資訊安全宣導

2016.12.13

吳文達

wdwu@niu.edu.tw

宜蘭區網中心
ILAN REGIONAL CENTER

網路與伺服器可能的攻擊

1. DDos分散式阻斷服務攻擊
2. ATP攻擊
3. 密碼猜測
4. Buffer Overflow攻擊應用程式
5. ARP攻擊

網路與伺服器可能的攻擊

1. DDos分散式阻斷服務攻擊
2. AT
3. 密
4. Bu 應用程式
5. ARP攻擊

網管人員：
部署資安設備、伺
服器安全設定

網站應用程式可能的攻擊

依據 OWASP Top 10

A1 - Injection（注入攻擊）
A2 - Cross Site Scripting (XSS)（跨站腳本攻擊）
A3 - Broken Authentication and Session Management（身分驗證功能缺失）
A4 - Insecure Direct Object References（不安全的物件參考）
A5 - Cross Site Request Forgery (CSRF)（跨站冒名請求）
A6 - Security Misconfiguration（安全性設定疏失）
A7 - Failure to Restrict URL Access（限制URL存取失敗）
A8 - Unvalidated Redirects and Forwards（未驗證的導向）
A9 - Insecure Cryptographic Storage（未加密的儲存設備）
A10 - Insufficient Transport Layer Protection（傳輸層保護不足）

網站應用程式可能的攻擊

依據 OWASP Top 10

A1 - Injection（注入攻擊）
A2 - Cross Site Scripting (XSS)（跨站腳本攻擊）
A3 - Broken Authentication and Session Management（身分驗證功能缺失）
A4 -
A5 -
A6 - Security Misconfiguration（安全性設定疏失）
A7 - Failure to Restrict URL Access（限制URL存取失敗）
A8 - Unvalidated Redirects and Forwards（未驗證的導向）
A9 - Insecure Cryptographic Storage（未加密的儲存設備）
A10 - Insufficient Transport Layer Protection（傳輸層保護不足）

系統開發人員：過濾、阻擋

現今的網路犯罪趨勢

※駭客的目的已經改變

- 轉向以金錢為目的

※駭客的目標轉向一般的使用者

- 大範圍的傳播給網路使用者(個人電腦)取代針對少數伺服器的入侵

現今的網路犯罪趨勢

※多種手法
- 零時差攻擊
- 透過社交工程手法
- 藉由社群網路傳播

※最終目的
- 引誘使用者安裝惡意控制軟體(殭屍電腦)
- 竊取使用者電腦裡的資料
- 騙取金錢

個人資訊安全-日趨重要

1. Facebook社交平台詐騙與防範
2. Line社交平台詐騙與防範
3. 網路釣魚詐騙與防範
4. 勒索病毒防範
5. 密碼原則
6. 個人電腦系統安全與備份

電子郵件-夾帶惡意連結、惡意程式

電子郵件-夾帶惡意連結、惡意程式

- 生活類 五月報稅天 網路報稅讓麻煩省一半！
- 生活類 怠速罰單終於開出，小心受罰!
- 生活類 還在為返鄉訂不到票煩惱嗎一高鐵預計新增四站！！
- 健康類 熱浪襲人 教你如何避免中暑
- 健康類 外食族 如何吃得更健康？超商減肥法！
- 健康類 腸病毒疫情升 正確勤洗手 出國應注意！

電子郵件-夾帶惡意連結、惡意程式

- 知識類 你看得出她是機器人嗎？美麗程度媲美葉子媚！
- 科技類 台灣之光！日內瓦展 我發明奪 42 金 世界第一！
- 科技類 線上就能觀看故宮收藏！快看看～
- 時事類 從日本核災看輻射線對眼球的影響！
- 趣味類 巨無霸高麗菜 重 30 臺斤超吸睛
- 美女類 私底下你沒見過的正妹主播！

Facebook 上的詐騙事件天天都在發生

網址: http://kikinote.net/article/20916.html

Facebook 詐騙事件，由早期的投票、收簡訊，到過年時爆紅的 LINE ID，最近則是新流行了留言按讚抽手機詐騙粉絲團來騙取網友們按讚分享

Facebook抽獎詐騙手法-盜取帳號

成立Facebook粉絲團內文表示購買了幾十台手機要送大家，只要留言和按讚就有機會抽到新款的手機iPhone 5、Galaxy S4、HTC One

Facebook抽獎詐騙手法-盜取帳號

抽 HTC Butterfly
一天就已經累計一萬三千個讚
一萬一千人分享，一萬兩千人留言

Facebook抽獎詐騙手法-盜取帳號

IPhone5 Galaxy S4 HTC ONE 抽抽樂
Like This Page · Sunday near Panchiaochen

我們已向HTC購買200台HTC NEW ONE 64GB目前正打算把它全都送出去，我們會以抽獎的方式來決定誰能得到這千載難逢的機會，方式如下:
1)讚我們的專頁
2)讚這張照片，並分享這張照片
3)然留言寫下你想要的顏色(黑,白)各100台
就有機會獲得全新HTC NEW ONE 64GB
這麼好康 你還在等什麼呢!!
抽獎日期為2013.5.20

Like · Comment · Share

15,765 people like this.

15,383 shares

View previous comments 6 of 16,258

按讚留言

有可能會被盜取個資，前往按讚的人也可能會被鎖定盜取帳號來做進一步詐騙

Facebook-LINE免費貼圖粉絲團

利用贈送付費貼圖來引誘轉載和留下 LINE ID 的手法

Facebook-LINE免費貼圖粉絲團

已經過期的貼圖已經不能下載，但也拿來當贈送的題材

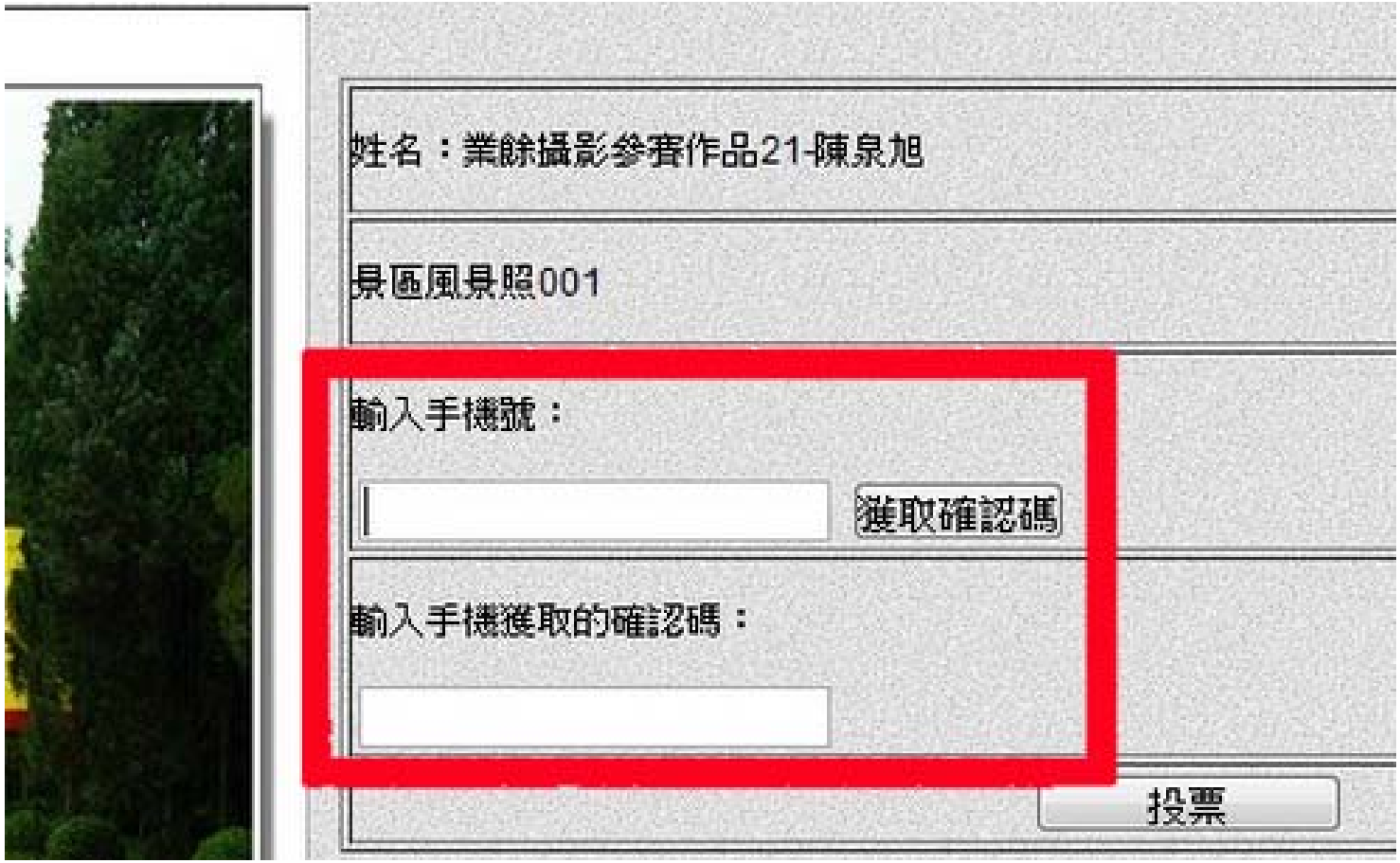
Facebook Messenger-可以幫我收封簡訊嗎？

許多朋友（通常是八百年都沒聯絡過的）接二連三在臉書密你「方便用你的手機幫我收一下簡訊可以嗎？」

Facebook Messenger-可以幫我收封簡訊嗎？

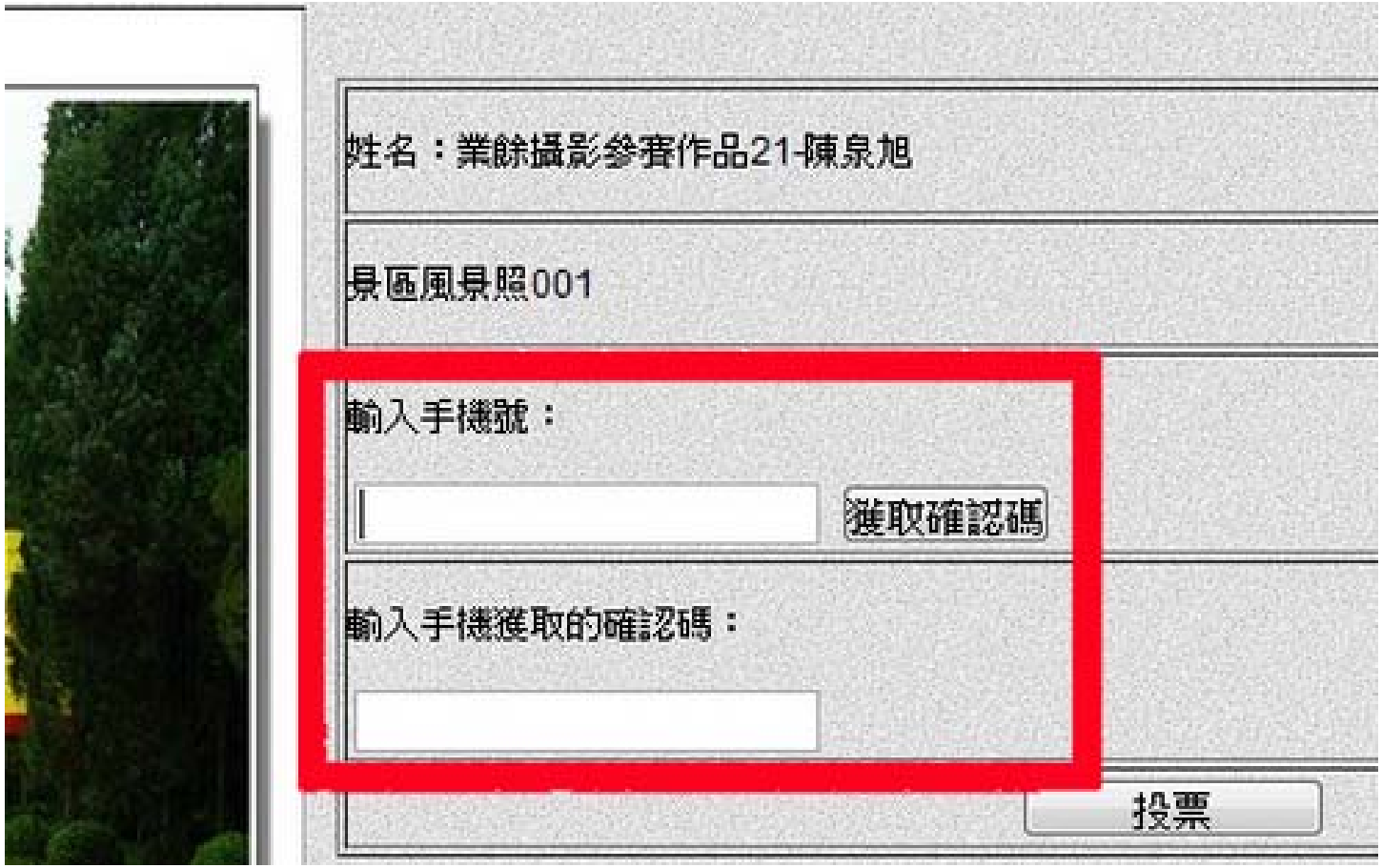
其實這個駭客手法就是盜用你朋友的**臉書帳號**問出你的**電話號碼**後進行**小額付費**，因為購物網站會發驗證碼到**手機**所以詐騙集團就會問你收到的**認證碼**幾號，進行線上付費。

Facebook Messenger-「可以幫我投票嗎？」



很多人可能都曾**幫朋友投票**衝人氣過，詐騙集團就是利用這個想法，特地做了一個很兩光的假投票網頁

Facebook Messenger-「可以幫我投票嗎？」



正常的投票網頁只會請你填入下方的驗證碼而已，但可不會特地要你輸入電話號碼，再把驗證碼傳到你的手機裡

Facebook 詐騙：團購社團邀你撿便宜的騙局

啥！連購物社團也有假的；莫名被加入購物社團，利用假商品來吸引你上勾

Facebook 詐騙：團購社團邀你撿便宜的騙局

詐騙集團盜用路人A的帳號之後先把路人A自己加入社團，接著再透過工具直接把 500 位好友全部加入社團

Facebook 詐騙：團購社團邀你撿便宜的騙局

1. 留言詢問價格不會得到回應（或者要你寫信去問）。
2. 以貨到付款方式讓會員降低心防（其實他要的是你的資料）。
3. 以宅配方式運送（原因同上）。
4. 購買和付款方式以 Facebook 訊息傳送，並要你留下姓名、手機和地址。

Facebook 詐騙：團購社團邀你撿便宜的騙局

1. 請停用「手機小額付款」機制
2. 不要理會 FB 上面的簡訊認證碼索
3. 請不要邀請別人加入類似購物社團
4. 請勿向來不不明的平台購買物品
5. 請大家一起來幫忙，檢舉這樣的垃圾社團，然後退出.....

詐騙三要素：

要電話、傳簡訊、給認證碼

調整 Facebook 帳號安全設定，遠離 「收簡訊」盜帳號等詐騙危機！

改密碼並不是一個很完整的解決方法，
因為你的電腦也許已經被植入木馬，
或者安裝了具有危險性的軟體而不自覺，
即使再怎麼改密碼，可能都難戒斷帳號常常被其他人操控的問題。

1. 檢查帳號有無異常活動情形
2. 發現問題時立即變更密碼！
3. 檢查帳號是否被異常裝置登入
4. 檢查帳號是否有異常連線
5. 當不明人士登入你的帳號，自動寄送通知

調整 Facebook 隱私設定，遠離 「收簡訊」盜帳號等詐騙危機！

調整 Facebook 隱私安全設定，遠離 「收簡訊」盜帳號等詐騙危機！

Facebook隱私捷徑

1. 誰可以看到我的東西？朋友
2. 誰可以與我連絡？所有人
3. 我該如何防止別人騷擾我？

調整 Facebook 隱私安全設定，遠離 「收簡訊」盜帳號等詐騙危機！

Facebook隱私捷徑

1. 誰看的到我往後的貼文？
2. 檢視我被標註的所有貼文和內容？
3. 其他人可以看到我的動態時報的哪些內容？

調整 Facebook 隱私安全設定，遠離 「收簡訊」盜帳號等詐騙危機！

最後一項為調整「你的個人檔案」隱私權限，裡頭會列出包含你填寫過的生日、工作經歷、學歷、現居城市、家鄉、透過後方的權限設定，你能夠決定誰看得到這些個人檔案，從這個步驟裡來調整。

LINE 和手機簡訊詐騙手法日新月異

突然收到一封簡訊，內容是Yahoo奇摩的認證碼!!!

LINE 和手機簡訊詐騙手法日新月異

之後立刻接到陌生電話(或隱藏號碼)，非常急促且有禮貌地說：「不好意思，我在用Yahoo奇摩認證的時候，手機號碼輸入錯誤，不小心輸入了您的號碼，能不能請你把剛剛送進您手機簡訊上的驗證碼跟我講？真的很不好意思，拜託拜託！」

LINE 和手機簡訊詐騙手法日新月異

這是目前小額付款的漏洞，在線上購買遊戲點數卡或是通話卡，在做購買動作時，廠商系統會要求輸入**手機號碼**，然後再發一組認證碼到手機上，而後把收到**簡訊**上的**認證碼**輸入系統後，就完成小額付款的動作了！

LINE 和手機簡訊詐騙手法日新月異

根據 CM Security 實驗室使用群的感染率推算全臺 800 萬部 Android 手機，每日約有 4,000 多部 Android 手機中毒遭駭，病毒開發者透過手機小額付款機制漏洞，可詐取每位中毒手機用戶最高 5,000 元小額付款上限金額，致使，近一週以來，累積詐騙金額恐達上億元之譜

LINE 和手機簡訊詐騙手法日新月異

宅急便病毒化身35種簡訊

若不小心受簡訊內容引誘，點進該病毒連結，就會被誘導下載「小額支付大盜App」，直接導致金錢損失。

LINE 和手機簡訊詐騙手法日新月異

LINE詐騙流程

點了網址

↓

下載惡意程式

↓

取得最高權限

↓

小額付款買遊戲點數 → 換取現金

目前最新型詐騙手法，歹徒利用流行的Line或臉書軟體，以傳訊息「裝熟」或「恫嚇」方式，讓人點選其附上的連結網址，一連結就被植入並啟動木馬程式，並利用被害人名義以小額付款功能購買遊戲點數等等…

LINE 詐騙語錄-亂槍打鳥招數(絕對不能按)

「這是那晚你沒來的照片，我被整慘了！」
「我在墾丁拍的照片，你覺得哪張最好看？」
「朋友家的狗狗參加人氣比拼，幫忙讚一下！」
「被偷拍的是你嗎？」
「老同學來看我現在的照片，能想起來我是誰嗎？」

你不能相信 LINE 的裝熟簡訊

LINE 詐騙語錄-亂槍打鳥招數(絕對不能按)

LINE 詐騙語錄-個資外洩-手機電話號碼跟全名

「ＸＸＸ(你的全名)，這是我哥的新女友，是你同學嗎？」

→ 可能改成我爸、我弟之類的

「ＯＯＯ(你的全名)，這是上次聚會照片，你好好笑喔！」

→不熟悉的簡訊號碼，網址千萬不要亂點啊！

「ＸＸＸ(你的全名)，還記得我嗎？」

→ 超高危險的陷阱！藉著人的好奇心以及對失聯故友的期待，極有可能就給他點下去了！

LINE 帳密被盜高危險群

1. 設定「公開ID」
2. 在公用電腦登入 LINE
3. 允許手機通訊錄自動加入好友
4. 授權 LINE 遊戲讀取你和好友的個人資料
5. 同一組帳號密碼通用，導致Facebook、信箱等帳密遭破解，LINE也隨之被盜用
6. 沒有使用電腦版 LINE，卻沒關閉「允許自其他裝置登入」
7. 沒有定期更改密碼

LINE防詐騙的解決方法！

1.取消設定「自動加入好友」

如果對方有你的電話號碼，而你的LINE又有綁定號碼的話，就會被加入對方的好友名單。

LINE防詐騙的解決方法！

2.取消「允許用ID加入好友」

也許你的e-mail帳號或是其他Blog帳號等等，跟你的LINE ID是一樣的，很容易被有心人士猜到、找到你的LINE喔！

LINE防詐騙的解決方法！

3.LINE 阻擋非好友／廣告訊息

勾選「阻擋訊息」
→就不會收到非好友的訊息了喔！

LINE防詐騙的解決方法！

5.取消電信小額付款機制

※目前能植入木馬程式的大都是Android作業系統；電信小額付款雖定有上限，但沒限定一天使用幾次，有被害人一天損失三萬元

※請儘快聯絡你的手機服務商，將「小額付費」功能給關閉，（雖然是「小額」，但也有可能收到上千元的帳單！）。

LINE防詐騙的解決方法！

6. 舊版本 Line 隱藏漏洞，因此建議隨時更新

LINE防詐騙的解決方法！

7. 謹慎使用電腦版 Line

需要使用時才開啟，平時關閉該功能：

I. 設定方式：其他→設定→「我的帳號」→「允許自其他裝置登入」，避免駭客取得的帳密後從電腦登入。

II. 電子郵件帳號應設定密碼並定期變更。

LINE防詐騙的解決方法！

8.取消允許自其他裝置登入

發現帳號遭盜，立刻進入「其他」→「設定」→「我的帳號」後，把「允許自其他裝置登入」的打勾取消，並設定「換機密碼」

LINE防詐騙的解決方法！

9.避免在公用電腦登入個人LINE帳號(Facebook也是)

LINE好友加入方式 -透過行動條碼

禁止使用不易驗證對方身份之方式加入好友，如禁止使用「邀請(SMS、Email、Facebook、WhatsAPP)」及「搖一搖」功能加入好友，建議以下方式加入好友：

(1) 透過行動條碼(雙方同時進行以下步驟)： 設定方式：其他→加入好友→行動條碼

LINE好友加入方式-透過 ID 加入好友

(2) 透過 ID 加入好友(雙方同時進行以下步驟)：
設定方式：

※被加入好友者：設定→個人資料→開啟「允許透過 ID 加入好友」。

※加入者：其他→加入好友→ID 搜尋→輸入欲加入好友之 ID。

※被加入好友者：設定→個人資料→取消「允許透過 ID 加入好友」。

LINE好友加入方式-當心「山寨好友」Line詐騙

志明

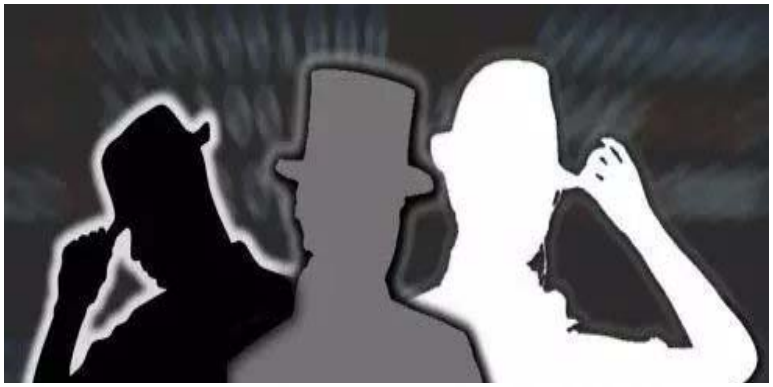
志明

確認加入好友之正確性：

1. 使用者應檢視好友名單內好友名稱是否具唯一性（如，不應同時出現兩個相同或類似的好友名稱）
2. 別人可以下載你的line照片，然後把暱稱改成你的名字，再把你封鎖，然後完全可以冒充你，其他人無從分別

哪個
才是
志明??

什麼是網路釣魚？



網路釣魚的運作手法是：

網上銀行線一個誘騙上仿銀行站，上或PIN進設立站碼。網網密料。模可）偽偽、資會他站的在號密犯其網真者帳機罪或的亂用入類路（易可使登此網站交幾使入碼

什麼是網路釣魚？

通常網路罪犯會假借某家銀行或金融機構的名義，散播大量不實郵件，並於郵件內容中附上偽網站的連結。姑且不論收到這些郵件的人是否為銀行客戶，僅有少部分的人會落入此種詐欺陷阱中，使網路罪犯成功詐取金錢。

什麼是網路釣魚？

http://gdfgas.com.cn 怎麼會是要輸入yahoo帳號密碼????

什麼是網路釣魚？

假網址：
http://yahootw.baoidc.cn/

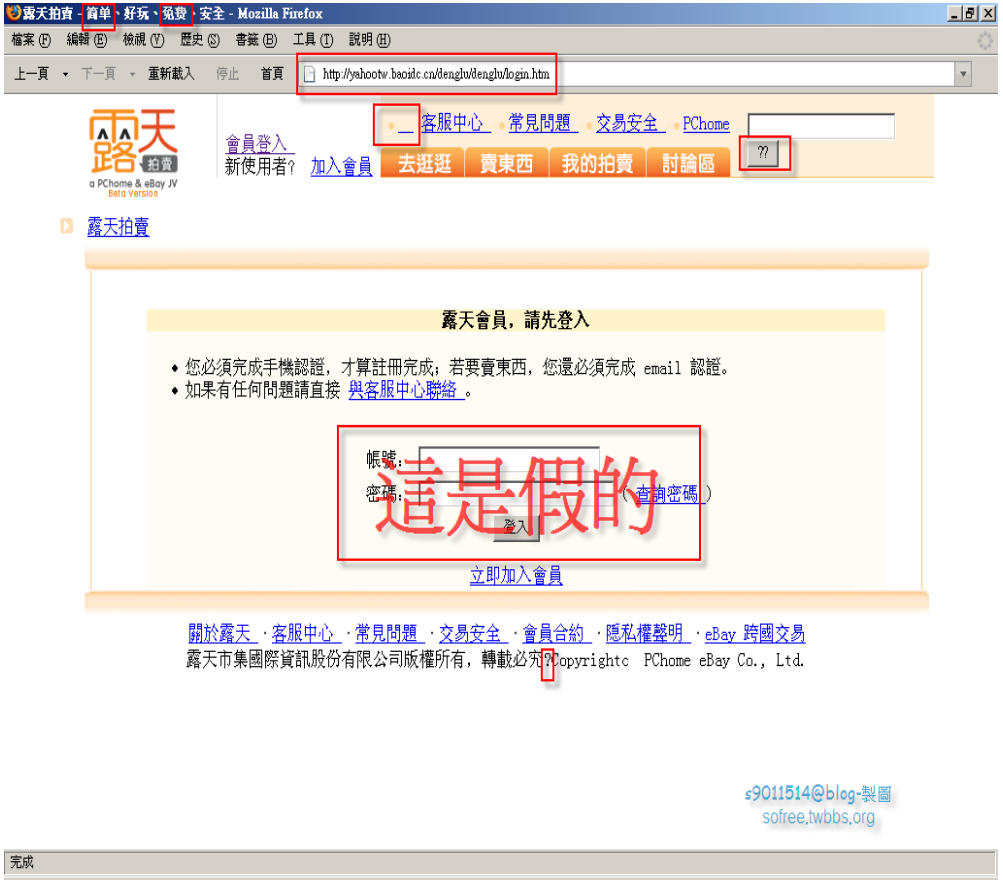
基本上，Yahoo網域的網址，至少都要有『yahoo.com』這字眼

什麼是網路釣魚？

假網址：
http://www.bidyahooo.com/

這個沒注意看，真的會弄錯，因為他申請的網域和yahoo很逼近

什麼是網路釣魚？



假網址：

http://yahootw.baoidc.cn/denglu/denglu/login.htm

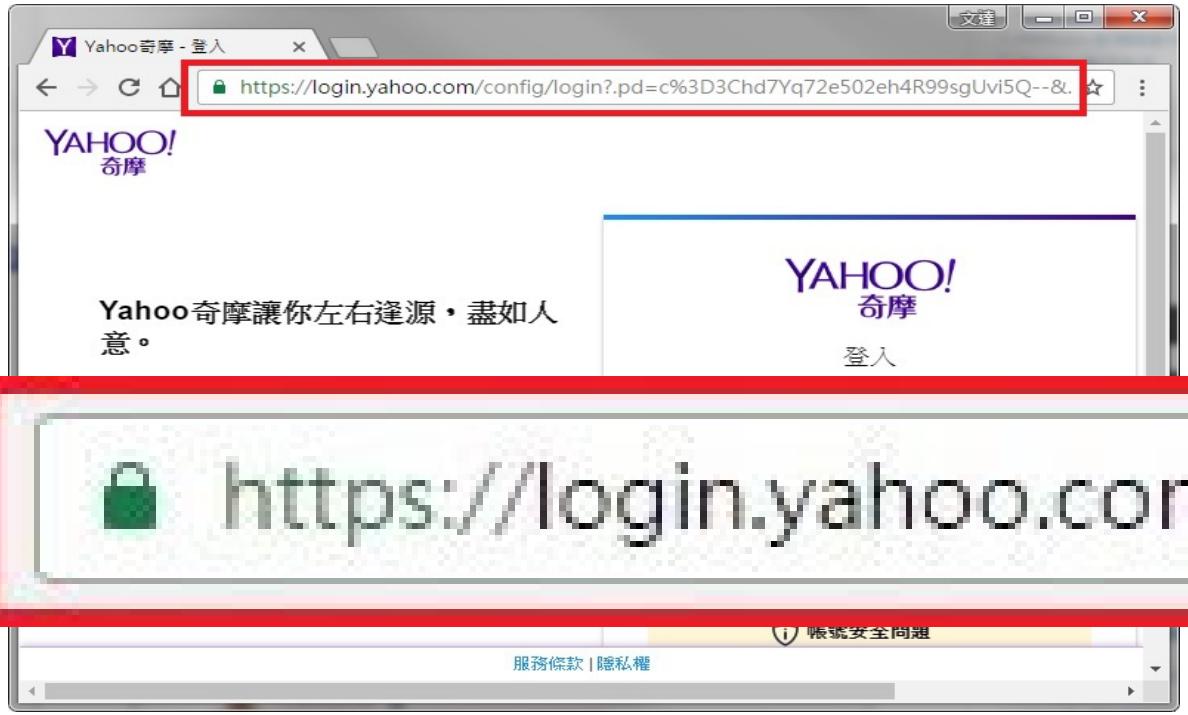
這一個整個很誇張，網頁錯誤連篇，還有簡體中文字

網址也很奇怪，一看就知道是假的，不過沒注意的人，還是可能會上當，請小心!!

什麼是網路釣魚？


真
假
土地銀行入口網站 - Windows Internet Explorer
http://www.landbank.com.tw/
http://www.1andbank.com.tw/
Google 日曆
土地銀行入口網站
土地銀行 LAND BANK
www.landbank.com.tw
關於土銀
土銀業務
最新動態
金融資訊
理財資訊

什麼是網路釣魚？



https://login.yahoo.com/config/login?.pd=c%3D3Chd7Yq72e502eh4R99sgUvi5Q--&.src=auc&.intl=tw&.done=https://tw.bid.yahoo.com/

這是真的

什麼是網路釣魚？

這是真的

真網址：

https://member.ruten.com.tw/user/login.htm

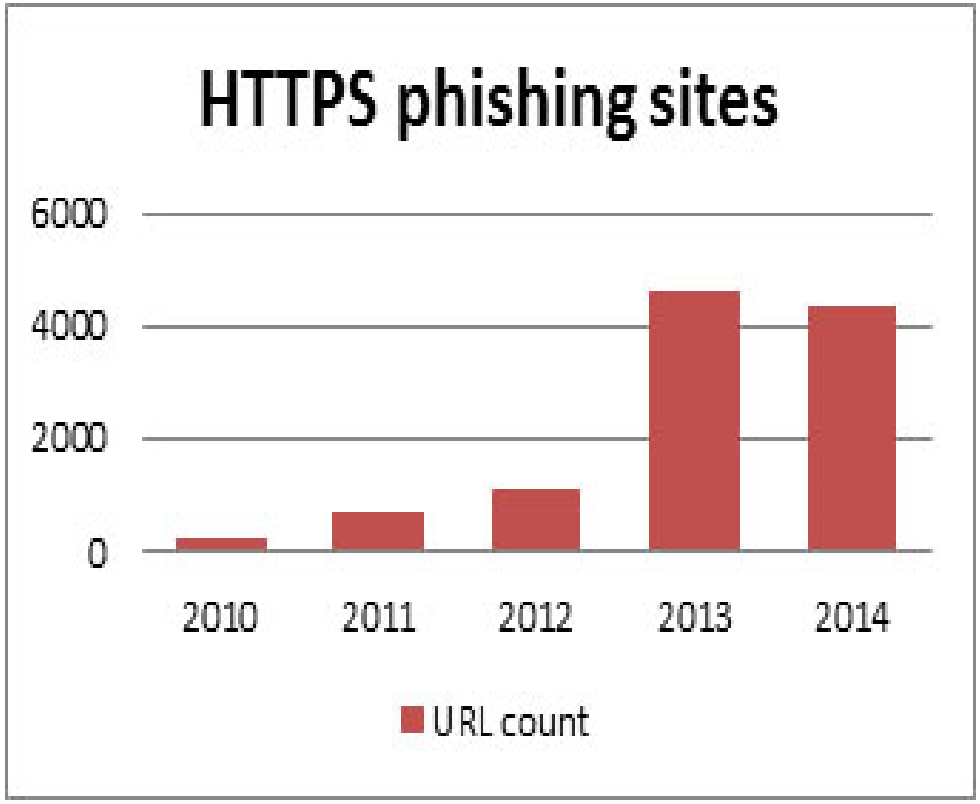
*請參照憑證授權單位敘述中的詳細資訊。

發給:	*.ruten.com.tw
簽發者:	Symantec Class 3 Secure Server CA - G4
有效期自	2016/ 5/ 17 到 2017/ 5/ 18

如何保護自己不受網路釣魚攻擊？

（1）對於詢問您個人資料的信件提高警覺
（2）不要隨意點選信件中的網址連結及開啟附件
（3）勿貪小便宜點選好康連結
（4）定期檢查交易紀錄與網站帳號
（5）透過加密的網頁功能傳送個人資料
（6）使用安全有效的防護產品
（7）主動回報釣魚網站資訊

如何保護自己不受網路釣魚攻擊？



HTTPS鎖頭保證安全嗎?

根據調查結果顯示，使用HTTPS釣魚網站的數量在增加，我們預期它在2014年後半因為假期季節的到來會有倍數的成長。

如何保護自己不受網路釣魚攻擊？

如何辨識網站是否安全？

1. URL是否以「https://」為開頭

2. 憑證網域名稱與網址相符

例：憑證有yahoo.com

網址https://www.yahoo.com

由於網路釣魚者無法偽造以上這兩種項目

什麼是勒索軟體

- 勒索軟體是一種讓受害者不能夠存取他們電腦的惡意軟體。
- 它的目的是要威脅受害者付出贖金來讓系統或資料復原。勒索軟體分成兩種，一種是加密型勒索軟體，另外一種是限制系統
- 運作的勒索軟體（例如將受害者系統鎖住，除了付贖金之外，不能做其他動作）。

勒索軟體的流行原因

1. 金流的隱匿性(比特幣)：

勒索軟體最終的目的是從中得利，所以金流一向是勒索軟體所重視的，金流必須具有匿名性而且可靠，2009年出現的**比特幣**剛好符合這個特性。

勒索軟體作者不再需要使用預付卡這類的付款機制，而是可以直接透過網路匿名交易比特幣來獲取不法收益，最重要的是，很難發現他們的行蹤。

2. 獲利很高：

而當惡意駭客發現使用勒索軟體的獲利能力很高時，便大量撰寫勒索軟體來增加收益，部分更開始經營勒索軟體服務。

2016年六大勒索病毒

1. JIGSAW:《奪魂鋸》殺人魔現身勒索軟體:「I want to play a game with you…」
2. CERBER：會說話的加密勒索軟體,台灣是攻擊目標
3. MICROP:V怪客現身,假冒海關所用的貨物進出口表格,誘騙使用者啟用巨集
4. Crysis: 已從中毒電腦移除,還能再度感染系統 ！ Crysis 透過暴力破解遠端桌面協定（RDP）散播
5. CryLocker: 打包中毒系統資料後,用PNG圖檔上傳 Imgur 相簿
6. Stampado: 每六個小時就會有一個隨機檔案被永久刪除，96小時後解密金鑰就會永遠消失

勒索軟體所造成影響

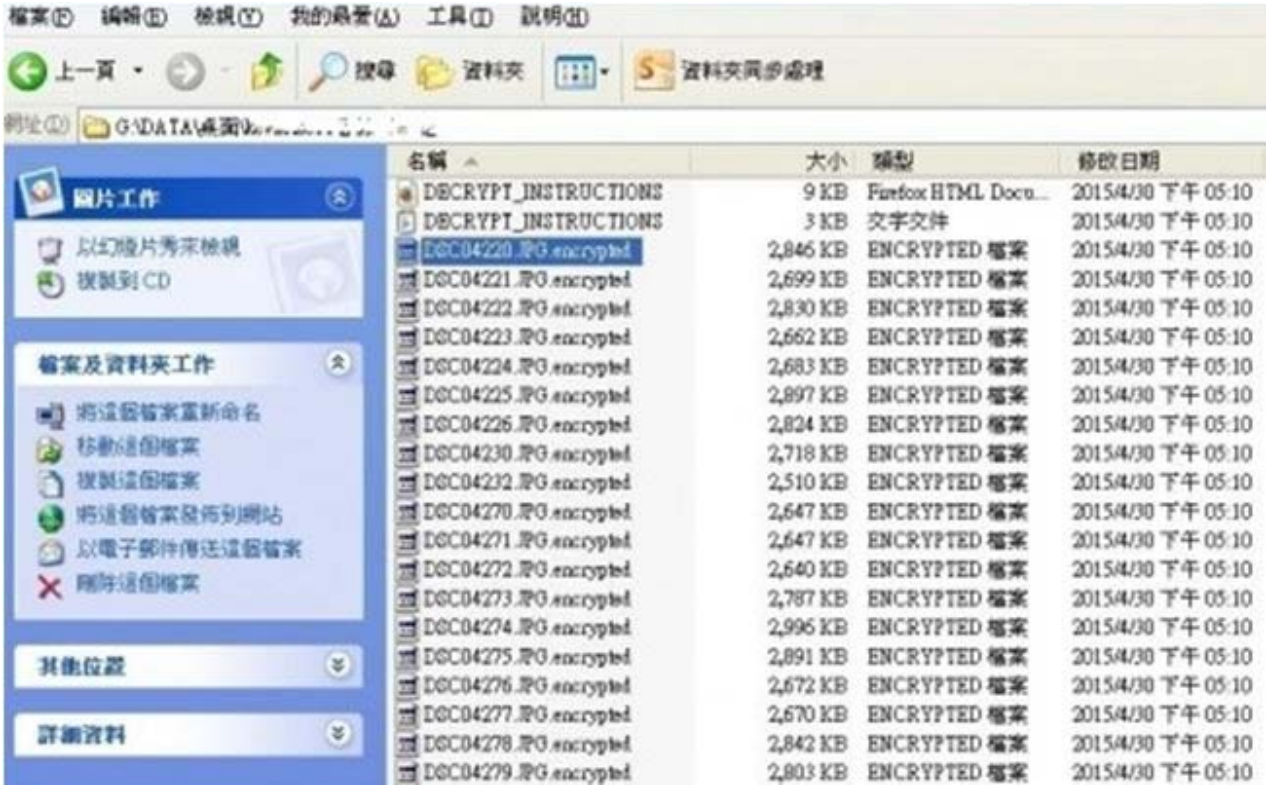
1. 限制系統運作類型

駭客讓使用者無法正常使用電腦，直到使用者付出贖金，才能正常使用系統，這種類型不是對檔案加密，而是鎖住電腦。

2. 檔案加密類型

駭客會針對目標檔案使用加密演算法進行加密，多為文件與影音照片，讓使用者無法開啟自己的檔案，由於文件與影音照片對大部分使用者的價值較高，所以願意付出贖金的意願也會更大。

勒索軟體所造成影響



中了此類病毒後會優先攻擊文件、圖片、影音資料被加密，文件檔案會多一串「encrypted」的字眼

勒索軟體所造成影響

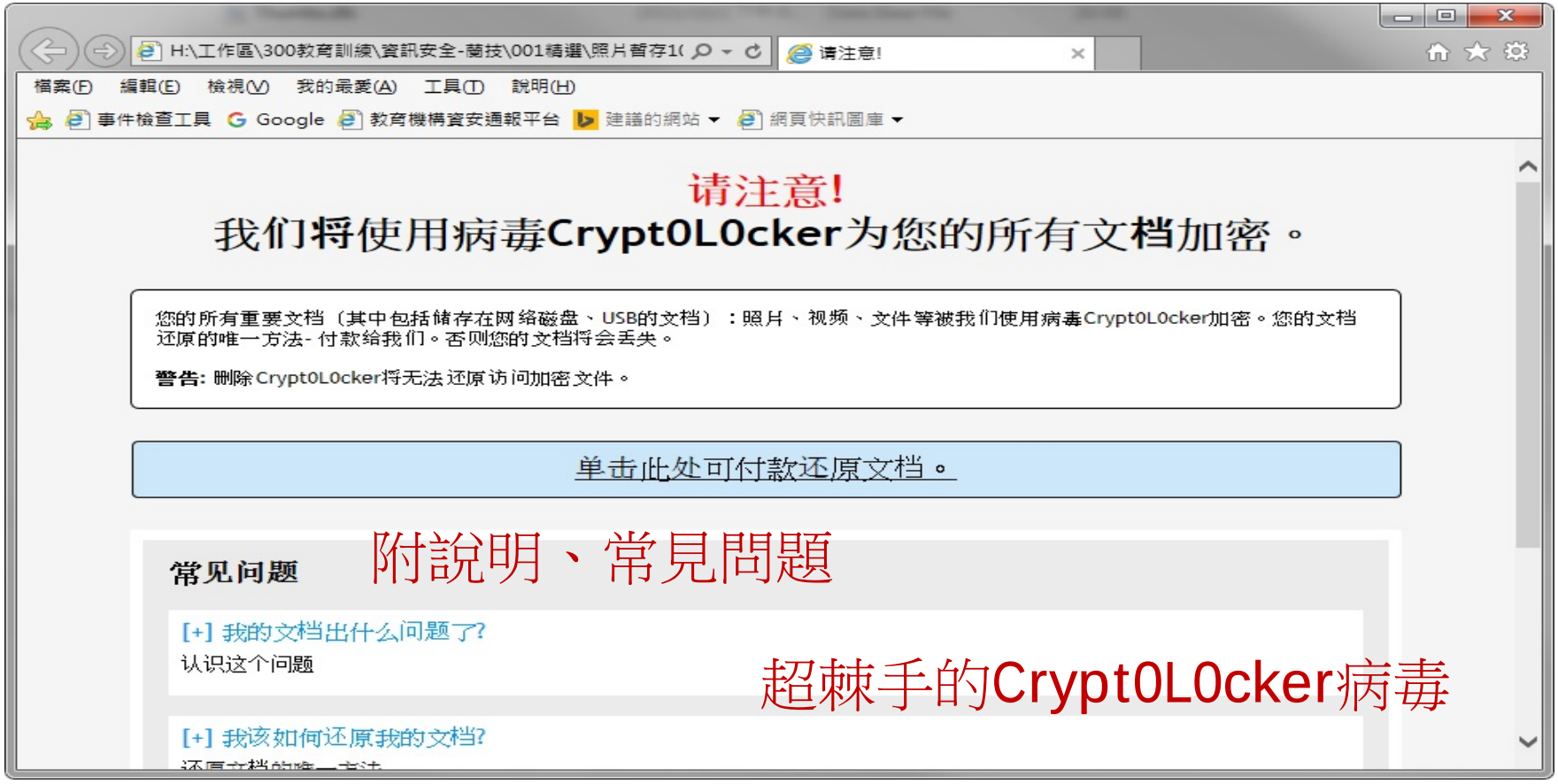
讀我檔案--付款說明

勒索軟體所造成影響

讀我檔案--付款說明

指名-$比特幣

勒索軟體所造成影響


H:\工作區\300教育訓練\資訊安全-蘭技\001精選\照片暫存1(
请注意!
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
事件檢查工具 Google 教育機構資安通報平台 建議的網站 網頁快訊圖庫
请注意!
我们将使用病毒CryptOLOcker为您的所有文档加密。
您的所有重要文档（其中包括储存在网络磁盘、USB的文档）：照片、视频、文件等被我们使用病毒CryptOLOcker加密。您的文档还原的唯一方法- 付款给我们。否则您的文档将会丢失。
警告: 删除CryptOLOcker将无法还原访问加密文件。
单击此处可付款还原文档。
常见问题
附說明、常見問題
[+] 我的文档出什么问题了?
认识这个问题
超棘手的CryptOLOcker病毒
[+] 我该如何还原我的文档?

勒索軟體的傳播途徑

1. 網路釣魚郵件：大部分的釣魚郵件都會將執行檔偽裝成文件檔案
2. 惡意廣告：只要瀏覽器或裝置顯示出惡意廣告，使用者就會受到攻擊
3. 網頁掛馬：在您的網頁上放入script導向裝載「漏洞攻擊套件(Exploit Kit)」的網頁
4. Botnet：Botnet的地下組織開始提供勒索軟體的服務(RaaS)
5. 先滲透再攻擊：例如透過TeamViewer的漏洞下載並執行
6. 主動橫向感染：透過遠端桌面的漏洞來橫向感染他人電腦

勒索軟體的防治

1. 不上鉤：標題特別吸引人的電子郵件務必停看聽。
2. 不打開：不隨便打開電子郵件附件檔。
3. 不點擊：不隨意點擊電子郵件夾帶的網址。
4. 要備份：重要資料要備份。
5. 要確認：開啟電子郵件前要確認寄件者身分。
6. 要更新：作業系統、應用程式(例如Flash, Acrobat, Office、防毒軟體病毒碼一定要隨時更新。

就是密碼設定太過簡單才讓你身處危險

在電腦與網路的世界裡，我們都是透過不同的帳號，來代表每個人不同的身分，而「密碼」就是用來檢查身分正不正確的工具；

你可以試著想像：帳號就像我們住的房子而密碼就是大門的門鎖，如果帳號 沒有設定密碼，就像是大門沒有上 鎖，陌生人也可以自由進出，對我 們的安全就會造成很大的威脅！

利用「暴力破解」很快就能猜到你的密碼

什麼是「暴力破解」呢？就是有心人士利用電腦程式，
反覆嘗試輸入各種組合的密碼，直到密碼被破解為止。

因為密碼是由字元組合成的，如果密碼的長度太短，
或是沒有混合使用數字、英文大小寫或特殊字元

這種強度不足的「弱密碼」就會在短時間內被破解囉！

利用「暴力破解」很快就能猜到你的密碼

密碼長度	英文字母 (26 字元)	英文字母+數字 (26+10 字元)	英文字母大小寫 (52 字元)	含特殊符號字元 (96 字元)
4	0	0	1 分鐘	13 分鐘
5	0	10 分鐘	1 小時	22 小時
6	50 分鐘	6 小時	2.2 天	3 個月
7	22 小時	9 天	4 個月	23 年
8	24 天	10.5 個月	17 年	2287 年
9	21 個月	32.6 年	881 年	21 萬 9000 年
10	45 年	1159 年	45838 年	2100 萬年

一定要避免的密碼設定方式

以下的密碼設定方式都非常不安 全，請一定要避免：

1. 不設定密碼（把密碼設為空白）
2. 使用簡單的字元組合（例如1234、abcd、111111 等）
3. 密碼和帳號相同
4. 使用生日、身分證字號、英文名 字等個人資料
5. 使用學校、班級名稱

要盡量避免的密碼設定方式

以下是大家常使用的密碼設定方式，雖然很容易記憶和使用，可是密碼強度似乎不足，我們應該盡量避免：

1. 常用的英文單字或片語(如superman、hello 等)
2. 隨意的數字組合
3. 連續的字元組合（如mnopqr、87654等）或重複的字元組合（如kkkkkk、888888）
4. 鍵盤的按鍵順序組合（如asdfgh、1qaz 等）

密碼的安全設定原則

(1)不要使用懶人密碼：

懶人密碼就是使用者為了好記，使用很簡單的密碼（如123456），甚至不設定密碼，或將密碼和帳號設成一樣，這種沒有強度的密碼設定，是非常危險的喔！

密碼的安全設定原則

(2)長度與複雜度

密碼長度至少應該設定8碼以上，而且要混合大小寫英文字 母、數字和特殊符號。因此，符合安全要求的密碼至少包含 下列項目：

一個大寫英文字母

一個小寫英文字母

一個數字

一個特殊字元，如：！ @ # $ % & 等

密碼的安全設定原則

(3) 密碼不要有明顯的含義

設定密碼時應該避免只使用單字或片語，因為有心人士只要利用字典將所有單字逐一進行測試，就可以破解密碼，另外，也要避免使用具有特殊意 義的名詞（如：家人的姓名或 生日等），才不會讓有心人士很容易就能猜到你的密碼喔！

密碼的安全設定原則

(4) 避免設定相同的密碼

不可以為了方便，就把自己所有的網路服務都設定成相同的 帳號與密碼，這樣有心人士只 要知道你的一組帳號密碼，就 可以盜用你所有的網路身分。

Gmail、Facebook、Line、Y拍、露天等等

密碼的安全設定原則

(5)定期更新

密碼設定除了要符合以上的各種要求之外，定期更新密碼也很重要喔！建議大家至少每60~90天就要重新設定一組新的密碼。

密碼設定小撇步，好記不糊塗！

讓複雜的密碼變得輕鬆好記！

※穿插法

將兩個英文字或數字穿插，不過若使用兩組數字穿插可就沒有意義囉！

範例：Good 與 2012 穿插後變成 G2o0o1d2

密碼設定小撇步，好記不糊塗！

※字母位移法

將英文字母往前或往後移動幾個位置，如將 A 往後移動一位變成 B。

範例：GOOD 往後移動一個字母變成 HPPE

密碼設定小撇步，好記不糊塗！

※順序位移法

將原本有意義的字元重新排列 順序，就可以降低字面的明顯意義，例如將奇數與偶數字元對調，或自己可以設定任何一種規則來進行字元移動。

範例：將 GOOD 字元以 2143 重新排序變成OGDO

密碼設定小撇步，好記不糊塗！

※輸入法變化

其實中文輸入法就是一種最簡單又有效的變換方式，只要把中文字的拼音轉換成鍵盤上的字母，簡單的密碼也可以變成難以猜測和理解的密碼囉！

範例：將「大家好」
使用注音輸入法成為 284 RU8 CL3。

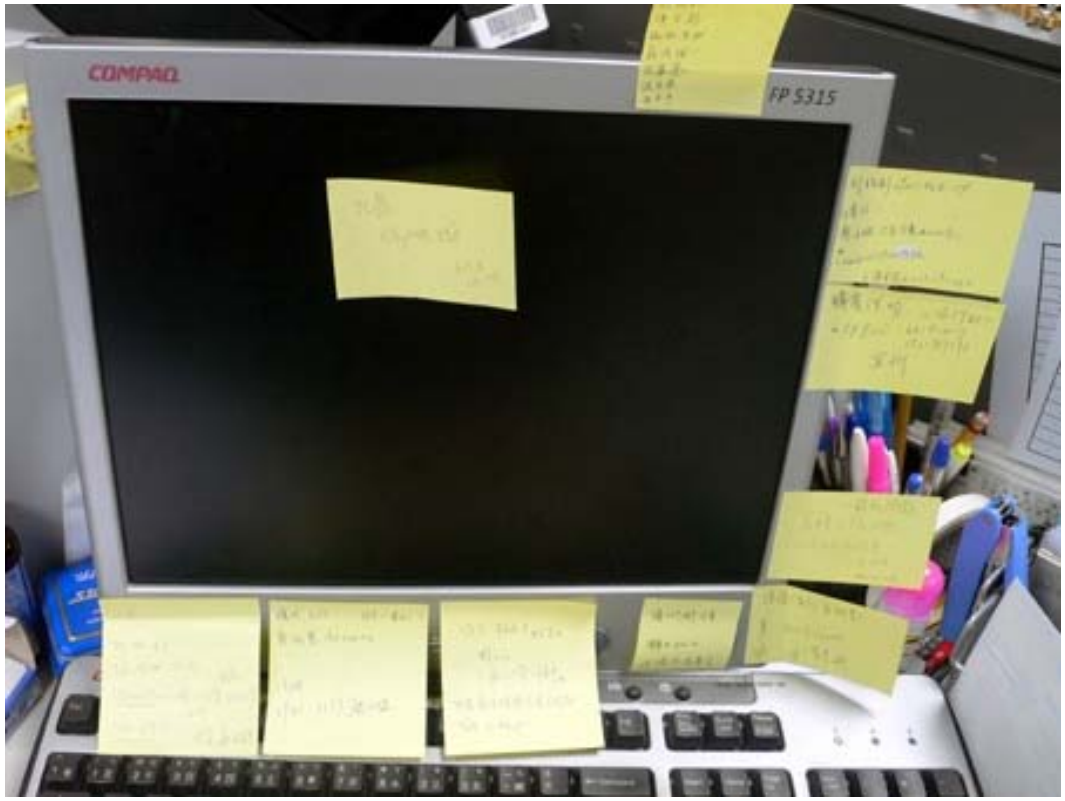
密碼設定小撇步，好記不糊塗！

※鍵盤位移法

利用電腦鍵盤按鍵的位置進行字元移動，例如 A 向右移兩位 為D，B向左移一位為V。

範例：將GOOD在鍵盤向左位移兩個字母變成 DUUA

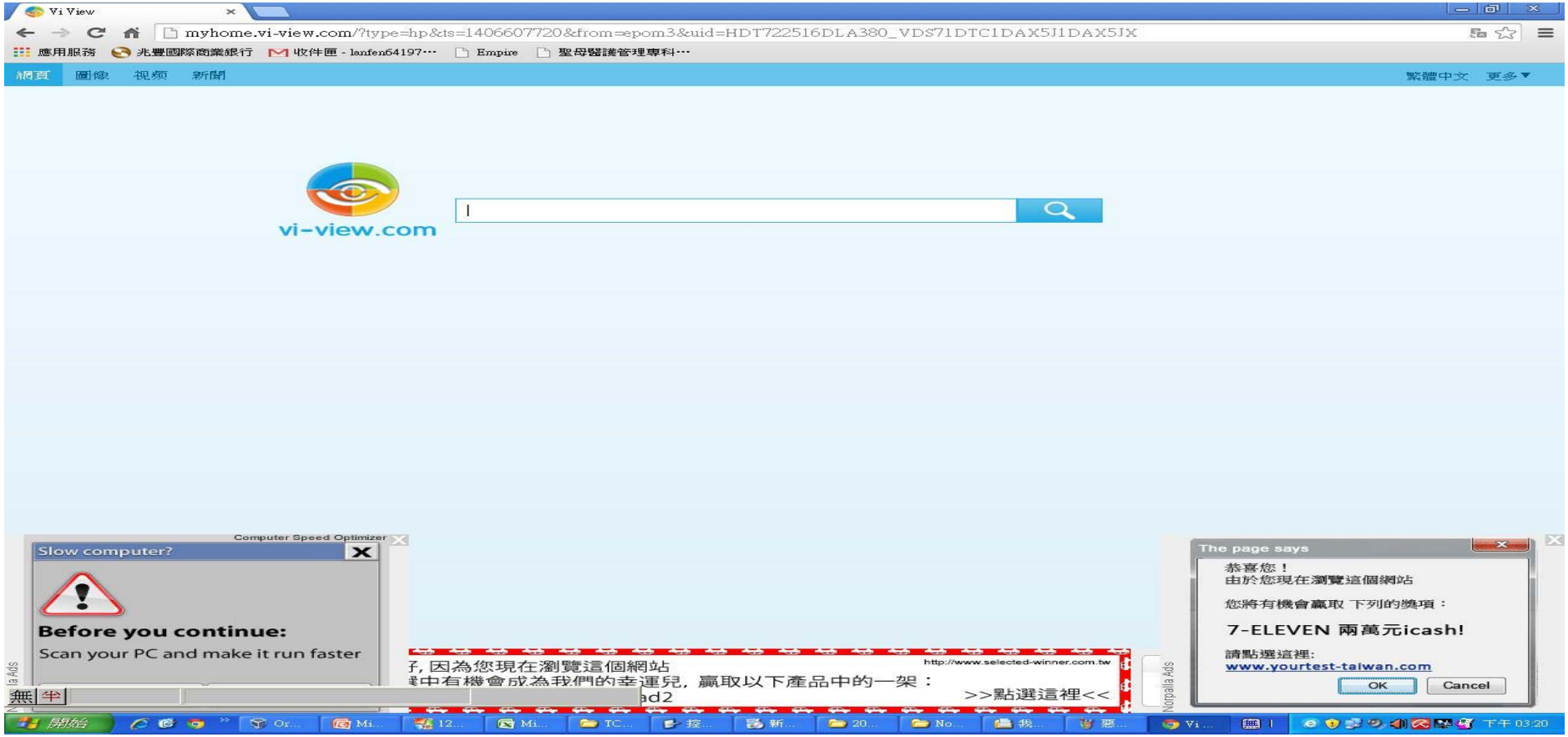
密碼設定小撇步，好記不糊塗！



密碼貼在螢幕上???

USB病毒交互感染，被植入木馬

安裝非法軟體~電腦中毒、瀏覽器被綁架



安裝影片快播軟體~被植入惡意程式

安裝盜版軟體~被植入惡意程式

個人電腦作業系統、應用程式、防毒定期更新

Windows Updata

防毒軟體病毒碼更新

Adobe flash Play

Java Runtime

個人電腦資料要備份嗎?

硬碟會壞嗎?

- 硬碟是會壞的，而且不只是硬碟，所有儲存裝置都會壞。
- 因為儲存的裝置會壞所以我們才要備份。
- 換一個地方存檔不叫備份，要多存一份才叫備份。
- 現在的硬碟越來越不可靠了，因為大家只想買低價產品，廠商就算做得出耐用的硬碟也是沒人要買（因為會比較貴），這是市場劣幣逐良幣的結果。

資料備份幾份?備份到哪?

資料備份基本認知

1. 至少備份**二份以上**
2. 使用自動排程備份軟體
3. 雲端硬碟資料同步
   (注意機敏資料)

結　論

1. 不要輕易透露您的個人資料(手機、生日、姓名)
2. 請勿開啟不明來源之連結
   (透過Email、facebook、Line、手機簡訊等等跟您裝熟)
3. 各服務帳號、密碼不要相同、定期更改
4. 密碼長度大於8碼、符合複雜性

結　論

5. 不下載、不安裝盜版軟體、非官方提供軟體程式
6. 不要在公用電腦，使用您的帳號登入網站服務
7. 不要在公用電腦使用USB隨身碟、或切換為防寫
8. 作業系統定期更新、安裝有效防毒軟體
9. 資料要備份(不然被勒索就…沒救了)

有獎徵答：

1.網路詐騙有哪三要素?

有獎徵答：

1.網路詐騙有哪三要素?

ANS：問電話、傳簡訊、給認證碼

有獎徵答：

2.如何防治勒索病毒?

有獎徵答：

2.如何防治勒索病毒?

ANS：(1).不點擊不明連結

(2).資料要備份

(3).系統要更新

有獎徵答：

3.密碼複雜性為何?

有獎徵答：

3.密碼複雜性為何?

ANS：長度大於8
英文數字混合大小寫
含特殊符號

謝謝聆聽!!!

宜蘭區網中心
ILAN REGIONAL CENTER