國立屏東科技大學
National Pingtung University of Science and Technology

資安新知社交工程與挖礦

中華電信學院高雄所
陳益源

大綱

- 社交工程與防範
- 通行碼管理
- 安全電子郵件
- 瀏覽網站安全介紹
- 數位貨幣與挖礦

1.社交工程

電子郵件社交攻擊是駭客常使用的一種方式

互動方式
聊天、寄信、影音、檔案分享、部落格、新聞群組

真心朋友?
網路駭客在左右，
稍有不慎生風險。

長期潛伏
長期蒐集資訊
多重攻擊路線
組合式攻擊

社群網路為資訊的交流與分享提供了新的途徑。

社交工程

網路釣魚就像是現實生活的詐騙集團

偵查第九大隊　網路釣魚的目的希望達到受害者數量最大化

發稿時間　2013/5/27 上午 08:23:03

標題　偵破駭客偽冒健保局名義寄發惡意電子郵件盜取1萬多筆個資案

http://cib.kcbc.tw/News/Detail/27986

我們學到什麼?

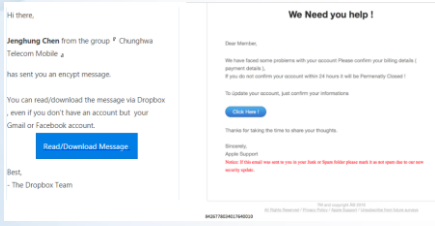
- 不開啟來路不明的電子郵件
- 不點選公務無關的超連結及附檔。

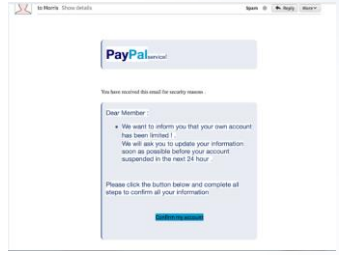
社交工程

講師畫面空間
請勿輸入文圖

網路釣魚透過逼真的仿造手法詐騙

幾乎每天都可以收到類似的釣魚信件　　若不細看背後的URL，很難留意到不同



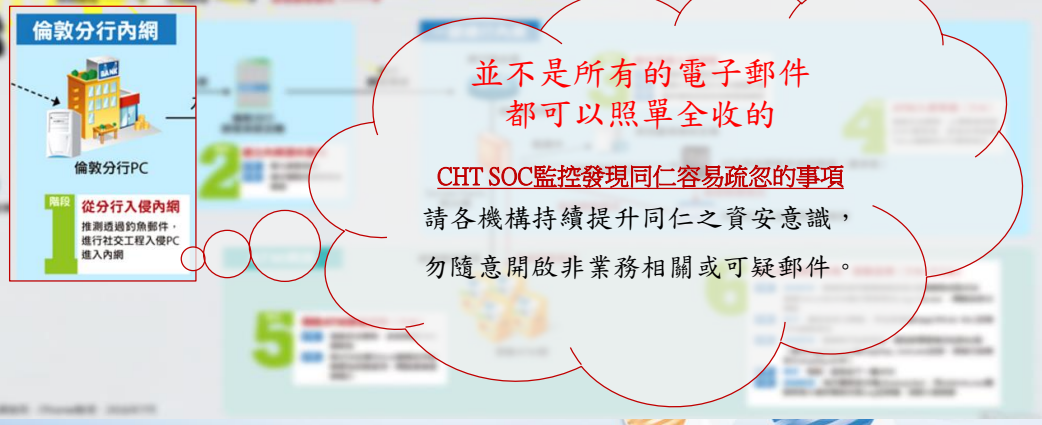


抄襲官方網站的登入頁面，但是資料卻傳到其他地方

透過圖片與超連結偽裝成檔案下載資訊

社交工程

案例分享:因釣魚郵件引發之社會案件



並不是所有的電子郵件
都可以照單全收的

CHT SOC監控發現同仁容易疏忽的事項

請各機構持續提升同仁之資安意識，

勿隨意開啟非業務相關或可疑郵件。

社交工程

案例分享：希拉蕊郵件門影響美國大選

使用私人電子郵箱和位於家中的私人伺服器收發公務郵件，涉嫌違反美國《聯邦檔案法》關於保存官方通信記錄的規定

公私分明

公務郵件和私人郵件的收取要分開，以免機敏資料外洩。

外部抽獎活動

公司的郵件帳號勿做私人用途使用，
私人的信件也勿轉寄到公司的郵件帳號處理

電子郵件社交工程防範(1/4)

透過電子郵件進行社交工程攻擊之常見手法

- ❑假冒身分(公務機關、金融機構、電信業者、熟人、同事、往來廠商等)
- ❑以熱門議題、大眾關切主題為郵件標題及內容
- ❑夾帶附件(含惡意程式)，誘使使用者點選後植入木馬程式
- ❑夾帶超連結，騙誘收件人連結至釣魚網站

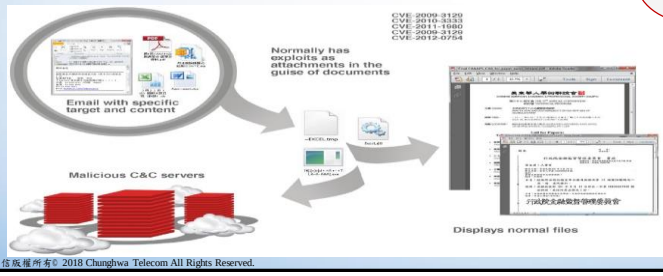
電子郵件社交工程防範(2/4)

要小心~釣魚郵件變成勒索軟體的攻擊管道

70%

常見釣魚郵件附檔檔案類型
.XLS、.PDF.DOC、.DOCX
(from 趨勢科技研究報告2012 年)

感染過程中的第一步就是開啟網路釣魚郵件



並不是所有的電子郵件
都可以照單全收的

-提高警覺-

郵件附件要求開啟巨集功能
(如EXCEL、word等)

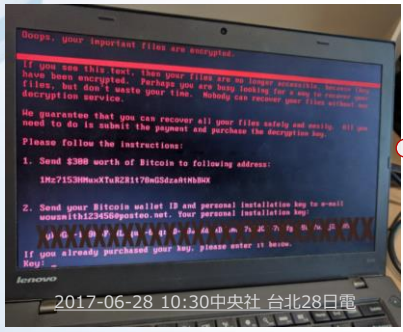
-確認郵件真偽-

以電話或其他非Email方式

8

電子郵件社交工程防範(3/4)

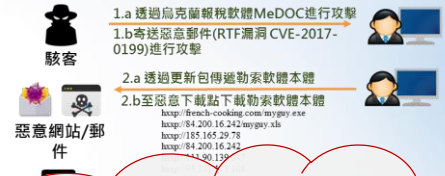
新版勒索病毒「佩提亞」來勢洶洶



受駭者：
俄羅斯石油公司Rosneft、
全球最大廣告公司WPP、
全球最大航運集團馬士基集團、
烏克蘭政府、
烏克蘭銀行體系等單位
都遭受大規模駭客攻擊。

石油
航運
政府機構
銀行體系

修正程式
防毒軟體
最新版本



-提高警覺-

當使用者收到用發票、水費或電費收據為名等來路不明或奇怪的電子郵件，記得不要點選信件內的任何連結

-確認郵件真偽-

以電話或其他非Email方式

9

電子郵件社交工程防範(4/4)

防範措施
6不
3要

1. 不開啟 寄件者為陌生名字之信件
2. 不開啟 寄件者為公司同仁，但非公司網域之信件 (cht.com.tw)
3. 不開啟 與公務無關之主旨信件及附檔
4. 不開啟 以非公務信箱寄送公務之信件
5. 不點選 非公務網址之連結
6. 不開啟 密碼直接放在E-mail裡的加密壓縮附件

1. 要將收信軟體設定為純文字瀏覽功能
2. 要關閉收信軟體的郵件預覽視窗功能
3. 要關閉收信軟體的郵件自動下載顯示郵件中圖片功能

簡訊社交工程防範(1/3)

行動裝置普及，簡訊詐騙成為台灣近期社交工程的新手法。

詐騙簡訊從何而來?

簡訊社交工程防範(2/3)

針對中華電信員工詐騙簡訊

公司提供以下三項建議措施

權限或帳密異動

本公司資訊系統之權限或帳密異動不會透過簡訊超連結方式，通知同仁登入網頁。

提高警覺

請各位同仁提高警覺，收到類似釣魚簡訊請勿點選超連結，並通報所屬機構資安專責人員。

立即更換

若曾連至該釣魚網站，請立即更換LDAP密碼。

12

簡訊社交工程防範(3/3)

-防範郵件帳號被入侵-

檢查本公司
WebMail登入紀錄是否正確?

檢查 登入時間

檢查 連線位址

13

辦識惡意郵件要領(1/6)

收到主旨前有標示[外部郵件])之信件，請提高警覺防範惡意攻擊

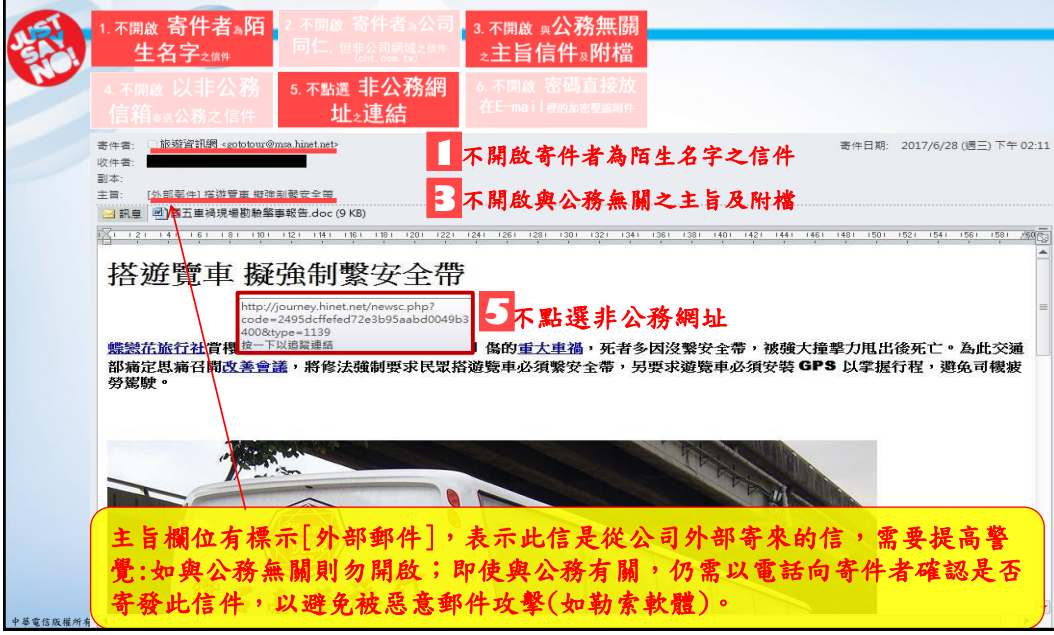
3要設定功能：

1. 要設定收信軟體為純文字瀏覽功能
2. 要關閉收信軟體的郵件預覽視窗功能
3. 要關閉收信軟體自動下載顯示郵件中圖片功能

6不開啟事項：

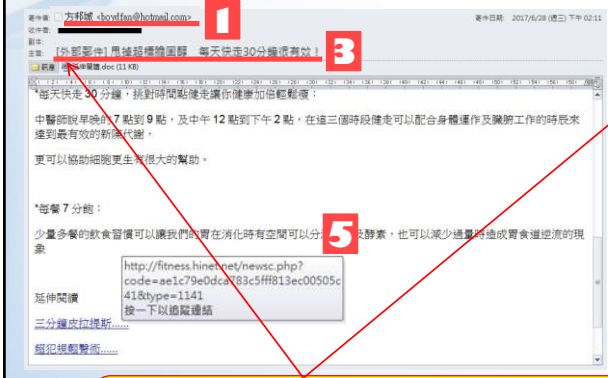
1. 不開啟寄件者為陌生名字之信件
2. 不開啟與公務無關之主旨信件及附檔
3. 不點選非公務網址之連結
4. 不開啟寄件者為公司同仁，但非公司網域(cht.com.tw) 之郵件
5. 不開啟以非公務信箱寄送公務信件，或自身業務與信件內容無關

辦識惡意郵件要領(2/6)



辨識惡意郵件要領(3/6)

1. 不開啟 寄件者為陌生名字之信件
2. 不開啟 寄件者為公司同仁, 但非公司網域之信件 (cht.com.tw)
3. 不開啟 與公務無關之主旨信件及附檔
4. 不開啟 以非公務信箱寄送公務之信件
5. 不點選 非公務網址之連結
6. 不開啟 密碼直接放在E-mail裡的加密壓縮附件



主旨欄位有標示[外部郵件]，表示此信是從公司外部寄來的信，需要提高警覺:如與公務無關則勿開啟；即使與公務有關，仍需以電話向寄件者確認是否寄發此信件，以避免被惡意郵件攻擊(如勒索軟體)。

16

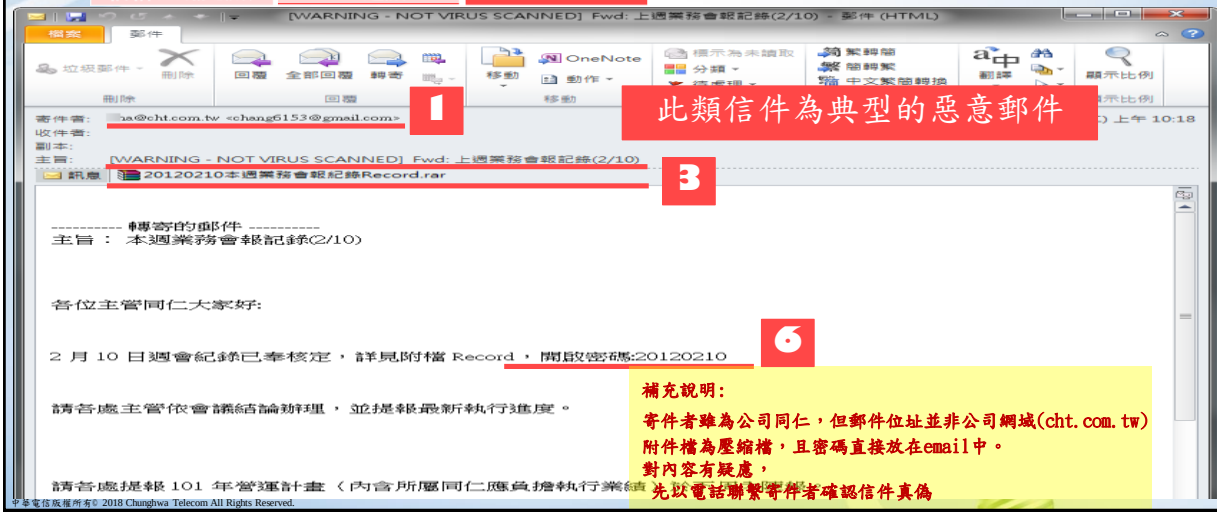
辨識惡意郵件要領(4/6)

1. 不開啟 寄件者為陌生名字之信件
2. 不開啟 寄件者為公司同仁, 但非公司網域之信件 (cht.com.tw)
3. 不開啟 與公務無關之主旨信件及附檔
4. 不開啟 以非公務信箱寄送公務之信件
5. 不點選 非公務網址之連結
6. 不開啟 密碼直接放在E-mail裡的加密壓縮附件

辨識惡意郵件要領(5/6)

JUST SAY NO!

1. 不開啟 寄件者為陌生名字之信件
2. 不開啟 寄件者為公司同仁, 但非公司網域之信件 (cht. com. tw)
3. 不開啟 與公務無關之主旨信件及附檔
4. 不開啟 以非公務信箱傳送公務之信件
5. 不點選 非公務網址之連結
6. 不開啟 密碼直接放在E-mail裡的加密壓縮附件



補充說明:
寄件者雖為公司同仁，但郵件位址並非公司網域(cht.com.tw)
附件檔為壓縮檔，且密碼直接放在email中。
對內容有疑慮，
先以電話聯繫寄件者確認信件真偽

辨識惡意郵件要領(6/6)

想知道更多？

105-106年社交工程郵件點擊主旨彙整

這些郵件前面都有“[外部郵件]”字樣

【快來看】年金改革方案 十大重點看這裡	地震來了! 爭取黃金逃命10秒APP大進擊
甩掉超標膽固醇　每天快走30分鐘很有效！	大齡單身女神　賭你光看外表絕對猜不出她幾歲
別再用寶特瓶裝水了！各項研究告訴你它可怕的真相！	海洋暖化速度 近年持續加快
駭客攻擊8家券商 金管會：恐還有下波	不斷溫柔撫摸小倉鼠 就能目睹超萌事件發生
領務局LINE新功能 出國旅遊添保障	掀開團購價格的謎底
認識禽流感	餓過頭才吃飯 亂了代謝易罹糖尿病
勞動部長：周休二日落實 就沒7天國定假日	「想離職又捨不得這份薪水...」給工作人的２１個解答
批「柿子挑軟的吃」 李來希：年改會只敢對公務員開刀	登革熱茲卡病毒染南美 美發旅遊警示
勒索軟體肆虐! 如何避免您的電腦變磚塊	賞櫻不只在日本 全球最美櫻花大道夢幻繽芬
一銀ATM遭駭被盜8000萬，專家告訴你問題出在哪？	

2.通行碼管理規則(1/4)

通行碼猶如鑰匙

存取系統提供相關服務及資料

妥善保管通行碼 ▶ 外洩 ▶ 駭客利用

通行碼管理規則(2/4)

若通行碼強度不足非常容易被破解

Q: 請問您是否曾經因方便將通行碼設為123456？

A: 2016 冠軍 最糟通行碼

2016 list is based on **over 5 million** passwords posted or for sale on the Internet

Almost **4% of people** use the worst password, **123456.**
Just over **10% of people** use one of the **25 worst passwords .**

from : https://www.teamsid.com/worst-passwords-2016/

通行碼管理規則(3/4)

通行碼安全性強化方法

提高通行碼複雜度 ▶ **避免使用易猜通行碼** ▶ **定期更換多組通行碼**

APPLE123

↓ 改變大小寫與符號

aPplE1@3

↓ 加入隨機字元與符號

aPpl~EIfU1@3K

RANK	PASSWORD	CHANGE FROM 2015
1	123456	Unchanged
2	password	Unchanged
3	12345	2↗
4	12345678	1↘
5	football	2↗
6	qwerty	2↘
7	1234567890	5↗
8	1234567	
9	princess	
10	1234	
11	login	
12	welcome	

APPLE123

APPLE123_fb

APPLE123_email

1.重複或者順序數字密碼
2.英文單字密碼
3.鍵盤排列密碼 (駭客知道鍵盤排列會符合密碼規則)
4.生日密碼 (實際上變動位數只有六位19xx xx xx)
5.中文姓名拼音/注音密碼 (對岸駭客也懂)

通行碼管理規則(4/4)

針對公司而言
通行碼

重要性
公司內部各資訊系統使用SSO(單一帳號/密碼)登入，故通行碼的保管更行重要。

定期更換
通行碼應定期(每90天)更換。

通行碼常見錯誤樣態

具備複雜度
避免被駭客猜中或破解。
例如：長度、使用大寫及小寫英文字母、阿拉伯數字、特殊符號

通行碼設定長度限制

一般使用者
通行碼長度至少為8碼

系統維運者
通行碼長度至少為12碼

通行碼常見錯誤樣態

通行碼常見錯誤樣態(1/4)

使用**弱密碼或密碼**以**明文**存放在電腦上，容易造成帳密**被破解**或**被竊取**。

當年英國威廉王子這張照片發佈不到一天，就被追全面下架，不過內容早就被備份了....你看到問題了嗎?

The Royals Watch

Prince William makes up his bed on base. A 24-hour shift means staying close to ...

THESTAR.BLOGS.COM

我們
學到什麼?

隨時提高警覺，
擁有危機意識，
勝過一切資安管控機制

From http://thestar.blogs.com/.a/6a00d8341bf8f353ef017c33d0173a970b-pi

通行碼常見錯誤樣態(2/4)

設備**未修改預設密碼**，容易造成**駭客**使用預設密碼即可**存取設備**。
(使用google搜尋就可以找到各種設備的預設密碼)

「北韓版Facebook」被破解　帳密竟然出奇地簡單

2016/06/01 16:46:00

文／卡卡洛普

北韓大約從今年四月起就屏蔽Facebook、Twitter、Youtube等知名社群網站，那當地人要怎麼透過社群交流呢？答案就是用他們自己創建的StarCon來分享生活！

我們
學到什麼?

關閉
系統或設備
之預設帳號及通行碼
ADMIN　ROOT
Administrators

Andrew Mckean(**駭客是年僅18歲的蘇格蘭少年**)表示他其實**無意要破解**只是簡單在用戶名稱輸入「admin」，通行碼輸入「password」就登入系統，他也沒想到管理者權限的帳密如此簡單

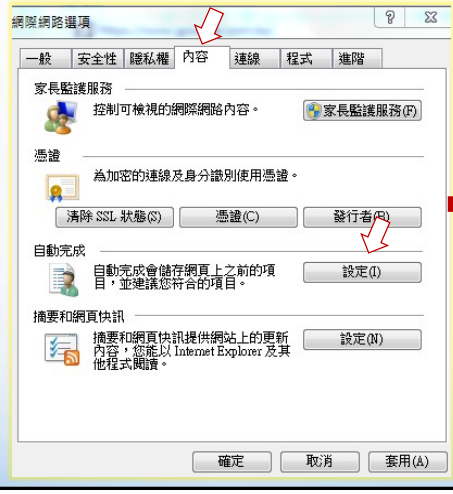
通行碼常見錯誤樣態(3/4)

在共用電腦上存取本公司系統,瀏覽器開啟自動儲存通行碼功能,容易造成帳號/通行碼外洩。

關閉

自動儲存通行碼功能步驟如下：

- 點按[工具]
- [網際網路選項]
- [內容]
- [設定]功能
- 表單上的使用者名稱及密碼



通行碼常見錯誤樣態(4/4)

使用同一帳號/通行碼登入所有網站,容易造成帳號/通行碼外洩。

祖克柏臉書帳號遭駭　密碼竟然是…

記者黃日暉／綜合報導

2016.06.07 / 10:51

採用弱通行碼
且通行碼共用

根據《華爾街日報》報導，　From http://www.nownews.com/n/2016/06/07/2126587
祖克柏在社群網站「推特」（Twitter）和「Pinterest」的帳號
日前遭駭客入侵，駭客是先駭進他在另一個社群網站「LinkedIn」，
並破解出通行碼為「dadada」後，
再用此通行碼順利駭入他其他網站的帳號。

我們學到什麼?

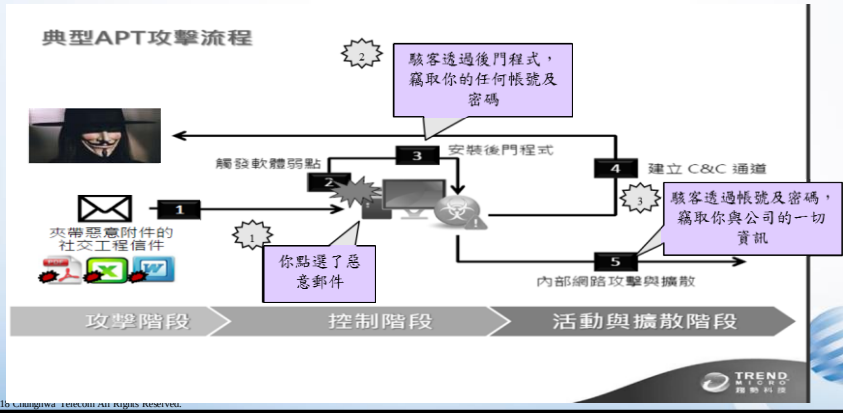
車馬衣裘可與親友共，
唯通行碼不行

27

雙因子認證對通行碼的重要性(1/3)

Q:為何要使用雙因子認證？

A:一般的LDAP帳號及通行碼很可能因為員工誤點惡意郵件而被竊取。



28

雙因子認證對通行碼的重要性(2/3)

好處

密碼外洩的另一道防線

協助偵測有人嘗試登入你的帳號

絕對不是意味著我們可以~~使用懶人密碼~~

29

雙因子認證對通行碼的重要性(3/3)

兩步驟驗證機制

雙因子認證	=	傳統帳號 傳統密碼	+	OTP(一次性密碼) 晶片卡 生物因子
2FA Two Factor Authentication				

中華電信 Chunghwa Telecom　Google　facebook　Microsoft　YAHOO!

雙因子認證的推動(1/2)

為強化資訊系統的安全性，
本公司重要資訊系統及系統維運作業已採用雙因子認證。

使用 員工憑證 登入資訊系統

若使用員工憑證，需將員工識別證插入讀卡機並輸入PIN CODE)

使用 LDAP帳號通行碼 + OTP通行碼 登入資訊系統

OTP通行碼會經由簡訊傳送到員工在LDAP登錄之公務手機門號。

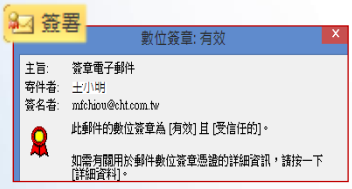
雙因子認證的推動(2/2)

32

3.為什麼要使用安全電子郵件?

33

安全電子郵件介紹



如同在實體文件上簽名，**數位簽章**用來確認寄件人的真實身分。當大家都使用簽章的方式寄送電子郵件，就會更容易辨別假冒寄件者的惡意郵件。

寄送電子郵件時，為了保護信件內容防止被偷窺或遭竄改，可進行「郵件加密」。收件者需要備妥識別證，藉由員工憑證才能開啟郵件內容。

34

建立安全電子郵件要領(1/2)

•**數位簽章(需插卡)**:**確保完整性、驗證性、不可否認性**

發信端

收信端

驗章:**驗證成功**，
收信端便可確保郵件的完整性、確認寄信人身份！

郵件伺服器

35

建立安全電子郵件要領(2/2)

收信端

•加密:機密性

發信端

憑證伺服器
(repository.cht.com.tw)

網路

郵件伺服器

解密(需插卡)：
僅限收信人本人才能解密，閱讀信件內容！
如：薪工單、考成表都經過加密，這些郵件通知只有本人才能開啟。

36

提升電子郵件安全措施(1/4)

【3要】

要將收信軟體設定為純文字瀏覽功能

要關閉收信軟體的郵件預覽視窗功能

要關閉收信軟體自動下載顯示郵件中圖片功能

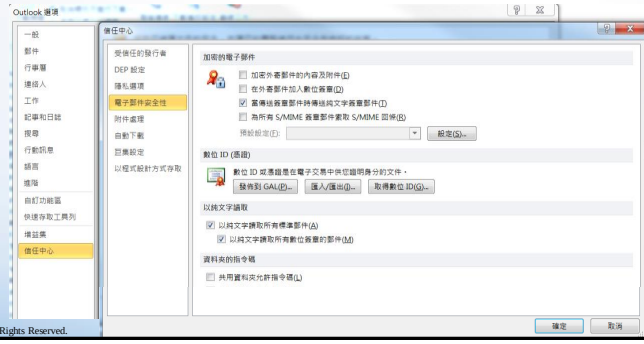
收到主旨前有標示[外部郵件])之信件，請提高警覺防範惡意攻擊

37

提升電子郵件安全措施(2/4)

【3要】1.要將收信軟體設定為純文字瀏覽功能

使用**Outlook 2010** 版本之設定步驟及畫面如下:
點按[檔案]➡[選項]➡[信任中心]➡ [信任中心設定]
再點選[電子郵件安全性]標籤➡
在純文字讀取部分勾選[以純文字讀取所有標準郵件]、及[以純文字讀取所有數位 簽章郵件]功能。

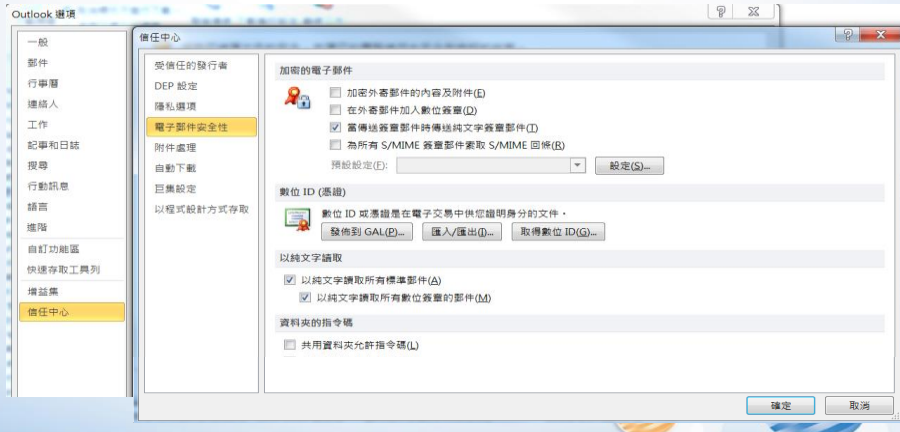


提升電子郵件安全措施(2/4)

要將
收信軟體
設定為
純文字瀏覽

要關閉
收信軟體
郵件預覽視窗

要關閉
收信軟體
自動下載顯示郵件中圖片功能

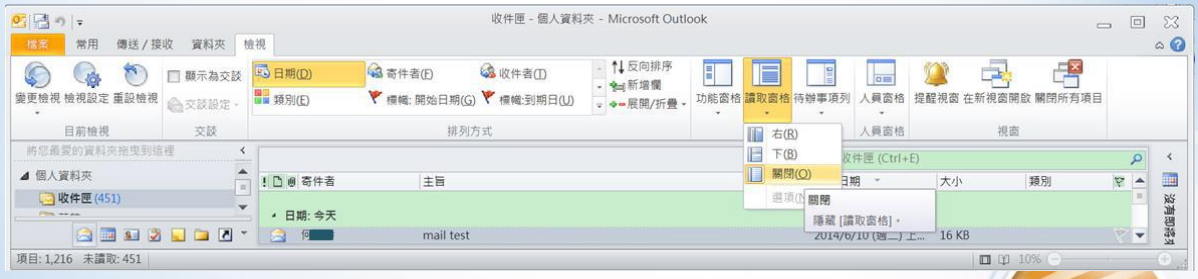


提升電子郵件安全措施(2/4)

要將
收信軟體
設定為
純文字瀏覽

要關閉
收信軟體
郵件預覽視窗

要關閉
收信軟體
自動下載顯示郵件中圖片功能

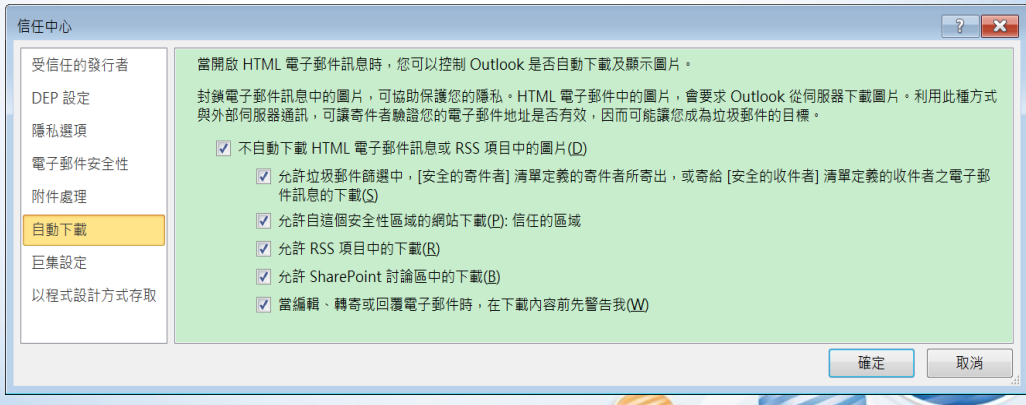


提升電子郵件安全措施(2/4)

要將
收信軟體
設定為
純文字瀏覽

要關閉
收信軟體
郵件預覽視窗

要關閉
收信軟體
自動下載顯示郵件中圖片功能



中華電信版權所有© 2018 Chunghwa Telecom All Rights Reserved.

4 網頁綁架案例

瀏覽器首頁又被綁架了？拒絕惡意程式，移除廣告外掛，恢復首頁

當你在網路上單純的瀏覽網頁的時候，背後其實有許多廣告商以及搜尋引擎網站在分析你的網路行為，並將你賣到其它網站去。

網路交易要透過安全模式
避免在公開網站洩漏個人資訊
防火牆、反間諜軟體保護
刪除Cookie

將你的瀏覽器設為隱私模式自保
瀏覽器上的輔助工具（BHO）

常見的BHO工具列
Babylon Toolbar
Ask Toolbar
Search.conduit.com
Hao123

https://www.techbang.com/posts/13222-reduce-malicious-toolbar-the-browser-hangs-restore-modified-home?reload_posts=true

42

網頁綁架案例

下載了軟體，瀏覽器被綁架了或不時跳出廣告畫面。

該事件是由「火絨安全實驗室」所揭露，他們發現用戶透過百度旗下的網站 skycn.net 和 soft.hao123.com 下載任何程式時，都會被暗中植入惡意代碼，成為被監控的管道。
被感染的電腦，會出現瀏覽器、首頁、搜尋引擎全部被綁架的狀況，流量也會傳送至 hao123 網站。除了會讓網頁被導向 Hao123 網站外，連廣告連結都會被竄改、成為 hao123 獲利的管道。

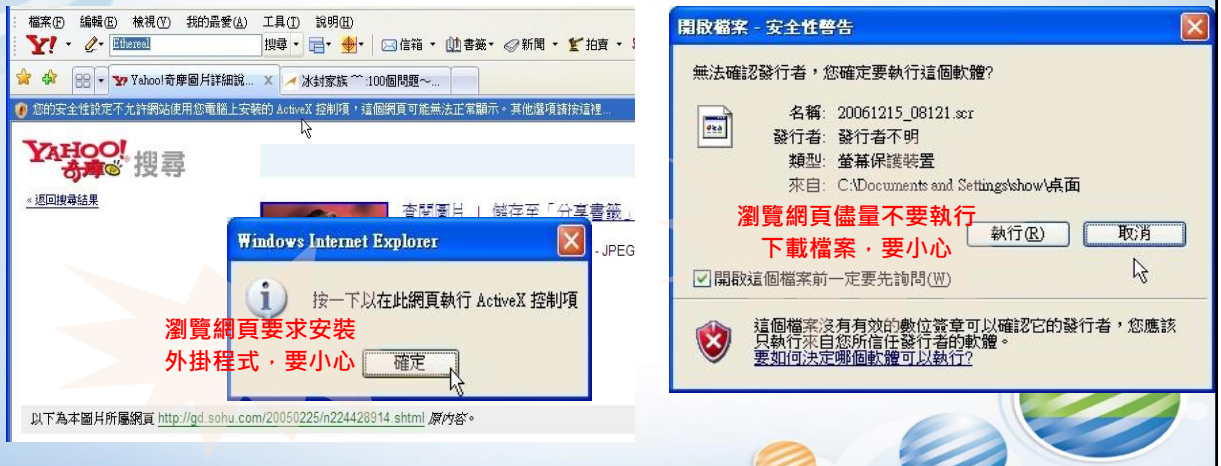
http://3c.ltn.com.tw/news/29070

網頁綁架案例

利用類似網址 騙取個人資料

網頁綁架案例

瀏覽網頁時被要求安裝軟體或被要求執行軟體



網頁綁架案例

瀏覽器擴充漏洞可能導致資料外洩或用戶曝光，Firefox、Chrome與Safari都受影響？

研究人員利用特定的列舉攻擊手法，繞過主要瀏覽器的防護機制，取得使用者的擴充程式資訊，可能使得Tor、VPN用戶身份曝光。

文/ 林妍溱 | 2017-08-29 發表

讚 4.5 萬 按讚加入iThome粉絲團 讚 0 分享 G+

研究人員發現Firefox、Safari及Chrome擴充程式機制出現漏洞，可能導致使用者的擴充程式被看光，致使以Tor或VPN匿名的用戶身份曝光。

西班牙德烏斯托大學研究人員Iskander Sanchez-Rola指出，擴充程式和瀏覽器的密切關係使其成為明顯的攻擊目標，用來竊取資訊與密碼、瀏覽上網活動記錄等等。雖然瀏覽器也加入了防護方式，像是存取控制設定及隨機URI(URI Randomization)機制，但Sanchez-Rola及其同僚進行的一項研究顯示，透過特定列舉攻擊（enumeration attack）手法，可繞過主要瀏覽器的防護功能，致使資訊曝光。

https://www.ithome.com.tw/news/116560

網頁綁架案例

挖礦綁架臺灣曝光第一例，遭害苦主保哥現身說法

三個月前一時興起採用的知名聊天外掛小工具，最近突然遭人加料植入了Coinhive挖礦程式碼，連小工具官方技術長都沒發現，放到CDN上的程式碼副本已經變質了

文/ 何維鴻 | 2017-11-05 發表

讚 4.5 萬 按讚加入iThome粉絲團 讚 288 分享 G+

9月19日，保哥（多奇數位創意技術總監黃保翕）在臉書上，公開了自家網站所用聊天外掛工具遭植入Coinhive程式的消息，是臺灣網站遭挖礦綁架事件曝光的第一例。

https://www.ithome.com.tw/news/117998

9月下旬有一天，一位瀏覽部落格的用戶，向黃保翕反應，只要開啟他的部落格The Will Will Web，瀏覽器的CPU使用率，就會衝破50%，甚至滿載，可是一離開保哥的部落格，CPU使用率馬上又會下降。

網頁綁架案例

不只海盜灣暗藏採礦程式，Chrome擴充程式SafeBrowse也有！

https://www.ithome.com.tw/news/116945

目前SafeBrowse已遭Google下架。有趣的是，SafeBrowse團隊向Bleeping Computer及Google喊冤，宣稱他們已經好幾個月沒有更新該程式，完全不知道發什麼事，顯然是被駭了。日前才傳出駭客鎖定Chrome擴充程式的開發人員進行網釣攻擊，在取得開發人員帳號之後挾持擴充程式並嵌入廣告機制，惟目前並不確定SafeBrowse是否也是受害者之一。

網頁綁架案例

黑色產業覬覦瀏覽器挖礦，5億訪客不知電腦變礦工
【災情持續擴大，全球每天新增300個挖礦網站】

挖礦綁架植入手法開始多元化

瀏覽器挖礦技術還在持續變化，而挖礦綁架手法也開始進化，一來開始出現更多種類的挖礦程式，除了Coinhive，還有JSEcoin、CryptoLoot、MineMyTraffic，以及10月底出現的Papoto，有意用瀏覽器挖礦者開始有更多選擇，而資安黑名單要封鎖的挖礦程式網址，也越來越多，甚至防不勝防。

- 藏在網頁頁尾程式碼
- 直接植入知名部落格平臺WordPress核心網頁
- 有影音網站跳出的Flash Video Player安裝提醒視窗中，暗中執行挖礦程式
- WordPress已有一項挖礦免費擴充套件，直接安裝就可以啟用瀏覽器挖礦功能，來偷用用戶的CPU資源
- 含有採礦能力的行動App，利用內建Webview動態載入JavaScript與原生程式碼注入來閃避偵測

https://www.ithome.com.tw/news/117995

瀏覽網站安全要領

Chrome、Firefox、Microsoft Edge 瀏覽器誰最安全(2016 年瀏覽器安全報告)？

作者 T客邦 | 發布日期 2016 年 11 月 09 日 8:30 | 分類 網路 , 資訊安全

根據 NSS Labs 表示，這次測試主要是測試瀏覽器兩大項目的安全，對應社群網路散布的惡意軟體（SEM）以及釣魚網站的阻隔。而測試的瀏覽器版本分別是：

- Google Chrome: Version 53.0.2785
- Mozilla Firefox: Version 48.0.2
- Microsoft Edge 38.14393.0.0

1. 釣魚網站安全測試：

微軟的 Edge 瀏覽器以 91.4% 的阻擋率奪冠，Chrome 阻擋率為 82.4%，Firefox 的阻擋率為 81.4%。

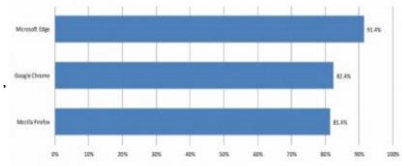


Figure 1 – Average Block Rate

2.SEM 的安全測試：

Edge 以 99.0% 的阻擋率最高，
Chrome 的阻擋率為 85.8%，
Firefox 依然還是第三，只有 78.3%。

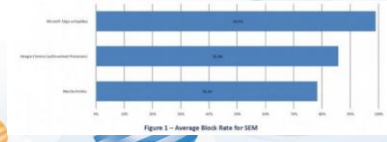


Figure 1 – Average Block Rate for SEM

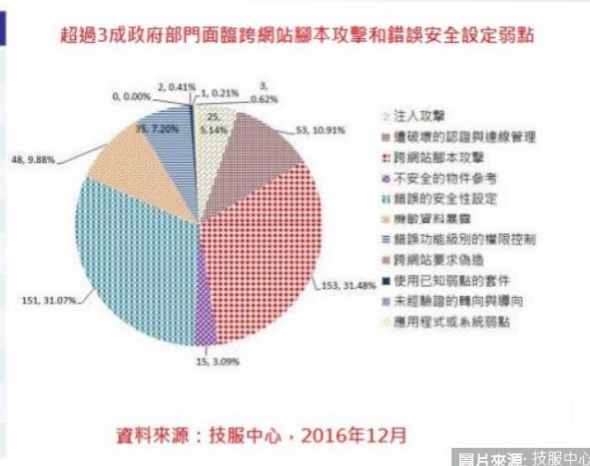
https://technews.tw/2016/11/09/microsoft-edge-is-way-more-secure-than-chrome-and-firefox/

瀏覽網站安全要領

3成重要政府官網不夠安全，恐因XSS漏洞害民眾

行政院進行網路攻防演練時，有超過3成的政府機關都有跨網站腳本程式攻擊（XSS）和錯誤的安全設定的漏洞問題。

排名	弱點類型	比例
1	跨網站腳本攻擊	31.48%
2	錯誤的安全性設定	31.07%
3	遭破壞的認證與連線管理	10.91%
4	機敏資料暴露	9.88%
5	錯誤功能級別的權限控制	7.2%
6	注入攻擊	5.14%
7	不安全的物件參考	3.09%
8	應用程式或系統弱點	0.62%
9	使用已知弱點的套件	0.41%
10	未經驗證的轉向與導向	0.21%
總計		100%



圖片來源: 技服中心

這種攻擊手法主要是允許駭客將惡意程式碼（包含HTML和使用者端的腳本語言）注入到網頁上，當其他網路使用者瀏覽已經被注入惡意程式碼的網頁時，就會受到影響。

瀏覽網站安全要領

瀏覽器首頁又被綁架了？拒絕惡意程式，移除廣告外掛，恢復首頁

將你的瀏覽器設為隱私模式自保
瀏覽器上的輔助工具（BHO）

常見的BHO工具列
Babylon Toolbar
Ask Toolbar
Search.conduit.com
Hao123

用Browser Repair Tools協助清除IE垃圾
Toolbar Cleaner進階清掃工具
Avast's browser cleanup tool

https://www.techbang.com/posts/13222-reduce-malicious-toolbar-the-browser-hangs-restore-modified-home?page=2&related_post=true

瀏覽網站安全要領

海盜灣綁架瀏覽器挖礦獲取利潤，透過 Adblock Plus 就能阻擋

作者 T客邦 | 發布日期 2017 年 09 月 29 日 8:00 | 分類 數位貨幣, 科技教育, 網路 Follow G+ 讚 248 分享

無立即危險，可透過 Adblock Plus 阻擋

海盜灣這種「借用」使用者電腦的硬體資源挖礦的行為，主要問題在於沒有主動告知使用者，可能會有潛在法律與道德的問題。但是相較於植入惡意程式、竊取信用卡等機密資料，或是將使用者電腦做為其他網路攻擊的跳板，挖礦對資安層面的危害沒有那麼大，頂多因為大量運算的關係，而讓電池續航力下降。

相對傳統透過廣告投放方式獲利，挖礦或許能取得更高的利潤，且不像廣告會影響閱讀舒適度（但瀏覽網頁過程中會加速電量消耗，或讓電腦變慢），這種新型態獲利管道是否會成為往後網站的商業模式，目前還未能看出端倪。

不過一般人一定對這種「不告之借」的舉動不滿，其實只要透過 Adblock Plus 等阻擋廣告軟體，過濾掉挖礦程式，就能避免電腦受到影響。

以海盜灣的情況為例，是使用 Coin Hive 提供的 JavaScript 程式，所以只要阻擋廣告軟體加入下列過濾條件，就能杜絕海盜灣的挖礦行為。

過濾條件

add coin-hive.com/lib/coinhive.min.js

或許我們也不用太過擔心以後有越來越多網站導入挖礦模式，因為總會有對應的過濾工具，能夠組止這種竊取運算資源的舉動。

https://technews.tw/2017/09/29/pirate-bays-kidnapping-browser-mining-profits-via-adblock-plus-can-stop/

瀏覽網站安全要領

杜絕彈出式廣告、Youtube影片廣告，網路廣告全部擋

Chrome安裝步驟

https://www.techbang.com/posts/13175-eliminate-pop-up-ads-youtube-video-advertising-online-advertising-all-gear

瀏覽網站安全要領

如何避免自家電腦淪為礦工？

檢測可能藏有挖礦程式的要領

- 開啟系統監控CPU使用率的工具，是否連上特定網頁時，CPU使用率突然飆高，關掉網頁後卻又恢復正常，就可能藏有挖礦程式。
- 使用Chrome瀏覽器時，按下F12打開開發者工具，查看Network功能分頁，若開啟的網頁藏有挖礦程式，會出現異常網路流量。
- 因挖礦網站須連回Coinhive伺服器才能進行挖礦作業，因此，企業只要封鎖Coinhive網址的連線行為，就能阻止。
- 廣告過濾程式如AdBlock Plus和AdGuard可以直接阻擋Coinhive的JavaScript程式。
- Chrome瀏覽器也出現了幾款專門封鎖挖礦行為的外掛，如AntiMiner、No Coin、MinerBlock等。
- 需注意所用的第三方套件，最好用程式碼掃描工具，過濾挖礦程式的API，或是避免出現挖礦程式函式庫的連結，也要避用剛推出而未有大量使用者的套件，尤其是整合多功能的複雜套件。

瀏覽網站安全要領

透過瀏覽器的隱私模式去看危險的網站就不會被追蹤監控？

作者 T客邦 | 發布日期 2017 年 03 月 13 日 8:10 | 分類 資訊安全

以 Chrome 瀏覽器來說，透過無痕模式，你可以確保當你的瀏覽器關閉之後，不會保存任何的歷史紀錄、Cookies 或是密碼。但是在過程中，你下載的檔案或是你創造的書籤，將還是會保留。而 Firefox 的隱私模式也是類似的模式。

不過，它的功能也僅此而已。你可以打開 Chrome 的說明，在 Chrome 的官網說明頁是這樣描述：

「無痕模式」或是「隱私模式」 ≠ 真正安全

> 無痕模式的運作方式：無痕模式會開啟新的專用視窗，讓您在私密狀態下瀏覽網際網路，而且 Chrome 不會記錄您造訪了哪些網站。您可以在無痕式視窗與您開啟的其他一般 Chrome 瀏覽視窗之間切換。不過，只有在使用無痕式視窗時，才是處於私密狀態。
>
> 他人仍可查看一些資訊：無痕模式只能禁止 Chrome 儲存您的網站瀏覽活動，但無法防止其他來源查看您造訪過哪些網站，包括：
>
> - 網際網路服務供應商
> - 您的雇主（如果您使用公司電腦）
> - 您所造訪的網站

https://technews.tw/2017/03/13/browser-privacy-mode-as-you-think-of-security/

瀏覽網站安全要領

透過瀏覽器的隱私模式去看危險的網站就不會被追蹤監控？

Chrome 瀏覽器上的無痕模式只有一個功能，那就是關機後將你儲存在電腦上的瀏覽紀錄和網站 cookies 清除掉。不過網站依然可以追蹤你的 IP，你的瀏覽也並沒有得到加密。
你搜尋了什麼 Google 還是一清二楚，即使匿名瀏覽也沒用。

瀏覽網站安全要領

解決 Chrome 首頁被綁架或跳出廣告，下載這個官方工具就搞定

如果電腦安裝來歷不明的軟體，除了會出現資安問題，常常首頁還會被綁架或不定時彈出色情小廣告，即使修改 Chrome 設定也無法解決。

Google 推出的軟體移除工具下載網頁
目前 Beta 版可以清理30種以上的惡意軟體
下載網址：http://goo.gl/T6bxcq

58

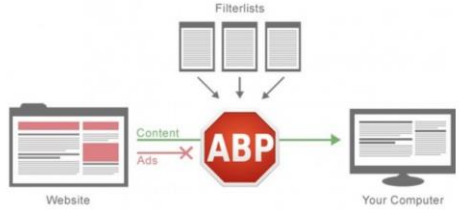
瀏覽網站安全要領

擋廣告外掛 Adblock Plus：所謂的「大公司付費放行廣告」，背後真相其實是這樣

https://technews.tw/2015/02/10/story-about-adblock-plus/

為求突破 Adblock Plus 廣告封鎖，Google、微軟打算繳交過路費

作者 36Kr | 發布日期 2015 年 02 月 03 日 16:18 | 分類 Facebook, Google, 網路 Follow G+ 讚 1,083 分享



Adblock Plus 是一家德國初創公司做的全球最流行的免費廣告過濾外掛程式之一，目前在 Firefox、Chrome、Safari、Opera 瀏覽器和 Android 手機、平板上均可使用，下載量達到 3 億，月活躍使用者達 5,000 萬，根據金融時報消息，幾家大公司目前都與 Adblock Plus 外掛程式有付費協議，想交「過路費」換「通行證」，具體金額未知。目前，Google、Amazon 拒絕評論此事，微軟則肯定了這種合作，並聲稱會尊重消費者的選擇。

https://technews.tw/2015/02/03/adblock-plus-google-microsoft-amazon/

59

瀏覽網站安全要領

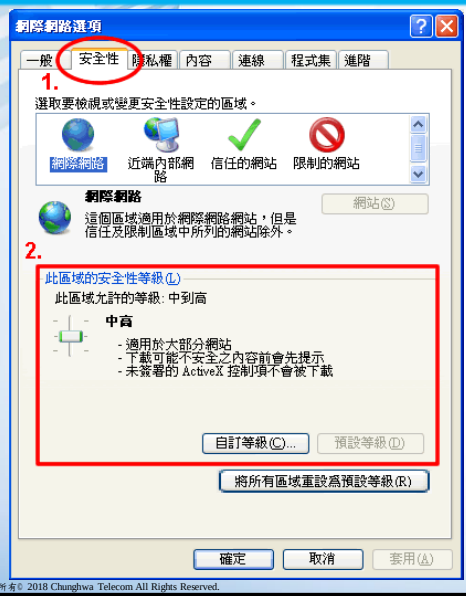
Google 對 AdBlock 的反擊！只要偵測到安裝，就不讓你跳過廣告

Youtube 逆襲：安裝 AdBlock 用戶無法跳過廣告

為了要讓 Youtube 頁面上廣告不被過濾掉，Google 想出一個對策，那就是安裝 AdBlock Plus 的用戶在看 Youtube 平台上的影片時，必須把影片撥放前完整版廣告看完，重點是沒有「略過廣告」這個選項。如果用戶想要跳過廣告，就只能選擇解安裝 AdBlock 或是將 Youtube 放進白名單（whitelist）裡。外界猜測，Google Chrome 經過一番的努力之後，終於找到如何躲避 AdBlock Plus 的偵察系統，順利播出廣告。不過，AdBlock Plus 也不甘示弱的回應，只有在 Chrome 瀏覽器才會有這樣情形出現，只要換其他瀏覽器就沒這些問題存在。

https://technews.tw/2015/09/09/adblock-google/

瀏覽網站安全要領

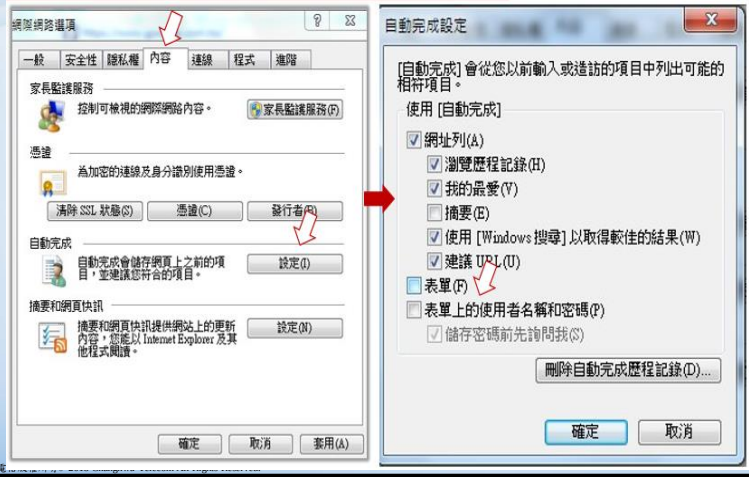


❑ **防範訣竅：**

- **對於經常使用且可信任的網站，可預先於工具列中設定該網址為可信任，以避免瀏覽器在高安全層級設定下，導致網頁無法正常讀取之困擾。**
- **建議將讀取網頁瀏覽器安全層級設定為中安全性以上。**

瀏覽網站安全要領

3. 在共用電腦上存取本公司系統，瀏覽器開啟自動儲存通行碼功能，容易造成帳密外洩。



關閉IE11
自動儲存通行碼功能
步驟如下：

➡點按[工具]
➡[網際網路選項]
➡[內容]
➡[設定]功能

瀏覽網站安全要領

- 定期刪除 Cookies
- 定期刪除 暫存檔
- 定期清除 記錄

- 方法：
- 在 IE 中
- 工具\網際網路選項

5. 數位貨幣與挖礦

01

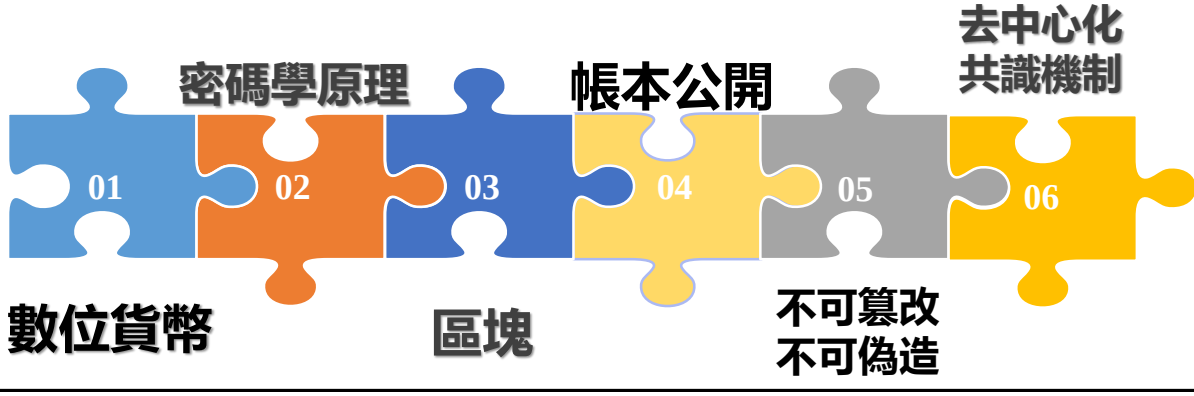
貨幣雲端化

1. 加密貨幣?
2. 挖礦獎勵?
3. 加密貨幣和區塊鏈有什麼關係?

02

貨幣總量恆定化

1.加密貨幣有沒有用完的一天呢?
2.中本聰是如何分配比特幣的?
3.2100萬枚比特幣夠分嗎?




加密貨幣
密碼學原理
帳本公開
去中心化
共識機制
挖礦獎勵是加密貨幣的發動機
數位貨幣
區塊
不可篡改
不可偽造


加密貨幣
密碼學原理
帳本公開
去中心化
共識機制
01
區塊鏈為加密貨幣的技術核心
數位貨幣
區塊
不可篡改
不可偽造

#	貨幣	匯率	24 小時	總市值	流動性	開發方	社群	大眾關注度	總計	最近 7 天
1	比特幣 BTC	US$9,301	0.35%	US$158,408,351,081	US$2,361,886,111	96.26%	89.75%	43.26%	85.80%	
2	以太幣 ETH	US$753.84	3.30%	US$75,131,976,947	US$2,629,598,850	92.44%	73.95%	39.67%	79.63%	
3	EOS	US$18.45	7.75%	US$15,562,684,384	US$2,032,223,927	87.32%	67.73%	35.66%	75.56%	
4	XRP									
5					US$436,448,548	88.47%	64.58%	37.00%	72.51%	

挖礦

到底要挖什麼礦呢?

01

挖礦

任何人皆可參與加密貨幣活動，透過稱為「挖礦」的電腦運算獲得加密貨幣

02

礦機

中央處理器CPU圖形處理器GPU這類用來挖礦的裝置稱為「礦機」

03

挖礦獎勵

礦工都解答一個超級難數學題，誰先解答出這道題誰就有優選記賬權，獲得記賬權就會有對應代幣獎勵。

暫時性
網站挖礦程式

挖礦綁架臺灣曝光第一例，遭害苦主保哥現身說法

三個月前一時興起採用的知名聊天外掛小工具，最近突然遭人加料植入了Coinhive挖礦程式碼，連小工具官方技術長都沒發現，放到CDN上的程式碼副本已經變質了

文/ 何維鴻 | 2017-11-05 發表

看文章也會CPU使用率滿載

只要開啟他的部落格，瀏覽器的CPU使用率，就會衝破50%，甚至滿載，可是一離開保哥的部落格，CPU使用率馬上又會下降。

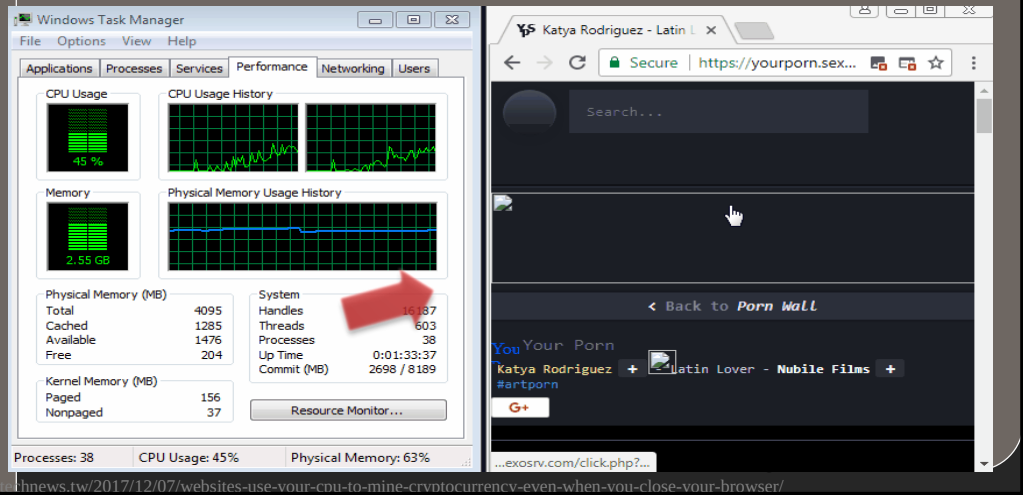
9月19日，保哥（多奇數位創意技術總監黃保翕）在臉書上，公開了自家網站所用聊天外掛工具遭植入Coinhive程式的消息，是臺灣網站遭挖礦綁架事件曝光的第一例。

https://www.ithome.com.tw/news/117998

隱藏式
網站挖礦程式

關閉瀏覽器也能偷挖礦？這是一種騙術

即使訪客關閉瀏覽器之後也會持續在背後偷偷挖礦。其手法是將瀏覽器縮小至工作列隱藏，如此就能繼續慢慢挖礦，所以使用者可能不會特別注意到，但 CPU 用量



https://ithnews.tw/2017/12/07/websites-use-your-cpu-to-mine-cryptocurrency-even-when-you-close-your-browser/

綁架瀏覽器事件，如何阻檔呢?


灣綁架瀏覽器挖礦獲取利潤，透過 Adblock Plus 就能阻擋

即危險，可透過 Adblock Plus 阻擋

過濾條件

add coin-hive.com/lib/coinhive.min.js

全部擋

彈出式廣告

Youtube影片廣告

網路廣告

s://technews.tw/2017/09/29/pirate-bays-kidnapping-browser-ng-profits-via-adblock-plus-can-stop/

https://www.techbang.com/posts/13175-eliminate-pop-up-ads-youtube-video-advertising-online-advertising-all-gear

- 74 -

檢測可能藏有挖礦程式的要領

01 CPU使用率

開啟系統管理員**監控**CPU使用率，偵測是否連上特定網頁時，CPU使用率突然飆高，關掉網頁後卻又恢復正常，就可能藏有挖礦程式。

02 網路流量

使用Chrome瀏覽器時，**按下F12**打開開發者工具，查看Network功能分頁，若開啟的網頁藏有挖礦程式，會出現**異常**網路流量。

03 連線行為

因挖礦網站須連回Coinhive伺服器才能進行挖礦作業，**封鎖**Coinhive網址的連線行為。

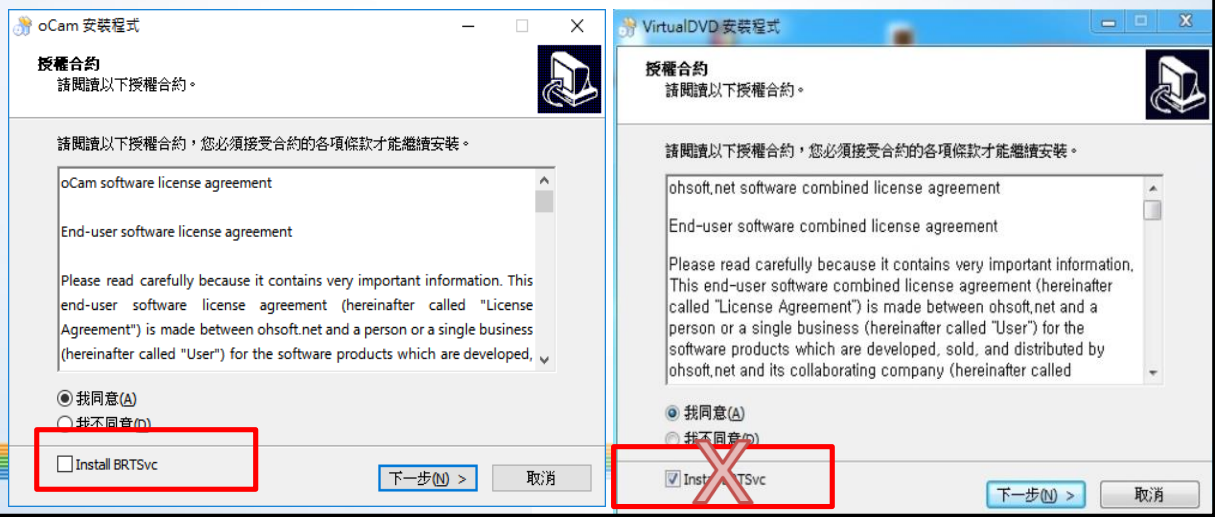
04 過濾程式

廣告過濾程式如AdBlock Plus和AdGuard可以**直接阻擋**Coinhive的JavaScript程式。

- 75 -

安裝軟體時，需留意預設安裝選項

- 免費版的 Ocam與Virtual DVD安裝程式



挖礦造成的影響

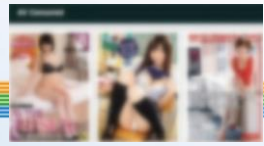
Free WiFi

星巴克Wi-Fi 遭加料，顧客手機筆電成挖礦機

YouTube

Youtube看影片變好慢？原來是駭客正在挖礦賺外快！

惡意廣告暗藏採礦程式，一點就中！



逛色情網站讓你的電腦成為免費礦工。

結語

- 同仁應提升警覺性及學會辨識惡意電子郵件(簡訊)的能力
  - 公司每年執行2次無預警電子郵件社交工程演練。
  - 落實「6不3要」避免電腦受駭。
  - 提高自身資訊安全警覺性
  - 軟體安裝需注意挖礦的風險
- 同仁應保管好通行碼以免外洩被駭客利用。
  - 不同的服務、系統、網站，應使用不同的通行碼，並定期更新。
  - 系統維運者，通行碼長度至少為12碼且至少每90 天變更一次。
  - 應使用高強度通行碼，以降低通行碼被破解的可能性。
  - 密碼不可以明文書寫，存放在可存取處，以免被竊取。
  - 不可使用系統預設帳號/通行碼，以免被駭客利用。
  - 瀏覽器應該關閉自動儲存通行碼功能，以免造成帳密外洩。
  - 使用公共電腦應避免儲存帳號/通行碼，離席時應檢查並清除資源回收桶。

結語

- 正確的危機意識與資安觀念
- 預防詐騙手法的攻擊
- 提高警覺，加強危機意識
- 不隨意開啟或下載郵件或軟體
- 定期做系統更新與資料備份的工作