資訊安全面面觀

108年4月23日

Hello

張二川

國立中央大學電子計算機中心
桃園區網中心

center28@ncu.edu.tw

CEH
CHFI
ISO27001 LA
PIMS LA

大綱

- 資通安全法簡介
- 資訊安全威脅現況
- 電子郵件社交工程與案例
- 桃園區網介紹

資通安全法簡介


教育體系因應
資通安全管理法之規劃說明
教育部資訊及科技教育司
108年1月21日
1


臺灣學術網路各級學校
資通安全通報應變作業綱要
1
教育部教育部資訊及科技教育司

資訊安全威脅現況

六大面向之全球資安威脅趨勢

進階持續威脅攻擊竊取機密資料

- https://blog.trendmicro.com.tw/?p=123

分散式阻斷服務攻擊癱瘓網路運 作

- DDOS

物聯網設備資安弱點威脅升高

- http://www.insecam.org/

關鍵資訊基礎設施資安風險倍增

- 美國政府武器系統缺乏嚴密的安全機制

網路與經濟罪犯影響電子商務與金融運作

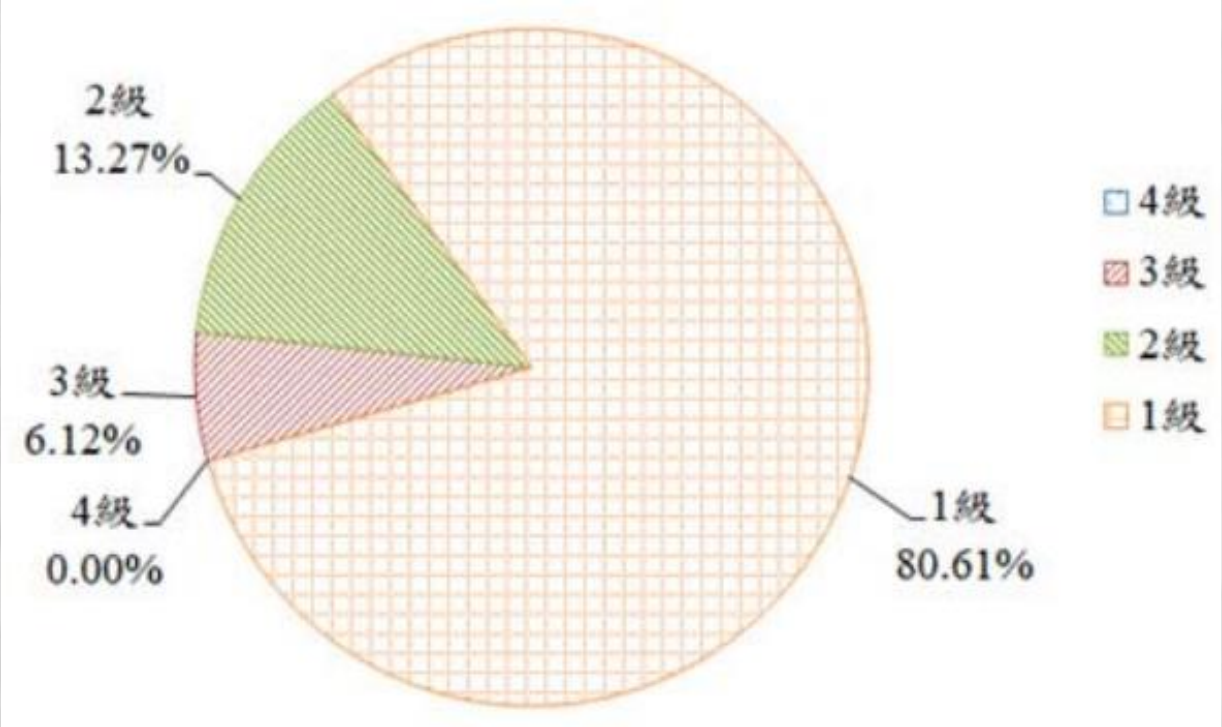
- 虛擬貨幣交易平台被駭

資安(訊)供應商持續遭駭破壞供應鏈安全

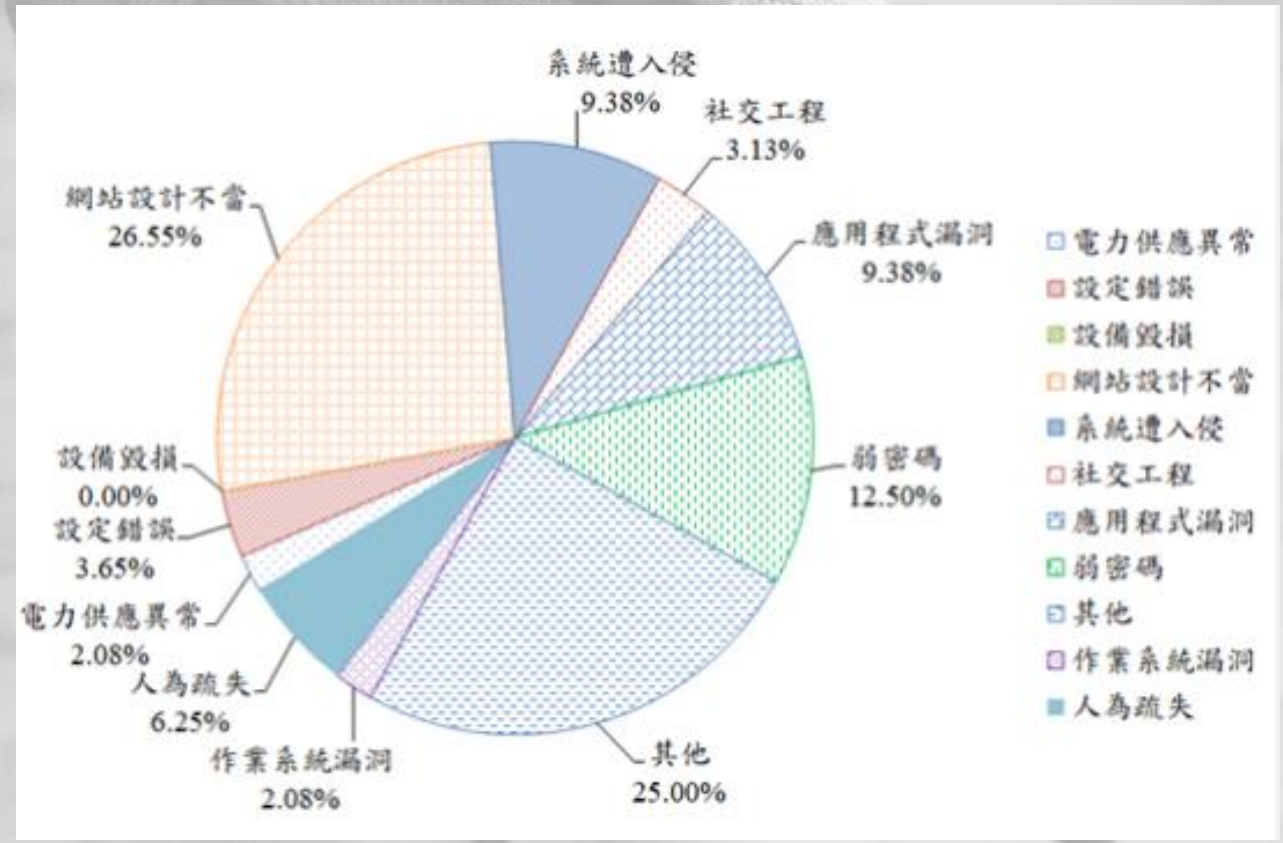
- 華碩事件(https://shadowhammer.kaspersky.com/)

¯ÑÀ³ÃìšðÀ»®×¯Ò - µØºÓ§ó-s³nÀé¾D§T«ü¡A±N¦Û°ÊÀ°§A¸Ë«á³ù - TechNe

政府資安威脅現況
107年第四季政府機關(構)通報事件



107 年第 4 季資安事件原因比率圖



電子郵件社交工程與案例

社交工程的定義

- 社交工程 (Social Engineering) 係利用人性弱點，運用簡單的溝通和欺騙技倆，以獲取帳號、通行碼、身分證號碼或其他機敏資料，來突破單位的資通安全防護，進行非法的存取、破壞行為。

- 「社交工程」，就是詐騙

社交工程的定義

- 目前常見的手法有透過電子郵件、電話、手機簡訊、即時通訊、網頁、偽冒的應用程式等管道，讓被害人主動的告知個人機密資訊或交付財物 。
- 是一種並非完全技術的資訊安全攻擊方式，即使建置完善的資安設備或高效能的防護系統，也無法完全防止社交工程攻擊

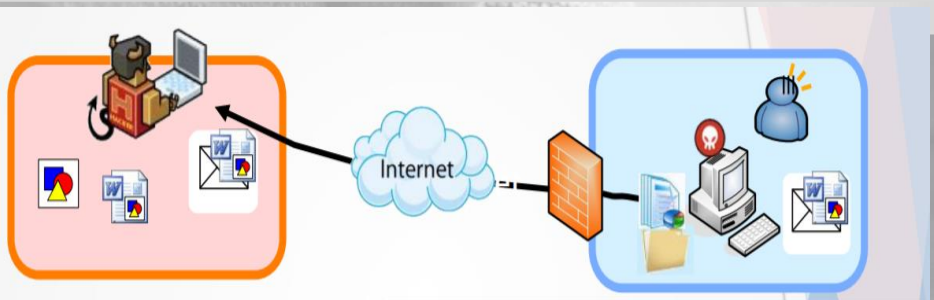
“您的許多連線可能都十分安全，唯有椅子和鍵盤之間的這個連線可能造成問題。”

--- 趨勢科技資安威脅研究專案經理 Jamz Yaneza

常見的社交工程攻擊手法

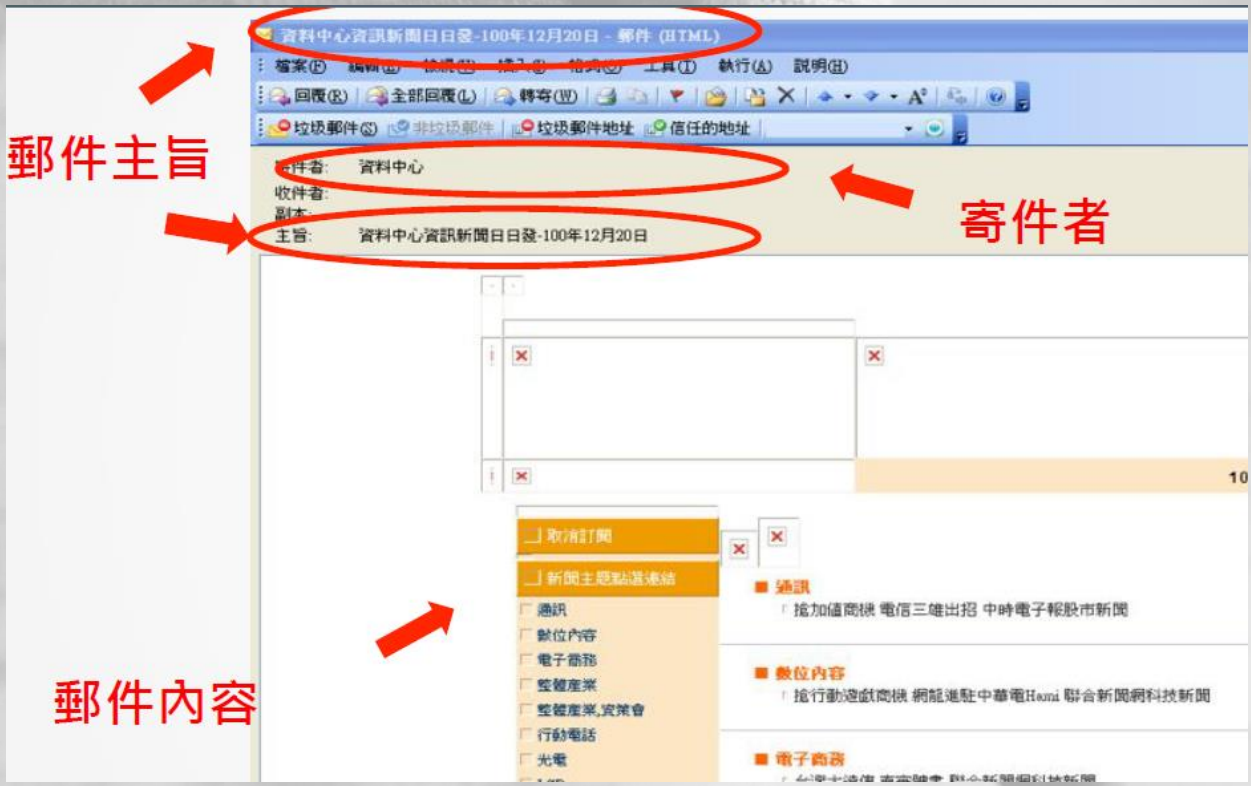
- 利用電話佯裝資訊人員，騙取帳號及通行碼。
- 偽裝委外廠商之維護人員或上級單位人員，乘機騙取帳號及通行碼。
- 圾圾翻找、偷窺強記、尾隨
- 利用電子郵件誘騙使用者登入偽裝之網站以騙取帳號及通行碼，如網路釣魚。
- 利用電子郵件誘騙使用者開啟檔案、圖片，以植入惡意程式、暗中收集機敏性資料。
- 利用提供工具、檔案、圖片為幌子，誘騙使用者下載，如偽裝的修補程式 、工具軟體等，乘機植入惡意程式、暗中收集機敏性資料或作為僵屍電腦。
- 利用即時通訊軟體，誘騙點選來訊中之連結後中毒。

電子郵件社交攻擊流程



1. 駭客設計攻擊陷阱程式 (如特殊Word 檔案)
2. 將攻擊程式偽裝成附件並夾帶於電子郵件中
3. 寄發電子郵件給特定的目標
4. 受害者開啟電子郵件
5. 啟動駭客設計的陷阱，並被植入後門程式
6. 後門程式逆向連接，向遠端駭客報到
7. 遠端駭客進行資料竊取

社交工程電子郵件組成


郵件主旨
資料中心資訊新聞日日發-100年12月20日 - 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)
垃圾郵件(K) 非垃圾郵件 垃圾郵件地址 信任的地址
寄件者: 資料中心
收件者:
副本:
主旨: 資料中心資訊新聞日日發-100年12月20日
寄件者
取消訂閱
新聞主題點選連結
通訊
數位內容
電子商務
整體產業
整體產業,政策會
行動電話
光電
通訊
搶加值商機 電信三雄出招 中時電子報股市新聞
數位內容
搶行動遊戲商機 網龍進駐中華電Hami 聯合新聞網科技新聞
電子商務
郵件內容

社交工程電子郵件主旨

令人緊張或鬆懈防備之郵件主旨

- ■關心提醒(請告訴身旁的女性朋友，小心電梯之狼)
- ■誇大聳動(世界末日大預言)
- ■郵件回覆(RE:會議參考資料)
- ■郵件轉寄(FW:簡易規劃日本自助旅行)

工作業務、生活時事等相關或令人感興趣之郵件內容類型

- ■政治新聞、特殊新奇
- ■生活議題、休閒娛樂
- ■社交群體、健康養生

社交工程電子郵件手法

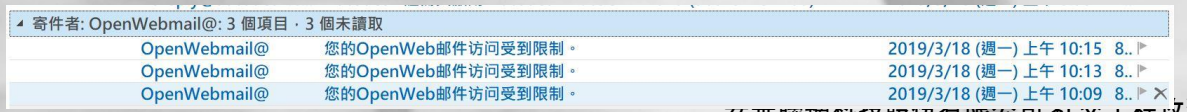
混淆視聽之郵件寄件者

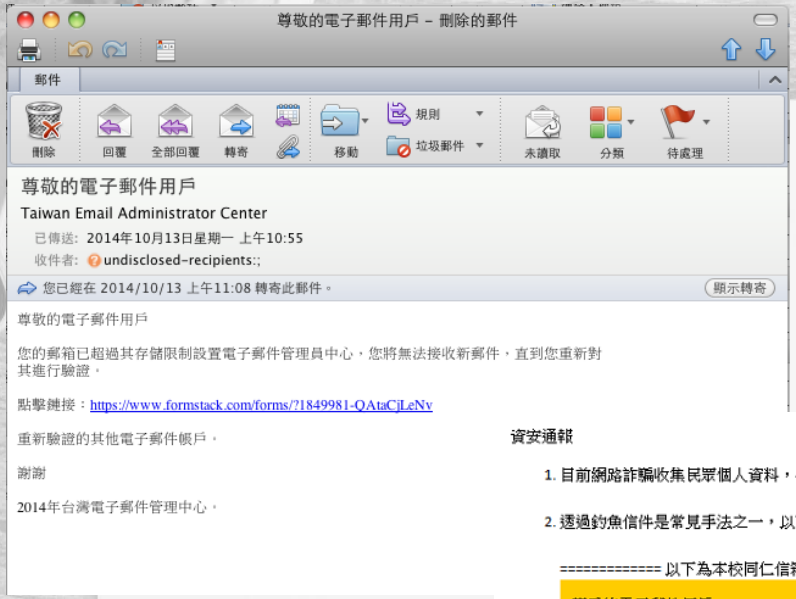
- ■偽裝身分(王小明、主任)
- ■偽裝機關(AB銀行、蝦皮商店)
- ■偽裝服務(論壇電子報、新聞)

附件夾帶病毒、蠕蟲、木馬程式及殭屍程式等惡意程式

郵件本文夾帶惡意連結

利用使用者端應用程式安全漏洞(未上更新修補)





資安通報

1. 目前網路詐騙收集民眾個人資料，手段與花樣繁多，敬請同仁們謹慎判斷。
2. 透過釣魚信件是常見手法之一，以下就是最近收到的信件，請勿理會。

========== 以下為本校同仁信箱最近接獲釣魚信件案例之一 ==========

親愛的電子郵件用戶，

您的郵箱已超過其存儲限制設置您的電子郵件管理員，並且您將無法接收新郵件，直到您重新對其進行驗證。

點擊鏈接： https://www.formstack.com/forms/?1774406-lwxXKalcwd

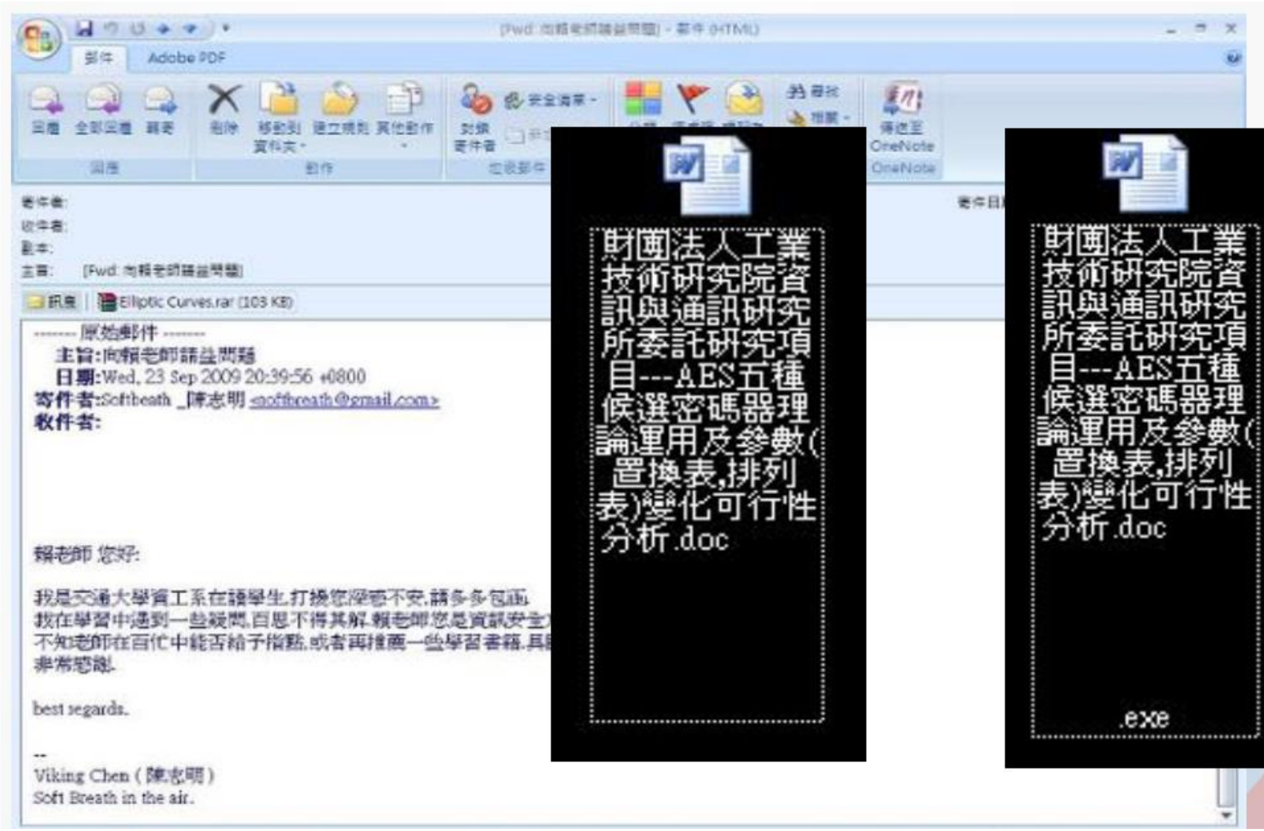
要重新驗證您的電子郵件帳戶

謝謝2014電子郵件管理員中心。

========== 以上內容，目的在詐騙使用者帳號、密碼 ==========

3. 詐騙集團會以事態嚴重、時間緊迫、違反法律等理由，讓詐欺對象心生害怕，失去戒心，然後就任其擺佈。

https://www.techbang.com/posts/20414-phishing-scam-hits-again-dont-be-misled-into-believing-that-electronic-postman-fishing-letters



[Fwd: 向賴老師請益問題]
Elliptic Curves.rar (103 KB)
-------- 原始郵件 --------
主旨:向賴老師請益問題
日期:Wed, 23 Sep 2009 20:39:56 +0800
寄件者:Softbeath _陳志明 <softbreath@gmail.com>
收件者:
賴老師 您好:
我是交通大學資工系在讀學生,打擾您深感不安,請多多包涵
非常感謝.
best regards.
Viking Chen (陳志明)
Soft Breath in the air.
財團法人工業技術研究院資訊與通訊研究所委託研究項目---AES五種候選密碼器理論運用及參數(置換表,排列表)變化可行性分析.doc
財團法人工業技術研究院資訊與通訊研究所委託研究項目---AES五種候選密碼器理論運用及參數(置換表,排列表)變化可行性分析.doc .exe

https://blog.trendmicro.com.tw/?p=17208

https://www.youtube.com/watch?v=MYQmbNRwzM8

網頁釣魚

網路釣魚（Phishing）就是網路犯罪份子通過偽造的電子郵件或是網站來誘騙你的個人資料，像是帳號名稱和密碼。

網頁釣魚

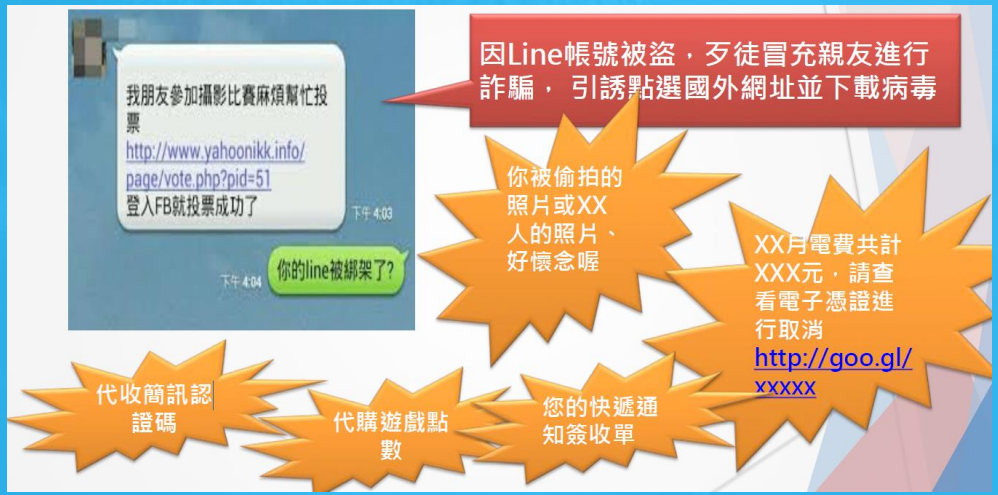

中華航空公司 China Airlines - Windows Internet Explorer
CHINA AIRLINES
華夏
班機離到動態
透過航班時間表，旅程安
http://www.china-airlines.com/ch/schedule/s_check.htm
中華航空公司 China Airlines

Line 簡訊惡意連結網址

➜「恭喜獲得全聯禮券」

➜「恭喜!!!你是今天的幸運用戶，能獲得一台蘋果iPhone...」

➜分享給10位好友或50人的LINE群組，就能獲得好市多的300元抵用金



假市調真詐騙

https://blog.trendmicro.com.tw/?p=50162

手機也會中毒?

iPhone 也會中毒？
這到底是什麼？


●●●○○ 中華電信 4G
下午1:28
73%
dtwiosantiprog.dorkha.website
檢測到病毒!
這些有害的病毒可能會損壞設備的系統文件，
並且所有現有的聯繫人可能會丟失.
請稍候掃描正在運行...
71%
警告!
您的Apple手機已被感染病毒!
建議現在快速掃描.
關閉


●●●○○ 中華電信 4G
下午1:28
73%
dtwiosantiprog.dorkha.website
檢測到病毒!
這些有害的病毒可能會損壞設備的系統文件，
並且所有現有的聯繫人可能會丟失.
請稍候掃描正在運行...
37%
掃描: 7ios.lib.messages
安裝
取消

突然跑出這個

下午 11:00

已讀 不要按

已讀 千萬不要按

已讀 下午 11:26 那是騙人的

已讀 下午 11:27 按了就完了

……

我按了…

下載了…

下午 11:27

已讀

下午 11:27

【假通知】您的瀏覽器被(4)病毒嚴重損壞？假的GOOGLE手機病毒

Charles Yeh 星期二, 3月 27, 2018

用LINE分享給朋友看

你的手機上網時出現「您的瀏覽器被(4)病毒嚴重損壞」這樣類似 Google 的通知視窗嗎？還說「我們檢測到您XXXX為28.1%受損，因為從最近的成人網站（4）有害的病毒。」這樣嚇人的說明，事實上這完全就是 Android 系統手機用戶收到的惡意廣告！

【假LINE】新年動圖、米奇新年快樂、全家禮券活動全假的！還偽裝官方總標詐騙

【假LINE】最近LINE更新個資？改陽私設定一律拒絕？被曲解了

【易誤解】中研院有身體健康檢查、500塊錢的車馬費？別誤解了

【這真的】剛才台灣的公視新聞報導A型流感，美國46個州淪陷，是真的！

【這真的】LINE 傳「好好健康的人，怎麼會猝死」的訊息，是真的專家建議

【假知識】這種雞蛋不要買更不要吃？蛋殼上長刺點細菌感染的謠言

【假LINE】醫管局發出的通知？每次喝50-80cc的溫水抗流感？謠言啦！

【假LINE】明天早上3點至晚上7點，中國網絡開始清理黑頭？謠言啦！最早是微信的版本

【假LINE】美國的同學圈的帖？禁止日本食品進入美國的謠言

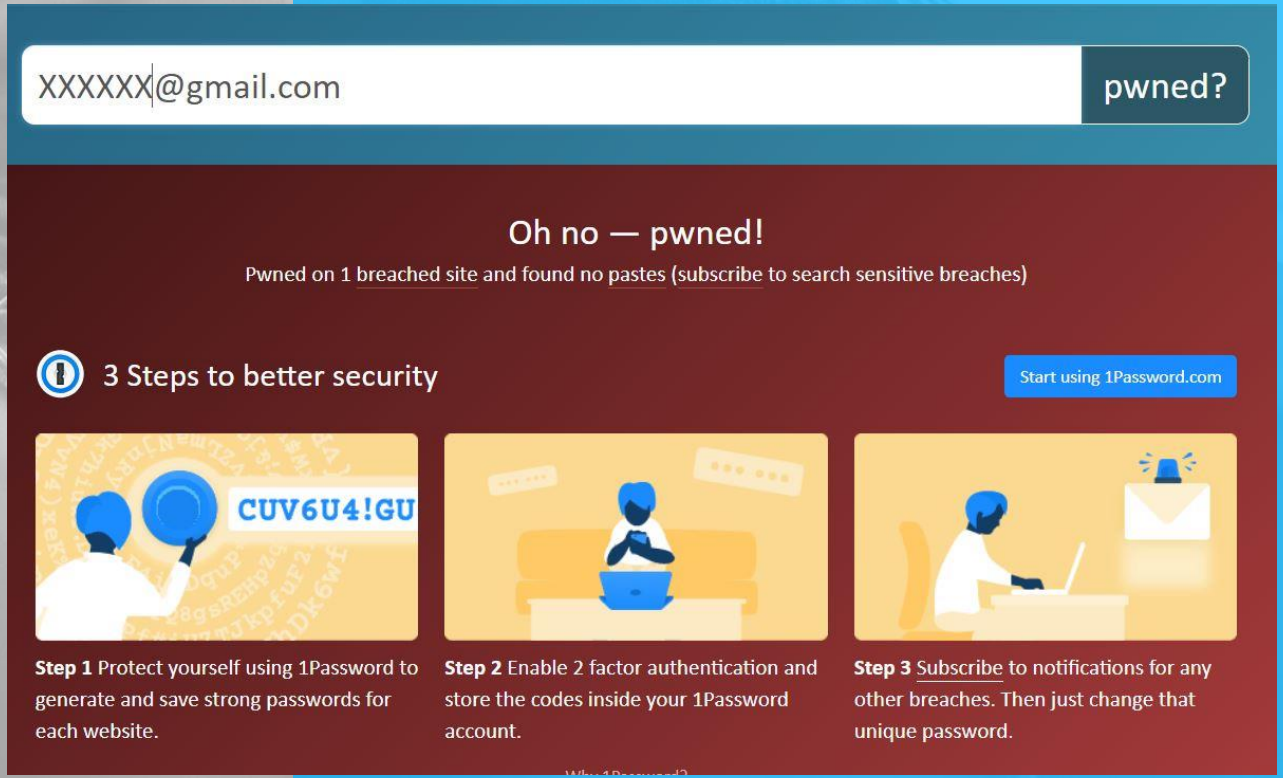
【假科學】LINE傳烏干達赤道上的影片，北半球和南半球水流漩渦不同？假的！

中風 內容農場
公益 化妝品
心肌梗塞 台電
交通 地震
好康 有毒
行銷手法 免洗筷


84% 11:54
下載
使用量：184.26 MB (共 54.00 GB)
Chrome 常用網頁
125 MB - 上次更新時間：11 小時前
今天 - 2019年3月12日
android-100618-3147afbd.apk
還剩 1 分鐘
13%
2019年3月9日
網路郵局契約部分條文修正對照表_108.03.pdf
476 KB • www.post.gov.tw

大量帳號密碼外洩

https://applealmond.com/posts/47116



XXXXXXX@g.ncu.edu.tw

pwned?

Good news — no pwnage found!

No breached accounts and no pastes (subscribe to search sensitive breaches)

3 Steps to better security

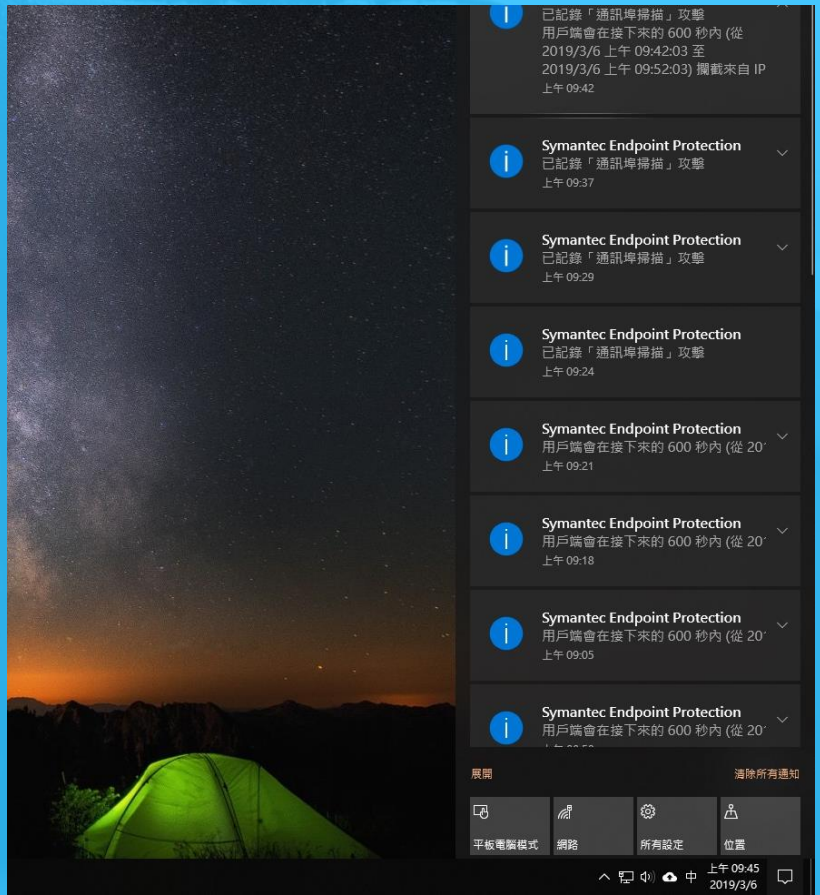
Start using 1Password.com

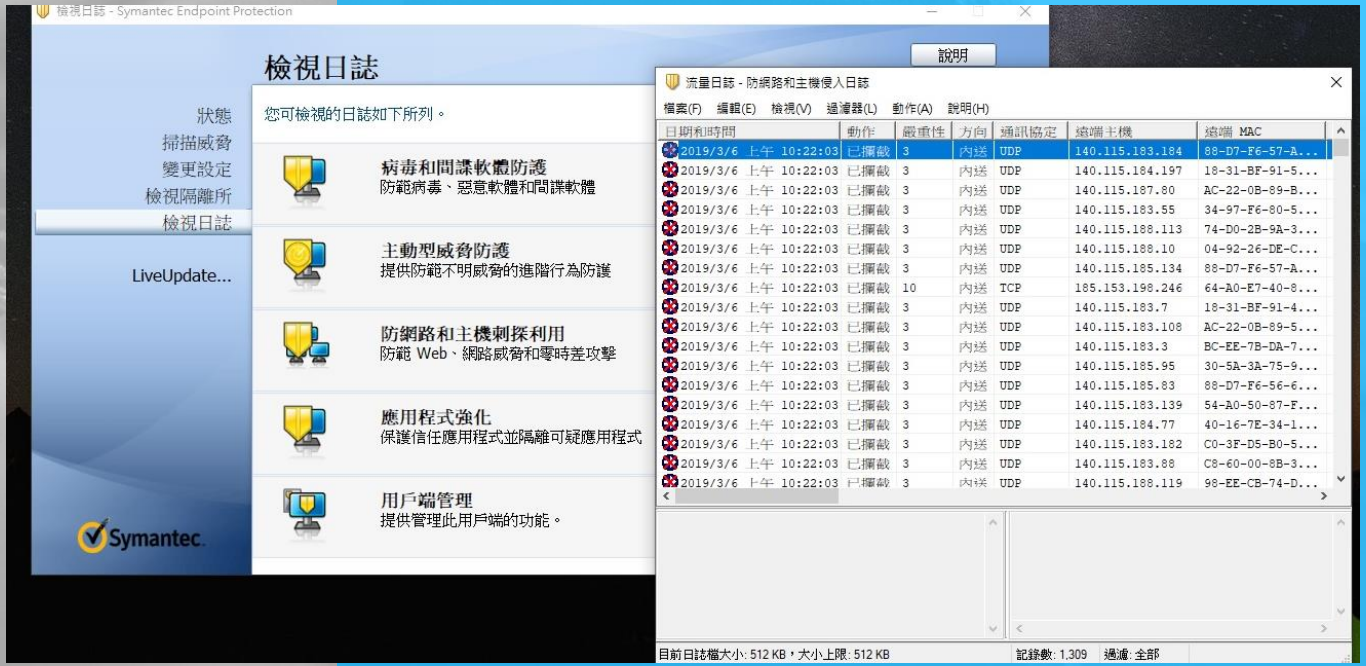
Step 1 Protect yourself using 1Password to generate and save strong passwords for each website.

Step 2 Enable 2 factor authentication and store the codes inside your 1Password account.

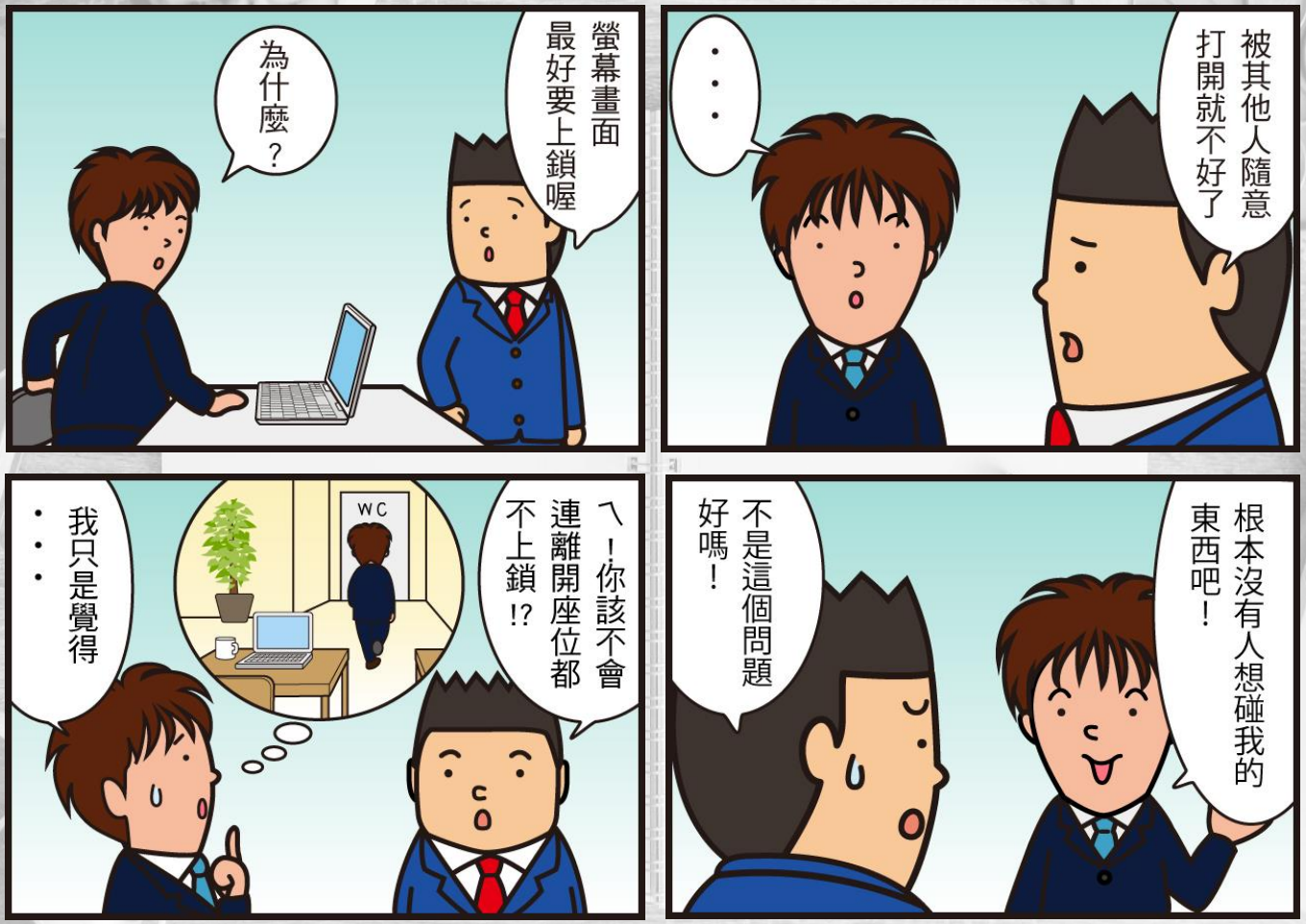
Step 3 Subscribe to notifications for any other breaches. Then just change that unique password.

我被攻擊了?


已記錄「通訊埠掃描」攻擊
用戶端會在接下來的 600 秒內 (從 2019/3/6 上午 09:42:03 至 2019/3/6 上午 09:52:03) 攔截來自 IP
上午 09:42
Symantec Endpoint Protection
已記錄「通訊埠掃描」攻擊
上午 09:37
Symantec Endpoint Protection
已記錄「通訊埠掃描」攻擊
上午 09:29
Symantec Endpoint Protection
已記錄「通訊埠掃描」攻擊
上午 09:24
Symantec Endpoint Protection
用戶端會在接下來的 600 秒內 (從 20
上午 09:21
Symantec Endpoint Protection
用戶端會在接下來的 600 秒內 (從 20
上午 09:18
Symantec Endpoint Protection
用戶端會在接下來的 600 秒內 (從 20
上午 09:05
Symantec Endpoint Protection
用戶端會在接下來的 600 秒內 (從 20
展開
清除所有通知
平板電腦模式
網路
所有設定
位置
中
上午 09:45
2019/3/6


檢視日誌 - Symantec Endpoint Protection
檢視日誌
說明
狀態
掃描威脅
變更設定
檢視隔離所
檢視日誌
LiveUpdate...
您可檢視的日誌如下所列。
病毒和間諜軟體防護
防範病毒、惡意軟體和間諜軟體
主動型威脅防護
提供防範不明威脅的進階行為防護
防網路和主機剝探利用
防範 Web、網路威脅和零時差攻擊
應用程式強化
保護信任應用程式並隔離可疑應用程式
用戶端管理
提供管理此用戶端的功能。
Symantec.
流量日誌 - 防網路和主機侵入日誌
檔案(F) 編輯(E) 檢視(V) 過濾器(L) 動作(A) 說明(H)
日期和時間 動作 嚴重性 方向 通訊協定 遠端主機 遠端 MAC
2019/3/6 上午 10:22:03 已攔截 3 內送 UDP 140.115.183.184 88-D7-F6-57-A...
2019/3/6 上午 10:22:03 已攔截 3 內送 UDP 140.115.184.197 18-31-BF-91-5...
2019/3/6 上午 10:22:03 已攔截 3 內送 UDP 140.115.187.80 AC-22-0B-89-B...
2019/3/6 上午 10:22:03 已攔截 3 內送 UDP 140.115.183.55 34-97-F6-80-5...
2019/3/6 上午 10:22:03 已攔截 3 內送 UDP 140.115.188.113 74-D0-2B-9A-3...
2019/3/6 上午 10:22:03 已攔截 3 內送 UDP 140.115.188.10 04-92-26-DE-C...
2019/3/6 上午 10:22:03 已攔截 3 內送 UDP 140.115.185.134 88-D7-F6-57-A...
2019/3/6 上午 10:22:03 已攔截 10 內送 TCP 185.153.198.246 64-A0-E7-40-8...
2019/3/6 上午 10:22:03 已攔截 3 內送 UDP 140.115.183.7 18-31-BF-91-4...
2019/3/6 上午 10:22:03 已攔截 3 內送 UDP 140.115.183.108 AC-22-0B-89-5...
2019/3/6 上午 10:22:03 已攔截 3 內送 UDP 140.115.183.3 BC-EE-7B-DA-7...
2019/3/6 上午 10:22:03 已攔截 3 內送 UDP 140.115.185.95 30-5A-3A-75-9...
2019/3/6 上午 10:22:03 已攔截 3 內送 UDP 140.115.185.83 88-D7-F6-56-6...
2019/3/6 上午 10:22:03 已攔截 3 內送 UDP 140.115.183.139 54-A0-50-87-F...
2019/3/6 上午 10:22:03 已攔截 3 內送 UDP 140.115.184.77 40-16-7E-34-1...
2019/3/6 上午 10:22:03 已攔截 3 內送 UDP 140.115.183.182 C0-3F-D5-B0-5...
2019/3/6 上午 10:22:03 已攔截 3 內送 UDP 140.115.183.88 C8-60-00-8B-3...
2019/3/6 上午 10:22:03 已攔截 3 內送 UDP 140.115.188.119 98-EE-CB-74-D...
目前日誌檔大小: 512 KB，大小上限: 512 KB
記錄數: 1,309
過濾: 全部

```
243     2019/3/4 上午 08:31:27  通訊埠掃描      次要    內送    TCP     185.153.196.85  0       64-A0-E7-40-88-41       140.115.184.100 0       88-D7-F6-54-93-8F
                                ncudarren       NCUDARREN       Default 1       2019/3/4 上午 08:28:16  2019/3/4 上午 08:30:25  有人正在掃描您的電腦。
244     2019/3/4 上午 08:31:27  主動回應        主要    內送    無      185.153.197.61  0       64-A0-E7-40-88-41       140.115.184.100 0       88-D7-F6-54-93-8F
                                ncudarren       NCUDARREN       Default 1       2019/3/4 上午 08:31:24  2019/3/4 上午 08:41:24  用戶端會在接下來的 600
秒內 (從 2019/3/4 上午 08:31:24 至 2019/3/4 上午 08:41:24) 攔截來自 IP 位址 185.153.197.61 的流量。
245     2019/3/4 上午 08:32:28  通訊埠掃描      次要    內送    TCP     185.153.197.61  0       64-A0-E7-40-88-41       140.115.184.100 0       88-D7-F6-54-93-8F
                                ncudarren       NCUDARREN       Default 1       2019/3/4 上午 08:28:18  2019/3/4 上午 08:31:24  有人正在掃描您的電腦。
246     2019/3/4 上午 08:33:42  已接受執行檔變更        資訊    外寄    UDP     239.255.255.250 0       01-00-5E-7F-FF-FA       140.115.184.100 0       88-D7-F6-54-93
-8F     C:\Program Files (x86)\Google\Chrome\Application\chrome.exe                                                     ncudarren       NCUDARREN       Default 1
2019/3/4 上午 08:32:40  2019/3/4 上午 08:32:40  應用程式在您上次開啟之後已變更，程序 ID: 9768
247     2019/3/4 上午 08:41:28  已斷開主動回應  資訊    無      無      185.153.196.85  0       N/A     140.115.184.100 0       N/A
                ncudarren       NCUDARREN       Default 1       2019/3/4 上午 08:40:26  2019/3/4 上午 08:40:26  解除始於 2019/3/4 上午 08:30:26 的「主動回應」。IP 位址
185.153.196.85 的流量攔截持續時間為 600 秒。
248     2019/3/4 上午 08:42:24  主動回應        主要    內送    無      185.153.196.85  0       64-A0-E7-40-88-41       140.115.184.100 0       88-D7-F6-54-93-8F
                                ncudarren       NCUDARREN       Default 1       2019/3/4 上午 08:42:18  2019/3/4 上午 08:52:18  用戶端會在接下來的 600
秒內 (從 2019/3/4 上午 08:42:18 至 2019/3/4 上午 08:52:18) 攔截來自 IP 位址 185.153.196.85 的流量。
249     2019/3/4 上午 08:42:29  已斷開主動回應  資訊    無      無      185.153.197.61  0       N/A     140.115.184.100 0       N/A
                ncudarren       NCUDARREN       Default 1       2019/3/4 上午 08:41:25  2019/3/4 上午 08:41:25  解除始於 2019/3/4 上午 08:31:24 的「主動回應」。IP 位址
185.153.197.61 的流量攔截持續時間為 600 秒。
250     2019/3/4 上午 08:43:19  通訊埠掃描      次要    內送    TCP     185.153.196.85  0       64-A0-E7-40-88-41       140.115.184.100 0       88-D7-F6-54-93-8F
                                ncudarren       NCUDARREN       Default 1       2019/3/4 上午 08:41:05  2019/3/4 上午 08:42:18  有人正在掃描您的電腦。
251     2019/3/4 上午 08:44:21  主動回應        主要    內送    無      185.153.197.61  0       64-A0-E7-40-88-41       140.115.184.100 0       88-D7-F6-54-93-8F
                                ncudarren       NCUDARREN       Default 1       2019/3/4 上午 08:44:18  2019/3/4 上午 08:54:18  用戶端會在接下來的 600
秒內 (從 2019/3/4 上午 08:44:18 至 2019/3/4 上午 08:54:18) 攔截來自 IP 位址 185.153.197.61 的流量。
252     2019/3/4 上午 08:45:22  通訊埠掃描      次要    內送    TCP     185.153.197.61  0       64-A0-E7-40-88-41       140.115.184.100 0       88-D7-F6-54-93-8F
                                ncudarren       NCUDARREN       Default 1       2019/3/4 上午 08:41:49  2019/3/4 上午 08:44:18  有人正在掃描您的電腦。
253     2019/3/4 上午 08:53:23  已斷開主動回應  資訊    無      無      185.153.196.85  0       N/A     140.115.184.100 0       N/A
                ncudarren       NCUDARREN       Default 1       2019/3/4 上午 08:52:19  2019/3/4 上午 08:52:19  解除始於 2019/3/4 上午 08:42:18 的「主動回應」。IP 位址
185.153.196.85 的流量攔截持續時間為 600 秒。
254     2019/3/4 上午 08:53:59  主動回應        主要    內送    無      185.153.196.85  0       64-A0-E7-40-88-41       140.115.184.100 0       88-D7-F6-54-93-8F
                                ncudarren       NCUDARREN       Default 1       2019/3/4 上午 08:53:58  2019/3/4 上午 09:03:58  用戶端會在接下來的 600
秒內 (從 2019/3/4 上午 08:53:58 至 2019/3/4 上午 09:03:58) 攔截來自 IP 位址 185.153.196.85 的流量。
255     2019/3/4 上午 08:54:58  通訊埠掃描      次要    內送    TCP     185.153.196.85  0       64-A0-E7-40-88-41       140.115.184.100 0       88-D7-F6-54-93-8F
                                ncudarren       NCUDARREN       Default 1       2019/3/4 上午 08:52:38  2019/3/4 上午 08:53:57  有人正在掃描您的電腦。
256     2019/3/4 上午 08:55:19  已斷開主動回應  資訊    無      無      185.153.197.61  0       N/A     140.115.184.100 0       N/A
                ncudarren       NCUDARREN       Default 1       2019/3/4 上午 08:54:19  2019/3/4 上午 08:54:19  解除始於 2019/3/4 上午 08:44:18 的「主動回應」。IP 位址
185.153.197.61 的流量攔截持續時間為 600 秒。
257     2019/3/4 上午 08:57:22  主動回應        主要    內送    無      185.153.197.61  0       64-A0-E7-40-88-41       140.115.184.100 0       88-D7-F6-54-93-8F
                                ncudarren       NCUDARREN       Default 1       2019/3/4 上午 08:57:22  2019/3/4 上午 09:07:22  用戶端會在接下來的 600
```



同時按下「Windows」鍵與「L」鍵的話，
就能立即將電腦上鎖

桃園區網介紹

桃園區域網路中心

→配合台灣學術網路運作
→TANet計畫規劃及執行
→TANET桃園區網維運(47個連線單位)
→TWAREN計畫規劃及執行
→桃園區網教育訓練及會議
→教育單位弱點檢測平台
→教育機構資安通報平台
→桃園區網資安檢測
→資安訊息公告與分享

http://www.tyrc.edu.tw

寄件者: 桃園區網公告: 14 個項目

桃園區網公告	[訊息轉發]【漏洞預警】Apache Solr存在安全漏洞(CVE-2019-0192)，允許...	2019/3/14 (週四) 下午 3:19
桃園區網公告	[通知] [公告] 108年3月12日(二) 9:00 ~ 12:00 中央大學機房發電機工程施工，...	2019/3/8 (週五) 下午 4:35
桃園區網公告	[訊息轉發]【漏洞預警】Google Chrome瀏覽器存在安全漏洞(CVE-2019-57...	2019/3/8 (週五) 下午 2:35
桃園區網公告	[訊息轉發]【漏洞預警】Cisco三款VPN路由器產品存在安全漏洞，允許遠端...	2019/3/7 (週四) 上午 11:43
桃園區網公告	[訊息轉發]【漏洞預警】部份單位 學生出入校園管理系統 存在 資料庫注入攻...	2019/3/6 (週三) 下午 2:01
桃園區網公告	[訊息轉發]【漏洞預警】Drupal存在安全漏洞(CVE-2019-6340)，允許攻擊者...	2019/2/25 (週一) 下午 2:52
桃園區網公告	[訊息轉發]【漏洞預警】Drupal存在安全漏洞(CVE-2019-6340)，允許攻擊者...	2019/2/25 (週一) 下午 2:51
桃園區網公告	[通知]108年桃園區網連線單位資安檢測服務申請將於：108年02月21日(四)至...	2019/2/21 (週四) 下午 4:12
桃園區網公告	[通知]區網網路斷線5分鐘	2019/2/21 (週四) 上午 11:05
桃園區網公告	[通知]桃園區網連線單位資安通報應變，自108年2月15日起，若無法於24小時...	2019/2/12 (週二) 下午 4:09
桃園區網公告	[通知]DNS Flag Day (20190201) 應變通知	2019/1/28 (週一) 上午 8:46
桃園區網公告	[訊息轉發]【漏洞預警】網路印表機設備未正確設置存在漏洞(ANA事件單通知...	2019/1/8 (週二) 下午 3:46
桃園區網公告	[會議]桃園區域網路中心管理委員會第63次會議暨資安講座(開會通知單將於近...	2018/12/27 (週四) 下午 4:20
桃園區網公告	[訊息轉發]【漏洞預警】電子學習平台Moodle出現嚴重CSRF缺陷，請儘速確...	2018/11/27 (週二) 上午 10:01

→資安事件通報事件超過24小時，暫時鎖定該IP連線

→電子郵件社交工程演練

→資安事件通報演練


感謝聆聽