主題：2019資安宣導

Ethan·Yang

近年資安趨勢

- 詐騙訊息無所不在
- 勒索軟體持續發威
- 物聯網設備資安威脅

  當東西都連上了網

  所有的事都與資安有關

- 駭客攻擊又快又準

美國又有兩個地方政府感染了勒索軟體

4月遭攻擊的德州波特郡政府決定自行修復系統，但目前只復原部份系統，造成許多員工無法上網、只能以紙筆方式來工作；而最新受害的巴爾的摩市政府，則是已經二度遭勒索軟體攻擊

文/ 陳曉莉 | 2019-05-09 發表

新聞

報導：駭客在黑市銷售近10億筆使用者資料

一名駭客從今年2月開始，陸續販售來自44個企業品牌的用戶個資，已五度釋出總共將近10億筆用戶資料，而且似乎還沒有停止的打算

文/ 陳曉莉 | 2019-04-16 發表

新聞

美國土安全部將官方機構修補重大漏洞的期限從30天縮短成15天

由於漏洞從揭露到遭受攻擊的時間間距愈來愈短，美國國土安全部頒布強制命令，要求聯邦機構必須在發現重大風險漏洞的15天內完成修補，而高度風險漏洞的修補期限則是30天

文/ 陳曉莉 | 2019-05-01 發表

Binding Operational Directive 19-02

April 29, 2019

Vulnerability Remediation Requirements for Internet-Accessible Systems

This page contains a web-friendly version of the Cybersecurity and Infrastructure Security Agency's Binding Operational Directive 19-02, *"Vulnerability Remediation Requirements for Internet-Accessible Systems"*.

A binding operational directive is a compulsory direction to federal, executive branch, departments and agencies for purposes of safeguarding federal information and information systems.

Section 3553(b)(2) of title 44, U.S. Code, authorizes the Secretary of the Department of Homeland Security (DHS) to develop and oversee the implementation of binding operational directives.

Federal agencies are required to comply with DHS-developed directives.

These directives do not apply to statutorily defined "national security systems" nor to certain systems operated by the Department of Defense or the Intelligence Community.

大綱

- 資訊安全概述
- 上網與社群媒體安全
- 郵件社交工程攻防實務
- 行動裝置攻防實務

資訊安全概述

資訊安全

資訊資產包含哪些內涵

- **資訊資產包含五類**
  - 人員、硬體、軟體、資料、文件
- **資訊安全的目的在保護資訊資產之**
  - 機密性 /Confidentiality
  - 完整性 / Integrity
  - 可用性 / Availability

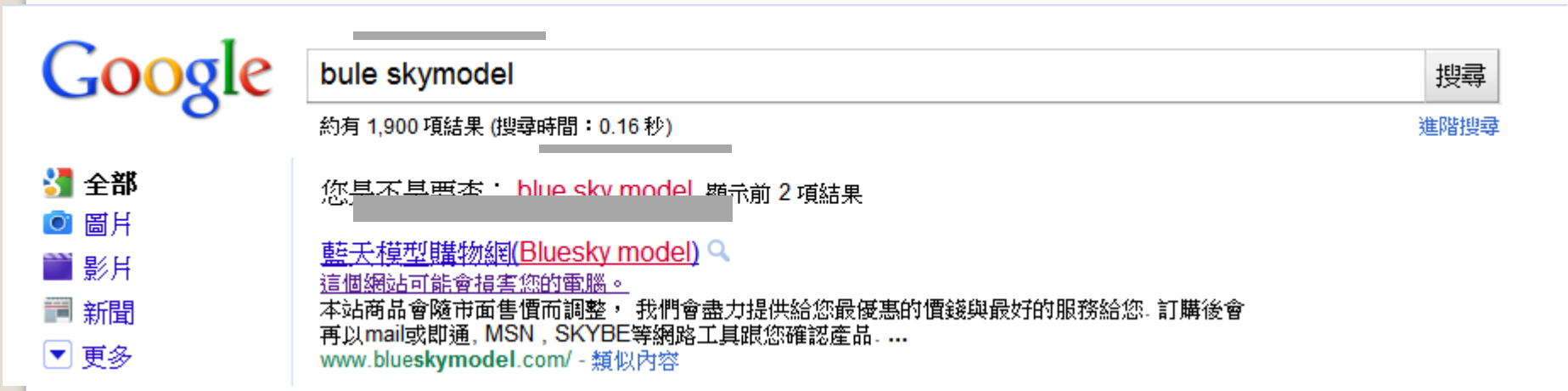
資訊資產

分組

上網與社群媒體安全

搜尋引擎安全嗎????

- Google會過濾搜尋出有問題的網站提示



警告- 造訪這個網站可能會損害您的電腦！

建議：

- 返回上頁並選擇其他結果。
- 嘗試其他搜尋方式以尋找所需資訊。

或者您也可以繼續前往 http://www.blueskymodel.com/ ，但風險需自行承擔。 如需有關我們所發現問題的詳細資訊，請造訪 Google 針對此網頁所產生的安全瀏覽診斷網頁。

如需進一步瞭解如何保護自己免在線上受到有害軟體的侵擾，請造訪 StopBadware.org 。

如果您是網站的擁有者，可以要求使用 Google 的網站管理員工具審查您的網站。 如需更多關於審查程序的資訊，請前往 Google 的網站管理員說明中心。

諮詢提供者：Google

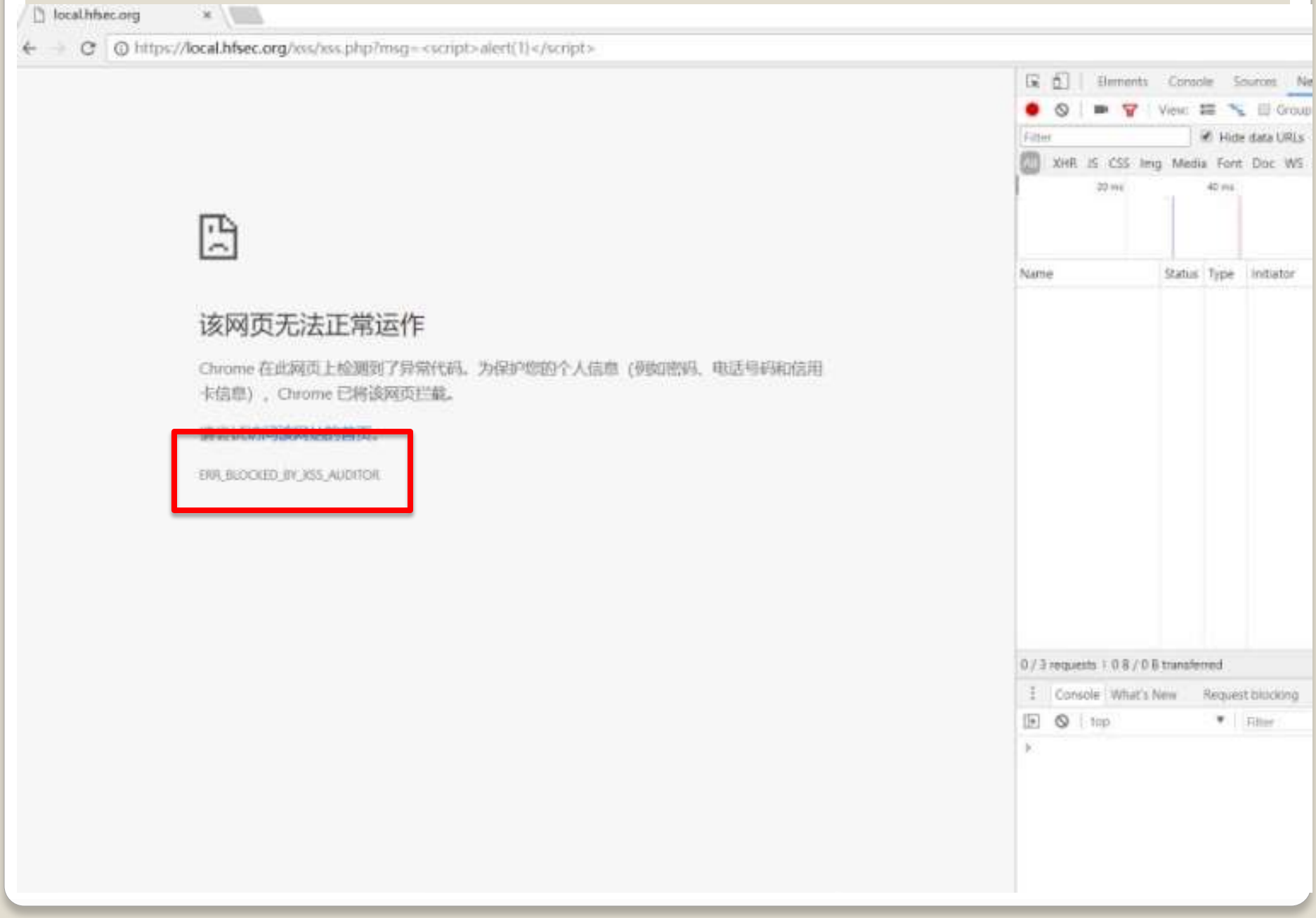
搜尋結果?廣告?


Google
所有網頁 圖片 新聞 網上論壇 更多 »
拍賣
搜尋
進階搜尋 | 使用偏好
搜尋所有網站 搜尋所有中文網頁 搜尋繁體中文網頁
所有網頁
Yahoo!奇摩拍賣
tw.bids-yahoo.com 物品交換中心,提供中古、新品、收藏品 Yahoo!奇摩拍賣玩FUN館Blog 參觀Blog
Yahoo!奇摩拍賣:拍賣,包括:精品,電腦,手機,數位相機,mp3,美容,中古車 ...
什麼都有、什麼都賣,名牌精品、電腦、手機、數位相機、電玩遊戲、中古車二手車、mp3、
美容保養品,歡迎來網拍挖寶!
tw.bid.yahoo.com/ - 62k - 2007年7月30日 - 頁庫存檔 - 類似網頁
Yahoo!奇摩拍賣:拍賣,包括:精品,電腦,手機,數位相機,mp3,美容,中古車 ...
五年級的廖瑞鳳談起網拍賣書,是一連串的偶然促成,去年她擔心健康問題,結束了化學工廠的
工作,但二度就業婦女在主客觀條件上,在職場呈現相當的弱勢,就這樣她開始嘗試網路拍賣~
詳細內容. 活動特輯. 成交滿$100 現刮50萬大獎 集金A! ...

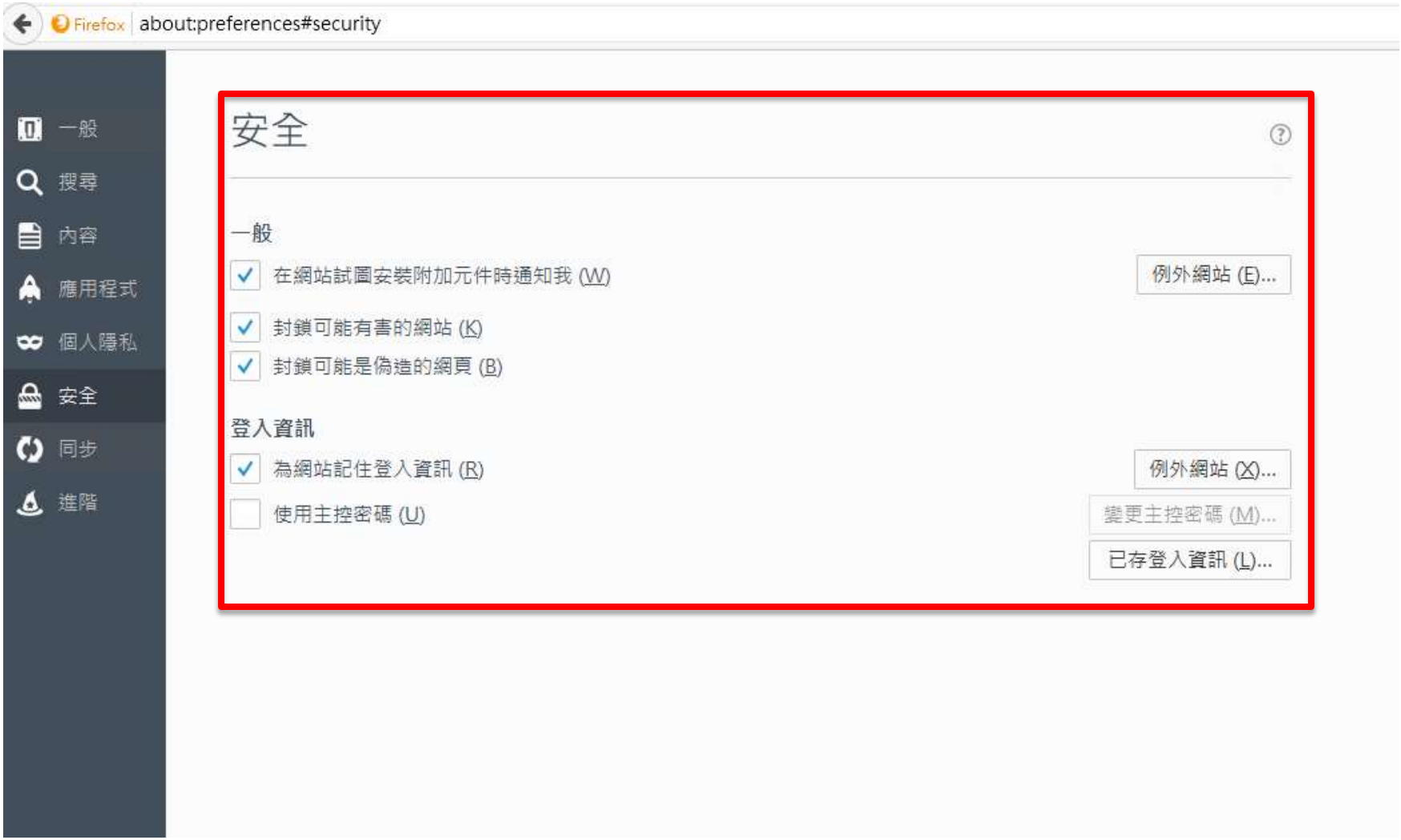
瀏覽器安全

- 上網瀏覽網頁，會用到的瀏覽器
- 瀏覽器能幫你做什麼呢??????????



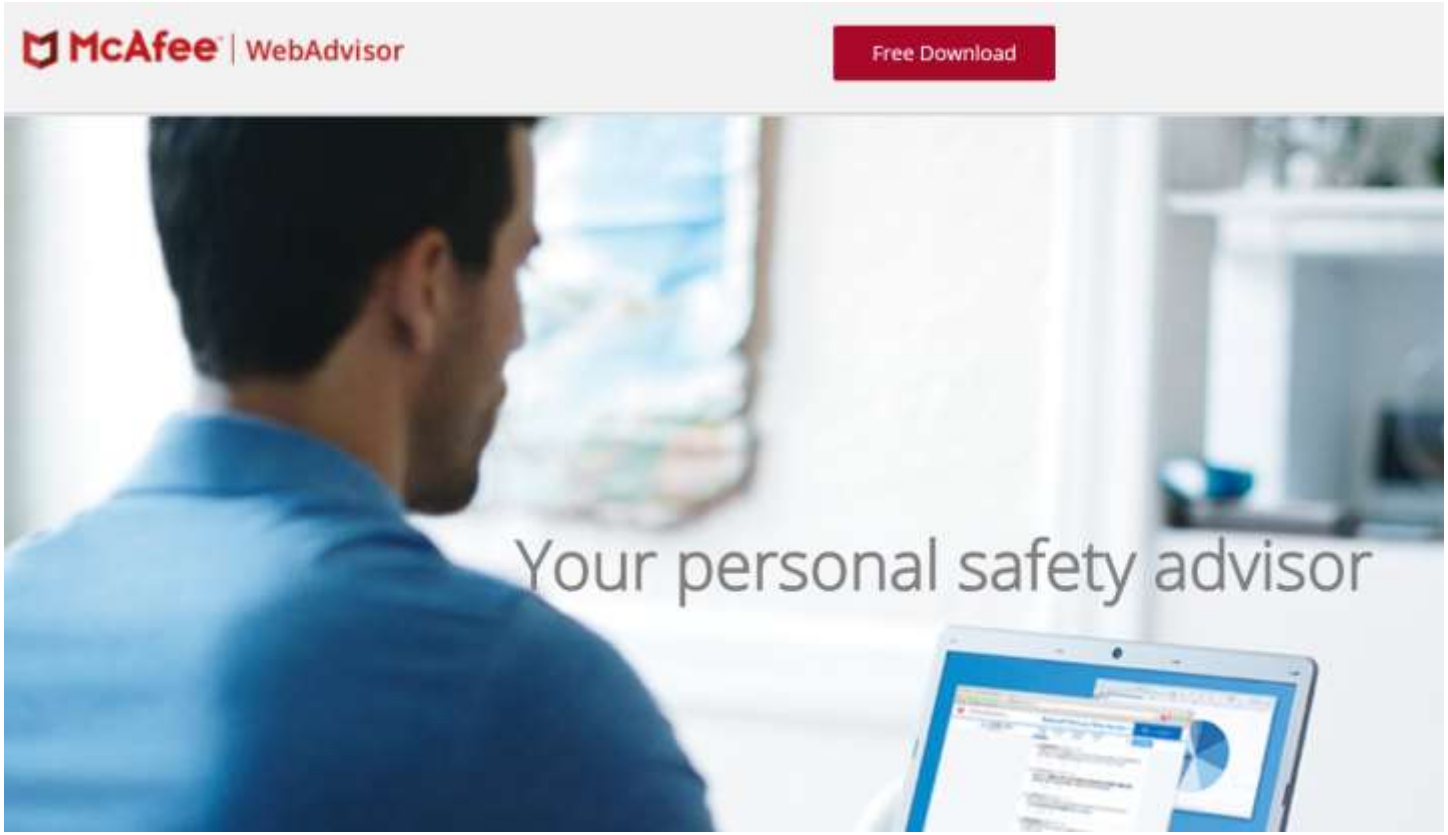

local.hfsec.org
https://local.hfsec.org/xss/xss.php?msg=<script>alert(1)</script>
该网页无法正常运作
Chrome 在此网页上检测到了异常代码。为保护您的个人信息（例如密码、电话号码和信用卡信息），Chrome 已将该网页拦截。
ERR_BLOCKED_BY_XSS_AUDITOR
Elements
Console
Sources
Hide data URLs
XHR JS CSS Img Media Font Doc WS
Name
Status
Type
Initiator
0 / 3 requests | 0 B / 0 B transferred
Console
What's New
Request blocking
top

瀏覽器安全設置


Firefox
about:preferences#security
一般
搜尋
內容
應用程式
個人隱私
安全
同步
進階
安全
一般
在網站試圖安裝附加元件時通知我 (W)
例外網站 (E)...
封鎖可能有害的網站 (K)
封鎖可能是偽造的網頁 (B)
登入資訊
為網站記住登入資訊 (R)
例外網站 (X)...
使用主控密碼 (U)
變更主控密碼 (M)...
已存登入資訊 (L)...

瀏覽器安全(InterExplorer)(Firefox)(Chrome)

- McAfee-網路釣魚軟體
  - 下載網址： www.siteadvisor.com




Google
皓鑭傳
https://baike.baidu.com/item/皓镧传 ▾ 轉為繁體網頁
《皓镧传》是欢娱影视、爱奇艺、腾讯影业、火凤燎原出品，李达超执导的古装剧情剧，由吴谨言、茅子俊、聂远、海铃、宁静、王志飞、谭卓、洪尧、姜梓新等主演。该剧讲述 ...
每集长度: 40分钟 首播时间: 2019年1月19日
集数: 62集/62集 制片人: 于正
皓鑭傳(雙語版) - 主頁- tvb.com
programme.tvb.com/drama/legendofhaolanthe0002/ ▾
2019年2月4日 - 皓鑭為救回小春，願意用少妃的秘密來換，她發現少妃在布帛寫的是韓在趙的細作名單。秦王孫覺得疑點重重，應該是少妃故... (更多). 播出日期: ...
「皓鑭」草草完結挨批網友挖出「真正結局」慘遭斷尾| 電視| 噓！星聞
https://stars.udn.com › 電視 ▾
6 天前 - 聶遠與吳謹言再續「延禧攻略」前緣之作「皓鑭傳」20日播出完結篇，最終飾演「呂不韋」的聶遠被貶，「皓鑭」吳謹言不知所蹤，並用字幕帶過嬴政成為「 ...
皓鑭傳劇集列表CN190119 List - Love TV Show 大陸電視劇
cn.lovetvshow.info/2019/01/cn190119-list.html ▾
皓鑭傳劇集列表CN190119 List. 皓鑭傳第62集大結局CN190119 Ep62 · 皓鑭傳第61集CN190119 Ep61 · 皓鑭傳第60集CN190119 Ep60 · 皓鑭傳第59集CN190119 ...

史萊姆

原作: 伏瀬　　出版社: 微雜誌社（日语：マイクロマガジン社）

作品概要 · 角色 · 設定

關於我轉生後成為史萊姆的那件事 - 在線看漫畫

https://tw.manhuagui.com/comic/17023/

本以為自己被人用刀刺死了，沒想到卻在異世界轉生成史萊姆？以能夠奪取對手能力的「捕食者」與精通世界真理的「大賢者」這兩樣獨有技為武器，史萊姆的大冒險即將 ...

關於我轉生後成為史萊姆的那件 ... · 第47回 · 第49話 · 川上泰樹

史萊姆的第一個家

www.slime.com.tw/

Gom Player v2.3.38.5300 中文版來了！免費而且功能完整的影片播放軟體，內建解碼器支援大多數的影片格式，有不能看的影片嗎？試試這套軟體。

軟體下載 - 史萊姆的第一個家

www.slime.com.tw/download.html

大家是否有經驗,知道軟體檔名卻不知道要去那下載! 告訴你一個小訣竅,你可以利用以下的檔案搜尋系統查出那裡可以下載! 中央大學Archie檔案搜尋 · 國立中山大學 ...

播放清單

影片

活動

貼文

關於

社群

相片

資訊和廣告

理科太太 Li Ke Tai Tai

昨天下午12:00 ·

你準備好連假要去哪裡出遊塞車了嗎？
被理科太太感化的你，想帶環保杯出遊
但不確定塵封已久的杯子還能不能用？
今天太太除了秀出私人收藏癖好
附贈號稱味覺靈敏的先生出演「舌尖上的飲料」

關於理科先生送的情人節禮物
https://youtu.be/TtnluzLGxgk

.

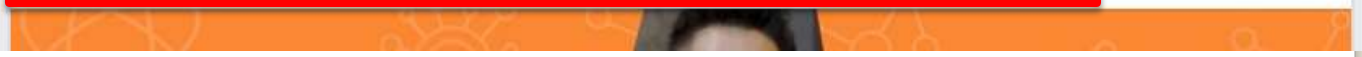
這次影片在 Youtube 上看
https://youtu.be/xQlVjj_20Gg

.

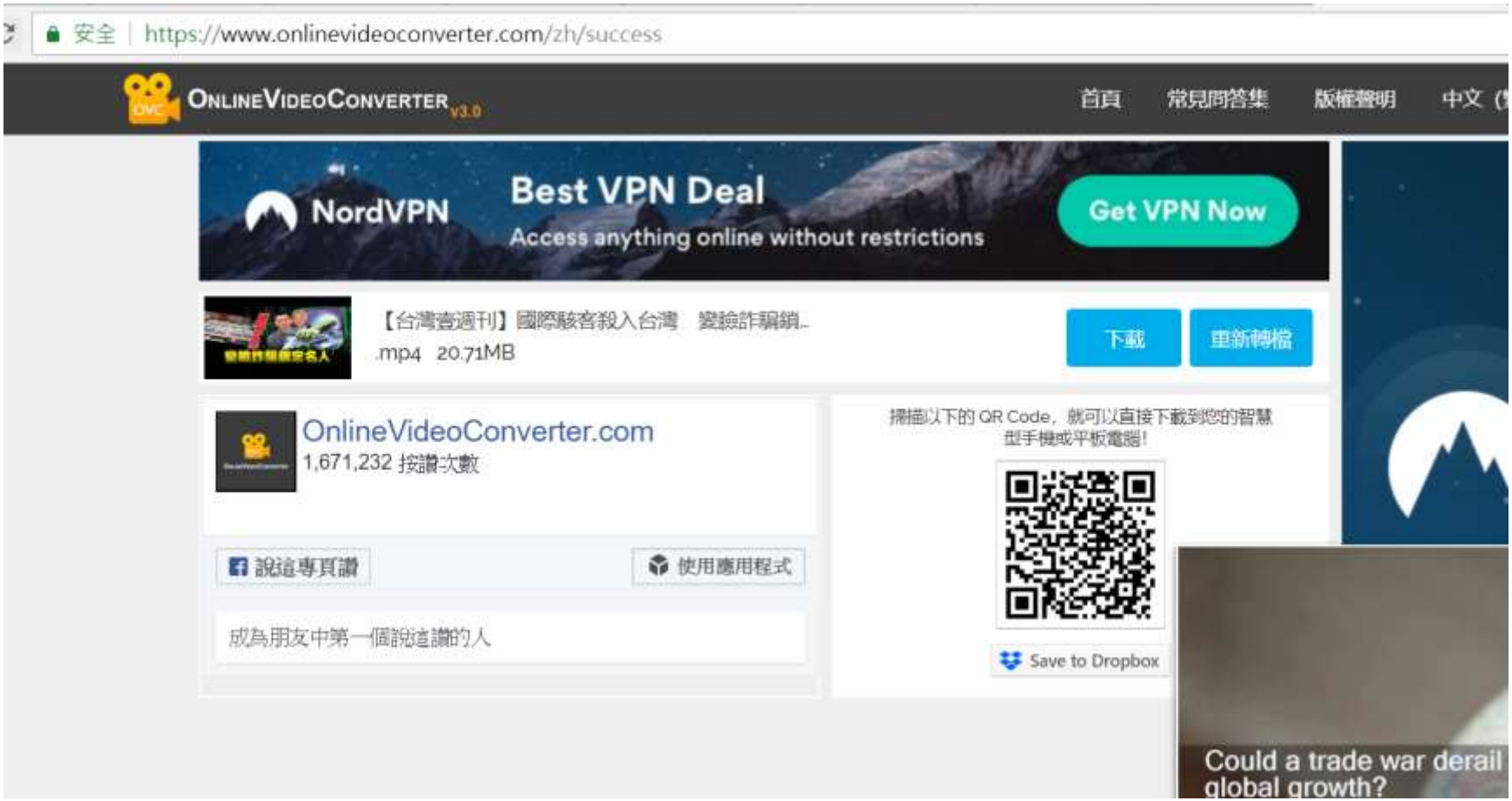
理科太太的IG很好看
https://www.instagram.com/liketaitai/

.

理科太太Youtube有花絮
https://www.youtube.com/liketaitai?sub_confirmation=1



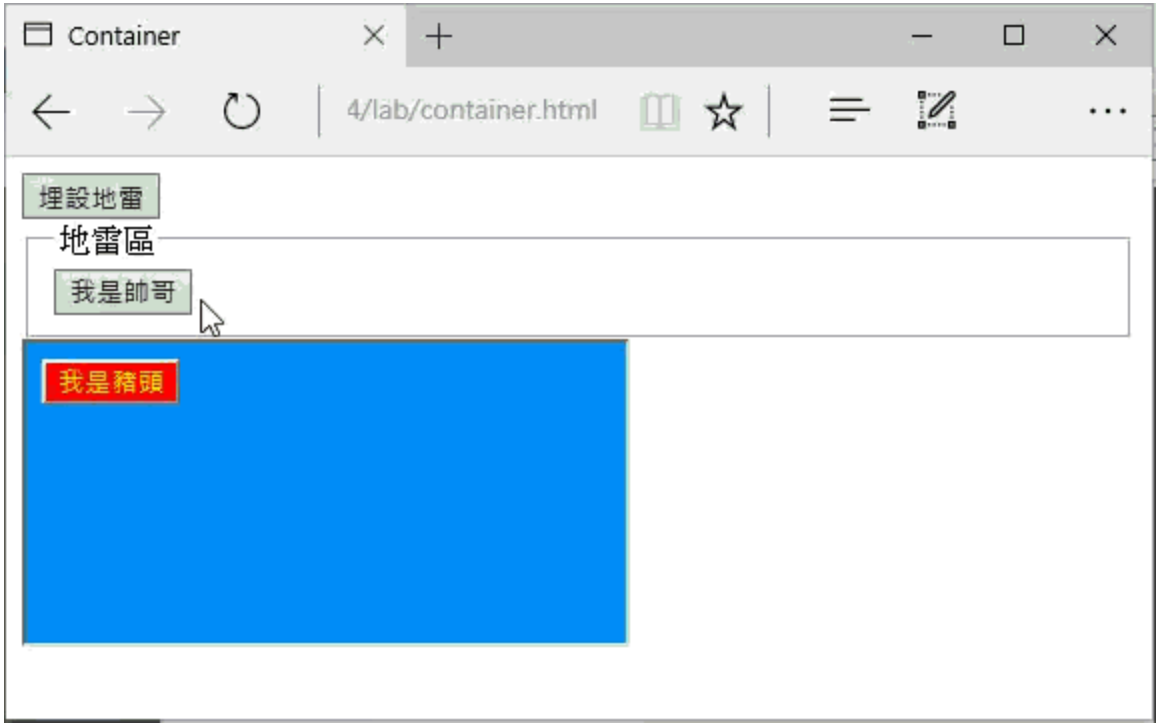
到底點到了什麼?


安全 | https://www.onlinevideoconverter.com/zh/success
OnlineVideoConverter v3.0
首頁
常見問答集
版權聲明
中文
NordVPN
Best VPN Deal
Access anything online without restrictions
Get VPN Now
【台灣壹週刊】國際駭客殺入台灣 變臉詐騙鎖...
.mp4 20.71MB
下載
重新轉檔
OnlineVideoConverter.com
1,671,232 按讚次數
說這專頁讚
使用應用程式
成為朋友中第一個說這讚的人
掃描以下的 QR Code，就可以直接下載到您的智慧型手機或平板電腦!
Save to Dropbox
Could a trade war derail global growth?

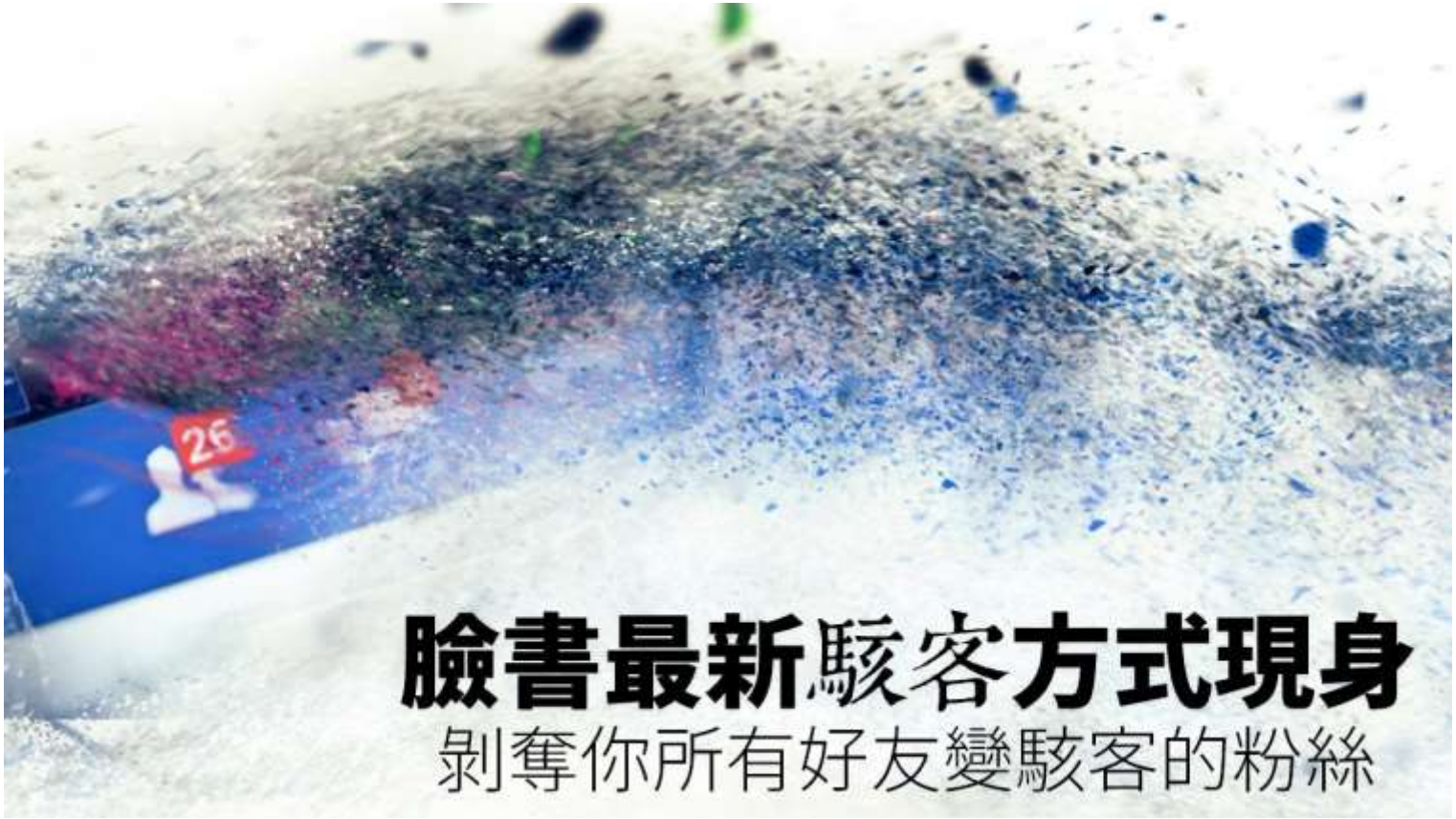
到底點到了什麼?


不安全 d4pzns404w1ni.cloudfront.net/WinLander_Multi_4/index.html?&ip=114.46.217.133&lang=zh&filename=Win%20Speedup%202018&domain=diraqi-...
Microsoft
Store
Products
Support
Search Microsoft.com
Windows
Security Scan
d4pzns404w1ni.cloudfront.net 顯示
需要立即行動
我們在您的PC上偵測到一個木馬病毒 (e.tre456_worm_Windows)。
點選「好」開始修復程序。
確定
您的系統
114.46.217.133
2018年9月2日星期日 11:55
您的PC感染了 3 病毒。我們的安全檢查發現了 2 惡意軟體和 1 釣魚/間諜軟體。系統損毀：28.1%。需要立即移除！
需要立即移除病毒，避免系統進一步損毀，應用、相片或其他檔案丟失。
發現 1 您的PC 上有釣魚/間諜軟體。 Windows.
您的個人資料和銀行資料有危險。
為避免更多損毀，請即刻點選「立即掃描」。我們的深度掃描將立即為您提供幫助！
4 分 14 秒剩餘，此後將永久損毀。
立即掃描 >>

到底點到了什麼?



臉書駭客手法
「奪舍」！讓你的帳號變空殼



臉書駭客手法
「奪舍」！讓你的帳號變空殼

臉書最新駭客手法

所有朋友被併吞、個人帳號變殘廢

盜用帳號→改名成「Kan World」
→把你的帳號變粉絲團→合併掉你

- 駭客第一步：盜用帳號
  - 今天之所以將這危險稱之為「駭客手法」而不是「臉書漏洞」，是因為駭客必須先成功盜用你的臉書帳號、獲得存取權，才能進行下一步動作。而盜用的手法，不外乎「釣魚網站騙使用者輸入帳號密碼」、「騙你下載瀏覽器外掛，安裝就中毒」、「在不安全的地方使用電腦」、「鍵盤側錄程式」、「電腦本身就中毒」等等。

臉書駭客手法
「奪舍」！讓你的帳號變空殼

- 駭客第二步：幫你改名
  - 駭客通常是利用「更改多語言姓名」方式幫你新增一個名字，例如「Kan World」，這個名字通常跟駭客在經營的粉絲團一樣或接近。
  - 臉書帳號除了我們常用的中文姓名外，還可以新增更多組姓名、例如匿名或「多語言姓名」。當駭客篡改你的多語言姓名時，你很可能根本無法察覺：因為對台灣人而言，帳號看上去完全沒變！
  - 檢查方式：進入「你的臉書個人頁／關於／有關你的詳細資料」，看看別名的地方，有沒有出現陌生的名字？如果出現了，快點點擊「選項／刪除」移除掉它，然後修改你的臉書密碼。

臉書駭客手法
「奪舍」！讓你的帳號變空殼

- 駭客第三步：把你的帳號申請成為粉絲團
  - 這一步是最狠的！因為一旦申請通過了，帳號持有人是沒有回頭路的。你的帳號從此就變成了一個「粉絲團管理中心」，你的朋友都會變粉絲團的粉絲，而不是私密好友。

臉書駭客手法
「奪舍」！讓你的帳號變空殼

- 駭客第四步：合併掉你！
  - 如果你以為，個人帳號被轉變成粉絲頁已經夠淒慘，那就大錯特錯了。別忘了，駭客之前已經幫你改名成「Kan World」，他們會先將他們自己也設定為粉絲專頁的管理員，再利用臉書提供的「合併重複的粉絲專頁」功能，將你的粉絲頁（裡面的粉絲都是你原來的好友）合併到他的粉絲頁去。
  - 於是，你的臉書帳號就像被「奪舍」一樣，你的好友全部被駭客給「吃掉、併吞」，變成駭客的粉絲；而你的臉書帳號，則什麼也不剩，沒辦法去朋友那邊留言、也沒辦法變回原來的樣子（這個動作是不可逆的）。

臉書駭客手法
「奪舍」！讓你的帳號變空殼

臉書駭客手法
「奪舍」！讓你的帳號變空殼

臉書駭客手法
「奪舍」！讓你的帳號變空殼

LINE安全設定

LINE個人資料安全設定1

- 取消自動加入好友功能
- 取消允許被加入好友選項

LINE個人資料安全設定2

- 隱私設定中取消公開ID

LINE個人資料安全設定3

- 於我的帳號中，如無使用個人電腦登入LINE，應取消允許自其他裝置登入

免費的麥當當?!


麥當當
讚
追蹤
分享
麥當當
8月21日下午6:01
歡慶麥當勞50週年 回饋消費者活動開始!!
想要領取免費套餐嗎？
活動辦法:
1.按讚並公開分享此篇文章
2.tag好友並底下留言 #我愛麥當勞…… 更多
麥當當
首頁
貼文
相片
社群
關於
資訊和廣告
建立粉絲專頁
超值午/晚餐
$0
麥當勞陪你抗漲
超值晚餐$0起
晚餐同享超值午餐優惠價
11:00~14:00
超值午餐長期供應
17:00~20:00
超值晚餐限期優惠

免費的麥當當?!


麥當當
50 years of Big Mac
麥當當
首頁
貼文
相片
社群
關於
資訊和廣告
Create Post
Write a post...
相片/影片
標註朋友
打卡
麥當勞
@mcdonalds.tw
首頁
評論
相片
分店地點
貼文
影片
活動
關於
分享

信義房屋

3 小時 ·

說這專頁讚

#信義房屋
感謝大眾一直以來的支持
為了回饋社會大眾拚命台灣經濟

#回饋社會大眾
本公司贊助送出
信義房屋 新北市精華地段 (40~45坪) 2間

抽房子說明:
只要在文章底下留言對信義的感想
5/30 將會從留言裡抽出2為幸運兒過戶房屋

沒有天上掉下來的房子 房仲、建商臉書遭盜用

2019-05-17 00:20 經濟日報 記者黃阡阡／即時報導

駭客這回瞄準房仲、建商！今（16）日有不肖業者假冒信義房屋臉書粉絲團，自稱感謝大眾支持，並舉辦留言「抽獎送房子活動」，另外，遠雄、潤泰也遭同樣的手法盜用。

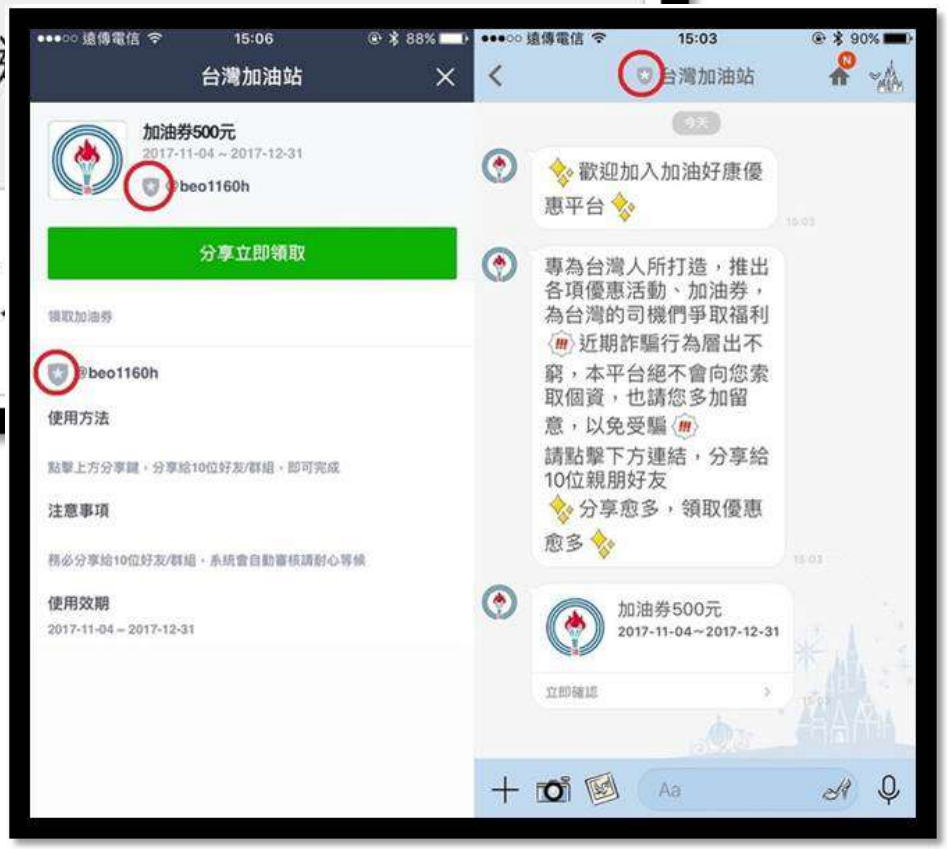
對此，信義房屋表示，並無舉辦任何抽獎活動，粉絲團遭到盜用，呼籲消費者勿受騙上當，並已報警處理，盜用臉書粉絲團者勿以身試法。

信義房屋表示，該假冒的粉絲團盜用信義房屋官方粉絲團大頭貼照片，並舉辦抽獎活動，只要消費者留下對信義房屋感想即可抽出二位民眾，過戶新北市精華地段房屋(40~45坪房屋)，該活動更吸引超過600多則留言，顯然已有許多民眾受騙上當。

LINE的真真假假

LINE的真真假假

	官方帳號	通過LINE審核、認證且有購買官方帳號服務的廠商
	認證帳號	通
	一般帳號	任何



ofacts 真的假的 | 轉傳..

看起來很可疑的謠言傳給我找解答

98,032

MedPartner美的好朋友

小幫手全新上線為你服務!

趨勢科技防詐達人

辨識！假的網購免費貼圖好康謠言

騙

,561

MyGoPen | 訊息查證

「擋騙」真人一對一幫你破解詐騙

110,012

美玉姨

諸君，我最喜歡八卦了!

119,259

趨勢科技防詐達人


18
好朋友
今天
免費會動的蠟筆小新
貼圖下載:
官方貼圖
免費領取!活動只
到今天!
下午2:37
下午2:42
Aa


24
好朋友
複製
Keep
刪除
回覆
轉傳
記事本
設為公告
長按轉傳
免費會動的蠟
貼圖下載:
官方貼圖
免費領取!活動只
到今天!
下午2:37
下午2:42
Aa

趨勢科技防詐達人


防詐達人
完成
趨勢科技防詐達人
趨勢科...
2
趨勢科技防詐達人
免費啓動的蠟筆小新貼圖下載:
官方貼圖
免費領取!活動只到今天!
NO!
汪！危險！訊息或網頁內有不安全連結。
Aa

趨勢科技防詐達人


年中巨獻，下單立減，全場滿2000
複製網址
Alibaka
4K
高清數位攝影機
3折激殺
【日本原裝進口】高性能4K高清數位攝像機，4K高清錄製，蔡司鏡頭，高倍變焦，五軸防抖，內置投影儀，夜視功能，全球聯保！【破盤下殺：第二件立減NT$1000】
首頁
客服
加入購物車
立即搶購 >
臉書廣告 退貨自救聯盟的貼文
讚
留言
分享
113
趨勢科技防詐達人
到Line貼上網址
【日本進口】高...
【日本原裝進口】
高性能4K高清數...
NO!
下午2:31
汪！危險！訊息或網頁內有不安全連結。
下午2:31
使用說明 | 分享給好友

趨勢科技防詐達人


164
好朋友群組(252)
下午2:52
趨勢科技防詐達人加入群組
將防詐打人加入群組
【日本進口】高...
【日本原裝進口】
高性能4K高清數...
已讀1
下午2:52
趨勢科技防詐達人
NO!
下午2:52
趨勢科技防詐達人
Aa


164
好朋友群組(252)
【日本進口】高...
【日本原裝進口】
高性能4K高清數...
已讀1
下午2:52
趨勢科技防詐達人
NO!
網站不安全時會自動出現警告
趨勢科技防詐達人
汪！危險！好朋友傳送的訊息或網頁內有不安全連結。
下午2:52
Aa

趨勢科技防詐達人

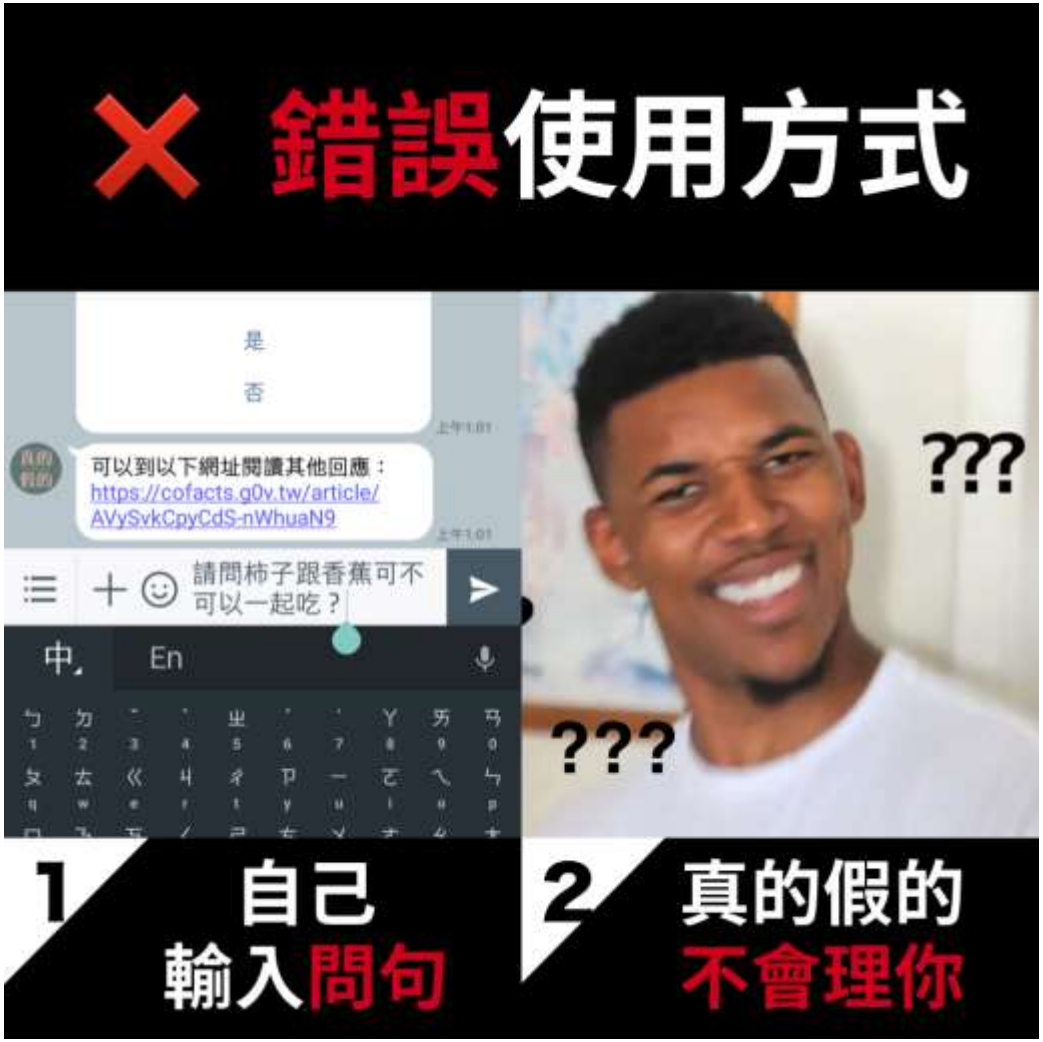

趨勢科技防詐達人
如果您覺得這不是安全連結，請回報給防詐達人。
感謝您，汪!
立即回報
點選立即回報
汪，您回報了:
感謝您 汪!
臉書廣告 退貨...
臉書各大社團都有的 #詐騙廣告 #臉...
上午11:36
使用說明 | 分享給好友

美玉姨


美玉姨
聊天
推薦
主頁
中華電信
下午3:15
23
美玉姨
炸了！致癌麥片風靡160多個國家？你吃的早餐，竟然危害這麼大？
已讀
下午4:55
這是謠言。
這是謠言理由🔎:
假的。不合格、有疑慮的蒸麥產品，自從2017年1月1日起就沒有輸入台灣的紀錄，而且台灣方面的檢驗規定草甘膦／嘉磷塞的殘留標準為「不得檢出」，所以吃麥片沒有致癌的疑慮。
https://www.rumtoast.com/10059/炸了！-致癌麥片風靡160多個國家-？dewayne-johnson罹癌原因跟吃
這是謠言理由🔎:
台灣事實查核中心已證實為部分錯誤資訊：
一、傳聞提及的美國人Dewayne Johnson確有其人，但其罹癌原因是工作上長期接觸除草劑中的草甘膦，並不是
Aa

《Cofacts 真的假的》

《Cofacts 真的假的》



《MyGoPen 訊息查證》

- 澄清謠言、破解詐騙、提供真實資訊及教學。可傳送可疑內容到 line，《MyGoPen》會在另一端做即時查核及回覆，但因為是真人一對一聊天，回覆速度相較於聊天機器人慢。

郵件社交工程攻防實務

郵件社交工程的定義

- 社交工程是什麼？
- E-mail社交工程攻擊方法及流程
- 社交工程信件的類型

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。

電話詐騙

- 常見電話詐騙內容
  - 你的小孩被綁架了！
  - 你的銀行帳戶被盜用了！
- 針對信用卡資訊的互動語音攻擊
  - 互動式的電話語音服務，也成為惡意人士嶄新的詐騙手法之一，歹徒利用從各種管道蒐集來的電話號碼，再透過完全自動化的語音系統，主動打電話給毫無防備的受害者，在大多數的情況之下，受害者因為擔心自己的信用卡被盜刷，就會依照語音的指示輸入相關資訊，包括信用卡號、有效日期和卡片背面的3位數安全碼，讓重要的個人信用卡資料落入壞人之手

不用技術也可以當駭客 – 只要打電話

駭客所需要的資訊

- 被害人姓名
- 被害人地址
- 被害人的亞馬遜email address
- 被害人的apple email addree

駭客打的第一通電話

想要在帳號中多增加一組信用卡號碼

請提供姓名、地址和email

提供被害人姓名、地址、email及任一組信用卡卡號

亞馬遜客服人員

新增信用卡卡號完成

駭客

駭客打的第二通電話

帳號遺失

請提供姓名、地址及信用卡卡號

提供被害人姓名、地址、及之前假冒的信用卡卡號

亞馬遜客服人員

註冊了一個新的電子郵件帳號，重設密碼，侵入被害人帳號，看到帳號底下所有的信用卡號末四碼

駭客

駭客打的第三通電話

要求重設 被害人iCloud電子郵件帳號

請回答安全認證問題

忘記了

請回答地址與信用卡末四碼

蘋果
客服人員

被害人的地址與信用卡末四碼

駭客

iCloud 帳號的暫時性密碼

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)

釣魚範本-人生就是跟自己賽跑

- 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賽跑為議題，以垃圾信件的大量發送手法發送測試信件於使用者

- 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

釣魚範本—有趣類型精彩畫庫

- 有趣類型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有趣內容的電子郵件，引誘使用者閱讀電子郵件甚至點擊內文中的超連結

- 對於有趣類型的電子郵件，攻擊者常常利用使用者認為此封信件很有趣幽默詼諧，進而轉寄，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

釣魚範本--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

釣魚範本--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

〔記者李悟宏／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。

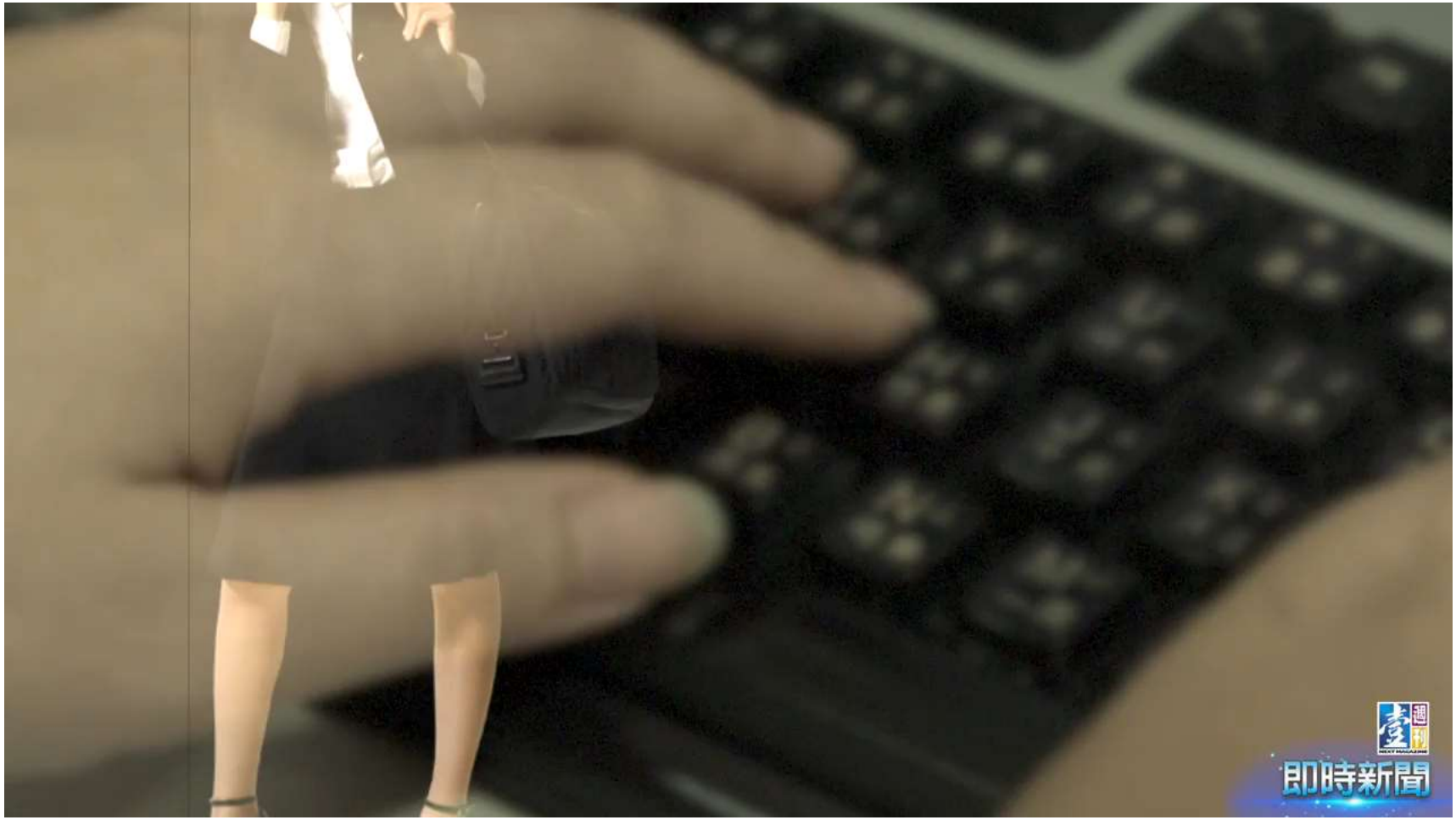
衛生局表示，根據統計，約有70%的癮君子曾嘗試戒菸，但因為毅志力不足，誘因太多及缺乏醫療專業指導，以致多數人的戒菸計畫功敗垂成。

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]

變臉詐騙



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，所以若是有做漂亮的信件，將會看不到！

收件匣 - Windows Live Mail

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

ESET NOD32 Antivirus

新增 回覆 全部回覆 轉寄 新增至行事曆 刪除 垃圾郵件 同步處理 登入

快速檢視

未讀取的郵件

連絡人的未讀取郵件

未讀取的摘要 (23)

Yniewu (ynie)

收件匣

草稿

寄件備份

垃圾郵件

刪除的郵件

寄件匣

新增電子郵件帳戶

郵件

行事曆

連絡人

摘要

新聞群組

尋找郵件

排序方式: 日期 遞減

下午 03:31
瑤瑤出新專輯囉^^~請大家多多支持

k1 2010/9/10
晚安您好

k1 2010/9/10
test

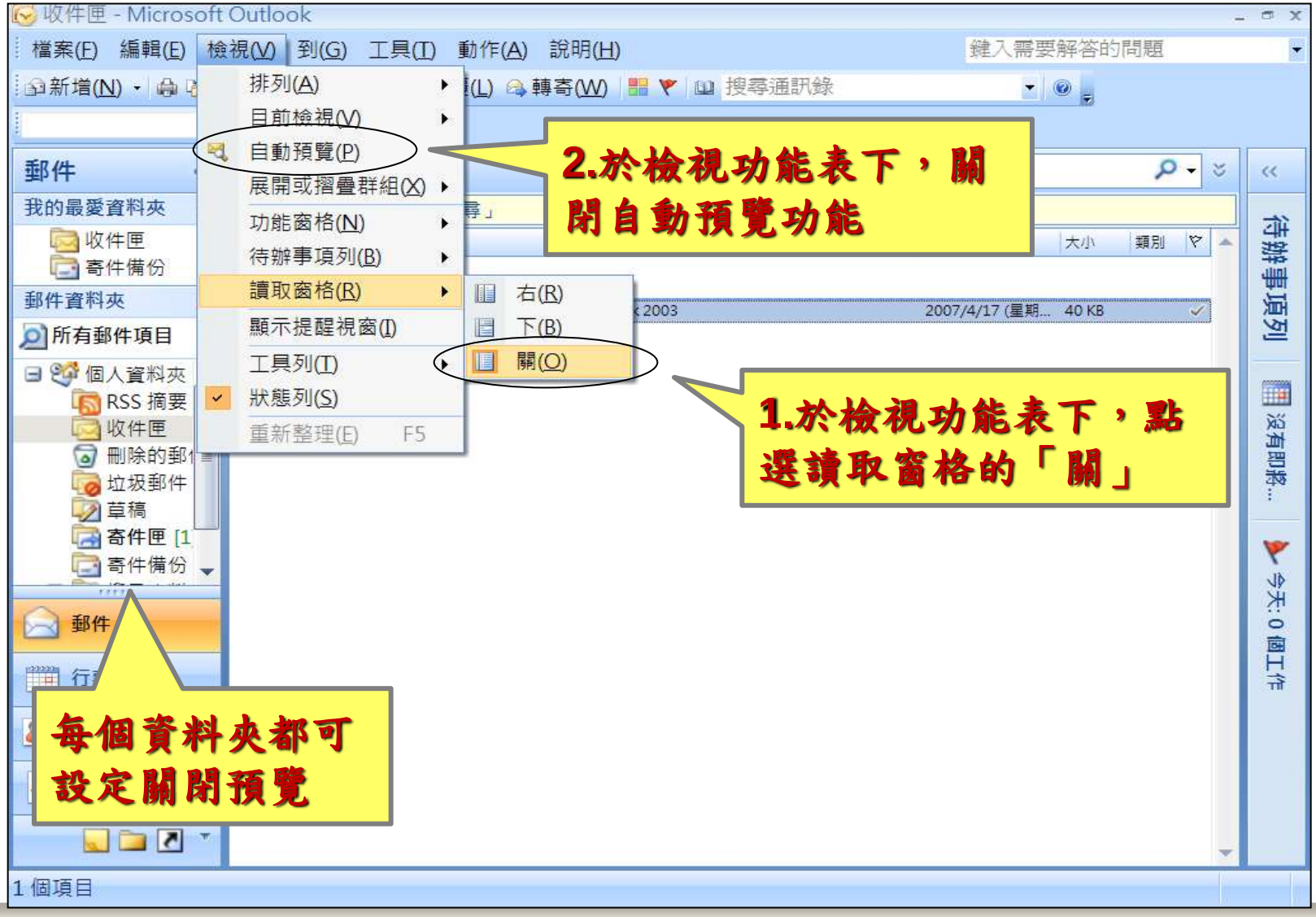
k1 2010/9/10
1234

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，

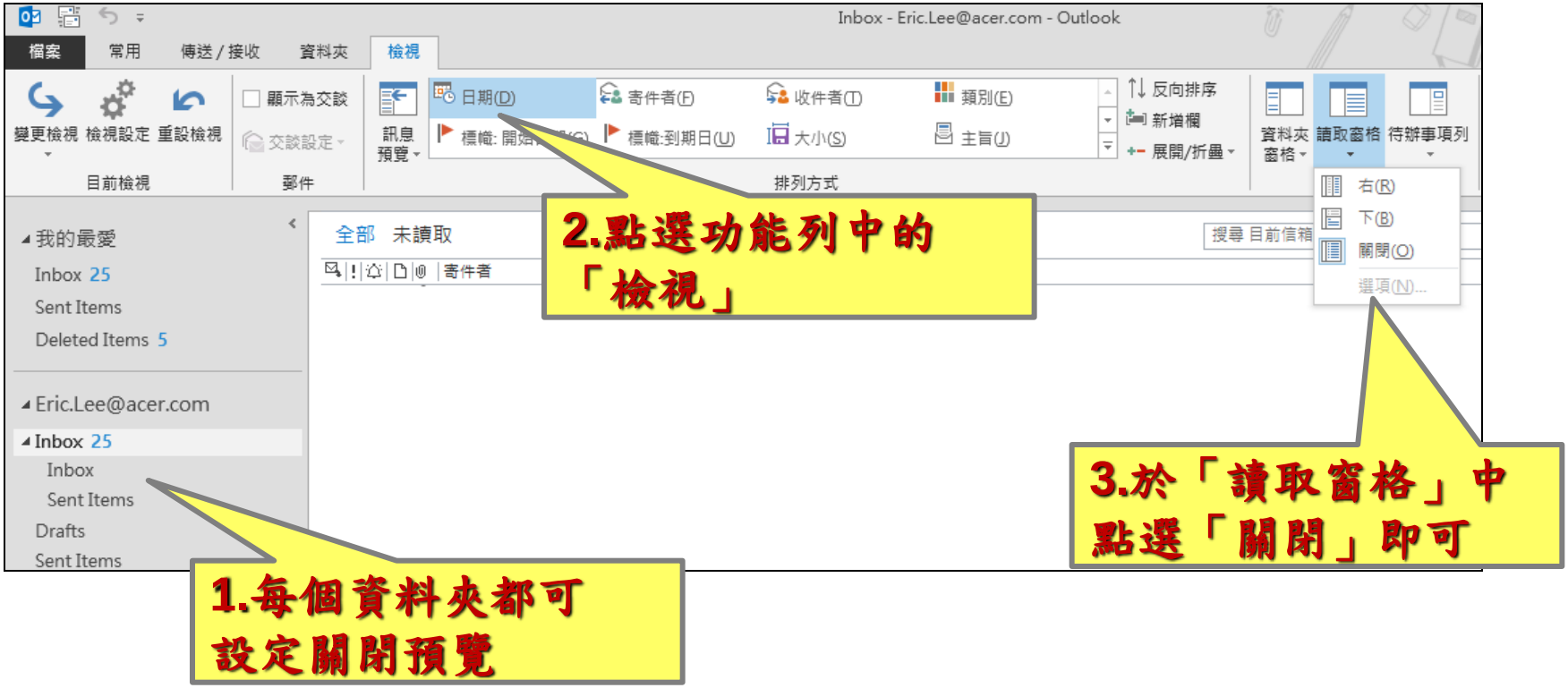
就怕再度與性感形象扯上邊，模糊宣傳焦點。瑤瑤最新主打《DiDiDa》獲選為「2011老夫子動畫電影」片尾曲，特別來賓老夫子與他的好夥伴大蕃薯現身相當搶鏡，在歌迷群中引起騷動，大蕃薯還特地穿上蓬蓬裙以「奶油大蕃薯」

關閉郵件預覽功能（Outlook 2007）



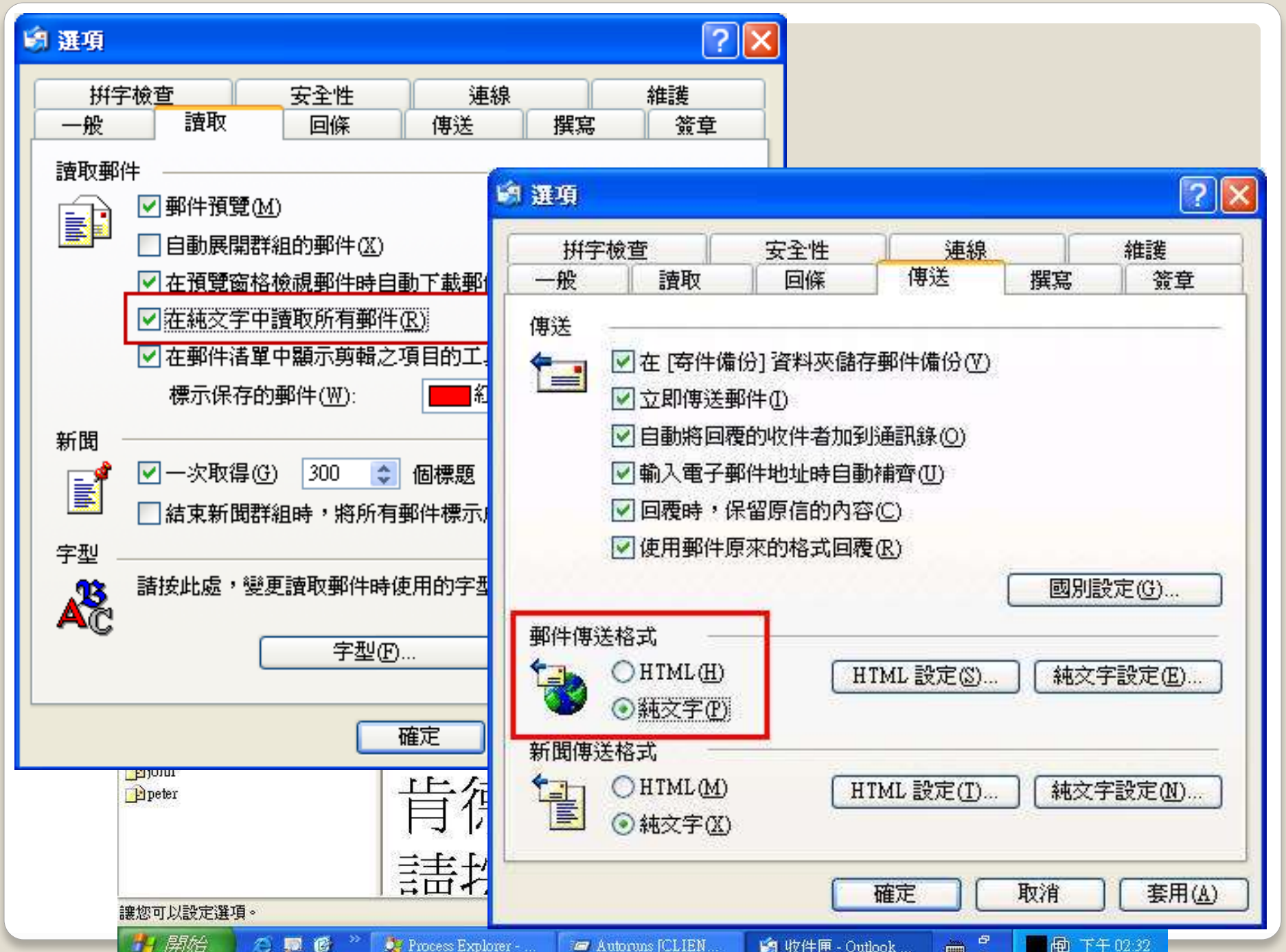
關閉郵件預覽功能（Outlook 2010）

關閉郵件預覽功能（Outlook 2013）



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)
- 公務用 (xxx@mail.xyz.gov.tw) 與個人E-Mail (xxx@yahoo.com)信箱請 分開使用
- 收件人改用「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

使用WebMail的考量

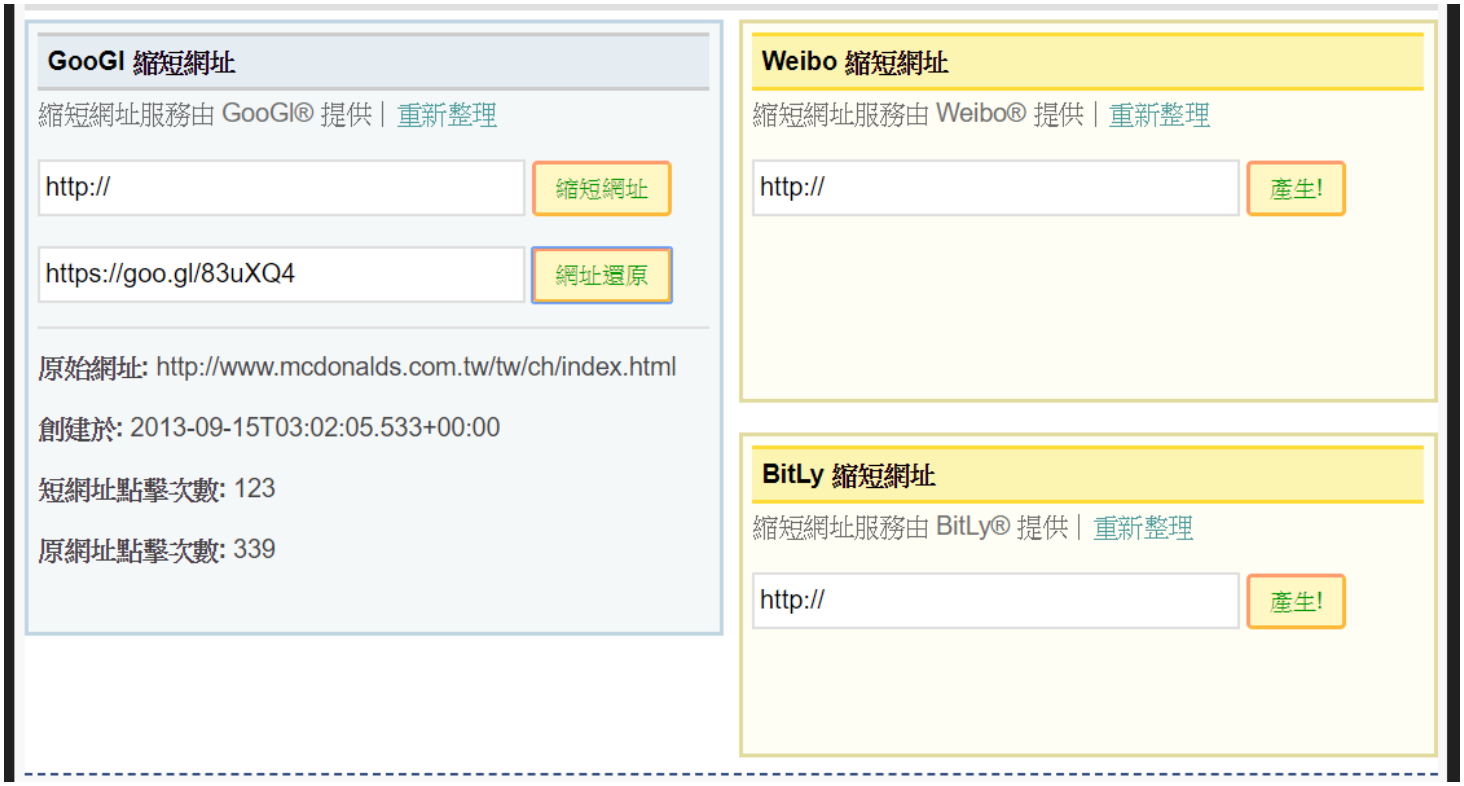
- 登入Web mail 信箱
- 點選【設定】
- 在【讀信相關設定】下方
  - 以文字方式顯示**HTML** 郵件
  - 以超連結方式顯示圖片附件
  - 關閉郵件內的 **JavaScript**
  - 關閉郵件內的 **embed/object/applet** 標籤


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

掃掃QR CODE

短網址好方便?

- https://goo.gl/83uXQ4
- Google谷歌



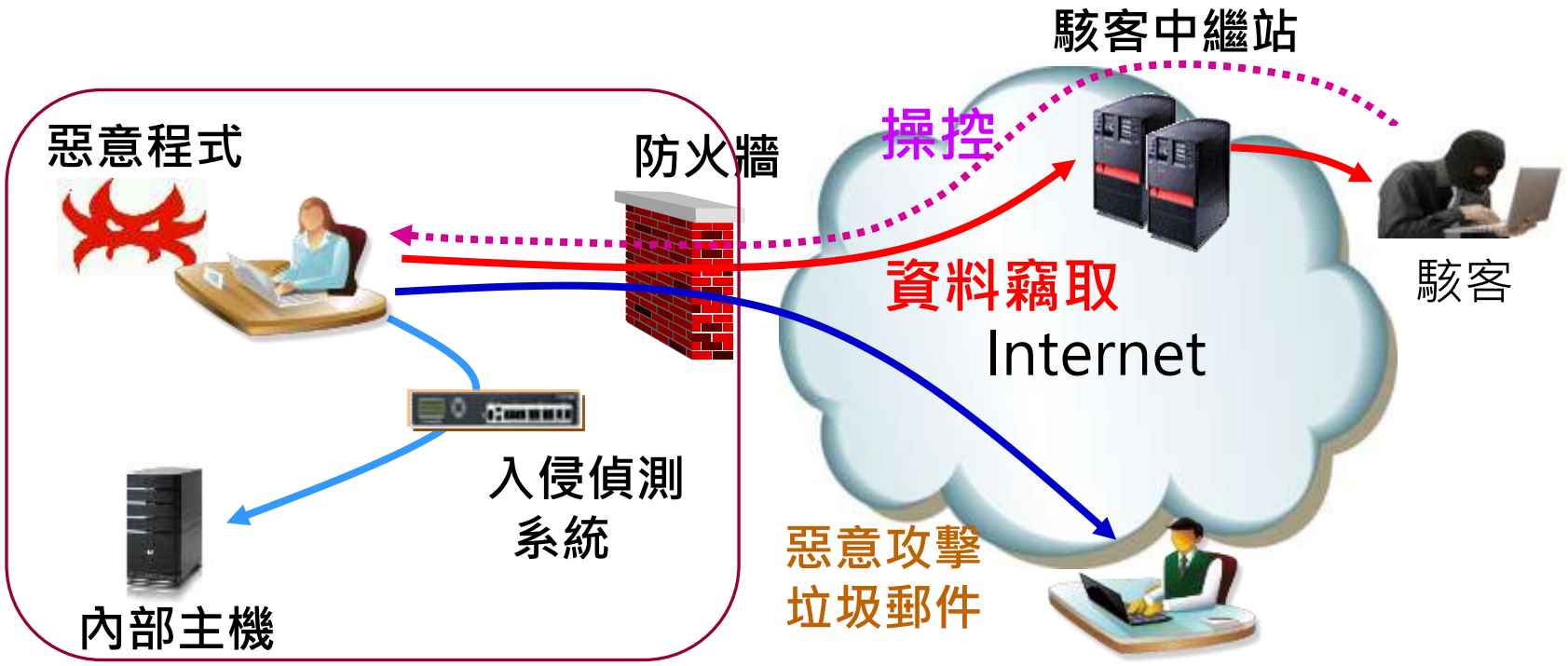
即時通訊軟體、社群網站

- 即時通訊軟體將惡意連結、檔案隱藏於訊息中，再應用社交工程的概念使被害者點選觸發
- FB留言中設置假連結，並將惡意程式、檔案隱藏於連結中，再應用社交工程的概念使被害者點選觸發

郵件社交工程防護停看聽

- 信件攻擊手法
- 社交攻擊手法

駭客到底想幹嘛?



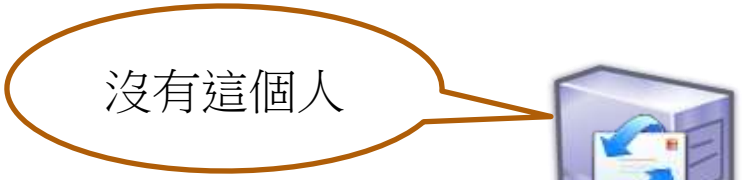
駭客手法-退信攻擊

- 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



郵件伺服器

網際網路

中華電信

使用者

駭客手法-跳板攻擊

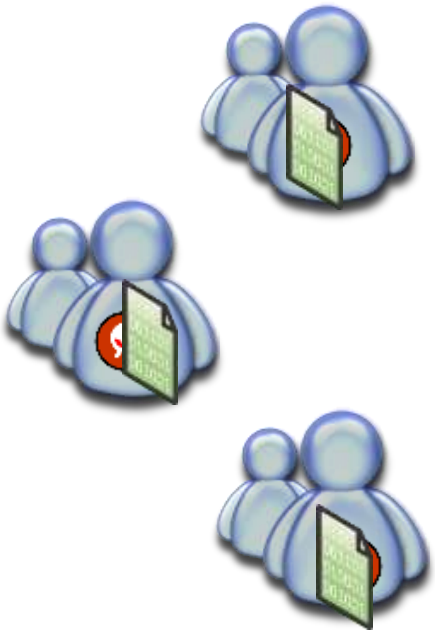
- 當您的電腦主機本身有啟用*SMTP Service*(外寄伺服器服務)，而且沒有加以防護時，被有心人士發現，進而不當使用您的網路頻寬及寄信功能，濫寄廣告信件，這就是您的電腦主機被當成廣告信跳板了!!
- 通常受害者不知道自己的電腦安裝了相關服務
- 常見微軟的作業系統，當有安裝了*IIS*功能，就會一同安裝*SMTP(*外寄伺服器服務*)*，此時若您的網路系統並未安裝防火牆，將 SMTP PORT 25 設為對外阻隔的話 ，基本上任何人都可以藉由您的 *SMTP Service* 寄發信件!! 您的電腦主機，就有可能被有心人士當成廣告信跳板，濫寄廣告信件!!

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

2018年度弱密碼公布 總有一個你用過

2018-12-26 由 安順網警巡查執法 發表于科技

近期，美國密碼公司SplashData公布了「2018年度弱密碼」列表，據悉，這些數據來源於網際網路上泄露的超過500萬個密碼，地區主要集中於北美和西歐。通過這些數據發現，計算機用戶仍然存在大量使用可預測、很容易猜到的密碼，使用這些密碼，存在潛在的被黑客攻擊的危險。


25 worst passwords of 2018 revealed
1. 123456
2. PASSWORD
3. 123456789
4. 12345678
5. 12345
6. 111111
7. 1234567
8. SUNSHINE
9. QWERTY
10. ILOVEYOU
11. PRINCESS
12. ADMIN
13. WELCOME
14. 666666
15. ABC123
16. FOOTBALL
17. 123123
18. MONKEY
19. 654321
20. !@#$%^&*
21. CHARLIE
22. AA123456
23. DONALD
24. PASSWORD1
25. QWERTY123

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


COMPAQ
FP5315

密碼背不起來怎麼辦？

- 用鍵盤上　注音符號　的位置。
- au/6w94

- 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、無蝦米)等
- 測試密碼強度：www.passwordmeter.com

密碼背不起來怎麼辦？

- 使用「自己的姓名」當密碼，是個『不好的建議』。
- 1qaz@WSX3edc

- 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：
- M3gp6jw/6uv/6

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!!!!!!!!

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

駭客手法-偽造攻擊

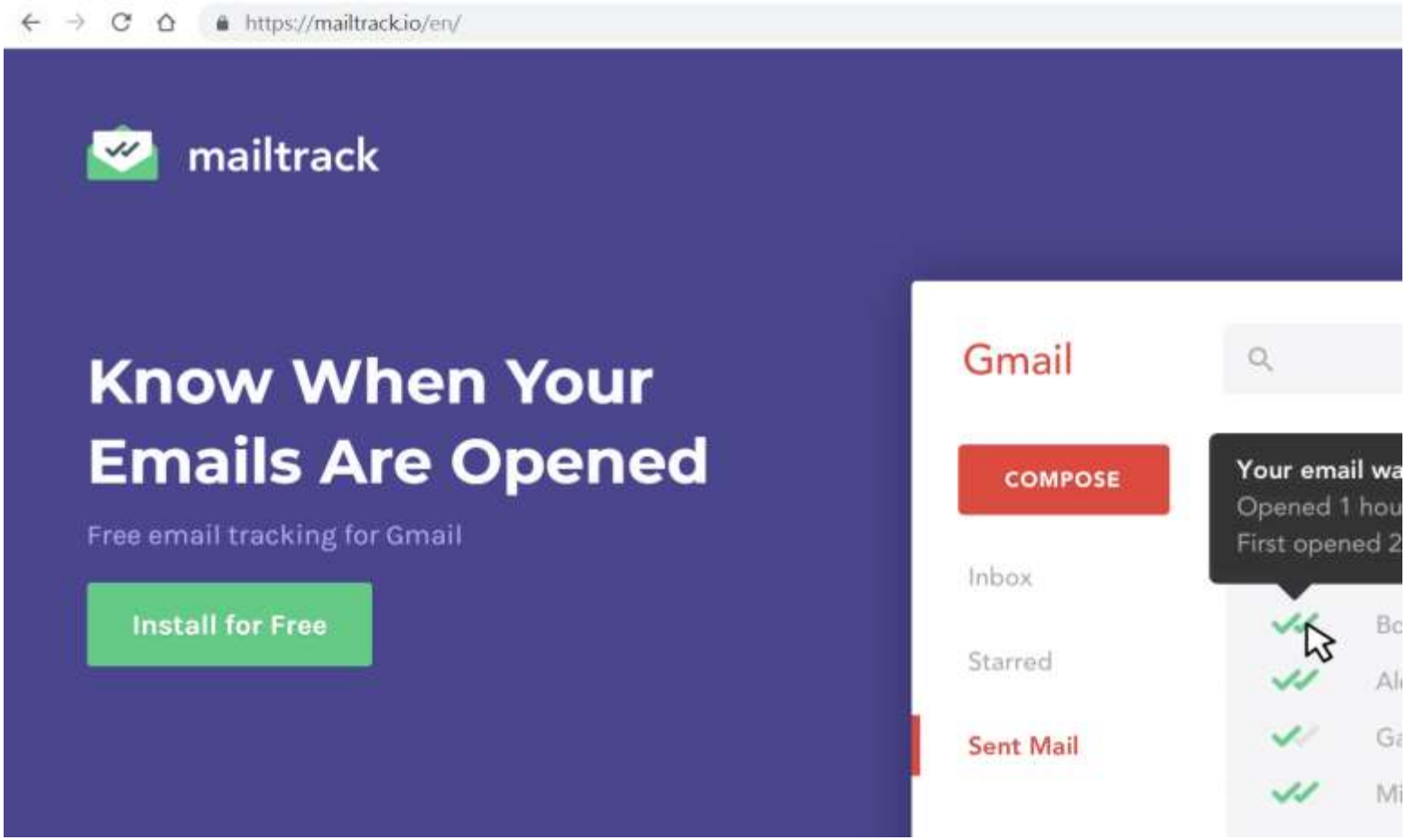
Demo time

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。

駭客手法-郵件跟蹤

- https://mailtrack.io/en/



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	

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

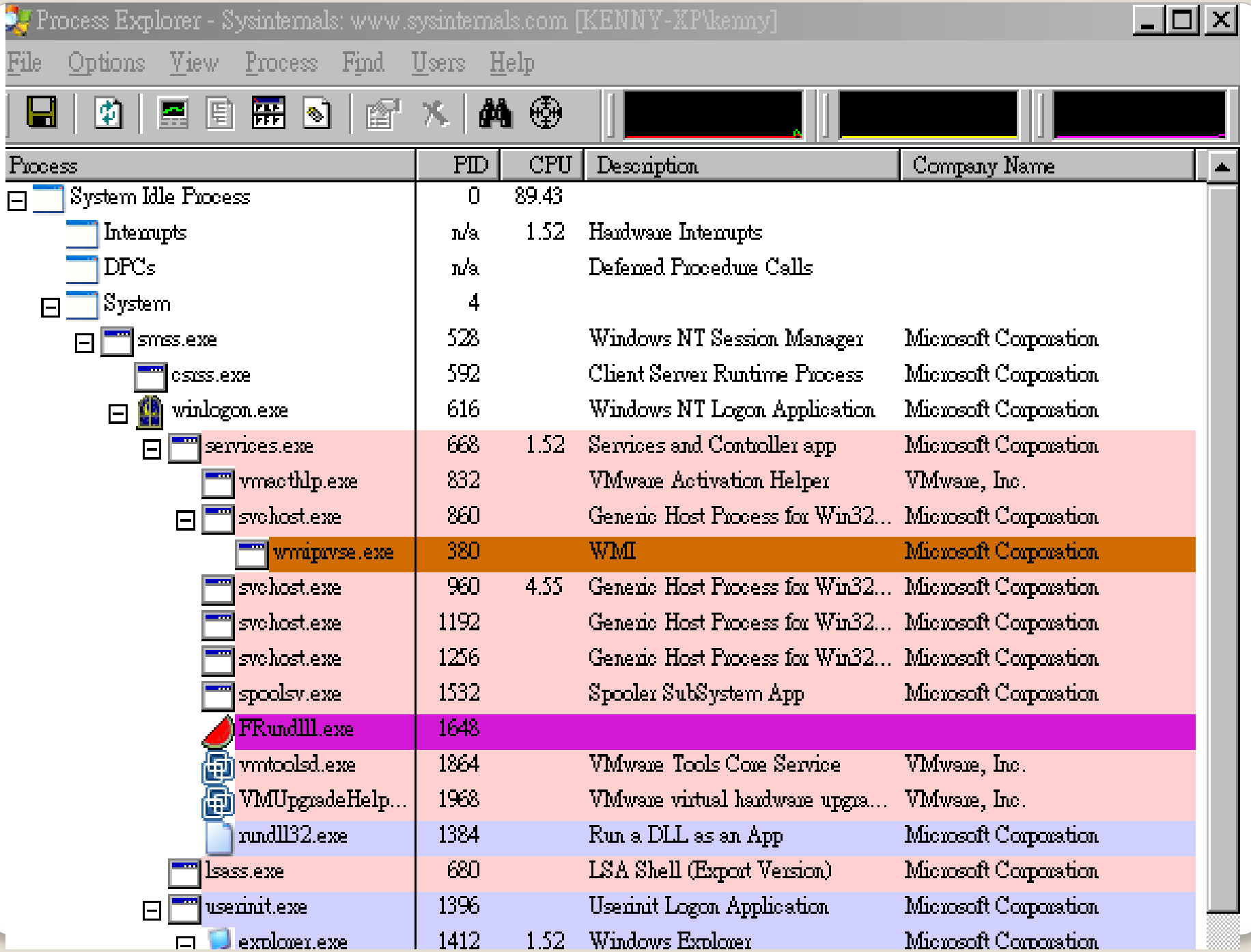
好用的進階版工作管理員

- 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

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

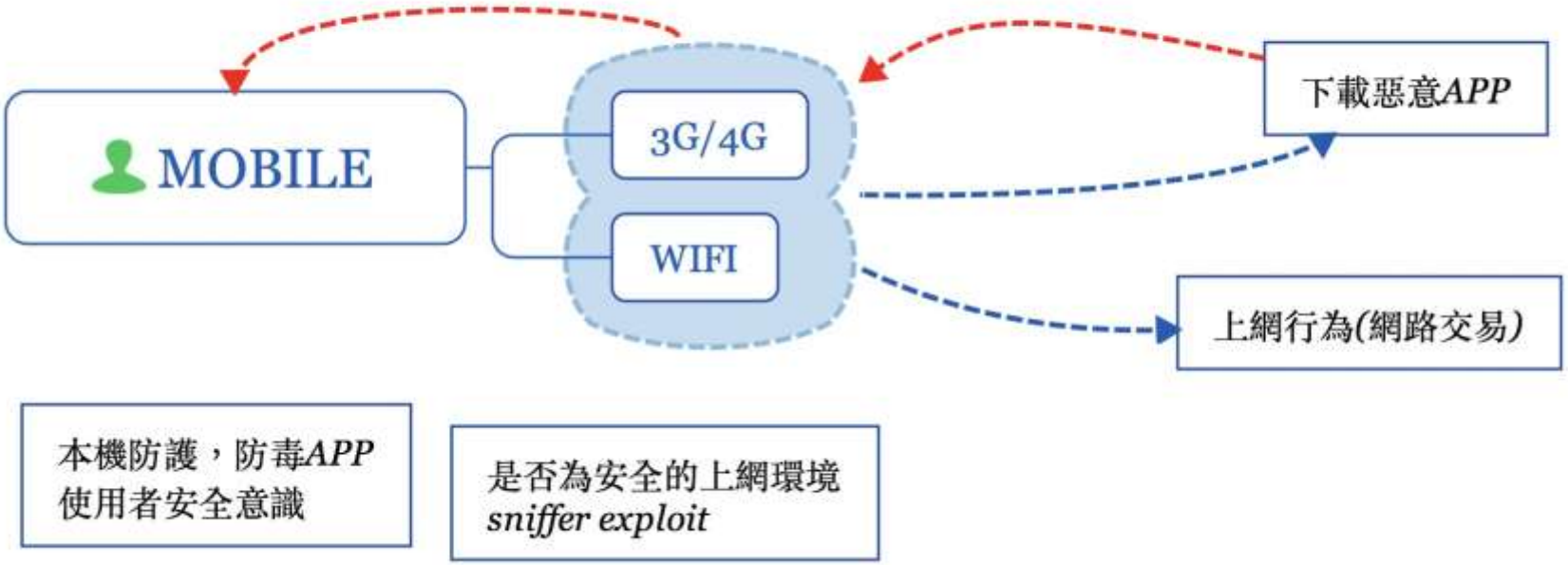
重點回顧

- 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！

行動裝置攻防實務

手機被駭資料外洩

行動裝置安全


MOBILE
3G/4G
WIFI
下載惡意APP
上網行為(網路交易)
本機防護，防毒APP
使用者安全意識
是否為安全的上網環境
sniffer exploit

App Store

ios

Google play

Android

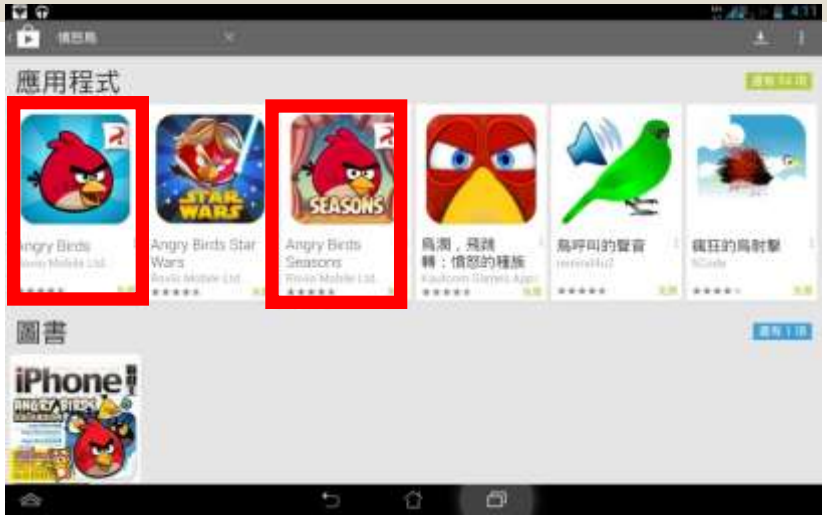
Windows 市集

Windows

Android系統APP安全(APP安裝原則)

Android系統APP安全(確認官網1)

- 右圖以 Angry Birds 及 Candy Crush Saga為例，是否注意到相同軟體及圖示一堆，且部分軟體圖示相似度很高，如要安裝相關軟體就須先了解該軟體設計廠商



Android系統APP安全(確認官網2)

- 右圖為Candy Crush Saga，其軟體廠商為紅色框部分，內有廠商公司網址是否為所要安裝APP之廠商網址，如觀看網址，仍無法確認，於安裝前可先點選進入該設計廠商網站審視確認。

Android系統APP安全
(詳細閱讀介紹與評論)

- 右圖為Candy Crush Saga，紅色框部分，為安裝前軟體介紹與使用者評論，除可協助確認個人手機安裝此APP效能與是否可使用，重點仍放置在該軟體是否為無問題軟體。

移動式個人裝置應用與安全 (APP安裝授權審視原則2)

- 詳細察看授權原則，另要注意是否全部查看如右圖紅框，尚有未查看部分，應全部瀏覽完畢。

移動式個人裝置應用與安全 (APP安裝授權審視原則3)

- 同上頁說明，審視完授權原則，應考慮所權原則是否合宜，如無問題再點選紅框中的繼續按鈕

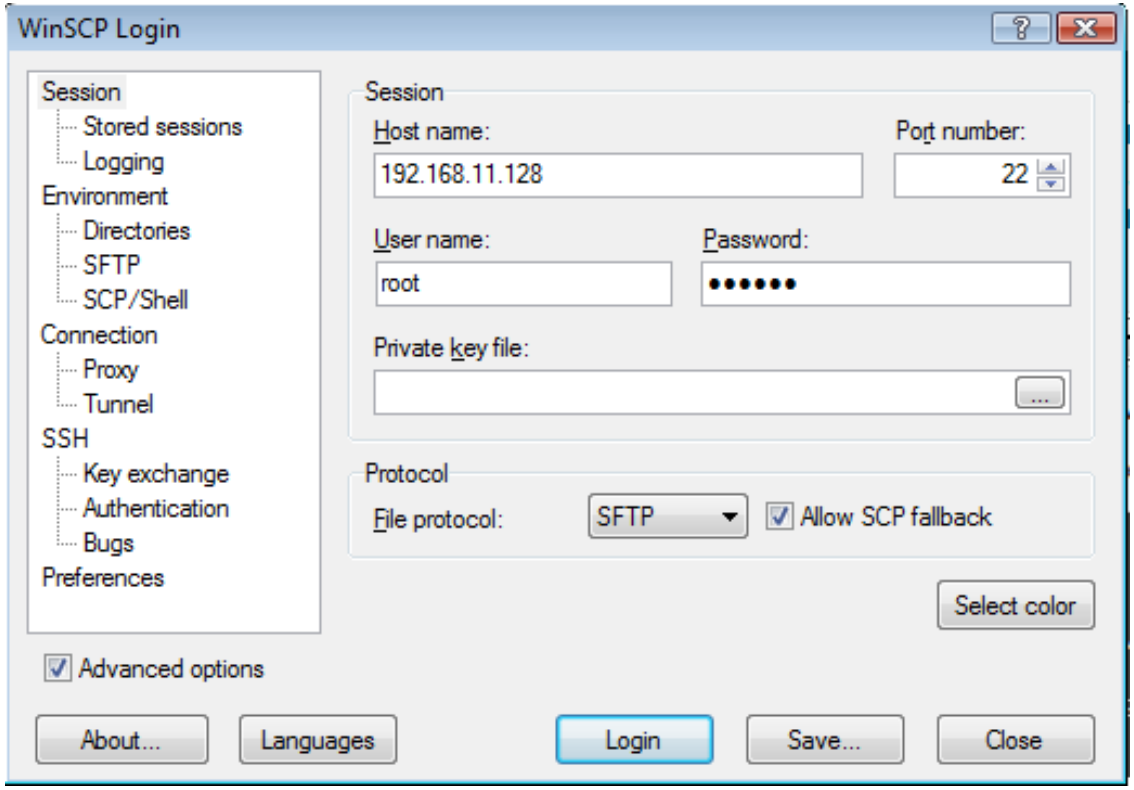
iPhone JB後 SSH 預設密碼

- 在iPhone裡面，許多遊戲或應用程式，像是有名的是需要付費才可下載的。

- 於是有許多用戶利用JB(Jailbreak)的技術，不但可以免費下載付費遊戲，還可以自由的存取iPhone裡面的檔案。

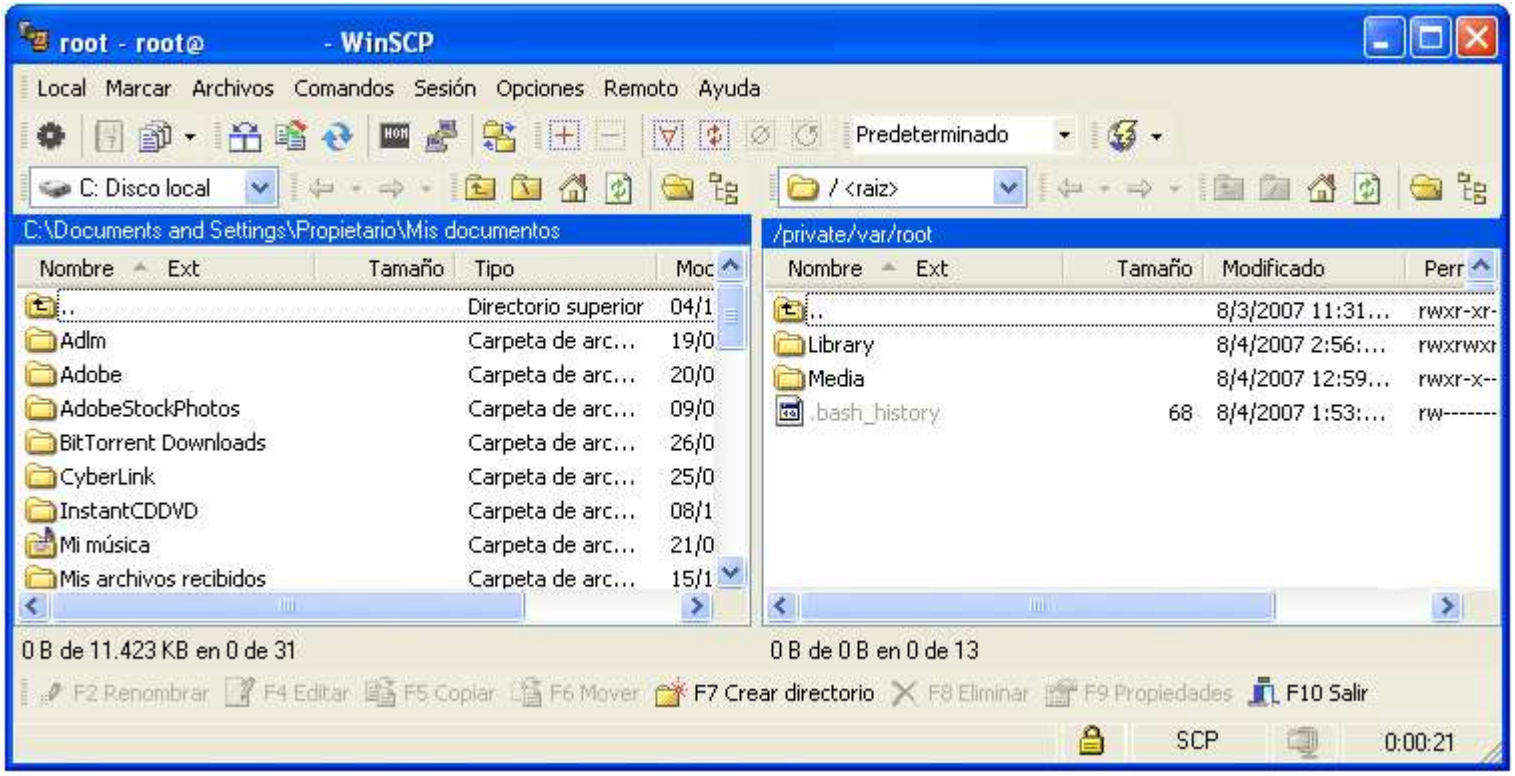
iPhone JB後 SSH 預設密碼

- iPhoneJB後，可利用遠端程式存取手機檔案。
- 但許多人不清楚，預設密碼一直都沒有改...



iPhone JB後 SSH 預設密碼

- 打入預設密碼alphine，即可存取JB後的手機。



iPhone SSH 預設密碼防治

- 若您的手機為JB過後的iPhone，並有安裝SSH，切記要更改預設密碼。

- 1. 在Cydia安裝MobileTerminal
- 2. 執行MobileTerminal後，打login再登入名稱打root而password打alpine。
- 3. 登入成功之後，再打passwd <新密碼> 更改密碼。
- 4. 再打login。但今次則在登入名稱login打mobile，而password則打alpine。
- 5. 打passwd <新密碼>開始更改密碼。
- 6. 重新啟動iPhone。

APK DEMO


Global全球
Property產業
Global全球 China
Trend超勢 Prop
Global
小米手機偷傳資料到北京？iT
NTDAPTV
認了！小米手機自動回傳個資 引網友撻伐

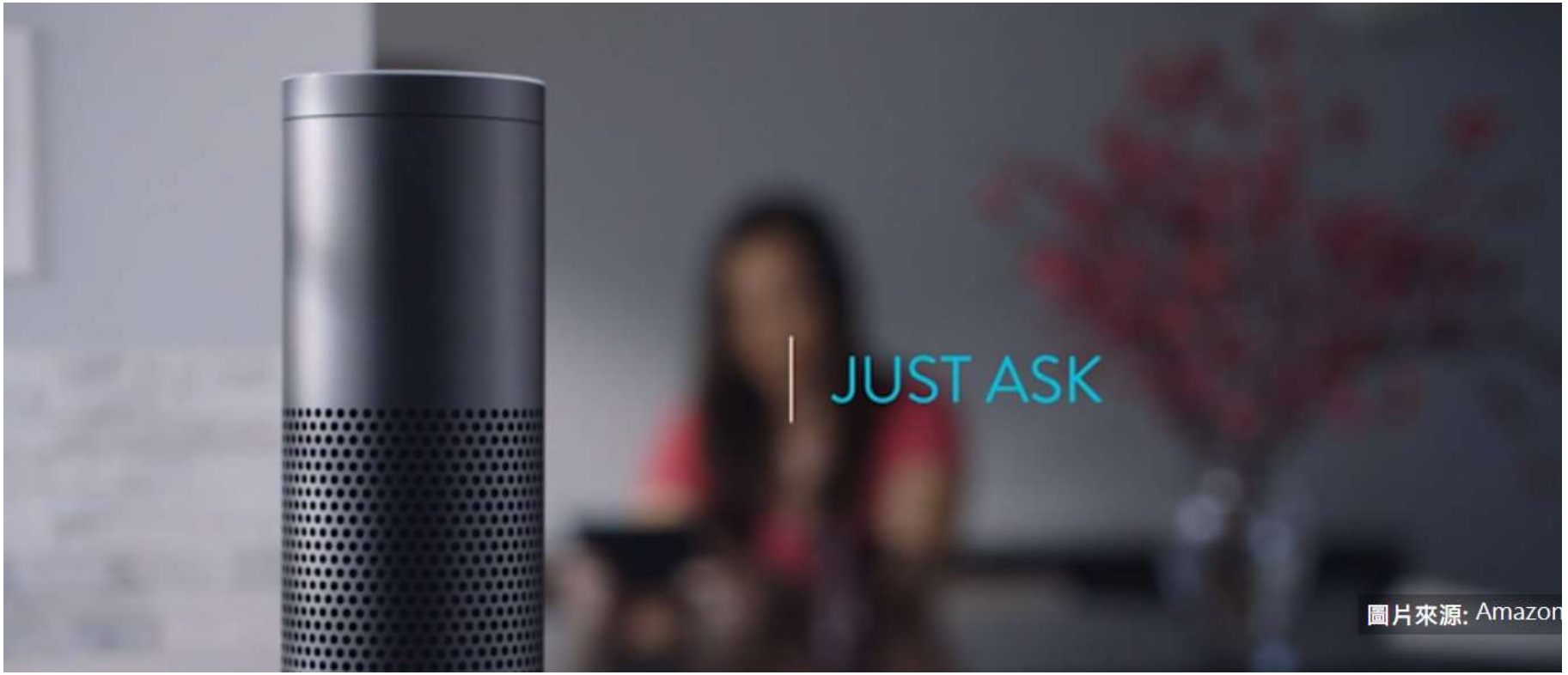
你的攝影機不是你的攝影機

ID	協議	來源 IP	目的 IP	來源連接埠	目的連接埠
1	UDP	192.168.2.42	42.157.163.134	44543	10001
2	UDP	192.168.2.42	110.43.39.133	44543	10001
3	UDP	192.168.2.42	110.43.68.2	44543	10001
4	UDP	192.168.2.42	120.92.67.36	49436	8053

顯示: 10 第一頁 上一頁 下一頁 最終頁 1/1 總計:4

你的攝影機不是你的攝影機

Amazon音箱-人工智慧?工人智慧?



工人智慧？傳Amazon以數千員工聽取Echo用戶對話來訓練Alexa

為了提供大量語音資料來訓練自家AI產品，Amazon讓員工側聽用戶對智慧喇叭Echo和語音助理Alexa的私人對話，引發侵犯個人隱私的爭議

文/ 林妍溱 | 2019-04-12 發表

彭博社報導，Amazon以數千名員工聽取及記錄智慧喇叭Echo產品用戶和人工智慧（AI）語音助理Alexa的對話，理由是為了訓練並提升Alexa的服務品質。

報導指出，Amazon在美國波士頓、哥斯大黎加、印度和羅馬尼亞的辦公室有上千名員工，每天9小時上班時段內聽取高達上千則由Echo錄下用戶對著Alexa下達指令的錄音檔、然後轉錄成文字、加註記，再餵回給Alexa 軟體，藉此訓練Alexa的口語理解能力，進而提升Alexa回應用戶指令的服務水準。羅馬尼亞曾參與過這項計畫的消息人士描述，負責這項工作的員工坐滿Amazon位於首都一棟大樓的三層樓辦公室空間。

Echo用戶的錄音檔由不同功能的Amazon員工處理，有人負責從語音檔內萃取出特定詞彙如「Taylor Swift」，然後加上流行音樂歌手的註記，有人負責轉錄和分析Alexa是否能適當回應用戶指令、另一些人記錄Echo一切錄下的聲音，包括背景噪音和用戶對話，包括兒童說的話。碰上一些難辨識的字句，員工們會利用Amazon公司聊天室軟體分享檔案，不過錄到好玩的也會彼此分享。

網站加密與安全性

- 在網站設計上，像是登入頁面，註冊頁面等涉及隱私的網頁，需要加密傳輸資訊以免被監聽!

機敏資訊未加密

- 金流服務(如信用卡刷卡)若未加密，將有很大的風險
  -

機敏資訊未加密

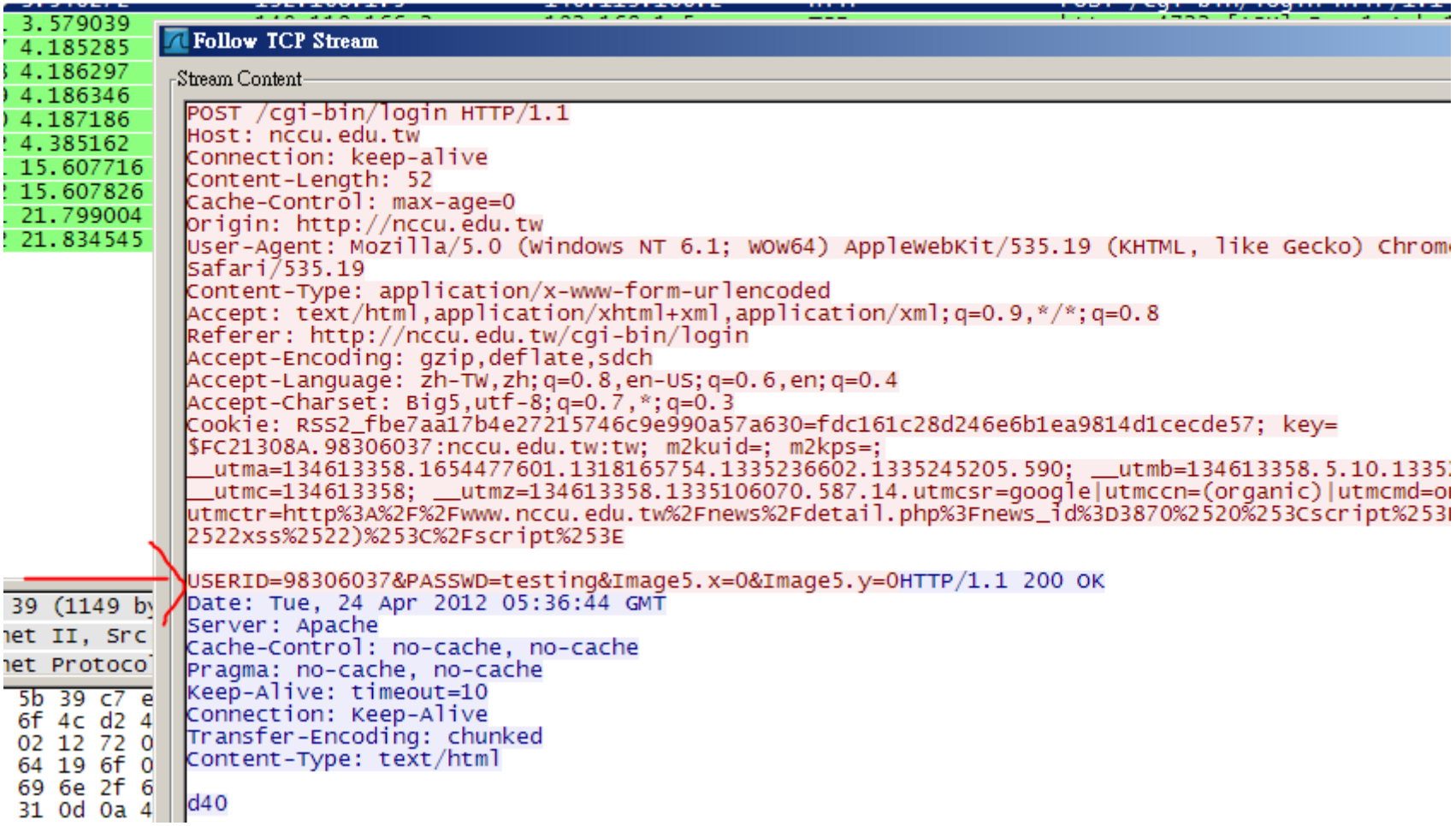
```
ID=0589DBA461E9CD60D7F5C008F2810DC3.tc1; _ga=GA1.2.1180088354.1426663003

?
randnum=0.42147008259780705&accountNo=0022812737&isdn=0973559037&shouldPay=1022&billing
Cycle=2015%2F02%
2F20&priorPay=1031&priorPayEd=1031&currtAppend=1022&currtPay=1022&payEndTime=2015%2F03%
2F08&customerName=%E9%BB%83%E6%96%87%E6%B2%
BB&pay=1022&cardNumber1=[redacted]&cardNumber2=[redacted]&cardNumber3=[redacted]&cardNumber4=[redacted]&backNum
ber=[redacted]&month=[redacted]&year=[redacted]&=%E4%BB%98%E6%AC%BE&ajaxRequest=trueHTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Cache-Control: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Pragma: no-cache
Content-Type: text/xml;charset=UTF-8
Transfer-Encoding: chunked
Date: Wed, 18 Mar 2015 07:18:16 GMT
```

登入頁面未加密


國立政治大學 Web Mail 系統
nccu.edu.tw/indexs.html
此網頁的身分未經驗證。
您到 nccu.edu.tw 的連線未加密。
網站資訊
您首次瀏覽此網站的日期為 2012/2/10。
這些是什麼？
回首頁
帳 號
密 碼
登 入
帳號(即您電子郵件地址中@符號之)
系 統 公 告
歡迎使用國立政治大學教職員生電子郵件系統
·有關本電子郵件系統使用說明請參考線上說明文件。
·電子郵件系統相關問題請e-mail至help@nccu.edu.tw
·電子郵件系統電話諮詢服務請於上班時間洽校內分機67157。

查看封包，發現資料未加密

Timestamp	HTTP server	Client	Username	Password	URL
10/05/2012 - 00:40:13	140.119.166.2	192.168.1.5	98305095	testing	http://nccu.edu.tw/indexs.html
10/05/2012 - 00:40:26	69.171.248.8	192.168.1.5	1000037885917...	5	http://www.facebook.com/?sk=welcome



網站加密與安全性

- 在網站設計上，像是登入頁面，註冊頁面等涉及隱私的網頁，需要加密傳輸資訊以免被監聽!
- 使用者在上網時要注意登入頁面是否有安全鎖的標誌，否則非常容易被監聽!

行動裝置GPS

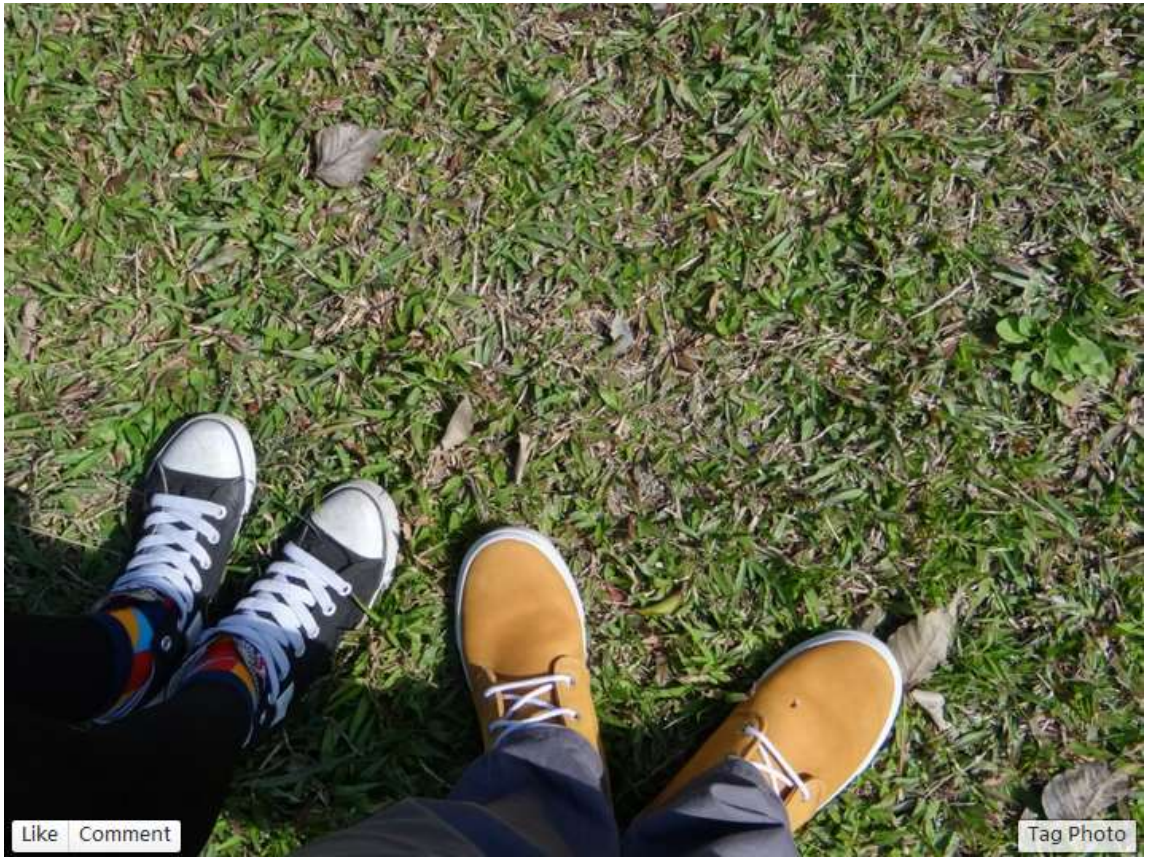
手機越貼近生活，包含的隱私機密資訊越多

圖片資訊

- 有位朋友上傳了照片至Facebook...
- Facebook竟然知道照片在哪裡拍的

Facebook如何得知圖片資訊

- 這張照片看得出來在哪裡拍的?



圖片中隱藏Exif資訊

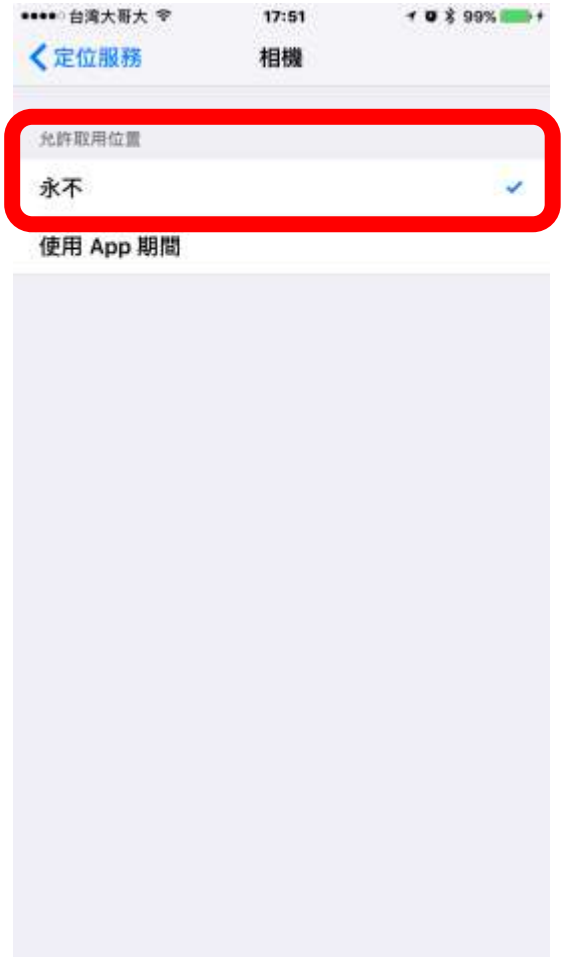
- 對於攝影師以下的資料最為值得參考：

- 相機型號，拍攝時間，焦距，快門速度，光圈
- 曝光程序，測光模式，白平衡，閃光燈
- ISO值，曝光補償

- 對於駭客以下的資料最為值得參考：
- GPS

如何防治照片資訊外洩?

- 拍照時若怕有隱私問題，把定位服務GPS關掉
- 可用其他軟體消除exif



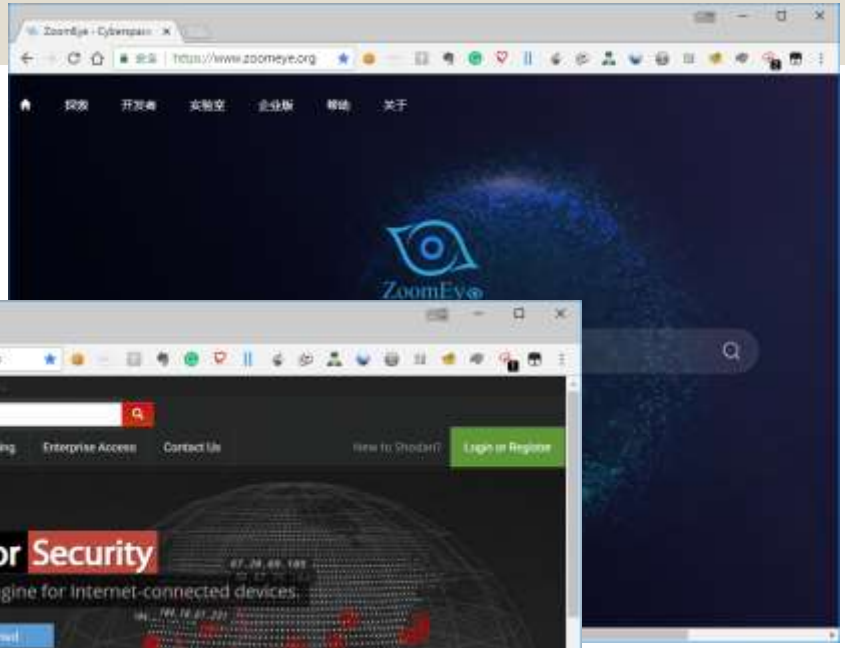
設備好方便，接上網路即可用

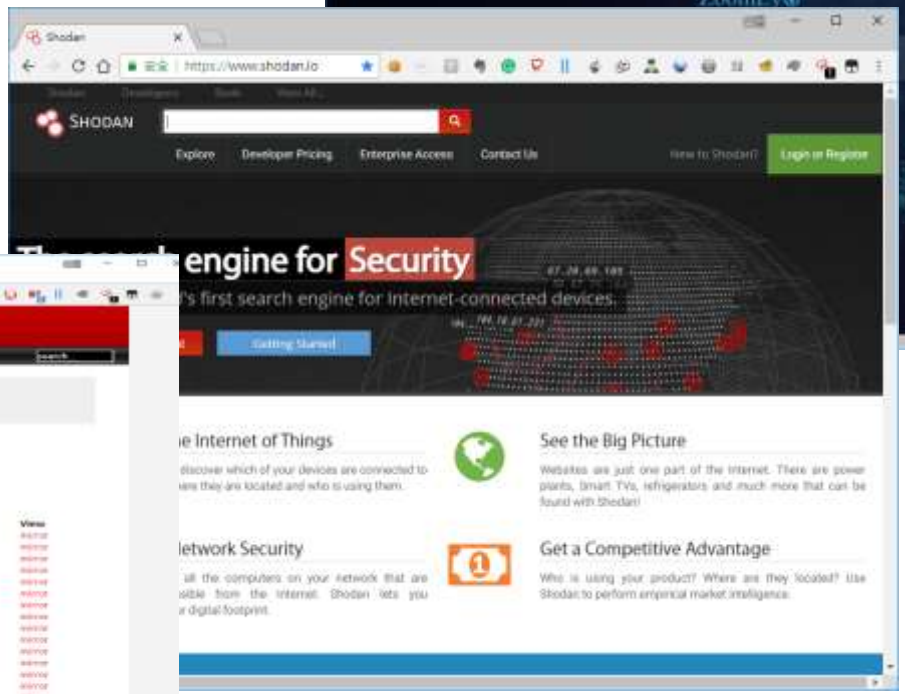
你的無線AP改密碼了嗎?

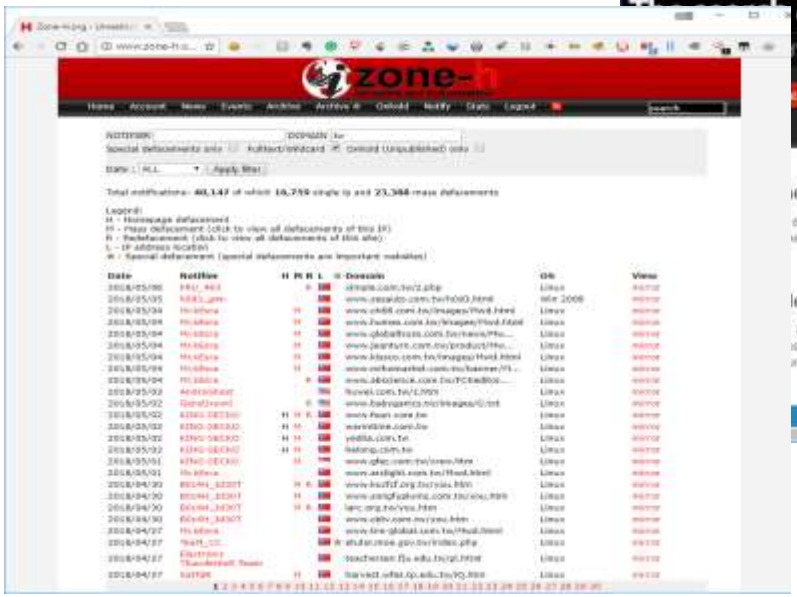
什麼是 Google Hacking

其他的搜尋引擎與資料庫

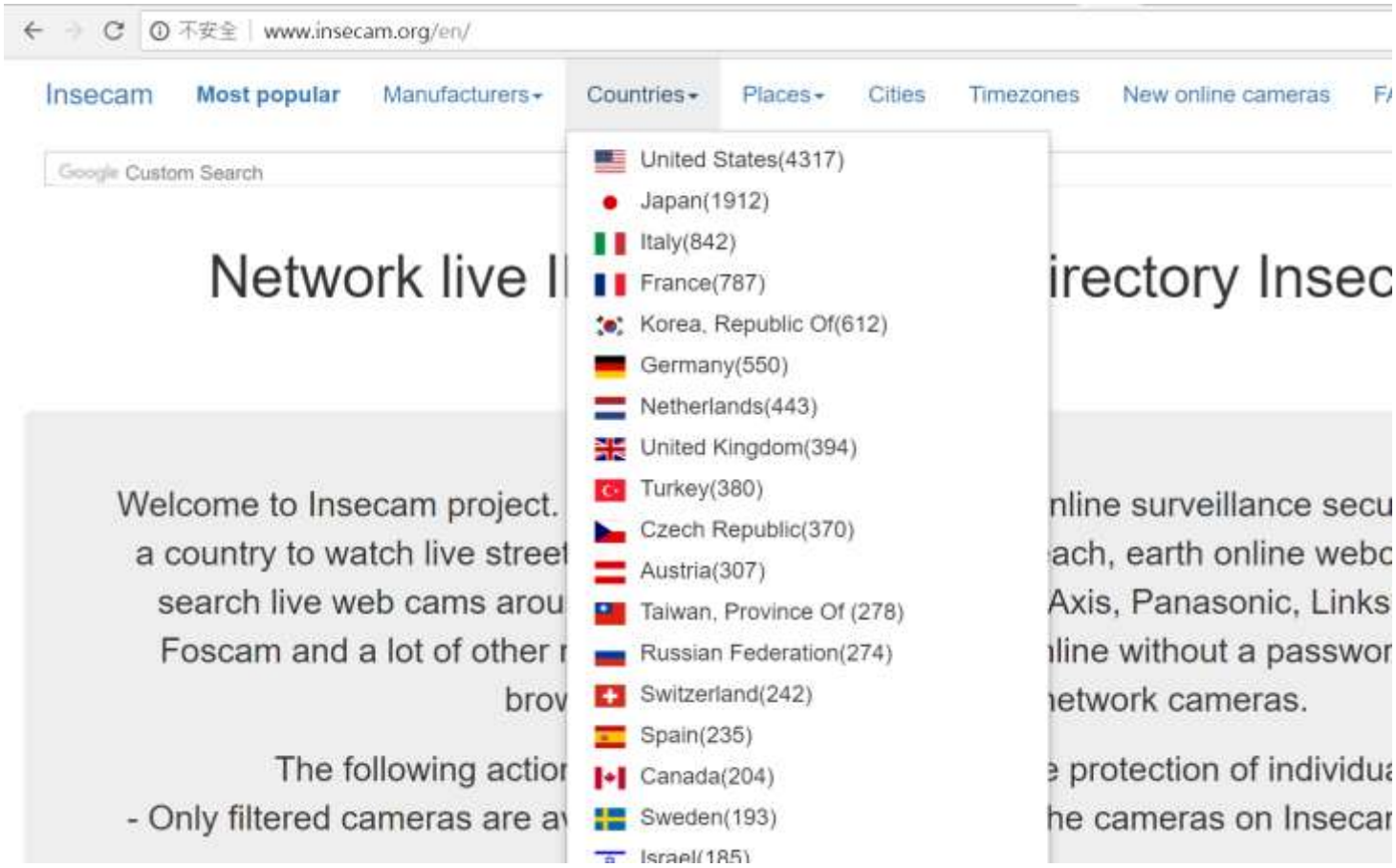
- Zone-h
- Shodan
- zoomeye







輕鬆環遊世界?!


不安全 www.insecam.org/en/
Insecam
Most popular
Manufacturers
Countries
Places
Cities
Timezones
New online cameras
Google Custom Search
United States(4317)
Japan(1912)
Italy(842)
France(787)
Korea, Republic Of(612)
Germany(550)
Netherlands(443)
United Kingdom(394)
Turkey(380)
Czech Republic(370)
Austria(307)
Taiwan, Province Of (278)
Russian Federation(274)
Switzerland(242)
Spain(235)
Canada(204)
Sweden(193)
Israel(185)

問題與討論