tsc 德飛
TSC CAPITAL GROUP
The Bridge to the Asia Pacific Region

農委會農業金融局
下半年度一般人員訓練

資安趨勢及個資保護宣導

實施日期：108年7月25日、 108年7月31日
授課講師：顧問部 顧問 莊銘輝

簡報大綱

一	資訊安全及個資保護宣導
二	資安威脅趨勢與案例
三	網路安全四撇步
四	Q&A

農委會農業金融局

一．資訊安全及個資保護宣導

資訊安全宣導-ISMS四階文件

- 辦公室自動化系統>檔案分享區 >第一組>3.資訊>資安相關要點及文件>農金局四階文件20190708.zip

資訊安全宣導-政策

行政院農業委員會農業金融局資訊安全管理規範

第一章、總則

一、行政院農業委員會農業金融局（以下簡稱本局）為強化資訊安全管理、維護網路資訊系統的正常運作、確保網路資訊傳輸交易安全，並保障本局電腦處理資料之機密性、完整性與可用性，特訂定本規範。

第二章、資訊安全組織與分工

二、成立資訊安全推行委員會，由督導資訊業務之副局長或高層主管人員負責擔任總召集人兼資通安全長，委員會成員由各單位指派人員兼任之，負責制定及定期評估本局資訊安全政策，並統籌負責推動、協調及督導資訊安全管理事項及資源調度之協調研議。

三、成立資訊安全推行委員會工作小組，由資訊單位主管擔任召集人，小組成員為資訊單位同仁及相關科室之同仁，負責制定、評估本局資訊安全之要點、程序及表單。

臺灣資通安全管理法上路一個月實施現況

iThome 2019-02-15

關於資通安全管理法實施現況，行政院資安處副處長徐嘉臨在2月14日揭露相關進度。各部會將在2月底完成資通安全維護計畫，至於關鍵設施提供者的納管，則是要到今年7月1日才開始執行。

基本上，在資通管理法細節的子法於去年11月發布後，今年1月1日已經正式施行。對於施法前後的差異，徐嘉臨簡單說明，過去政府在資安防護的要求上，規範屬行政命令位階，在資安管理法施行後，現在提高為法令之位階，因此針對納管機關有一致化、標準化之規範。

此外，過去偏重在公務機關，現在納管範圍擴大，增加特定非公務機關，也是比較不同之處，此外，還有在管理面、技術面與政策及整合面的改變。

5

資通安全管理法施行之後的變革

資料來源：行政院資通安全處

規範面

施行前

- 國家資通安全通報應變作業綱要 105.8.24
- 資訊系統分級與資安防護基準作業規定 104.7.29
- 政府機關(構)資通安全責任等級分級作業規定 104.1.20
- 行政院及所屬各機關資訊安全管理規範 88.11.16
- 行政院及所屬各機關資訊安全管理要點 88.9.15

➢ 屬行政命令位階，僅係上級機關對下級機關，規範機關內部秩序及運作，非直接對外發生法規範效力，對非公務機關並無強制力。

施行後

- 資安法+6項子法
  - 資通安全管理法施行細則
  - 資通安全責任等級分級辦法
  - 資通安全事件通報及應變辦法
  - 特定非公務機關資通安全維護計畫實形情形稽核辦法
  - 資通安全情資分享辦法
  - 公務機關所屬人員資通安全事項獎懲辦法

➢ 由過去行政命令位階提高法令之位階。針對納管機關有一致化、標準化之規範。

➢ 增加罰則之規定。
公務機關->懲處
特定非公務機關 ->罰緩

資料來源：行政院資通安全處

適用範圍面

施行前

- 資通安全管理相關規範僅適用於公務機關。
- 針對公營事業，係透過其主管機關之要求其辦理。

施行後

- 納管對象增加特定非公務機關
  - 考慮組織公共性、政府資源投入(資金/基金來自公帑)
  - 涉及與公共利益高度相關者或機能對國家安全及民眾影響重大者
- 特定非公務機關之稽核
  - 主管機關得稽核特定非公務機關
  - 中央目的事業主管機關應稽核關鍵基礎設施提供者
  - 中央目的事業主管機關得稽核公營事業、政府捐助之財團法人

資料來源：行政院資通安全處

管理面

施行前

- 「政府機關（構）資通安全責任等級分級作業規定」附表中，有管理面之應辦事項。
- 資安專責人員配置
  - A 級機關：2名
  - B 級機關：1名

施行後

- 要求各機關應進行責任等級分別，並依分級結果，訂定資通安全維護計畫，並提出維護計畫實施情形。
- 委外監督要求明文化，包括委外之前選任，及委外後監督。
- 各機關應有資通安全推動組織公務機關要求配置資通安全長
- 資安專責人員配置
  - A 級機關：4名
  - B 級機關：2名
  - C 級機關：1名
- 公務機關要求配置專職人員

資料來源：行政院資通安全處

技術面

施行前

- 資通安全等級分為A、B、C+、C級
- 「政府機關（構）資通安全責任等級分級作業規定」中，針對A、B級機關應辦事項要求
- C級機關應辦事項多授權各主管機關規定

施行後

- 資通安全等級分為A、B、C、D、E 等5級
- 「資通安全責任等級分級辦法」附表中，針對A~E級機關，皆明定對應之應辦事項
- 應辦事項增加：
  - 資安治理成熟度評估(A~B級之公務機關)
  - 政府組態基準(A~B)
  - 資通安全健診(A~C)

資料來源：行政院資通安全處

政策及整合面

施行前

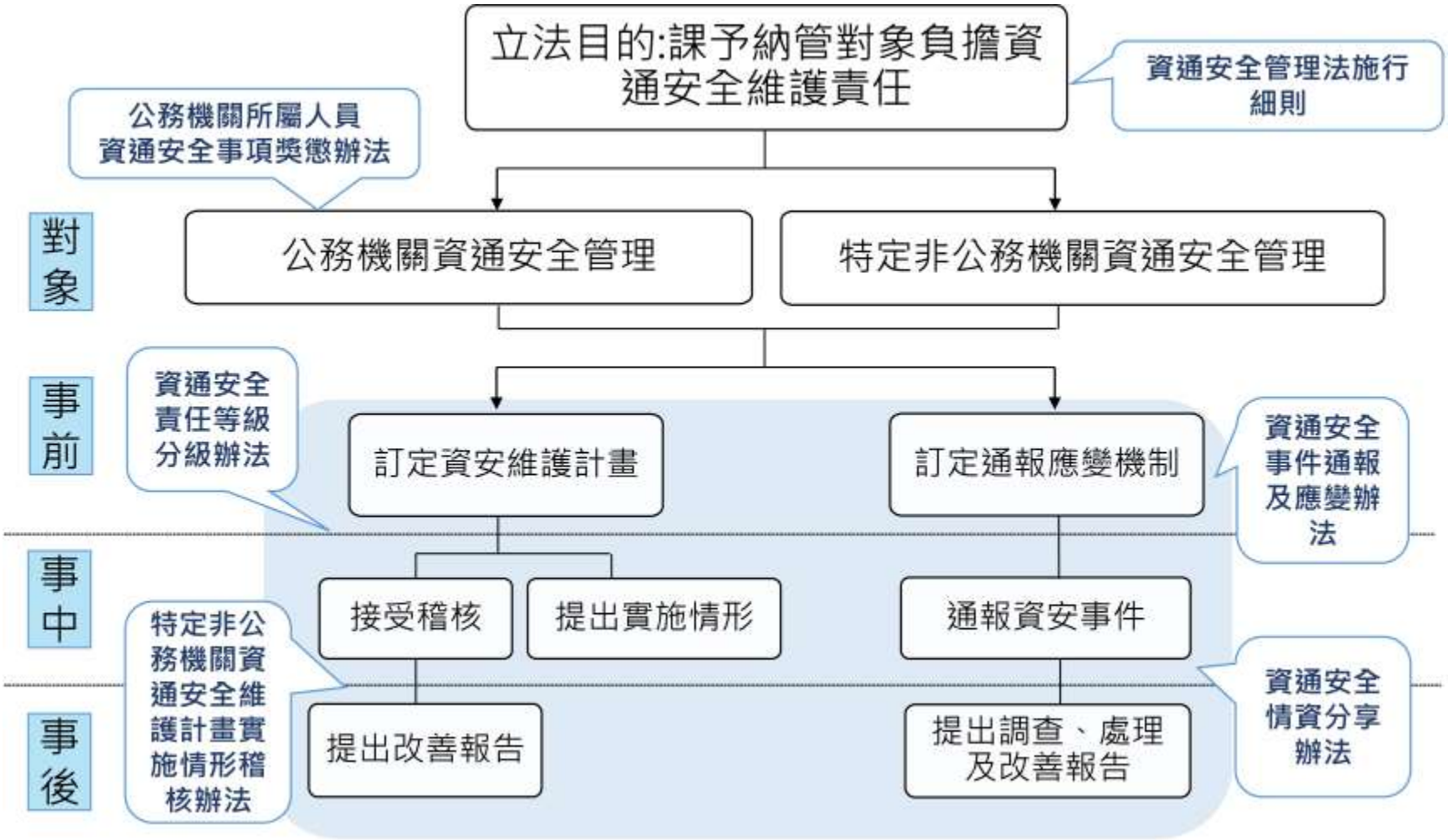
- 無明文規範。

施行後

- 新增資安情資分享機制，納入情資分析、整合與分享之內容程序、方法等規範。
- 政府應整合民間力量推動資通安全相關事項
  - 資安人才培育
  - 資安科技之研發、整合、應用、產學合作及國際交流
  - 資安產業之發展
  - 資安軟硬體技術規範、相關服務與審驗機制之發展
- 主管機關應送立法院備查文件

資料來源：行政院資通安全處

資通安全管理法及6項子法架構



資料來源：行政院資通安全處

谷歌違反GDPR 歐盟大刀裁罰5千萬歐元

非凡新聞 2019-01-23

大數據時代，消費者在網路上的軌跡或個資，越來越值錢，也讓隱私權更加受到重視！像法國資料保護署，日前就確定裁罰谷歌五千萬歐元，因為在告知用戶的個資被使用時，透明度不足，違反歐盟隱私法GDPR，而這也是GDPR上路以來最高罰款！

而在台灣，其實近來也有不少外商，因為隱私權政策引發爭議，專家就認為，目前台灣個資法的保護力道不足，未來修法應會朝向歐盟標準前進。

影片來源：https://www.youtube.com/watch?v=7K9egvF4YtE

13

台歐 GDPR 技術性諮商漸入深水區

中央社 2019-06-18

陳美伶 17 日表示，歐盟針對個資的蒐集、處理、利用，對台灣提出 18 項議題，國發會這次先就其中 8 項議題做說明，解釋台灣個資法的規範及執行細節，剩下的 10 項議題，則約好在今年秋天進行視訊會議討論。

陳美伶說，歐盟主要關注 2 大重點，一是跨境傳輸，因為台灣採「原則許可、例外不許可」，歐盟則為「原則不許可、例外許可」，正好相反，台灣與歐盟兩邊立法意旨不太相同，因此歐盟關注台灣的法律、執行過程，是否足以保護個人資料。

另一個重點則是台灣是否設置個資保護的獨立專責機關，陳美伶坦言，這是比較困難的部分，因為台灣組織改造相對剛性，去年行政院已責成國發會成立「個人資料保護專案辦公室」，屬於任務編組的型態。

14

個人資料的保護與使用

農委會農業金融局

二．資安威脅趨勢與案例

網攻竊走星國百萬人個資 目標李顯龍

大愛新聞 2018-07-21

新加坡醫療機構 150萬人的個資遭到竊取，是新加坡有史以來規模最大的網路攻擊，總理李顯龍和部長級官員都是受害者。

影片來源：https://www.youtube.com/watch?v=YIhwT2cKiRQ

17

「少爺殭屍」網路擴散！全球百萬筆個資遭竊

5 7 東森財經新聞台 2018-06-07

手機族要注意了！最近一款叫「少爺殭屍網路」正在大量擴散，玩家只要使用無線網路分享器上網連上手機，就可能被駭，目前全球有6000支Android手機被駭，被偷的個資超過100萬筆，台灣也有100多人受害！

影片來源：https://www.youtube.com/watch?v=7K9egvF4YtE

18

委內瑞拉指責美國網路攻擊其基礎設施

美國之音中文網 2019-03-13

委內瑞拉總統馬杜洛星期二(3/12)在電視直播中說：”經證實，這確實是一起來自美國的網路攻擊。我只能說攻擊來自休斯頓和芝加哥。對電力系統、通信網路和互聯網發動的攻擊來自美國這兩座城市。”

馬杜洛沒有提供上述指控的證據，但表示會請求中國等國家協助調查這起網路攻擊事件。

影片來源：https://www.youtube.com/watch?v=4L5tVfxF34g

19

銓敘部個資外洩

自由時報 2019-06-25

政府資安再傳重大疏漏！銓敘部驚傳有高達五十九萬筆文官服務單位、職稱等個資外洩，並遭國外網站揭露，銓敘部已緊急依資通安全管理法向行政院國家資通安全會報技術服務中心通報，銓敘部昨也指出，目前已請資安部門進行資料外洩原因調查，將確實檢討改進，另也依個人資料保護法規定，針對二十多萬受影響的當事人展開通知作業。

影響範圍包括從二〇〇五年一月一日至二〇一二年六月三十日間，中央及地方機關公務人員送審人員的歷史資料，實際影響人數則有二十四萬三千三百七十六人，欄位內容則包含身分證字號、姓名、服務機關、職務編號、職稱等。

20

世界經濟論壇2019年全球風險調查報告

- 科技風險項目包含網路攻擊、資料詐欺或竊盜、關鍵資訊基礎設施破壞與科技發展造成負面影響

10大影響風險

1. 大規模殺傷性武器
2. 緩解氣候變化與適應失敗
3. 極端氣候
4. 水資源危機
5. 重大自然災害
6. 生物多樣性喪失與生態系統崩潰
7. **網路攻擊(2018年排名第6)**
8. **關鍵資訊基礎設施破壞(※)**
9. 人為環境災害
10. 傳染病傳播

10大可能風險

1. 極端氣候
2. 緩解氣候變化與適應失敗
3. 重大自然災害
4. **資料詐欺或竊盜(2018年排名第4)**
5. **網路攻擊(2018年排名第3)**
6. 人為環境災害
7. 大規模非自願性移民
8. 生物多樣性喪失與生態系統崩潰
9. 水資源危機
10. 主要經濟體資產泡沫

資料來源：The Global Risks Report 2019 14th Edition, World Economic Forum
行政院資通安全處

全球資安威脅案例

進階持續威脅攻擊
竊取機密資料

2018/07 Timehop遭駭，導致上千萬用戶個資外洩

分散式阻斷服務
攻擊癱瘓網路運作

2018/03 GitHub遭史上最大DDoS攻擊

物聯網設備資安
弱點威脅升高

2018「少爺殭屍網路」針對家用路由器進行攻擊，感染範圍擴及全球55個國家

關鍵資訊基礎設施
資安風險倍增

2018 惡意程式VPNFilter攻擊特定工業控制系統

網路與經濟罪犯影響
電子商務與金融運作

2018/05 智利最大銀行遭駭，造成系統癱瘓與網路盜轉

資安(訊)供應商持續
遭駭破壞供應鏈安全

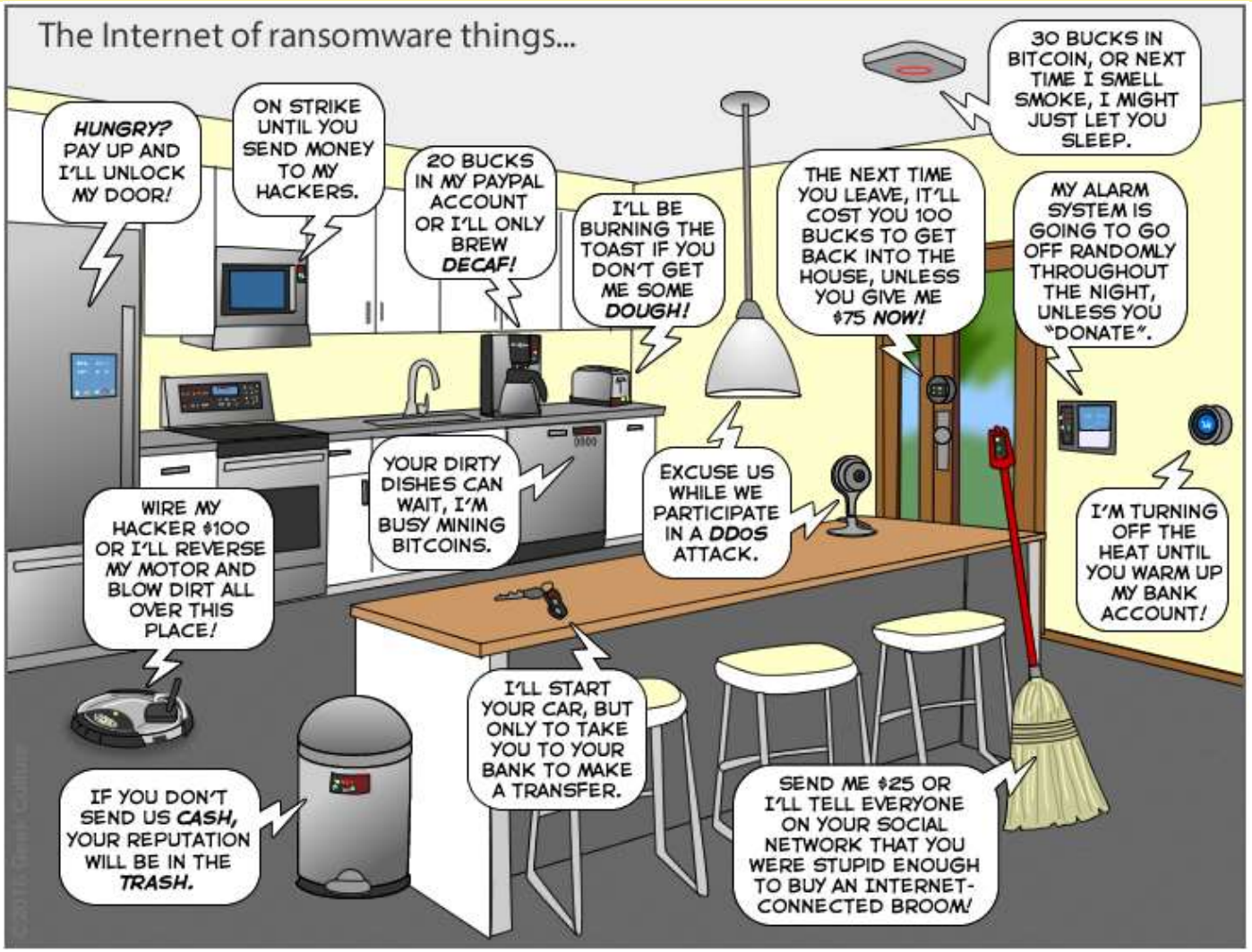
2018/11駭客以StatCounter為跳板入侵加密貨幣交易中心Gate.io

22

資料外洩數量不斷攀升

資料來源：https://breachlevelindex.com/

IoT裝置-網路犯罪集團的新大陸

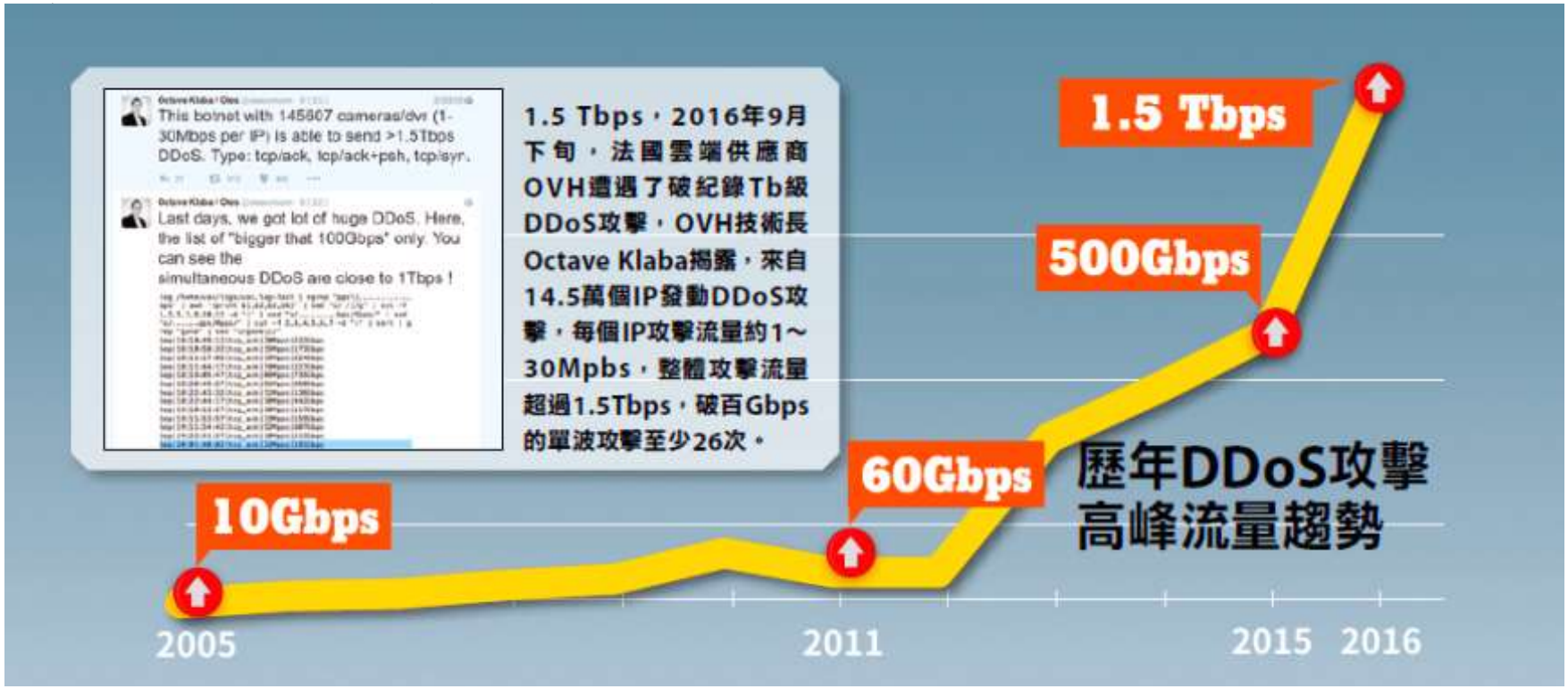


物聯網世界裡，每一個聯網裝置都可能成為攻擊物件

圖片來源：The Joy of Tech http://www.geekculture.com/joyoftech/joyarchives/2340.html

物聯網裝置參與DDoS攻擊

物聯網裝置將在分散式阻斷服務(DDoS)攻擊中扮演更大的角色，而工業物聯網系統也將成為



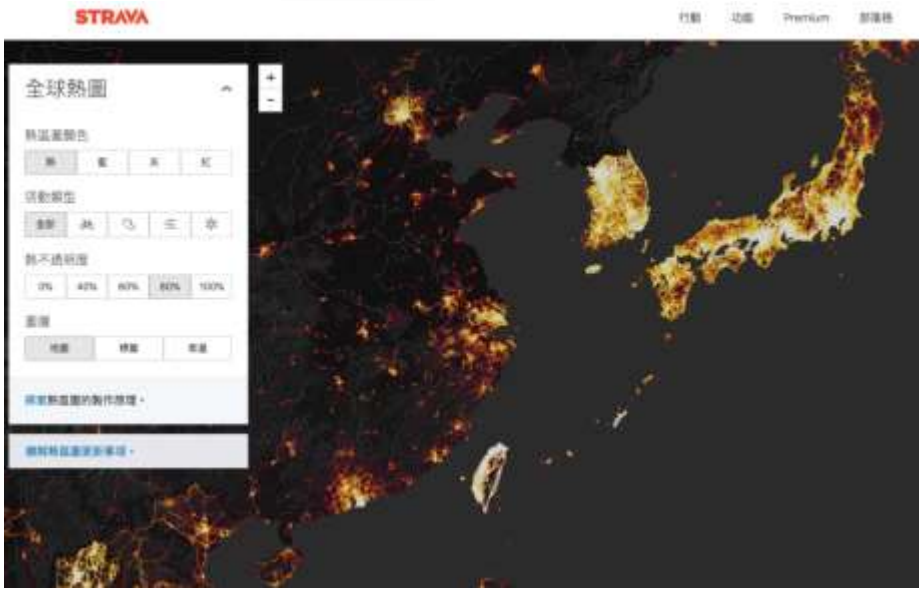
圖片來源：iThome https://www.ithome.com.tw/news/110135

令人驚奇的讀心術

影片來源：https://breachlevelindex.com/

凡走過必留下~數位足跡

- Google takeout



科技的逆襲

保護檔案
的
加密技術

勒索軟體

更多漏洞

IoT物聯網
的興起

機器學習
與區塊鏈
的
新興技術

駭客濫用

圖片來源：pixabay https://pixabay.com/

資安因應措施

更好的資安掌握度
與多層式資安防禦

良好的資安習慣與
持續防護

- 變更預設密碼
- 正確設定裝置以確保安全
- 隨時套用修補更新
- 防範社交工程技巧

圖片來源：pixabay https://pixabay.com/

農委會農業金融局

三．網路安全四撇步

層出不窮的詐騙

- LINE臭跩貓免費貼圖? 詐騙個資傳萬人上當

  民視新聞 2018-06-25

- 免費的最貴

利用人性的弱點

圖片來源：https://pixabay.com

【假好康】騙個資

有機會贏得 iPhone 或其他 Google 獎品

詢問你幾個問題，然後引導你最後去填相關資料，小心釣魚網站騙取個資。

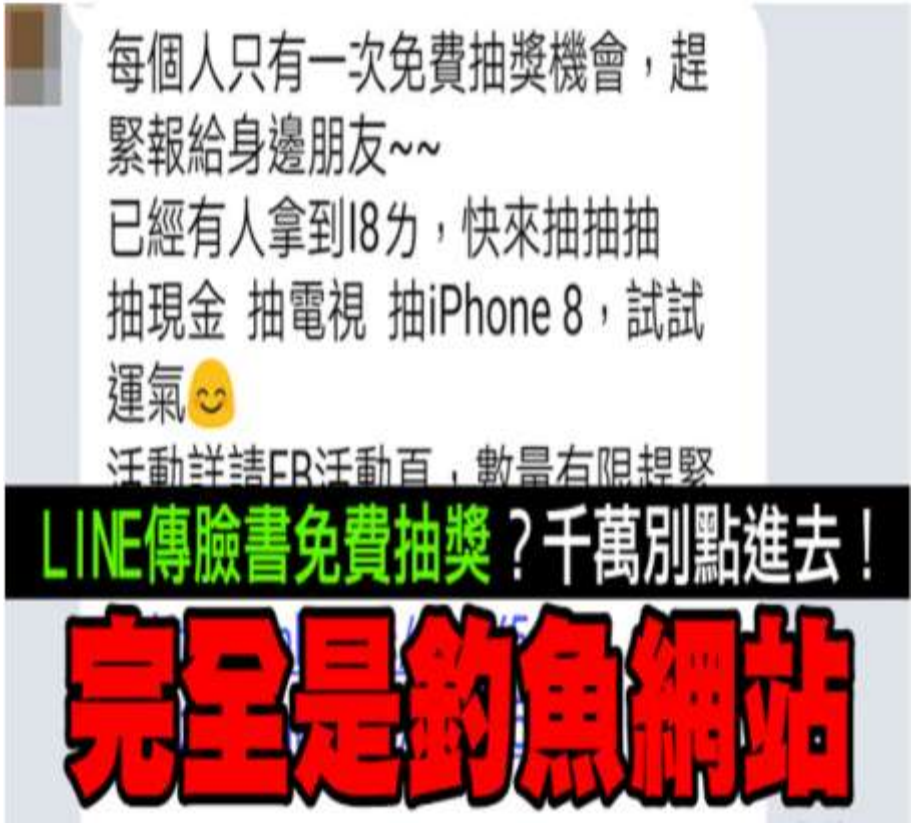
資料來源：http://www.mygopen.com/2017/11/google-iphone.html

(詐騙)Email 的通知連結

- 隨著手機更新然後從 iPhone 5 進化到 iPhone 8

資料來源： http://www.mygopen.com/2017/11/google-iphone.html

抽現金、抽電視、抽iPhone 8



第一個問題是: Google創辦人是誰

第二個是: 總部在哪?

第三個是:成立於幾年?

而且回答問題還有秒數限制

資料來源： http://www.mygopen.com/2017/10/iphone-8facebook.html

抽現金、抽電視、抽iPhone 8

➲ http://lnk.pics/18JY5

資料來源： http://www.mygopen.com/2017/10/iphone-8facebook.html

必須登入才能抽獎哦！

資料來源： http://www.mygopen.com/2017/10/iphone-8facebook.html

Line詐騙ID

刑事局統計，盜用臉書帳號，假借販售低價手機、演唱會門票等要求被害人親友加Line好久進行詐騙的案例越來越多

資料來源： https://www.ettoday.net/news/20180225/1119158.htm

中油假官方LINE帳號騙取個資

通訊軟體LINE上出現加入好友就可領取現金抵用券，中油澄清，從未成立相關的line上官方帳號，更沒有優惠，現在能看到的訊息都屬於詐騙，提醒民眾不要上當受騙。（圖／取自經濟部FACEBOOK）

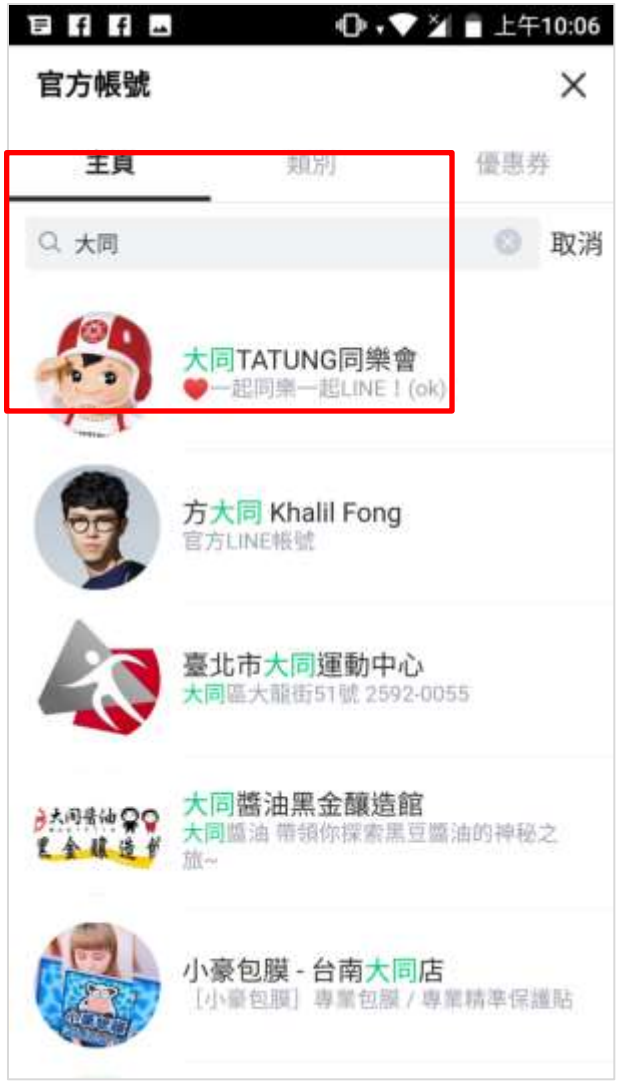
資料來源：https://www.ettoday.net/news/20180226/1119818.htm

真假官方帳號？

如何辨別LINE@生活圈帳號是否經過官方審查認證?

進入官方帳號頁面搜尋，進入後搜尋您想查詢的生活圈帳號

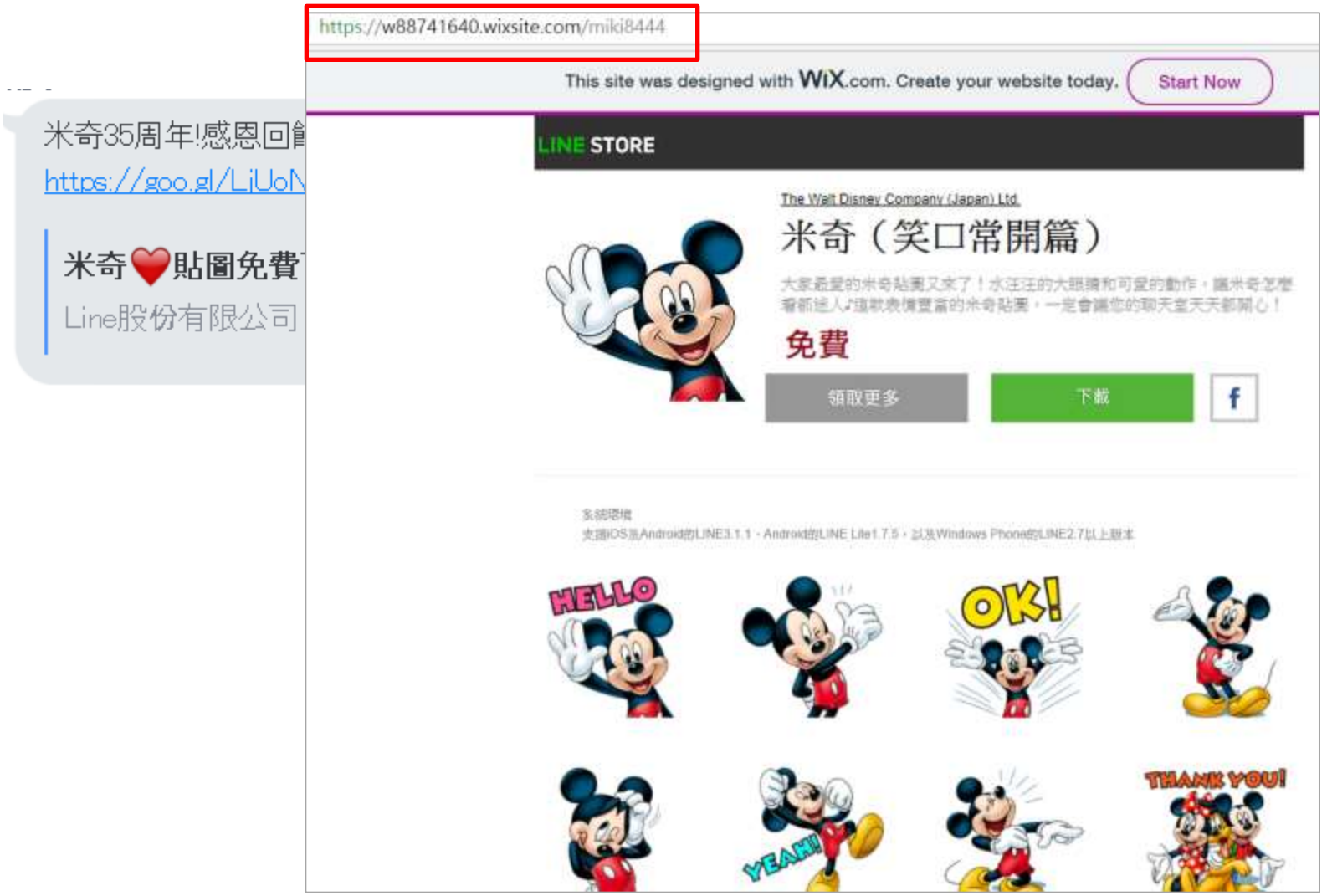
測試一下_真假官方帳號？



真假官方帳號？

再多折價券都是騙你的!　知名賣場的偽LINE帳號

免費貼圖_傳10人騙個資



FB也幫忙推Line貼圖？

讓你的電腦與智慧型手機遠離危害

1. 只瀏覽受信任或知名網站。
2. 智慧型手機一開始大多要用帳號、密碼註冊，甚至要輸入信用卡資料，所以要設定複雜的密碼。
3. 作業系統及軟體要隨時更新。
4. 購物或登入銀行網站時，避免用公共無線熱點。
5. 好好保管你的智慧型手機，不要被人偷走。

防範社交工程「四不一沒有」

除了停、看、聽之外~

不輕易相信

透過網路或電話非經正式授權的請求

不接受

陌生人的好友請求

不使用

公務信箱作為公開帳號

不公開

談論公務相關內容

沒有個資

就難以詐騙

農委會農業金融局

四．Q&A

TSC CAPITAL GROUP

The Bridge to the Asia Pacific Region

TSC – FB Site

TSC – Blog Site