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

桃園市政府教育局

資訊安全認知宣導課程

實施日期：108年08月16日
授課講師：資安顧問 宋亞倫

現任：德欣寰宇 顧問部 資安顧問

相關證照：ISO 27001 LA、ISO 29100 LA、BS 10012 (PIMS)

輔導經歷：

個人資料保護制度—

教育部、臺北市稅捐稽徵處、宜蘭縣政府(府內及所屬一級機關)、新北市政府稅捐稽徵處、新北市政府民政局、臺中市政府地方稅務局、花蓮縣地方稅務局、臺中市政府民政局、國立清華大學、國立高雄第一科技大學、景文科技大學、明新科技大學、內政部營建署、內政部消防署、財政部關務署基隆關等單位

資訊安全管理系統—

桃園市政府資訊科技局、桃園市政府地方稅務局、桃園市政府地政局、桃園市政府教育局、臺北市財政局、臺北市稅捐稽徵處、新北市政府稅捐稽徵處、新北市政府民政局、新北市政府警察局、新北市政府資訊中心、臺中市政府民政局、宜蘭縣政府(6個單位聯合輔導)、基隆市稅務局、考試院、考試院銓敘部、財政部關務署(關稅總局)、財政部關務署基隆關(基隆關稅局) 、財政部賦稅署、內政部營建署、內政部消防署、內政部役政署、交通部台灣鐵路管理局等單位

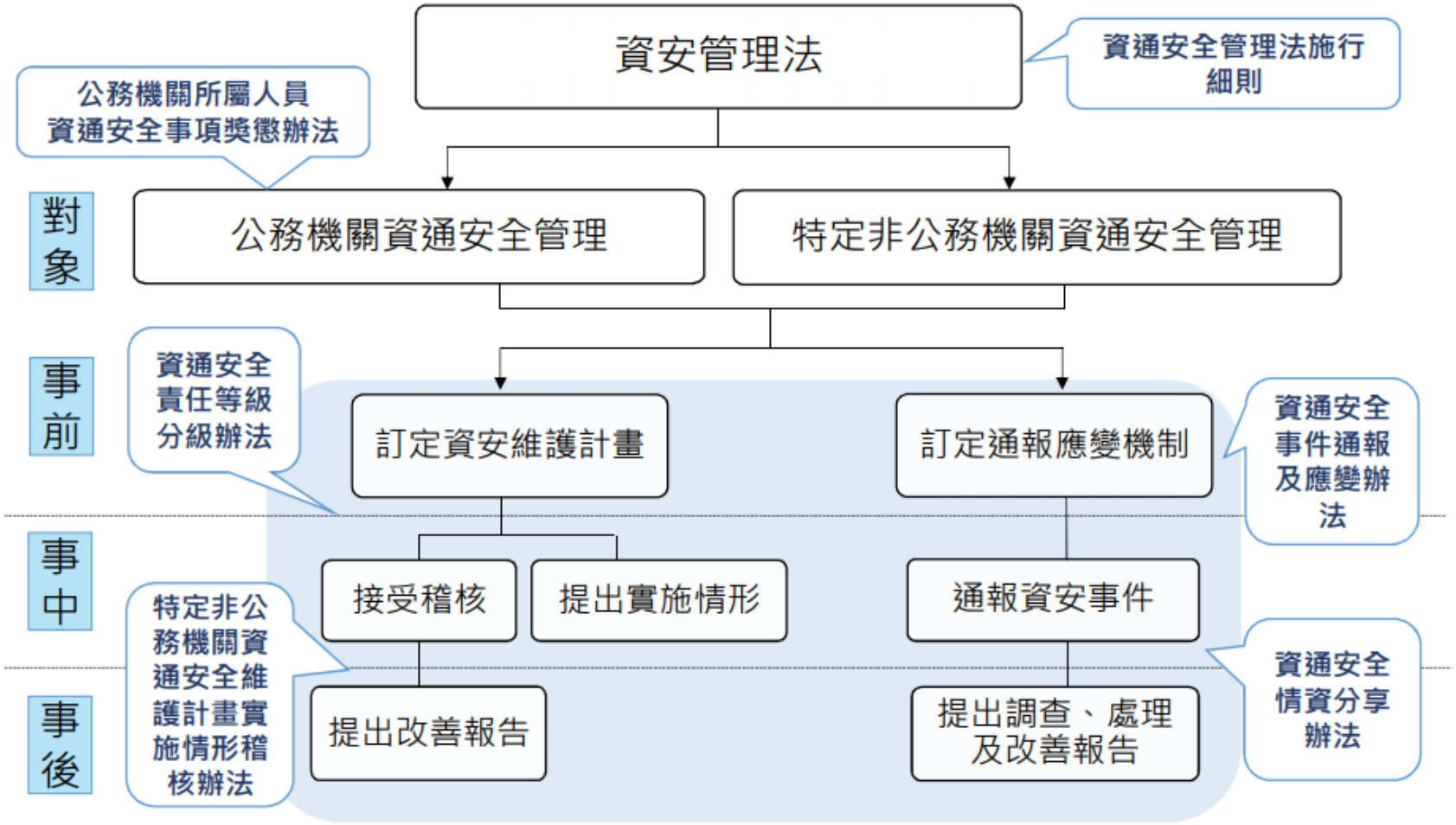
簡報大綱

一	資通安全管理法之因應
二	社交工程案例分享
三	資安防護重點
四	Q&A

資通安全管理法之因應

資通安全管理法簡介

- 資通安全法整體架構



Source：行政院技術服務中心「資通安全管理法簡介」

資通安全責任等級分級辦法

C級

- 各機關**維運自行或委外開發之資通系統者**，其資通安全責任等級為 C 級。

D級

- 各機關**自行辦理資通業務**，未維運自行或委外開發之資通系統者，其資通安全責任等級為 D 級。

公務機關應辦事項說明：管理面

制度面向	辦理項目	辦理內容	
		C級	D級
管理面	資通系統分級及防護基準	• 針對開發之系統進行評鑑 • 系統等級為高者2年內完成防護基準之控制措施	N/A
	資訊安全管理系統之導入及通過公正第三方之驗證	2年內全部核心系統導入ISMS	
	資通安全專責人員	專職人員1名	
	內部資通安全稽核	每2年至少辦理1次	
	業務持續運作演練	全部核心系統每2年至少辦理1次	

註：資通安全專職人員，指應全職執行資通安全業務者

公務機關應辦事項說明：技術面

制度面向	辦理項目	C級	D級
技術面	網站安全弱點檢測	全部核心系統每2年辦理1次	N/A
	系統滲透測試		
	資安健診	每2年辦理1次	
	資通安全防護機制	1年內完成： 防毒軟體、網路防火牆、及電子郵件過濾機制(若適用)啟用及必要升級更新	

公務機關應辦事項說明：認知訓練

制度面向	辦理項目	C級	D、E級
認知與訓練	資通安全教育訓練 -資通安全及資訊人員	12Hr/Year，至少1人	N/A
	資通安全教育訓練 -一般使用者及主管	**3Hr/Year，所有人員**	
	取得專業證照(維持有效)	應持有1張以上	N/A
	取得職能訓練證書(維持有效)	應持有1張以上	

資安法施行細則：委外管理

- 施行細則第四條：
  - 各機關依本法第九條規定委外辦理資通系統之建置、維運或資通服務之提供（以下簡稱受託業務），選任及監督受託者時，應注意下列事項：

1. 受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證。
2. 受託者應配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員。
3. 受託者辦理受託業務得否複委託、得複委託之範圍與對象，及複委託之受託者應具備之資通安全維護措施。

資安法施行細則：委外管理

- 施行細則第四條：
  4. 受託業務涉及國家機密者，執行受託業務之相關人員應接受適任性查核，並依國家機密保護法之規定，管制其出境。
  5. 受託業務包括客製化資通系統開發者，受託者應提供該資通系統之安全性檢測證明；該資通系統屬委託機關之核心資通系統，或委託金額達新臺幣一千萬元以上者，委託機關應自行或另行委託第三方進行安全性檢測；涉及利用非受託者自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。

資安法施行細則：委外管理

- 施行細則第四條：
  6. 受託者執行受託業務，違反資通安全相關法令或知悉資通安全事件時，應立即通知委託機關及採行之補救措施。
  7. 委託關係終止或解除時，應確認受託者返還、移交、刪除或銷毀履行契約而持有之資料。
  8. 受託者應採取之其他資通安全相關維護措施。
  9. 委託機關應定期或於知悉受託者發生可能影響受託業務之資通安全事件時，以稽核或其他適當方式確認受託業務之執行情形。

人員懲處

- 行政院Q&A：
  - 機關人員未依資安法、資安法授權訂定之法規或機關內部規範辦理資安事項，經主管機關、上級或監督機關評定績效不良，且疏導無效情節重大者，始可能進行懲處，機關人員如已依規定辦理者，不致受懲。

社交工程案例分享

世界經濟論壇2019年全球風險調查

10大影響風險

- **第7名**
  網路攻擊
  （2018年排名第6）
- **第8名**
  關鍵資訊基礎設施
  破壞

10大可能風險

- **第4名**
  資料詐欺或竊盜
  （2018年排名第4）
- **第5名**
  網路攻擊
  （2018年排名第3）

資料來源：The Global Risks Report 2019
14th Edition, World Economic Forum

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

駭客使用具有管理員權限的員工帳密，登入其雲端供應商網路後，建立新的管理員帳戶。登入其雲端服務進行環境偵查，隨後開始攻擊Timehop的主要資料庫並對外傳輸資料

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

GitHub遭到駭客攻擊，每秒傳送約1.27億個封包，尖峰攻擊流量達到1.35 Tbps，為目前史上最大的DDoS攻擊，駭客攻擊一度使GitHub至少斷線5分鐘

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

發現組織型駭客利用少爺殭屍網路，針對家用路由器進行攻擊，並誘騙利用該路由器連網之使用者下載惡意APP，竊取個人資料，計有20多萬台路由器被駭客掌控，至少6,000台行動裝置遭感染，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

思科旗下的Talos安全部門揭露1個已感染全球50萬台網路裝置的模組化惡意程式VPNFilter。VPNFilter可長期進駐於受駭裝置上，且對於Modbus SCADA協定的工業控制系統特別有興趣，它能監控裝置流量，竊取網站憑證，還能切斷裝置的連網能力或讓裝置無法使用

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

智利最大銀行(Banco de Chile)遭惡意程式入侵，計有逾9,000台員工電腦及500台伺服器無法開機，駭客更企圖趁亂利用SWIFT網路盜轉銀行金錢

資安(訊)供應商持續
遭駭破壞供應鏈安全

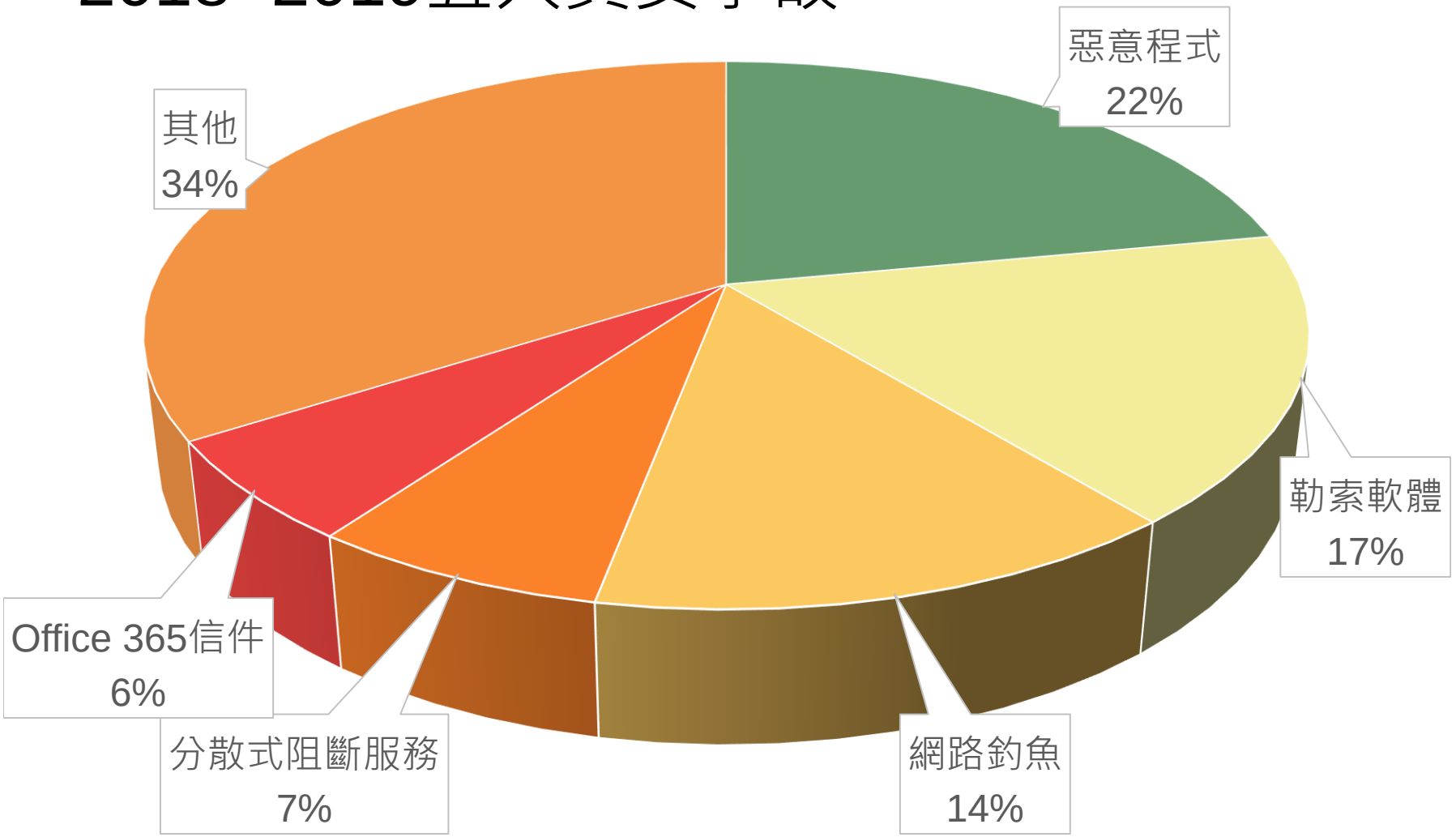
2018/11駭客以StatCounter為跳板入侵加密貨幣交易中心Gate.io

資安業者ESET揭露一起利用供應鏈漏洞入侵的事件，駭客先入侵熱門的網路分析平台StatCounter，藉以攻擊利用StatCounter分析流量的網站，受害者為加密貨幣交易平台gate.io，由於此為gate.io平台特有之URI，顯示駭客是瞄準比特幣的交易網頁而來

資料來源：行政院技服中心

Check Point：2019威脅

- 2018~2019五大資安事故



社交工程 - 簡介

- Social Engineering
- 不需要具備頂尖的電腦專業技術
- 利用人性弱點

常見手法：好奇心

圖片來源：https://pixabay.com

追劇詐騙

- Check Point：駭客利用《權力遊戲》引發一系列惡意詐騙活動

資料來源：TechNews

常見手法：優惠訊息

圖片來源：https://pixels.com

假抽獎、假貼圖

- 詐騙集團也慶祝母親節！各式假抽獎、假貼圖正瘋傳

資料來源：T客邦

中獎詐騙

- **20億彩券得主送賓士抽獎？**

LINE防詐騙機器人

- 趨勢科技
  防詐達人

- MYGOPEN

LINE防詐騙

常見手法：假冒身分

圖片來源：https://pixabay.com

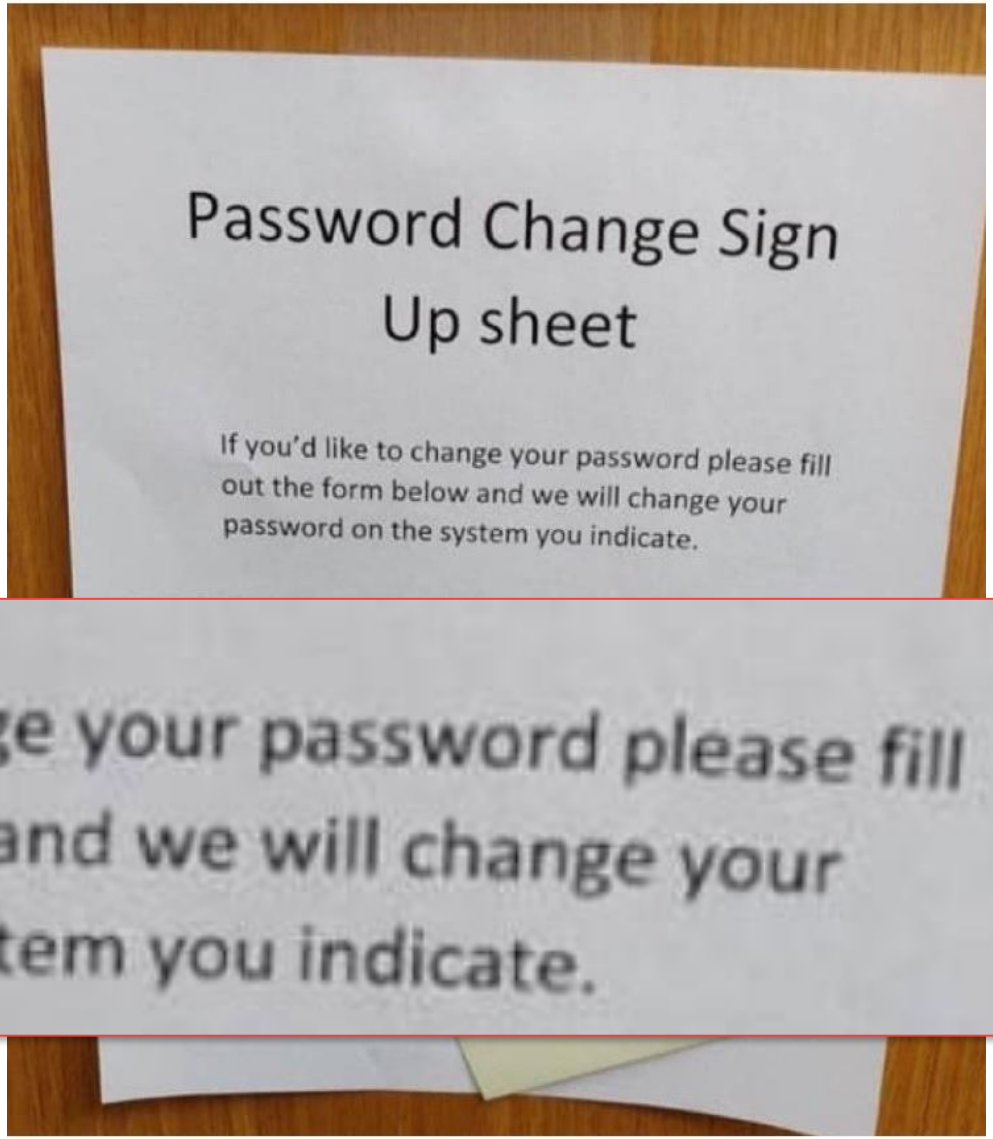
假冒身份索取講稿

- 社交工程詐騙！遭冒名索取韓國瑜講稿

資料來源：2019-06-26 聯合報

密碼調查

調查密碼設置之情形，請各位同仁協助填寫：



If you'd like to change your password please fill out the form below and we will change your password on the system you indicate.

網路釣魚

- 利用網路釣魚進行社交工程的過程

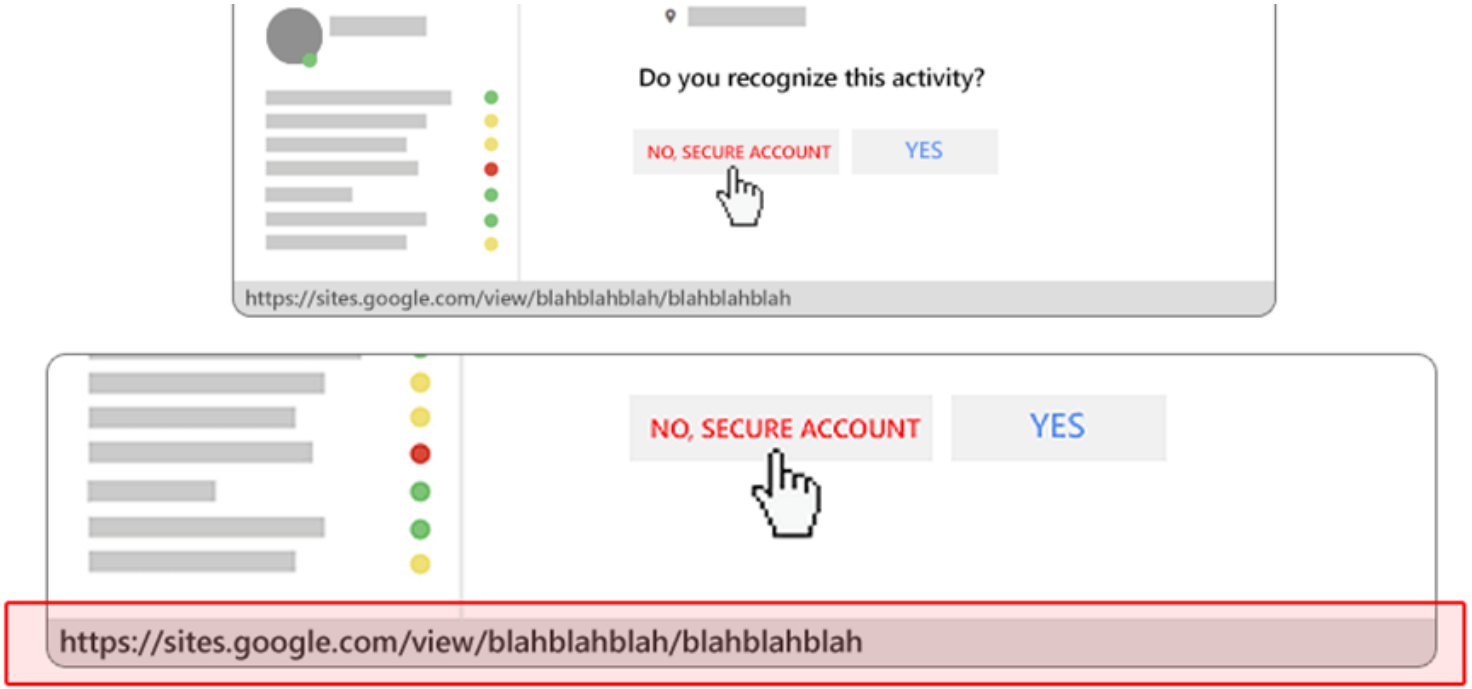
1. 創建幾可亂真廠商信箱帳號和山寨網站
2. 假借正常廠商名義大量寄送信件
3. 誘騙受害者點擊連結至山寨網站

facebook.com → my-face-book.com

4. 於山寨網站要求受害者填寫資料

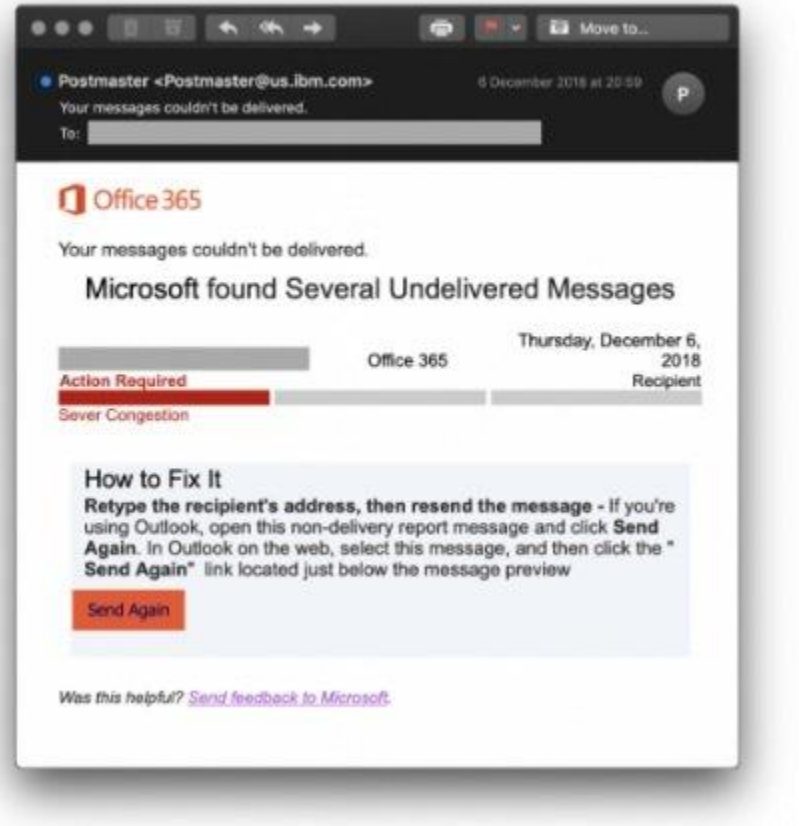
假冒Mail遭駭通知

- 伊朗駭客假冒Gmail和Yahoo Mail遭駭通知信來發送釣魚郵件，專門鎖定記者、社運人士和官員



假Office通知真釣魚

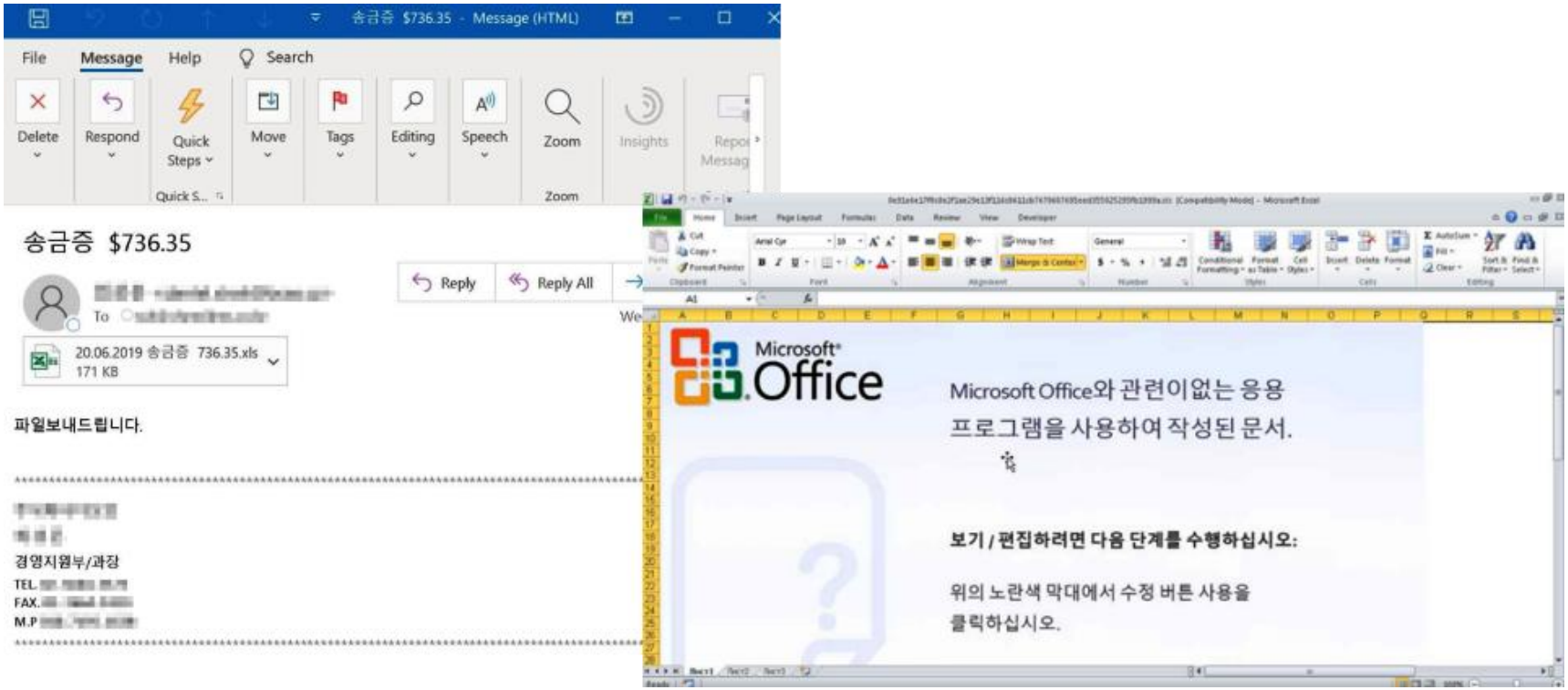
- 偽造的Office 365無法傳遞通知成為駭客網釣新手法



2018-12-17 iThome

Office文件暗藏遠端木馬程式

- 遠端木馬程式藉郵件Office文件巨集散布，臺灣、南韓皆傳受害



資料來源：2019-06-25 iThome

山寨網站

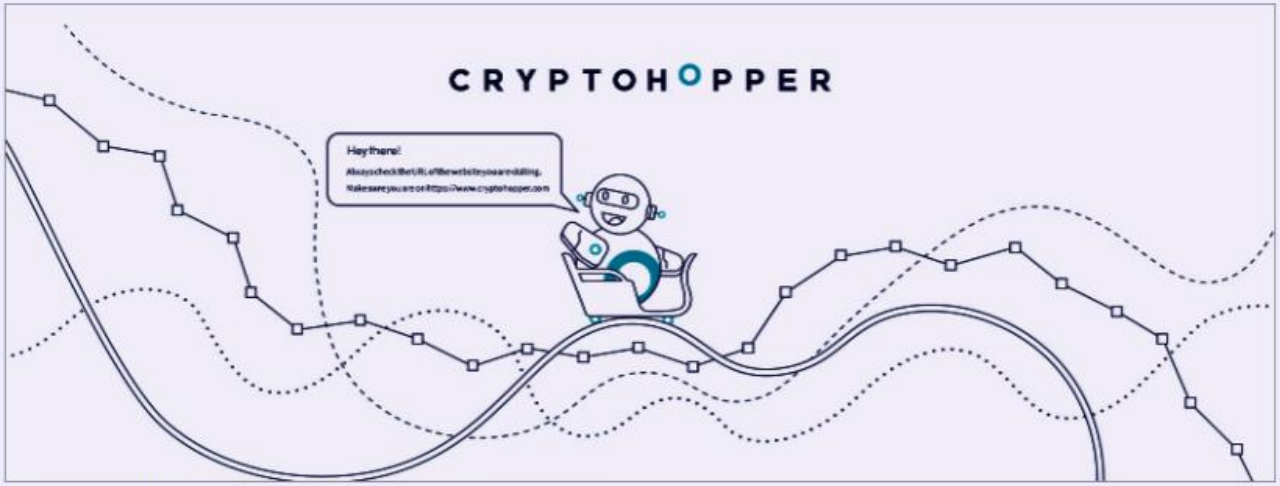
- 加密貨幣交易平台Cryptohopper有山寨版，可竊取受害者資料

由於這類釣魚網站介面幾乎和本尊長得一模一樣，使用者必須特別留意所造訪網站的網址是否正確，在執行任何自網路上下載的檔案時，最好先掃防毒

文/ 陳曉莉 | 2019-06-07 發表

讚 5.4 萬 按讚加入iThome粉絲團 讚 54 分享

Cryptohopper warns for phishing

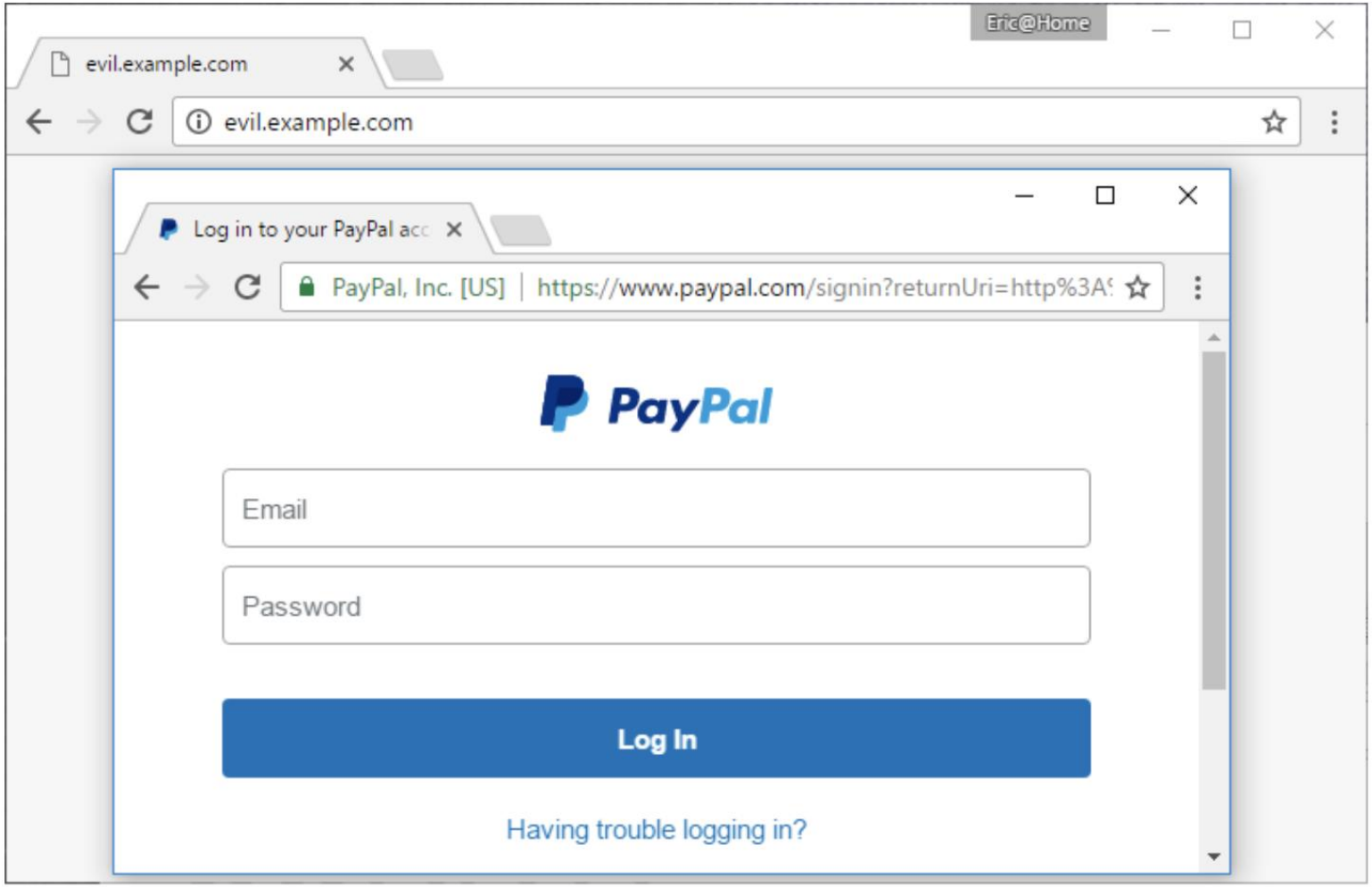


We recommend to always check whether the URL in your browser is correct.

資料來源：iThome

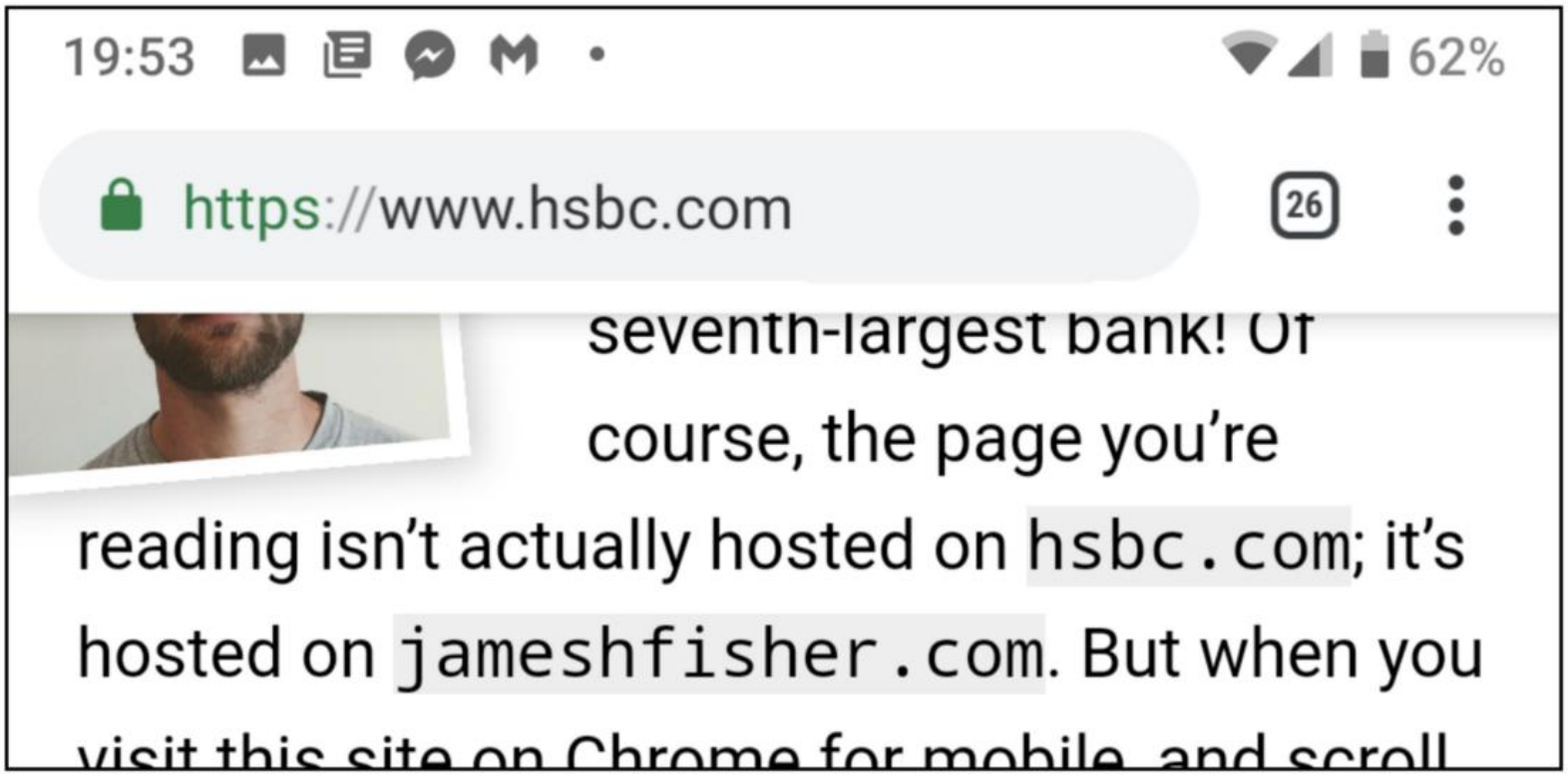
圖中圖

- Picture-In-Picture Attacks



假網址列

- 利用手機顯示網頁時，自動隱藏網址列



電話詐騙

- 「蘋果支援」客服電話藏詐騙　密碼、iCloud資訊全被盜

資料來源：ETtoday

傳訊 Apps 詐騙

- 好友傳來訊息（其實根本不是好友傳的。
- 手機裡資料或通訊錄可能被竊取濫用。
- 也會在不知不覺中透過電信商的「小額付費」功能把錢支付到詐騙集團口袋。

QR Code詐騙

- QR碼不能隨便掃！　陸媒曝網路詐騙新招

記者 黃星樺 / 攝影 高志宏 浙江 報導　2015/12/03 13:39

進階持續性滲透攻擊 (APT)

初步的入侵：利用一些釣魚網站或電子郵件來做為入侵的媒介。

建立立足點：植入惡意程式以掌握使用者系統。

取得管理者權限：利用破解密碼等方式取得該電腦管理者權限。

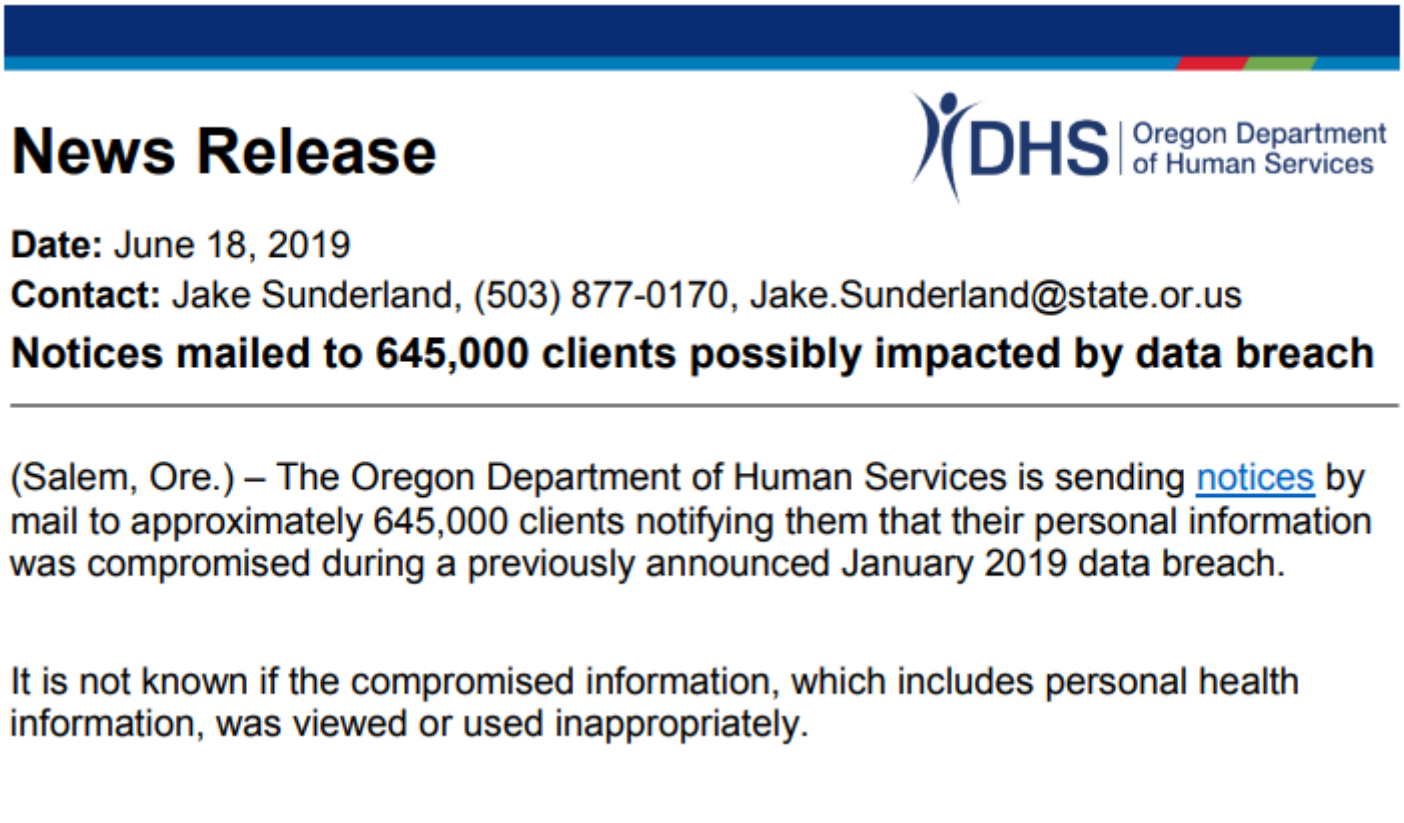
內部偵查與平行擴散：找尋該主機附近的其他主機或伺服器，並伺機取得其內部資料庫儲存之機密資料。

持續監控並完成任務：持續掌控資料庫伺服器或是主機，並將資料匯出達到竊取機密的目的。

社交工程可能為後續進階攻擊之源頭！

近期案例：資料外洩

- 美奧勒岡州健保署員工誤點網釣信件，害64萬人個資外洩



News Release

DHS | Oregon Department of Human Services

Date: June 18, 2019

Contact: Jake Sunderland, (503) 877-0170, Jake.Sunderland@state.or.us

Notices mailed to 645,000 clients possibly impacted by data breach

(Salem, Ore.) – The Oregon Department of Human Services is sending notices by mail to approximately 645,000 clients notifying them that their personal information was compromised during a previously announced January 2019 data breach.

It is not known if the compromised information, which includes personal health information, was viewed or used inappropriately.

資料來源： 2019-06-20 iThome

防範社交工程攻擊

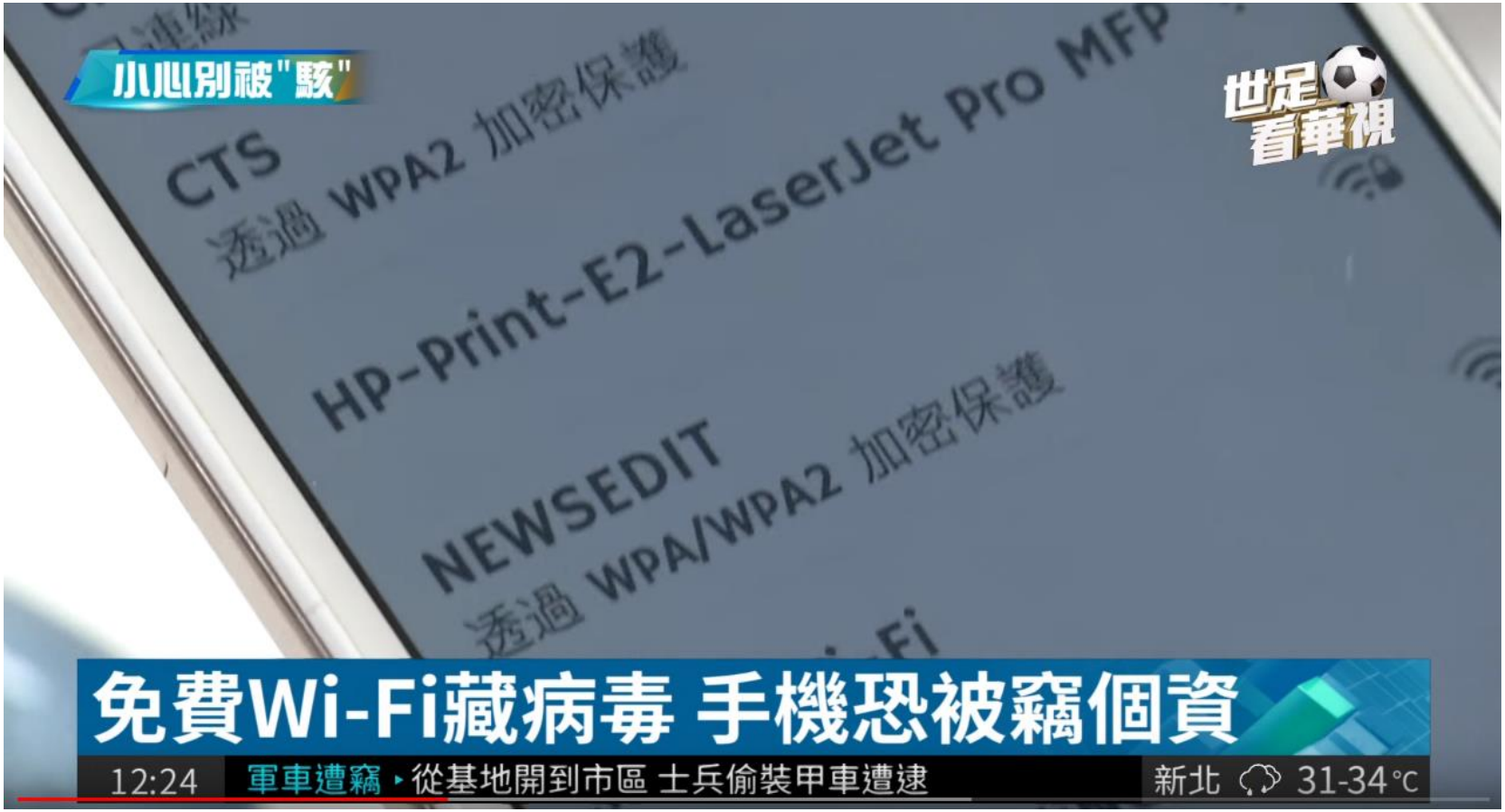
- **隨時提高警覺**
- 不未經確認即提供資料（公務及私人）
- 減少暴露之個人及公務資訊，避免成為攻擊目標
- 不開啟來路不明的電子郵件及附加檔
- 不連結及登入未經確認的網站
- 不下載非法軟體及檔案

資安及個資防護重點

免費Wifi的風險

資料來源：東森新聞 YouTube頻道

Wifi路由器暗藏少爺病毒

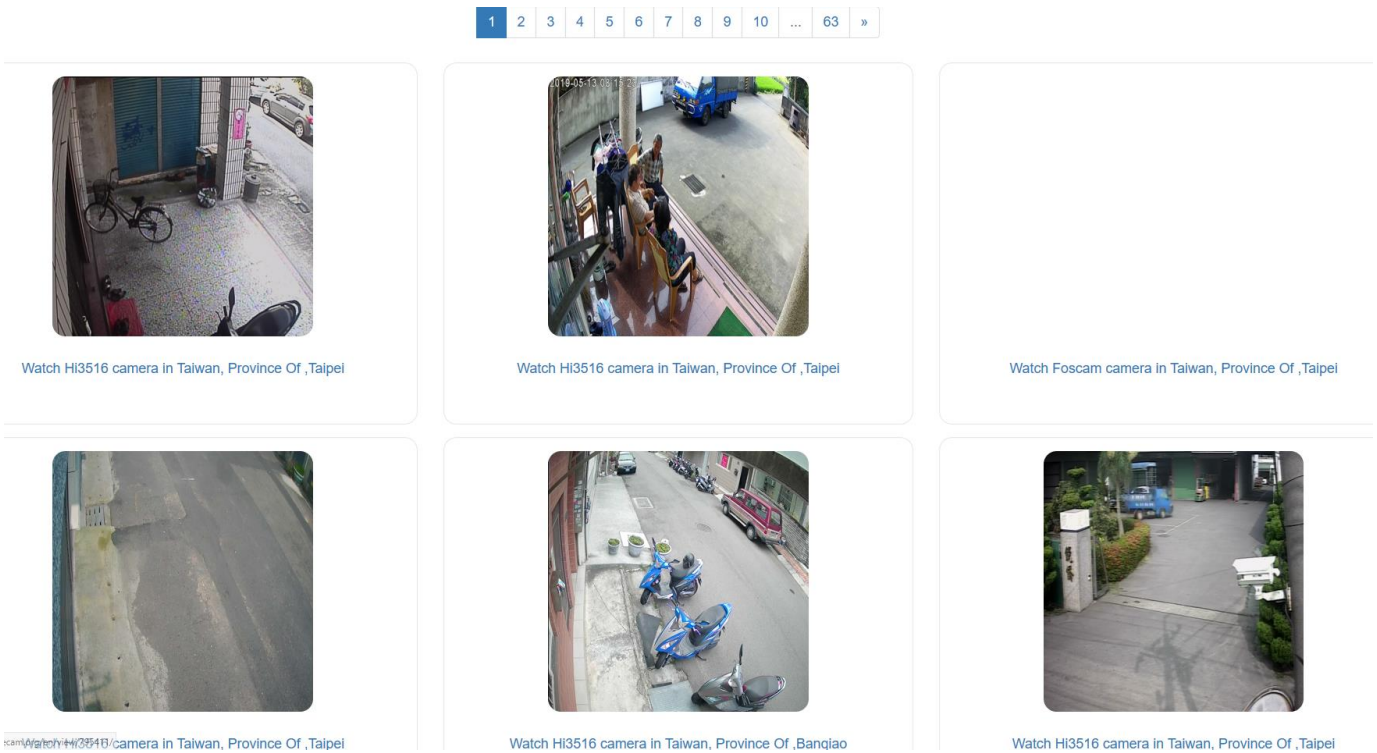


萬物聯網暗藏危機 萬物皆可駭

網路監視器遭駭 偷窺OL洗澡

物聯網安全 - 網路攝影機

- Insecam project
  http://www.insecam.org/en/



物聯網安全 - 搜尋引擎Shodan

- https://www.shodan.io/

物聯網危機

- 駭客只需要打開數萬台冷氣，就可以操控物聯網破壞區域電網

駭客只需要打開數萬台冷氣，就可以操控物聯網破壞區域電網

網易科技 發表於 2018年9月08日 08:30 | 收藏此文

讚 221

在上週三舉行的USENIX安全研討會上，來自普林斯頓大學電氣工程系的Saleh Soltan展示了一項令人憂心的研究成果：如果基於Wi-Fi的高功率設備變得越來越普遍，在達到一定的規模後，它們就可以被用來操縱一片相當大的區域內的電力需求。也就是說，它們可以導致局部停電甚至是區域電網的連鎖故障。

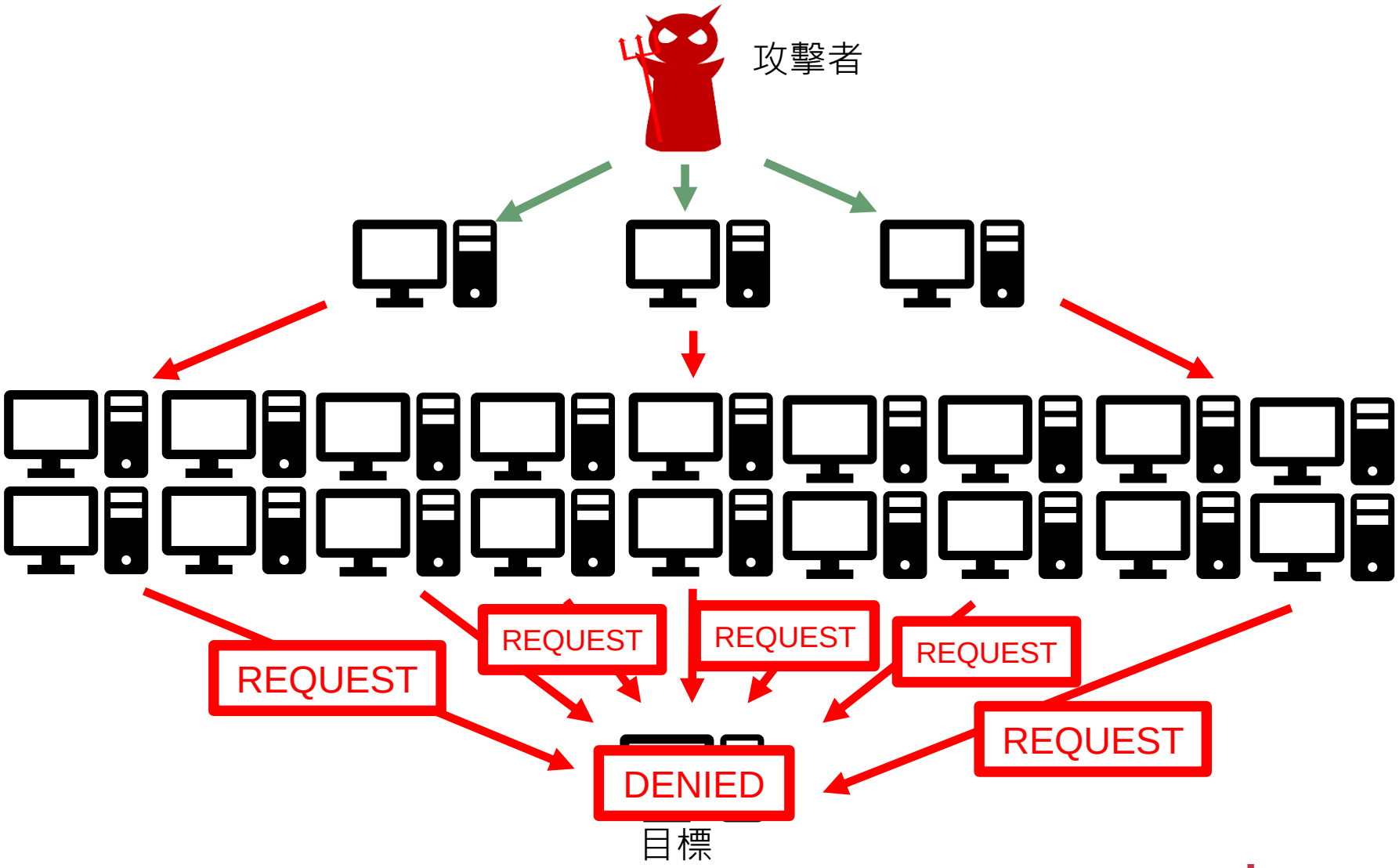
物聯網資安驗證標章

- 查詢通過驗證產品：NCC資通安全宣導網
  - (https://ise.ncc.gov.tw/)

物聯網安全 - 自我防範

- 確保物聯網裝置安全
  - 不使用不了解功能及風險之裝置
  - 更改預設帳號密碼
  - 加密傳輸資料
  - 做好系統防護和更新
  - 避免成為殭屍設備，保護自己也保護他人

分散式阻斷服務攻擊（DDoS）



通訊軟體遭攻擊

- 通訊軟體 Telegram 證實遭到中國大規模 DDoS 攻擊，起因於香港反送中抗議遊行

資料來源：2019/06/14 T客邦

中選會網站遭攻擊

- 投票日官網曾遭攻擊 中選會：未影響計票系統

資料來源：2018/11/28 中央社

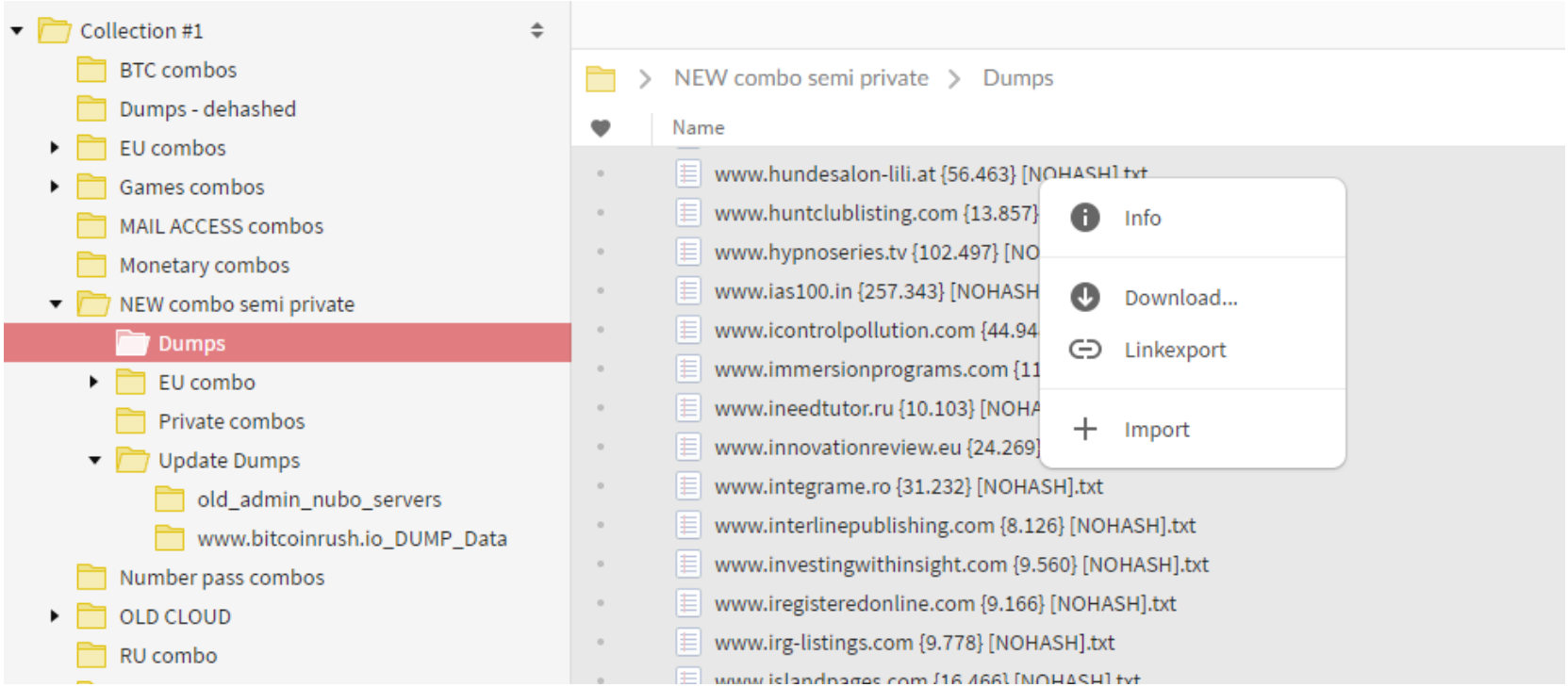
帳號填充攻擊

- 網站遭駭情勢日益惡化，助長利用外洩帳號密碼而成的自動化攻擊

資料來源：iThome

以公務郵件帳號申請外部服務

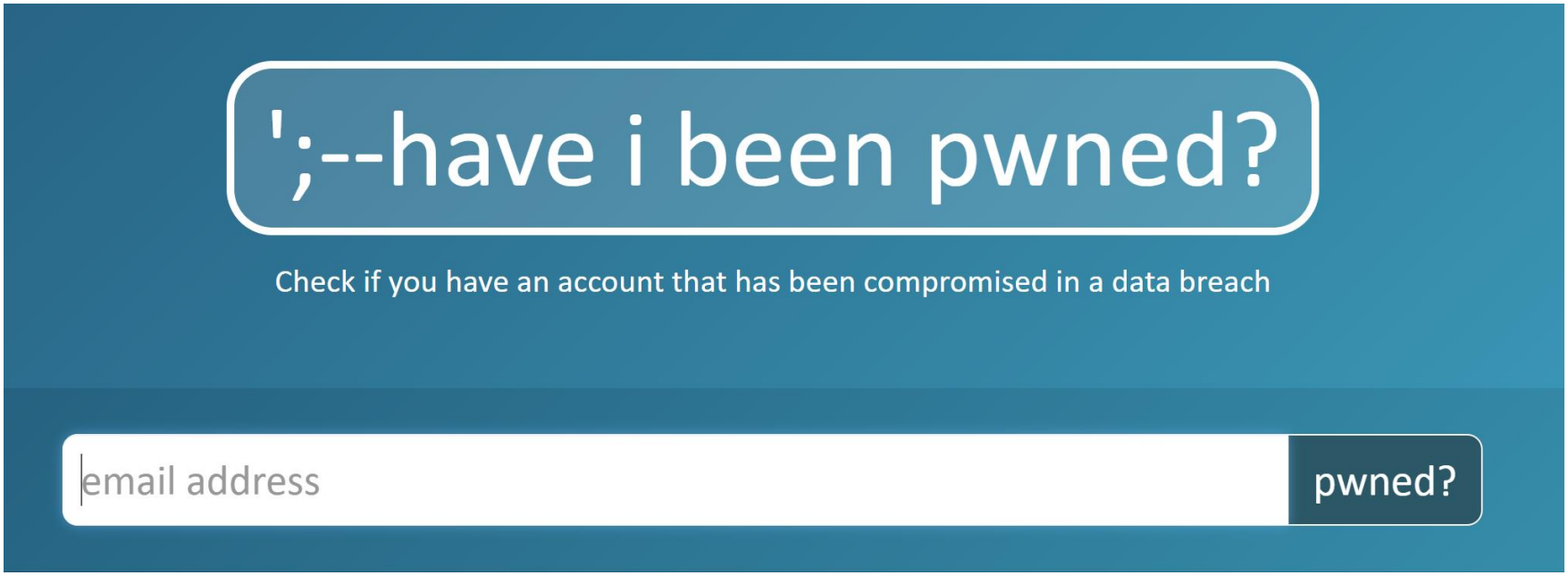
- 含有逾11億筆電子郵件+密碼的Collection #1資料庫現身駭客論壇



資料來源：2019-01-18 iThome

檢查帳號是否被駭

- Have I been pwned?



設定兩步驟驗證

- Google帳戶設定

設定兩步驟驗證

雙因子認證

Google：攻擊者繞過較弱兩步驟驗證

- 網路釣魚攻擊
- 接管電話號碼以攔截SMS一次性驗證碼

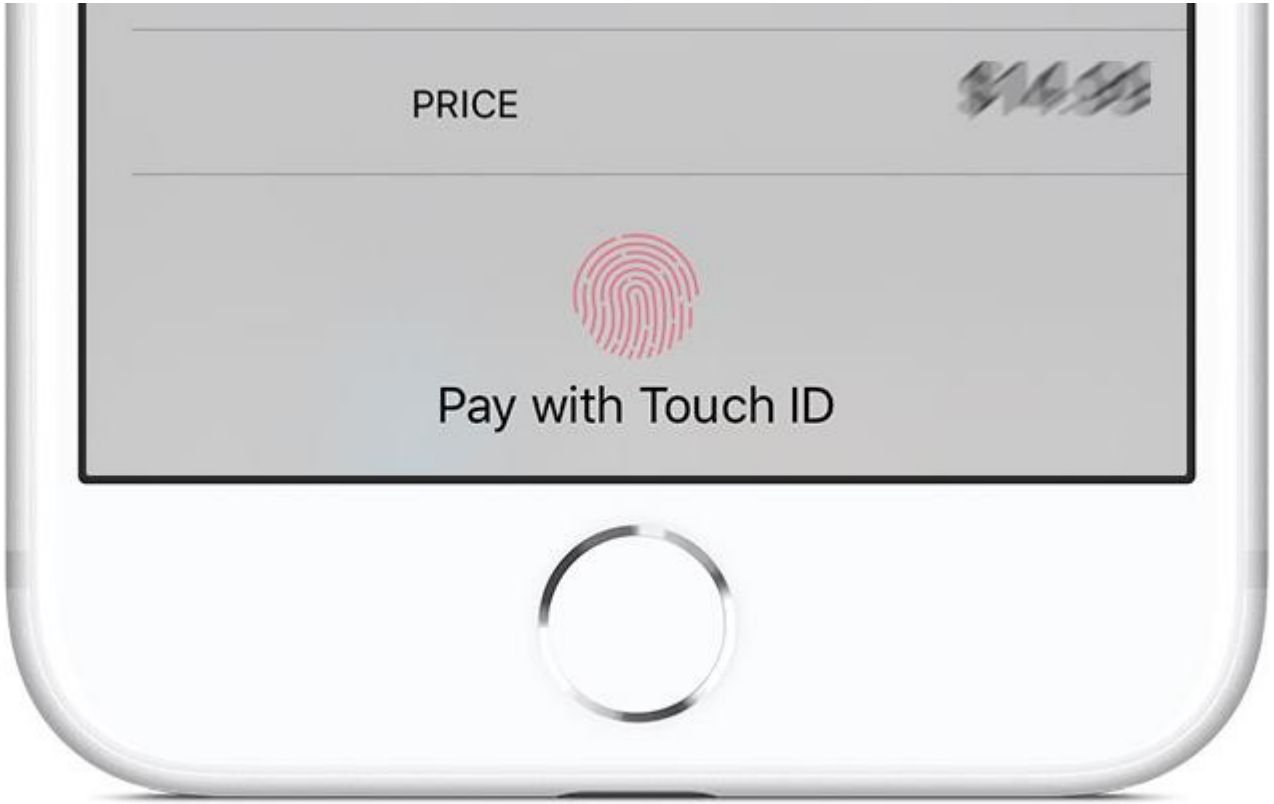
預測：

- 2019年，無密碼登入將會成為主流。

資料來源：iThome

Touch ID詐騙

- 詐騙iOS app死灰復燃，假量測心率真詐財



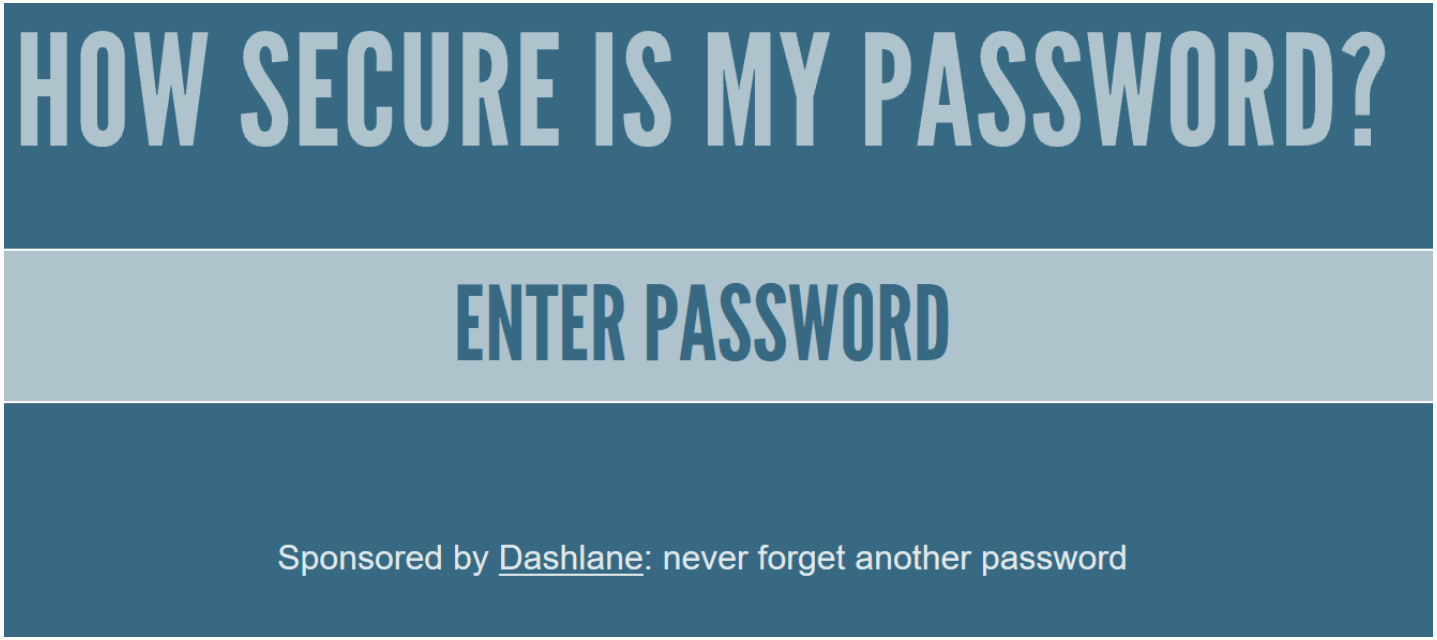
資料來源：2019-08-09 iThome

密碼強度很重要

- 德國20歲學生入侵近千名公眾人物帳號並公布他們的個資

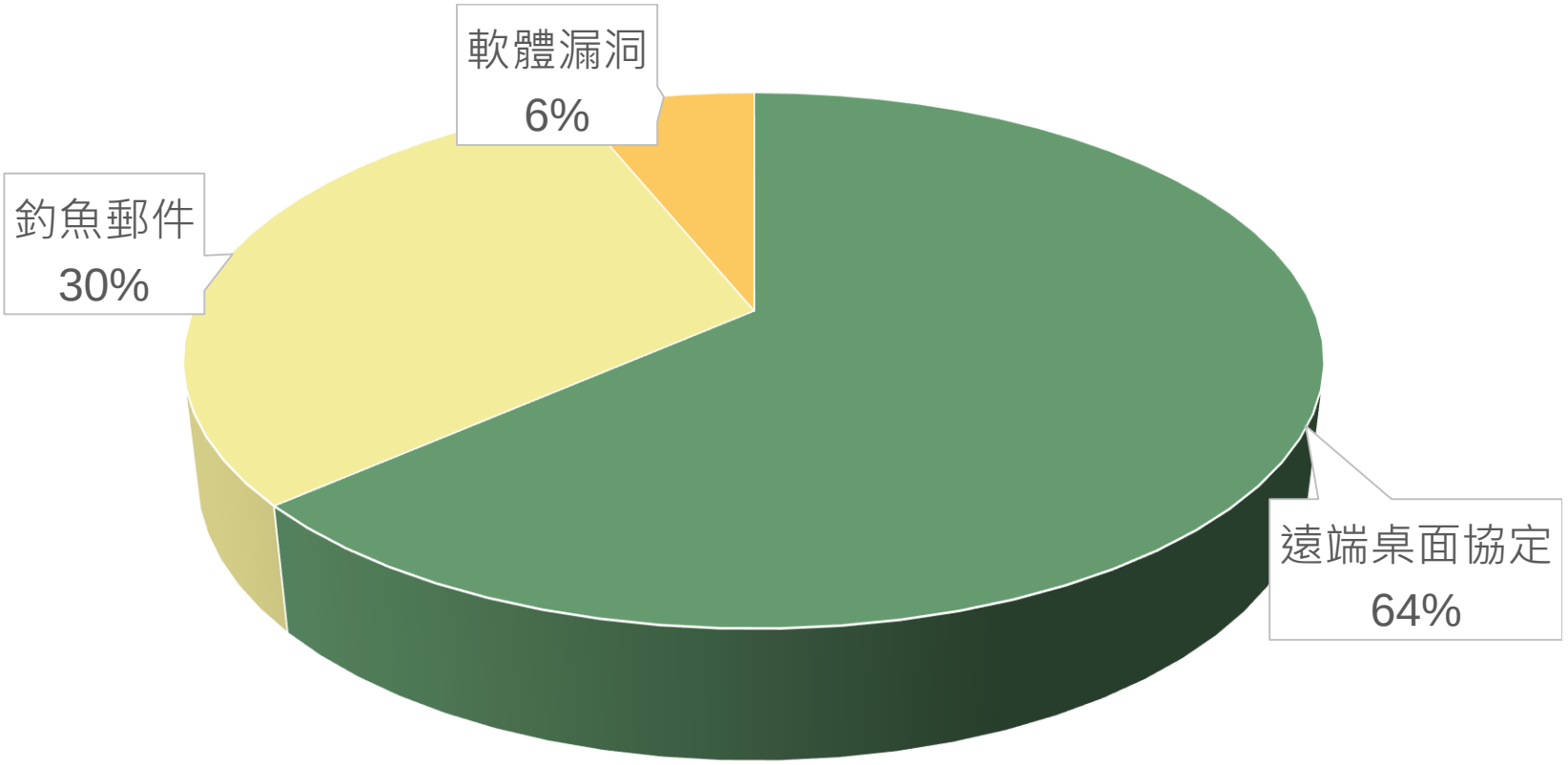
密碼小幫手

- 密碼短語
  - I LOVE TAIPEI→iLov3TaiP3i
- 檢查密碼強度
  - HOW SECURE IS MY PASSWORD?



勒索病毒

- **Coveware：RDP為勒索軟體入侵主要管道**



資料來源：iThome

勒索病毒感染

- 巴爾的摩市感染勒索軟體，沒付10萬美元贖金，後續重建成本將近2千萬美元

當地市政府除了找人來協助清除惡意程式或勒索軟體，也置換了軟硬體，這些清除重建工程加上其他無形損失，目前已花掉了1,800萬美元公帑

文/ 陳曉莉 | 2019-06-06 發表

讚 5.4 萬 按讚加入iThome粉絲團 讚 454 分享

Baltimore City Hall，Photo by Ashley Hughes on Google maps（shorturl.at/iMNV0）

勒索軟體攻擊

- 佛州Riviera Beach市遭勒索軟體攻擊，市議會表決同意支付60萬美元贖金

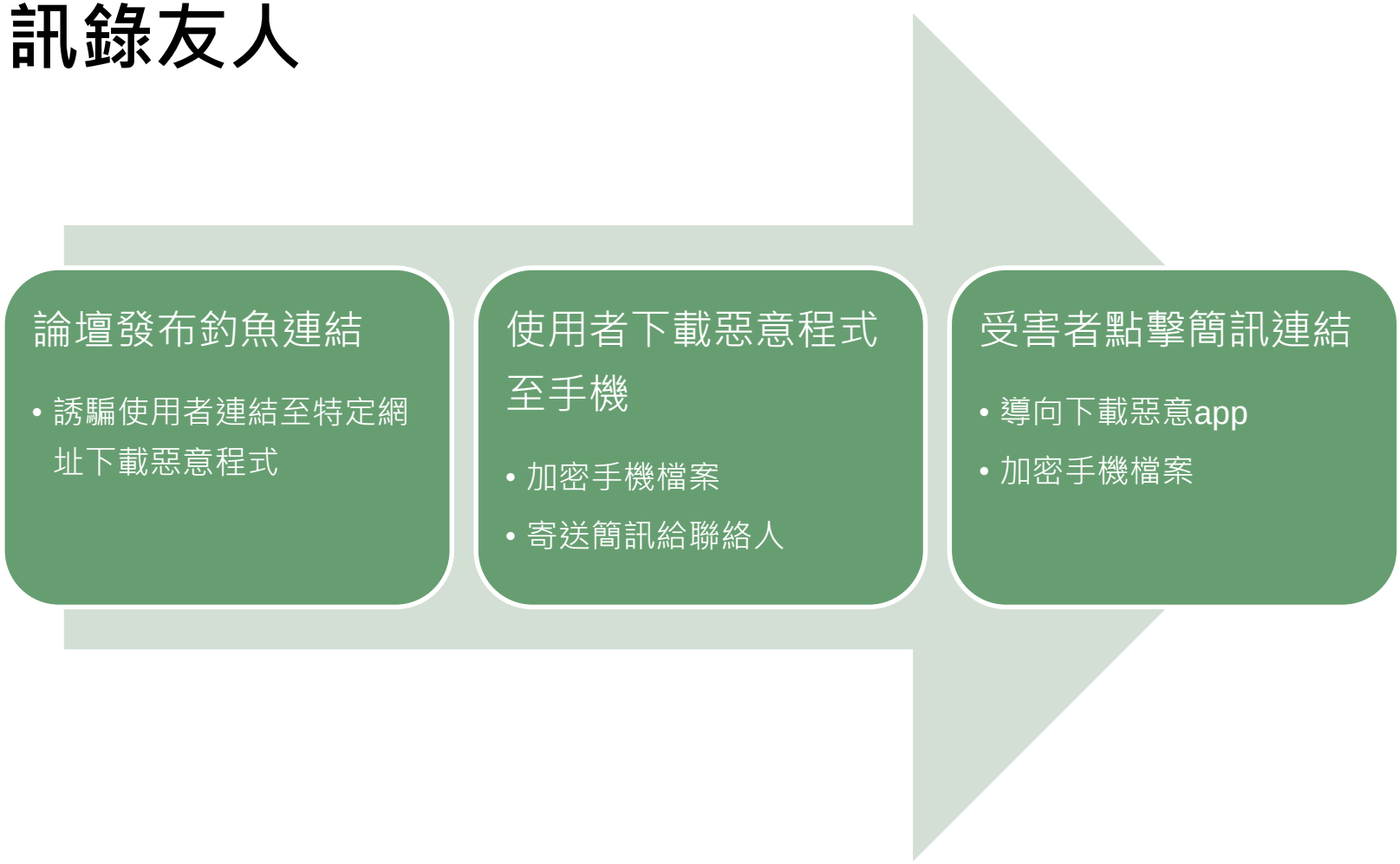
資料來源： 2019-06-24 iThome

病毒藏 USB 傳輸線一插電腦就中毒

- 改造 USB 傳輸線，一接上電腦就會自動輸入指令執行任務

手機簡訊傳播勒索軟體

- **新勒索軟體利用Android 手機簡訊傳給通訊錄友人**



勒索軟體 - 自我防範

- 勒索軟體防範安全建議：

定期備份重要文件

- 強烈建議備份兩份以上：一份保存在雲端（如Dropbox和Google Drive等雲端服務），另一份則採用物理方式保存（外接硬碟、備用筆記型電腦等）

定期檢查備份檔案

- 有時一次意外故障就可能會導致檔案損壞

不隨意點擊惡意連結

- 用戶應該對垃圾郵件防護設定進行調整，且千萬不要開啟來自未知寄件人發送的郵件附件

勒索軟體 - 自我防範

- 勒索軟體防範安全建議：

不要相信任何人

- 就算發送人是社群網站的朋友、工作同事或網路遊戲中的好友也不要輕易相信，因為很可能帳號已被網路犯罪份子盜用

使用強大的防毒程式保護

- 它能有效防止病毒侵入你的電腦；或病毒不幸潛入你的系統時，可利用其功能來保護重要檔案

定期升級作業系統、防毒軟體和應用程式

- 避免軟體中的弱點被網路犯罪份子利用而感染病毒。

勒索軟體 - 自我防範

- 勒索軟體防範安全建議：

發現異常程式，立即斷開網路

- 若最後檔案不幸被加密的話，依然還有機會可能恢復檔案

若不幸被加密，不支付贖金，除非這些檔案很重要

- 使用者一旦妥協支付贖金，網路騙子將會使用這些資金發動更大規模的網路攻擊，更加助長此類惡意行為

資料來源：http://www.jadespring.com.tw/internet-security-center/blog/blog-malware-20171211.html

勒索軟體 - 備份三二一

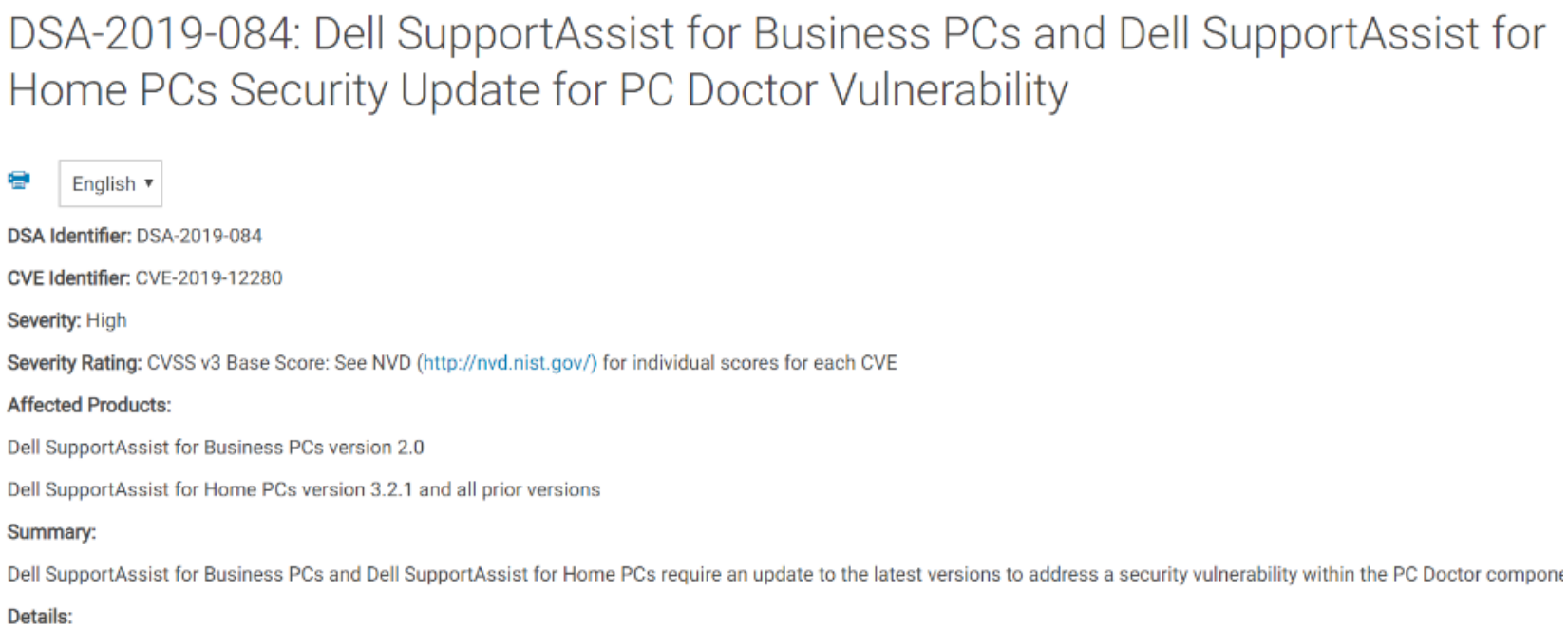
- 三份備份檔案
- 兩種不同的儲存媒體
  - 行動硬碟
  - USB
  - 雲端
- 一份放在異地

華碩雲端服務更新遭駭客入侵

- 臺灣資安業者揭露：5個A級政府機關及地方政府於4月被植入Plead惡意程式

Dell電腦預裝軟體安全漏洞

- Dell電腦預裝軟體SupportAssist含有可被接管的安全漏洞



DSA-2019-084: Dell SupportAssist for Business PCs and Dell SupportAssist for Home PCs Security Update for PC Doctor Vulnerability

English

DSA Identifier: DSA-2019-084

CVE Identifier: CVE-2019-12280

Severity: High

Severity Rating: CVSS v3 Base Score: See NVD (http://nvd.nist.gov/) for individual scores for each CVE

Affected Products:

Dell SupportAssist for Business PCs version 2.0

Dell SupportAssist for Home PCs version 3.2.1 and all prior versions

Summary:

Dell SupportAssist for Business PCs and Dell SupportAssist for Home PCs require an update to the latest versions to address a security vulnerability within the PC Doctor compone

Details:

資料來源： 2019-06-25 iThome

資訊安全自保之道

落實防範

- 安裝防毒軟體、確實更新
- 加強帳號密碼管理

提高警覺

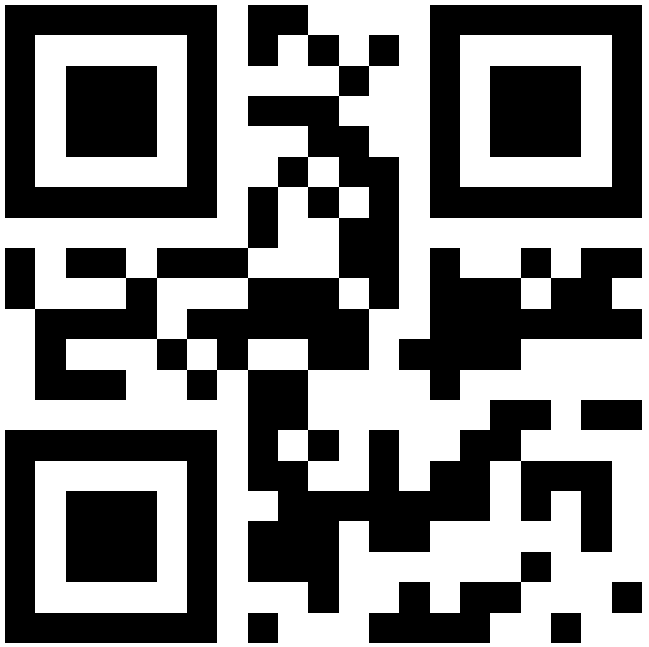
- 留意異常狀態、不輕信他人、謹言慎行

備援策略

- 做最壞的打算、最好的準備
- 備份三二一

課後回饋

立即掃描
參加活動抽免費電影票！



掃QR Code
免費獲得更多資安新知！

Q&A

TSC CAPITAL GROUP

The Bridge to the Asia Pacific Region

感謝您的參與

歡迎於活動後與講師討論您的任何疑問

本公司的臉書粉絲團及部落格可以找到更多資訊

TSC – FB Site

TSC – Blog Site