/...	6 KB	
@ Mail D...	Delivery Status Notification (Failure)	2010/10/...	15 KB	
@ Mail D...	Delivery Status Notification (Failure)	2010/10/...	16 KB	
@ Mail D...	Delivery Status Notification (Failure)	2010/10/...	17 KB	
@ Mail D...	Delivery Status Notification (Failure)	2010/10/...	17 KB	
@ Mail D...	Delivery Status Notification (Failure)	2010/10/...	6 KB	
@ Mail D...	Delivery Status Notification (Failure)	2010/10/...	17 KB	
@ Mail D...	Delivery Status Notification (Failure)	2010/10/...	15 KB	
@ Mail D...	Delivery Status Notification (Failure)	2010/10/...	15 KB	
@ Mail D...	Delivery Status Notification (Failure)	2010/10/...	16 KB	

待辦事項 沒有即將來... 今天: 0 個工作



# 密件副本



## 郵件附件檔

---

- ◉ 將附件檔「另存新檔」後掃描病毒，不可以直接點選2下打開。
- ◉ 修補「Microsoft Office」、「Adobe Reader」等的相關讀取程式的弱點。
- ◉ 如果不確定所收到的檔案是否有問題，使用「可疑檔案上傳分析」確認。



# 可疑檔案上傳分析：

- VirusTotal：免費線上病毒和惡意軟體掃描 <http://www.virustotal.com/zh-tw/>

[日本語](#) | [Slovenščina](#) | [Dansk](#) | [Русский](#) | [Română](#) | [Türkçe](#) | [Nederlands](#) | [Ελληνικά](#) | [Français](#) | [Svenska](#) | [Português](#) | [Italiano](#) | [简体中文](#) | [Magyar](#) | [Deutsch](#) | [Česky](#) | [Polski](#) | [Español](#) | [English](#)



VirusTotal 是一款可疑檔案分析服務，通過各種知名反病毒引擎，對您所上傳的檔案進行偵測，以判斷檔案是否被病毒、蠕蟲、木馬，以及各類惡意軟體感染。 [查看詳細訊息...](#)

[分析](#) | [統計訊息](#) | [電子郵件/直接上傳](#) | [關於 VirusTotal](#)

## 上傳檔案

服務負載 ?

## 選項

使用安全方式(SSL)傳輸 ?

如果您願意，同樣可以使用[郵件客戶端](#)來發送檔案。



# 可疑檔案上傳分析：

- VirSCAN.org：線上防毒引擎掃描網站 v1.00 目前支援 36 款防毒引擎
- <http://www.virscan.org/>

The screenshot displays the VirSCAN.org website. At the top left is the logo with the text "VirSCAN.org submit & scan your file". To the right is a form for uploading files, including a file input field, "瀏覽..." (Browse) and "上傳" (Upload) buttons, a language selection dropdown set to "繁體中文", and a server load indicator. Below the form are three instructions in Chinese regarding file size, supported formats, and password detection. A sidebar on the left contains a "功能表" (Menu) with links to "首頁", "關於VirSCAN", "查閱清單", "幫助我們", "BUG 反應", and "聯繫我們". Below the menu is a "支援廠商" (Supported Vendors) section listing logos for A-SQUARED, Ahn AhnLab, AntiVir, ARCABIT, evast!, and AVG Anti-Virus. The main content area has a section titled "關於VirSCAN" with two paragraphs of text and a "更多..." link. Below that is a section titled "目前掃毒引擎版本" (Current Antivirus Engine Versions) containing a table with columns for engine name, country, engine version, feature database version, feature database date, and last update time.

軟體名稱	國別	引擎版本	特徵庫版本	特徵庫日期	最新更新時間(CST)
a-squared	奧地利	3.0.0.126	2008.02.18	2008-02-18	2008-02-19 08:01:32
AhnLab V3	南韓	2008.02.19.00	2008.02.19	2008-02-19	2008-02-19 10:20:55
Arcavir	波蘭	1.0.4	200802181833	2008-02-18	2008-02-19 06:15:04
Avast	捷克	1.0.8	080218-0	2008-02-18	2008-02-18 19:45:43
AVG	捷克	7.5.51.442	269.20.7/1286	2008-02-18	2008-02-19 04:04:04
BitDefender	羅馬尼亞	7.60825.981796	7.17603	2008-02-19	2008-02-19 15:37:22
CA(VET)	美國	9.0.0.143	31.3.5546	2008-02-18	2008-02-18 17:53:58

http://www.virustotal.com/zh-tw/resultado.html?53c313e684900c1d48efdc1df4001005 Live Search

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

VirusTotal - 免費線上病毒和惡意軟體掃描 - 結果

KISing	19.42.01.00	2007.09.30	-
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: 595aa493b5c15679cb59e6f5edbeeb5091850dd0e

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.

掃描其它檔案

# 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。
- 關閉「啟動時傳送及接收郵件」、「每隔幾分鐘傳送及接收郵件」功能。
- 關閉「自動讀取窗格」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」。



# WebMail的傳送與接收

- WebMail的使用原則，跟本機Mail的注意事項也是一樣的。
- 但WebMail更需要注意「預覽視窗」以及「超連結」的點選。
- 雖然WebMail的附件檔並沒有收下來，但若不注意仍有可能發生點選到有毒附件檔。
- WebMail更需要經常「**變更密碼**」，來避免被他人竊取。
- **盡量避免**在他人或公用電腦中使用WebMail，有可能該電腦已經中毒。如果一定要用，使用前先掃毒、離開前請『**登出**』並要「清除瀏覽器的Cookie」，避免帳號密碼被記住。





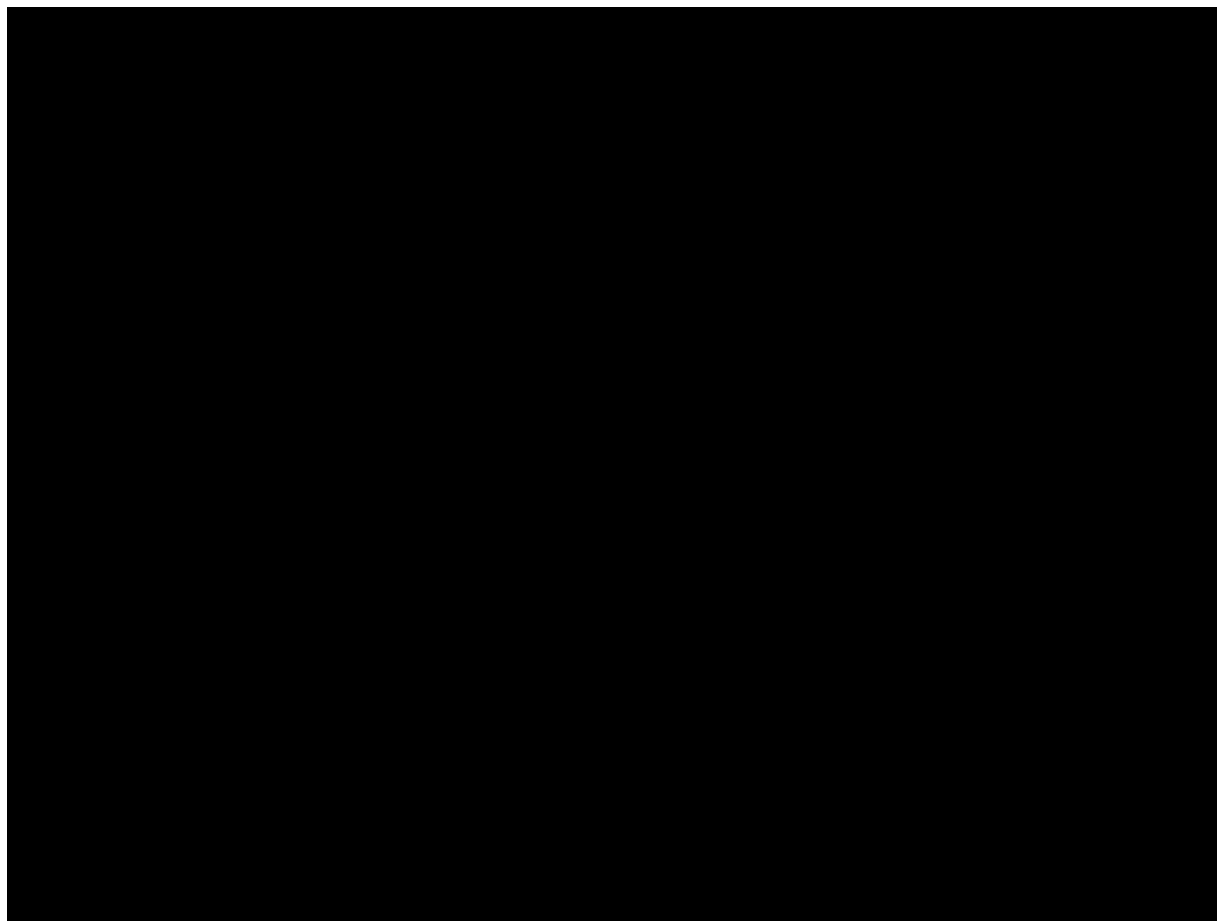
## 電子郵件重點項目

- ➡ 請勿開啟及預覽任何人所寄來的匿名、垃圾郵件。
- ➡ 就算是開啟了也請勿點選「超連結」。
- ➡ 開啟任何郵件的附件檔前，請記得「另存新檔」掃毒後再開啟。



# 如何防範- 網拍安全

---



麟瑞科技  
RING LINE CORPORATION



# 如何防範- 網站社交工程

## 善用會警告的搜尋引擎

Google™

搜尋

[進階搜尋](#) | [使用偏好](#)

搜尋： 所有網頁  中文網頁  繁體中文網頁  台灣的網頁

### 所有網頁

[Taiwan - 首頁](#)

這個網站可能會損害您的電腦。

cars, 2007.9.14 F1戰報, 土耳其站GP, [redacted] 車隊賽車跑完全程.完成比賽 [redacted] Racing F1 Team 決賽展開 ... cars, 2007.7.18 F1戰報, 英國GP, [redacted] Racing F1 Team 的Rubens Barrichello拿下第九名, Jenson Button則以第十名完賽 ...

[www.honda-taiwan.com.tw/home.asp](http://www.honda-taiwan.com.tw/home.asp) - [類似網頁](#)

[Taiwan - 首頁](#)

這個網站可能會損害您的電腦。

cars, 2007.7.18 F1戰報, 英國GP, [redacted] Racing F1 Team 的Rubens Barrichello拿下第九名, Jenson Button則以第十名完賽 ... cars, 2007.7.1 到 [redacted] Cars看專屬的 [redacted] Channel,即可享有花漾夏祭刮刮樂雙重中獎機會 ...

[www.honda-taiwan.com.tw/](http://www.honda-taiwan.com.tw/) - [類似網頁](#)

[ [www.honda-taiwan.com.tw](http://www.honda-taiwan.com.tw/) 的其它相關資訊 ]



麟瑞科技  
RING LINE CORPORATION



# 如何防範- 網站社交工程

<http://www.siteadvisor.com/>

The screenshot shows a Windows Internet Explorer browser window. The address bar contains a Google search URL for '病毒下載測試'. The page content shows search results for '卡巴斯基反病毒软件2010'. A red-bordered warning box from McAfee SiteAdvisor is overlaid on the page. The warning box has a red header with a white 'X' icon and the text: '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。' Below the header, the warning details the site's status: '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'. It lists three items: '75 個不安全下載' (75 unsafe downloads), '不安全網站連結' (unsafe website links), and '0 個快顯視窗' (0 pop-ups). A green checkmark icon is next to the '0 個快顯視窗' item. At the bottom right of the warning box, there is a link to '升級至 SiteAdvisor Plus' and a link to '讀取網站報告'.

McAfee SiteAdvisor 警告：

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



# 如何防範- 網站社交工程 <http://securebrowsing.finjan.com>

Finjan Vital Security- SecureBrowsing - Windows Internet Explorer

http://securebrowsing.finjan.com/

Google finjan 搜尋 分享 網頁註解 拼字檢查 翻譯 登入

我的最愛 建議的網站 網頁快訊圖庫 百度

Finjan Vital Security- SecureBrowsing

Home How does it work? Statistics Support About

## Finjan SecureBrowsing - Unified Web Security Solutions

Finjan SecureBrowsing provides you with safety ratings of URLs showing in your browser.

Utilizing innovative security technologies, proven in large enterprise environments, it helps keep you safe from online scams as you search and browse the web.

Internet Explorer Compatible

Firefox Compatible

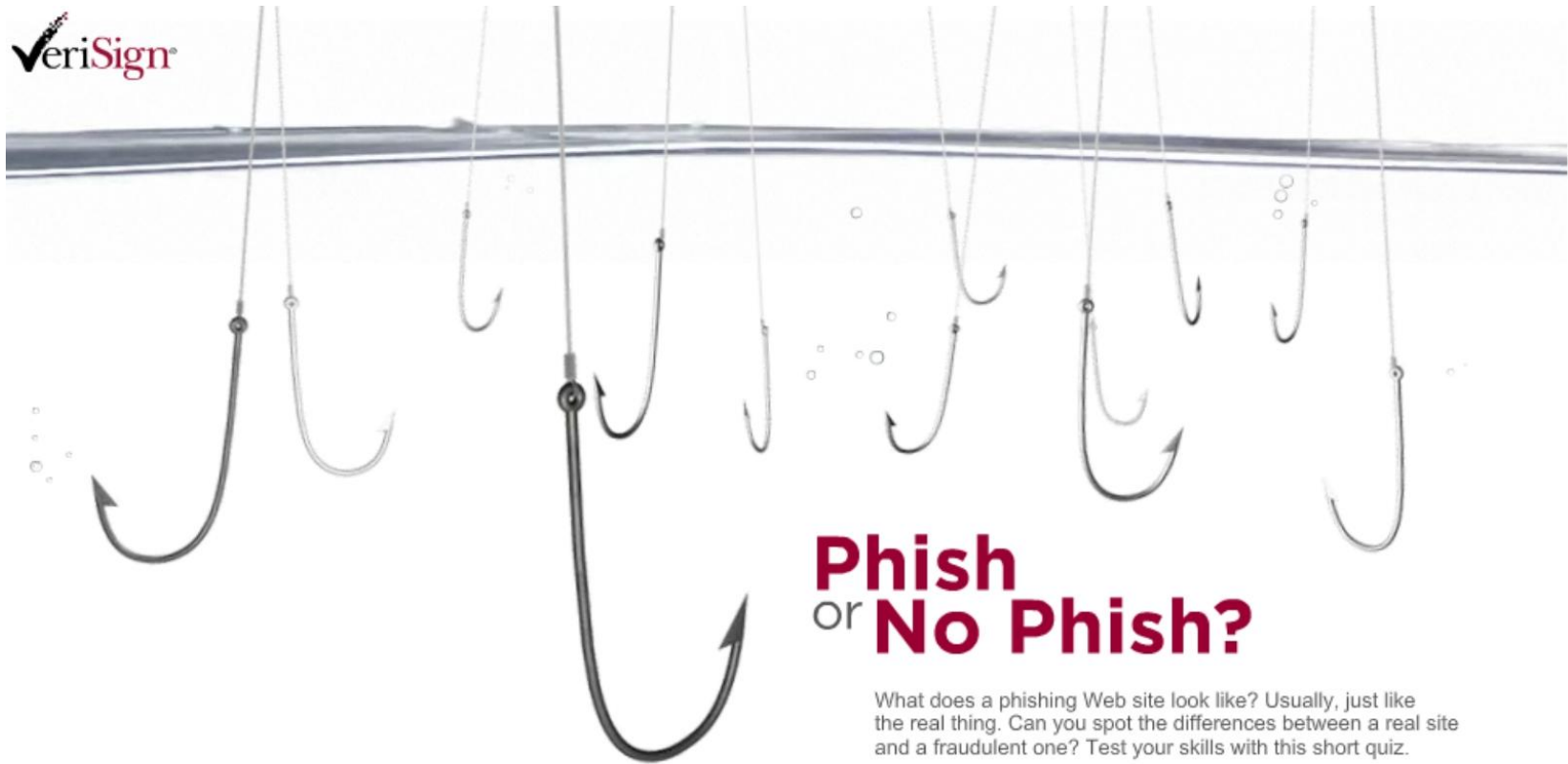
- The page is safe for browsing
- Page not available for scanning
- Use caution:** Potential spyware behavior was detected on this page

[learn more](#)

完成 網際網路 | 受保護模式: 關閉 100%

# 你上勾了嗎？

VeriSign



## Phish or No Phish?

What does a phishing Web site look like? Usually, just like the real thing. Can you spot the differences between a real site and a fraudulent one? Test your skills with this short quiz.

GET STARTED

<https://www.phish-no-phish.com/>

© 1995-2010 VeriSign, Inc. All rights reserved.



麟瑞科技  
RING LINE CORPORATION





# 哪一個網站有問題?

Trusted Bank - Microsoft Internet Explorer

File Edit View Favorites Tools Help

https://www.trusted-bank.com/secure/index.html

Trusted Bank

**This is a phishing site. But, it looks exactly like the real thing, doesn't it? Sometimes phishers mimic authentic Web sites perfectly. When this happens, there's only one way to verify that a site is real.**

Personal Banking | Small Business | Corporate Banking | Investment Services

Online Banking Sign In

Login

Username

Password

Sign In

Forgot your Account Number?

Sign In To Other Services

Online Investing

Go

Loans and Credit Lines  
Home Mortgage | Home Equity | Loans | Refinance | Student Loans | Auto Loans | Personal Loans | Personal Lines of Credit

Investments and Financial Management  
Investment Services | IRAs | Mutual Funds | Brokerage | Insurance | Private Consulting | Trust Services | 529 College Savings Plan | Learn about Investing

Financial Planning  
Saving and Budgeting | Tools and Calculators | Credit Management | Fraud Protection | Retirement | Investing | Estates | Taxes | Insurance

View Today's Rates

Mortgage

Go

About Us | Contact Us | Privacy Policy | Site Map | ABA/Routing Number  
© Trusted Bank and VeriSign, Inc. All rights reserved.

Local intranet

Trusted Bank - Microsoft Internet Explorer

File Edit View Favorites Tools Help

https://www.trustedbank.com/secure/index.html

Trusted Bank

TRUSTED BANK

Sign In | Help | Open An Account

Search

Personal Banking | Small Business | Corporate Banking | Investment Services

Online Banking Sign In

Login

Username

Password

Sign In

Forgot your Account Number?

Sign In To Other Services

Online Investing

Go

**Learn More About:**

Checking and Savings  
Checking Accounts | Savings | Accounts | CDs | Check Cards

Credit Cards and Prepaid Cards  
Credit Cards | Gift Cards | Your Online Credit Card Account | Credit Protection

Loans and Credit Lines  
Home Mortgage | Home Equity | Loans | Refinance | Student Loans | Auto Loans | Personal Loans | Personal Lines of Credit

Investments and Financial Management  
Investment Services | IRAs | Mutual Funds | Brokerage | Insurance | Private Consulting | Trust Services | 529 College Savings Plan | Learn about Investing

Financial Planning  
Saving and Budgeting | Tools and Calculators | Credit Management | Fraud Protection | Retirement | Investing | Estates | Taxes | Insurance

View Today's Rates

Mortgage

Go

About Us | Contact Us | Privacy Policy | Site Map | ABA/Routing Number  
© Trusted Bank and VeriSign, Inc. All rights reserved.

Local intranet





# 哪一個網站沒問題?

Trusted Bank - Microsoft Internet Explorer

File Edit View Favorites Tools Help

https://www.trustedbank.com/secure/index.html Trusted Bank Inc. [US]

Trusted Bank

TRUSTED BANK

Sign In | Open An Account | Search

Personal Banking | Small Business

Online Banking Sign In

Login

Username

Password

Sign In

Forgot your Account Number?

Sign In To Other Services

Online Investing

Go

About Us | Contact Us | Privacy Policy | Site Map | ABA/Routing Number

© Trusted Bank and VeriSign, Inc. All rights reserved.

Local intranet

The green address bar takes the guesswork out of identifying legitimate Web sites. Click Next to get your scores.

Trusted Bank - Microsoft Internet Explorer

File Edit View Favorites Tools Help

https://www.trusted-bank.com/secure/index.html

Trusted Bank

TRUSTED BANK

Sign In | Help | Open An Account | Search

Personal Banking | Small Business | Corporate Banking | Investment Services

Online Banking Sign In

Login

Username

Password

Sign In

Forgot your Account Number?

Sign In To Other Services

Online Investing

Go

About Us | Contact Us | Privacy Policy | Site Map | ABA/Routing Number

© Trusted Bank and VeriSign, Inc. All rights reserved.

Local intranet





# 並非每個網站都用 EV SSL

## 使用 EV 的安全網站專業版



### 真實 128 位元延伸驗證 SSL



使用最受信賴、最安全的 SSL 選擇，讓客戶放心地在線上購物：使用 EV 的 VeriSign® 安全網站專業版 SSL 憑證。延伸驗證可讓最新的高安全性 Web 瀏覽器顯示綠色網址列，而真實 128 位元 SSL 憑證則使每一位網站訪客都能夠體驗最強大的 SSL 加密。

- 延伸驗證，綠色網址列
- 最低 128 位元至 256 位元加密
- 250,000 美元保固
- VeriSign Secured® 全球安全網站認證標章
- 安裝檢查工具

#### 分開購買

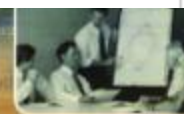
效期	價格
1 年	TW\$50,231
2 年	TW\$90,309 省下 \$10,153

購買

續約



麟瑞科技  
RING LINE CORPORATION



# 利用我的最愛

- ◉我的最愛是個很有用的東西



## 結論

---

- 社交工程利用的是人的弱點。
- 善用工具，降低網路社交工程危害。
- 除了工具，還有安全意識與警覺。



# Q & A

[Hoyeh\\_tsai@kh.ringline.com.tw](mailto:Hoyeh_tsai@kh.ringline.com.tw)

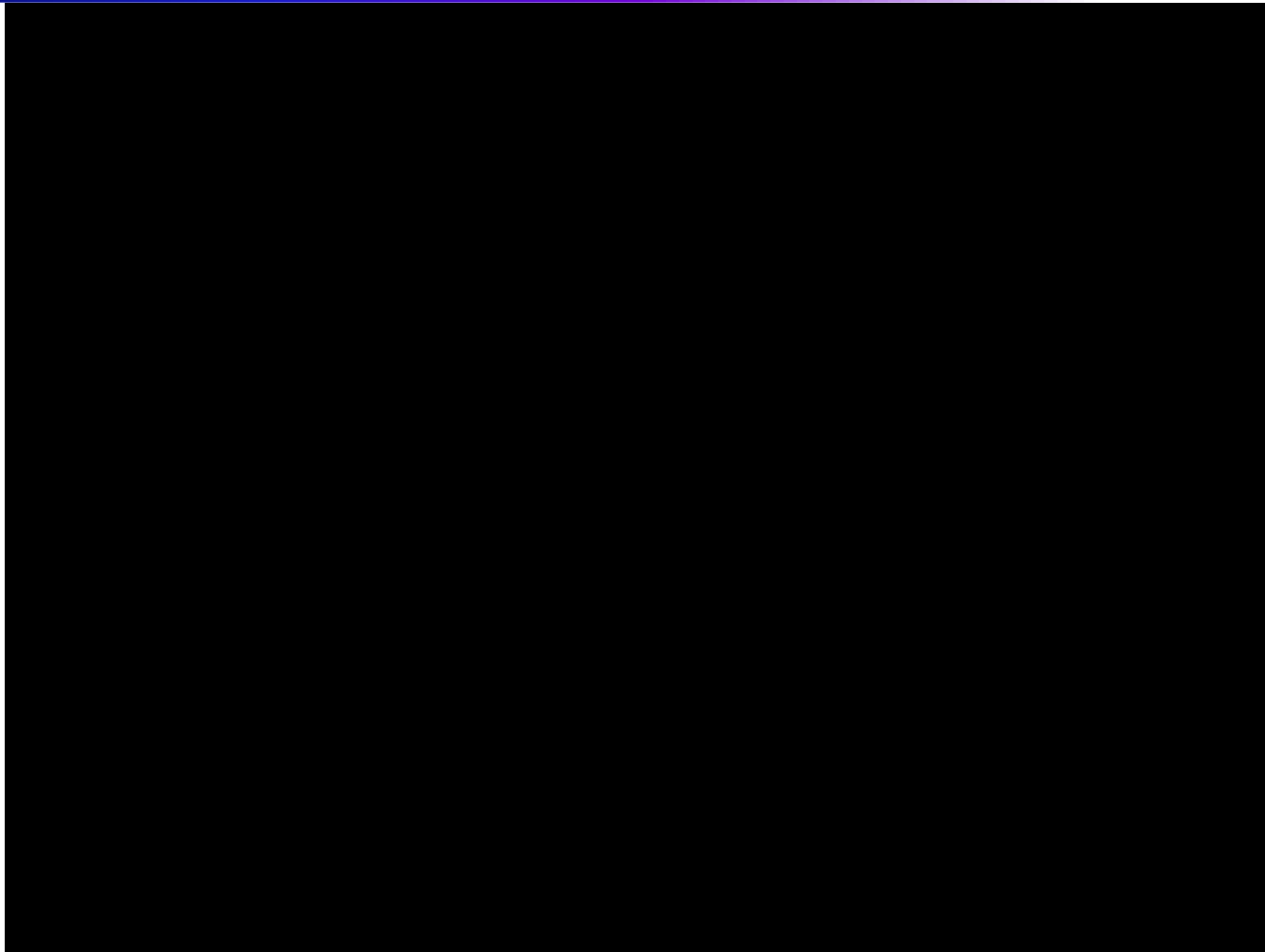


麟瑞科技  
RING LINE CORPORATION





# 希望您能分別真或假



麟瑞科技  
RING LINE CORPORATION

