TSC CAPITAL GROUP
The Bridge to the Asia Pacific Region

新竹縣教育研究發展暨網路中心
HCC EDU.Development and Information Institute

課程名稱：資通安全通識教育訓練

113年度資訊安全管理制度（ISMS）維運暨驗證服務案

授課日期：114年5月7日
授課講師：德欣寰宇科技股份有限公司 資安顧問 張寬增

簡報大綱

一	資安與個資之政策及法規宣導
二	社交工程防護
三	資訊安全概念、資安趨勢與案例分析
四	個人應注意之資安防護事項

資安與個資之政策及法規宣導

資通安全政策-全球資訊網

資訊安全政策，網址為:
https://www.hcc.edu.tw/var/file/1/1001/img/1903/171050569.pdf

本中心資通安全政策:宣導

- 為使本中心業務順利運作，防止資訊或資通系統受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，並確保其機密性（Confidentiality）、完整性（Integrity）及可用性（Availability），特制訂本政策如下，以供全體同仁共同遵循：

一、 確保個人隱私資料之機密性，防止非法使用。

二、 確保資通系統之完整性，防止人為意圖不法使用、竄改資料。

三、 確保資通系統之可用性，維持資通系統持續運作。

四、 符合國家法律、法令及法規之要求。

HCC-ISMS-01-001資通安全政策_V1.1-20250225　　資安宣導，以e-mail及內部公告等訊息，向同仁發布。

隱私權政策

➢ 隱私權政策網址為: https://www.hcc.edu.tw/p/412-1001-5674.php

首頁 / 隱私權政策

隱私權政策

隱私權政策 104.08.21

■隱私權保護政策

非常歡迎您光臨新竹縣教育研究發展暨網路中心網站(以下簡稱本網站)，本網站非常重視您個人的隱私權，因此制定了隱私權保護政策。為了幫 助您瞭解本網站如何收集、應用及保護您的個人資訊，請詳細閱讀本網站隱私 權保護政策(以下簡稱本政策)。本政策將幫助您了解，在您使用本網站所提供 的服務時，我們收集、運用及保護您個人資料的政策與原則。

個資宣導:教育部函

教育部 函

地址：10051 臺北市中山南路5號
承辦人：林文信
電話：02-7712-9092
電子信箱：ansel@mail.moe.gov.tw

受文者：教育部國民及學前教育署

發文日期：中華民國110年9月8日
發文字號：臺教資(四)字第1100122001號
速別：普通件
密等及解密條件或保密期限：
附件：學校使用資通系統或服務蒐集及使用個人資料注意事項 （附件一）

主旨： 檢送各級學校使用資通系統或服務蒐集及使用個人資料之注意事項(如附件)，請查照並轉知所屬。

說明：

一、鑒於學校使用雲端資通服務(如Google表單等)蒐集個人資料時，可能因設定不當而增加個資外洩及資安風險，請各校使用資通系統或雲端資通服務蒐集教職員、學生及家長個人資料者，應注意旨揭事項，以「最小化」為原則，降低風險，並請各校主管機關加強宣導並督導所轄學校。

另提醒教職員工在處理個人資料時，應注意以下法規：

(一)個人資料保護法第28條第1項「公務機關違反個人資料保護法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。」

(二)個人資料保護法第41條第1項「違反個人資料保護法有關特種資料的蒐集、處理或利用規定，足生損害於他人者，處二年以下有期徒刑、拘役或科或併科新臺幣二十萬元以下罰金。」

正本：各公私立大專校院、教育部國民及學前教育署、各直轄市及縣市政府教育局(處)

個資法的修訂大幅提高罰款:112年5月31

Before　　2023/05/31　　After

- 非公務機關若未採行適當安全措施來防止個資被竊、竄改、….，限期改正，屆期未改正者，按次處新台幣**2萬元以上20萬元以下罰鍰**。

《個人資料保護法》部分條文修正案三讀通過

- **主管機關為「個人資料保護委員會」**
- 修正個資法第48條，非公務機關若未採行適當安全措施來防止個資被竊、竄改….，情節重大者，處**15萬元以上1,500萬元以下罰鍰**；屆期未改正者，按次處15萬元以上1,500萬元以下罰鍰。

第 41 條

意圖為自己或第三人不法之利益或損害他人之利益，而違反第六條第一項、第十五條、第十六條、第十九條、第二十條第一項規定，或中央目的事業主管機關依第二十一條限制國際傳輸之命令或處分，足生損害於他人者，處五年以下有期徒刑，得併科新臺幣一百萬元以下罰金。

第 42 條

意圖為自己或第三人不法之利益或損害他人之利益，而對於個人資料檔案為非法變更、刪除或以其他非法方法，致妨害個人資料檔案之正確而足生損害於他人者，處五年以下有期徒刑、拘役或科或併科新臺幣一百萬元以下罰金。

個人資料保護法架構

- §1，為規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用，特制定本法。

第一章 總則(§1~§14)

第二章
公務機關對個人資料之蒐集、處理及利用
(§15~§18)

第三章
非公務機關對個人資料之蒐集、處理及利用
(§19~§27)

第四章
損害賠償及團體訴訟
(§28~§40)

第五章
罰則
(§41~§50)

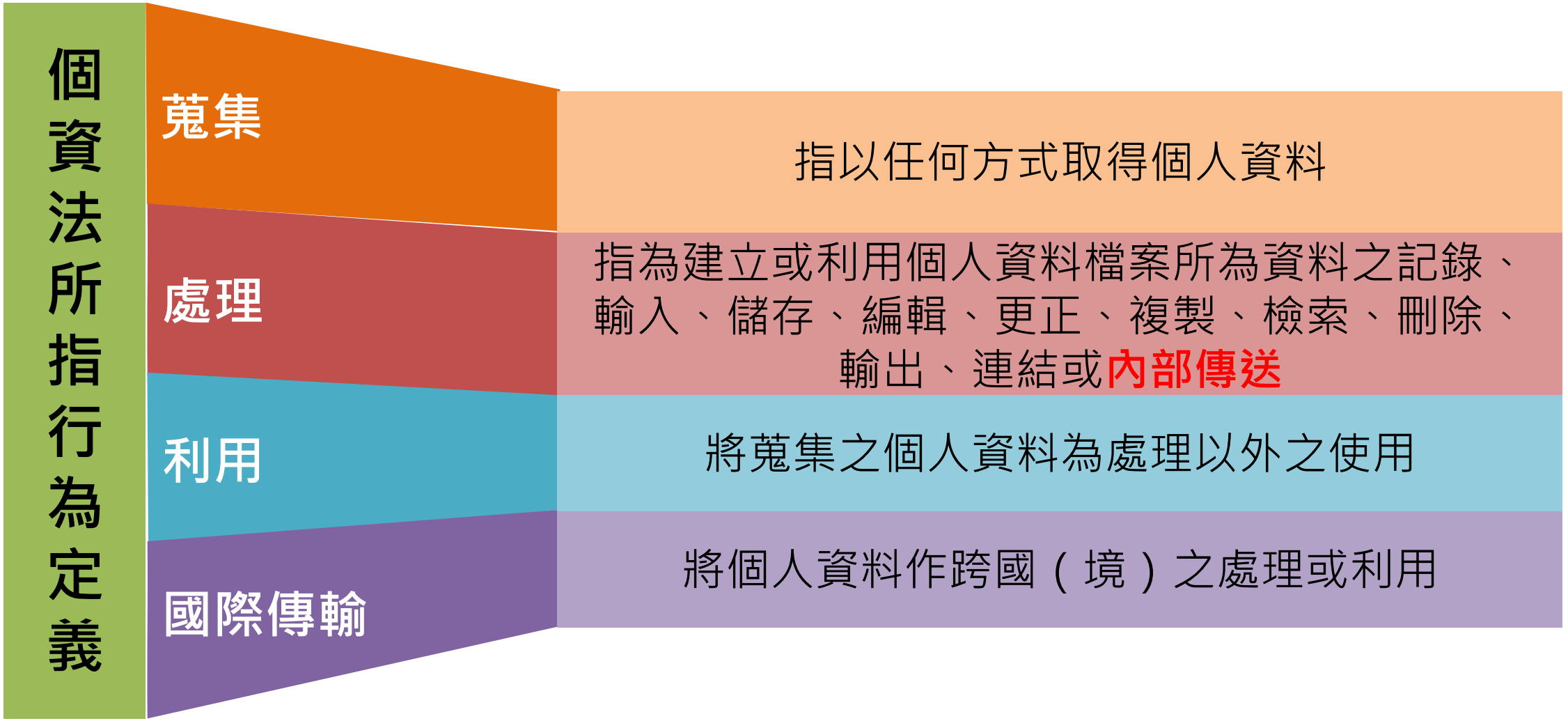
第六章
附則
(§51~§56)

個人資料保護法 - §2 個資定義

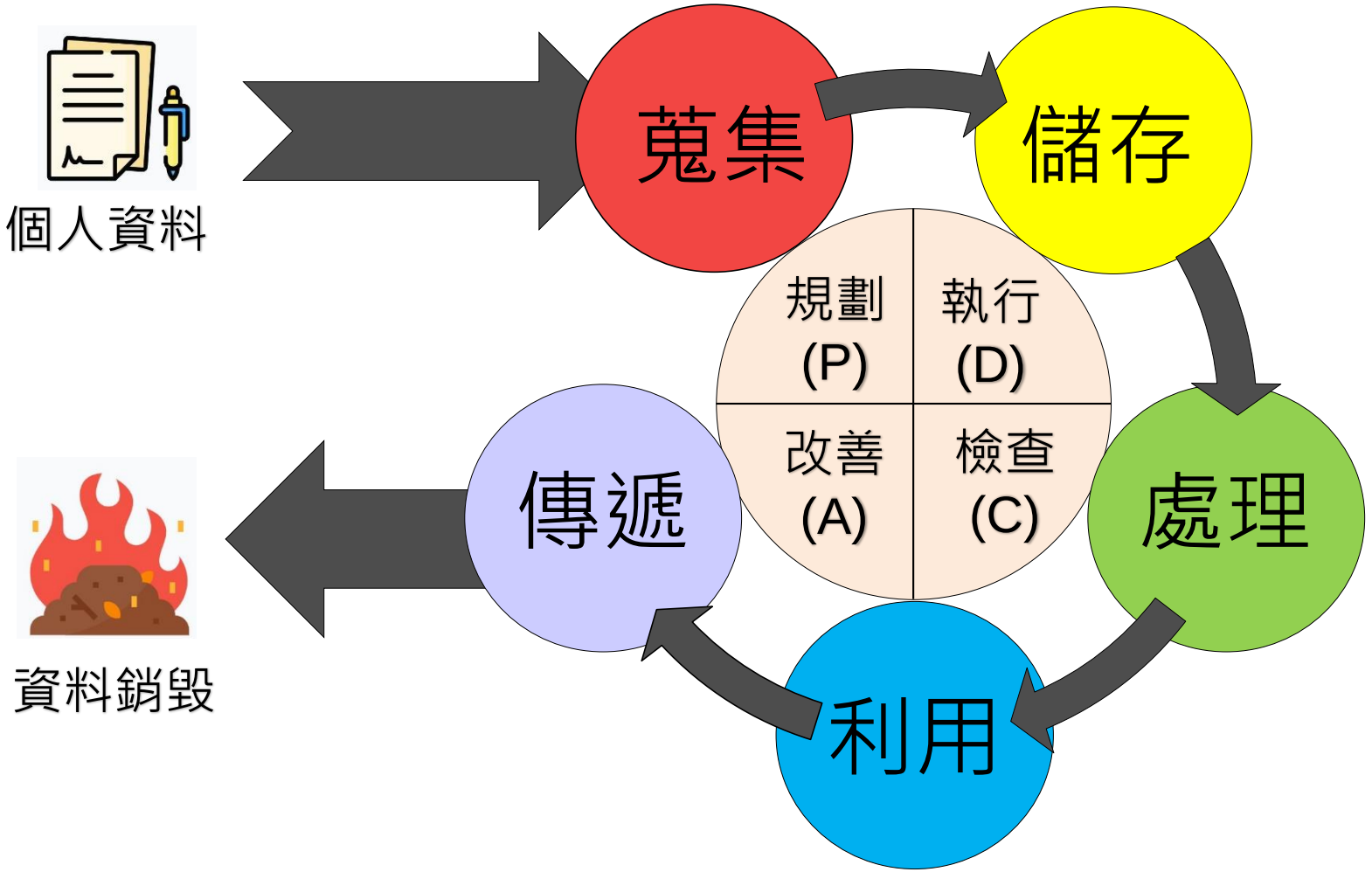
一般個資	特種個資
自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、聯絡 方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。	病歷、醫療、基因、性生活、健康檢查、犯罪前科

個人資料保護法 第6條
特種個資不得隨意蒐集處理利用，但有下列情形之一者，不在此限
1.法律明文規定。
2.執行法定職務或履行法定義務所必要，且事前或事後有適當安全維護措施。
3.當事人自行公開或其他已合法公開的個人資料。
4.公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。
5.經當事人書面同意。但逾越特定目的之必要範圍或其他法律另有限制不得僅依當事人書面同意蒐集、處理或利用，或其同意違反其意願者，不在此限。

個人資料保護法 - §2 個資法所指行為定義



個人資料之生命週期



個人資料保護法 - §3 當事人對自身個資之權利

§3，當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之：

一. 查詢或請求閱覽。
二. 請求製給複製本。
三. 請求補充或更正。
四. 請求停止蒐集、處理或利用。
五. 請求刪除。

§10

可拒絕當事人行使權利情形

一、妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益。
二、妨害公務機關執行法定職務。
三、妨害該蒐集機關或第三人之重大利益。

案例分享-新進人員夾檔錯誤導致個資外洩

中正大學傳出個資洩漏，通識中心要寄送學習講座的通知，卻不慎夾帶了學校5個學年的學生個資，包括身分證字號、電子郵件等基本個人資料，發給收信的200多名學生。

資料來源：https://news.ltn.com.tw/news/life/breakingnews/3320202

案例分享-校園案例

- 網站涉洩漏學師生個人資料

  事件由來：

  中部某所知名大學網站因控管不當，透過 Yahoo 、 Google 等搜尋引擎，便可直接取得該校就學貸款學生名冊，名冊內含學生身份證字號、貸款金額等個人資料，讓學生資料暴露於危險之中。

資料來源- https://iscb.nchu.edu.tw/2019/07/blog-post_95.html
教育部資訊及科技教育司

案例分享-校園案例

- 網站涉預防或解決方式：
  - ✓如果您必須要離開公用電腦一段時間，登出所有的程式並關閉所有可能含有機密資訊的視窗。
  - ✓網站應指派專人管理審核內容，以避免洩漏學生、教師個人資料。
  - ✓不適合公開的檔案不可存放在公開之網站上。
  - ✓網站上過期的資料應進行檔案刪除、不可只移除超連結，以免被搜尋引擎取得而被讀取。

對資通安全管理系統之優點、貢獻

- 對資通安全管理系統之有效性其貢獻及改善資訊安全的績效益處如下:

1.確保人員在適當的教育訓練或取得經驗後是能勝任其工作。

2.提高資通安全績效的收益可以降低不符合 ISMS 要求時所帶來的影響與衝擊。

例如:特定敏感性資料被竊取

更重要的主機被攻擊

組織聲譽及金錢損失

違反資通安全管理系統之後果

- 依據「公務機關所屬人員資通安全事項獎懲辦法」，當人員違反資通安全管理系統之後果如下:

  有下列情形之一者，予以懲處：

一、未依本法、本法授權訂定之法規或機關內部規範辦理下列事項，情節重大：

（一）資通安全情資分享作業。

（二）訂定、修正及實施資通安全維護計畫。

（三）提出資通安全維護計畫實施情形。

違反資通安全管理系統之後果

（四）辦理資通安全維護計畫實施情形之稽核。
（五）配合上級或監督機關資通安全維護計畫實施情形稽核結果，提出改善報告。
（六）訂定資通安全事件通報及應變機制。
（七）資通安全事件之通報或應變作業。
（八）提出資通安全事件調查、處理及改善報告。

二、辦理資通安全業務經主管機關、上級或監督機關評定績效不良，經疏導無效，情節重大。

三、其他違反本法、本法授權訂定之法規或機關內部規範之行為，情節重大。

社交工程防護

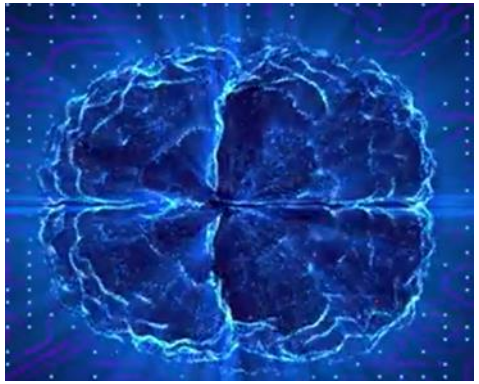
缺乏資訊安全意識

- 缺乏資訊安全意識可能造成的傷害:

一般使用者	單位組織
✓個人隱私的洩漏 ✓重要資料被加密勒索 ✓個人帳號權限被盜用	✓特定敏感性資料被竊取 ✓更重要的主機被攻擊 ✓組織聲譽及金錢損失

資安事件回顧:員工使用 ChatGPT，3 起機密資訊外洩

- 三星半導體員工提交專有程式原始程式碼給 ChatGPT，以修復錯誤。
- 某員工用 ChatGPT 輸入辨識缺陷晶片的測試模式，並要求改善。
- 使用應用程式將會議紀錄轉成檔案，再交給 ChatGPT 產生文件。



https://technews.tw/2023/04/06/samsung-fab-workers-leak-confidential-data-chatgpt/

行政院要求公務機關全面禁用DeepSeek AI服務

- DeepSeek AI服務的資料來源取得有違反著作權法相關法規的疑慮，並且其在模型訓練上也有思考審查、限制資料的問題。
- 此外，使用其服務可能使資料傳送至中國，在尚未釐清及排除疑慮之下，可能違反個資保護、侵害隱私，基於國家資通安全考量下，數位部已警示公務機關及關鍵基礎設施限制使用DeepSeek AI產品。
- 行政院重申在2019年公布「各機關對危害國家資通安全產品限制使用原則」，要求中央及地方機關（構）、公立學校、公營事業、行政法人，以及自行或委外營運提供公眾活動或使用場地，限制使用危害國家資通安全產品。因此，要求公務機關原則全面禁用Deepseek AI服務。

國家資通安全研究院
https://www.nics.nat.gov.tw/latest_news/announcements/Latest_Announcement/6924d1a7-9f1a-4097-9d61-dec9b25a5724/

資料來源:https://www.ithome.com.tw/news/1671842025-02-03

AI普遍使用，員工如何因應

近期資安事件:勒索軟體駭客組織CrazyHunter攻擊馬偕和彰基

衛生福利部
Ministry of Health and Welfare
促進全民健康與福祉

回首頁 | RSS | 雙語詞彙 | 部長信箱 | 網站導覽 En Aa

本部簡介 最新消息 便民服務 法令規章 衛教視窗 重大事件 本部各單位及所屬機關

最新消息
焦點新聞
真相說明
公告訊息
活動訊息
招標資訊
就業資訊

首頁 > 最新消息 > 焦點新聞

彰化基督教醫院遭勒索攻擊，衛福部迅速啟動全國資安應變機制

繼馬偕醫院後，彰化基督教醫院也遭受勒索軟體攻擊。最新的驗證報告顯示，攻擊軟體為「瘋狂獵人」（Crazy Hunter）。為了協助彰基應對危機，衛生福利部立即協調資安署資安專家南下，進駐醫院，協助隔離受感染的系統並進行病毒清除，落實相關防護措施。目前核心系統已全面恢復，僅部分非核心的二級系統仍在修復中。

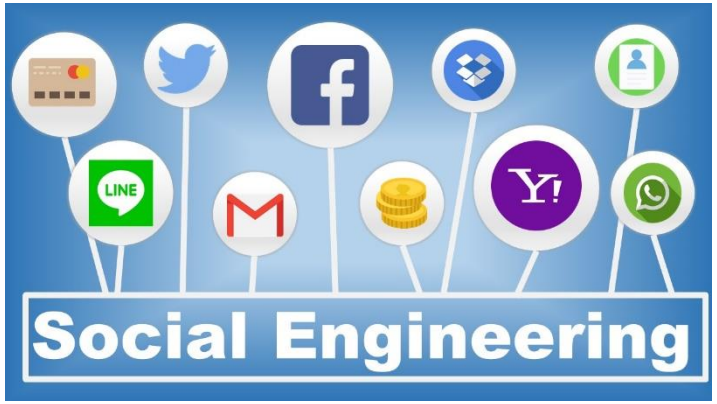
鑑於連續兩家醫院遭受攻擊，衛福部資訊處已將此事件定義為「系統性攻擊」，不排除其他醫院可能成為下一個目標。為此，資訊處今日迅速召集關鍵基礎醫院舉行緊急會議，由受攻擊的兩家醫院分享勒索軟體的清除與防禦經驗。會議中，來自馬偕醫院和彰化基督教醫院的資安團隊，以

近期資安事件:中壢長慎醫院遭駭客組織NightSpire攻擊

- 駭客組織聲稱竊得大量病歷資料，由於長慎醫院是老年專科醫院，專門照顧洗腎、糖尿病等慢性病患者，一旦資料外流，不光是病人隱私曝光，還有可能影響連續就醫的記錄，干擾醫生的診斷。
- 資安業者揭露他們的調查結果，駭客聲稱握有13萬張含有病徵及個資的醫療影像、10萬份電子病歷文件，以及數百萬筆實驗室、X光、CT、MRI的記錄。而對於駭客入侵的手法，竣盟科技認為很有可能透過釣魚郵件、社交工程，也不排除是利用尚未修補的已知漏洞得逞。

資料來源: https://www.ithome.com.tw/news/168545-20250420

何謂社交工程

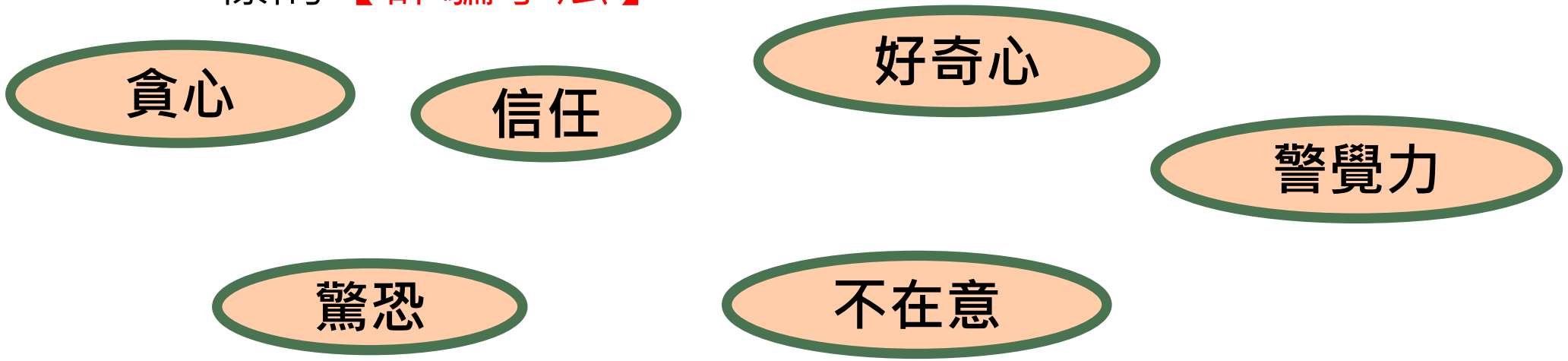


- 社交工程兩個基本要件：
  - 第一個是【人】
  - 第二個是【詐騙手法】
- 凡對【人】甚至於【特定對象】，使用各種【詐騙手法】，獲得不當資訊，來達到施騙者的目的，都可稱之為【社交工程】。

圖片來源：https://cms.aaasec.com.tw/index.php/2018/06/13/0005/

電子郵件社交工程

- 電子郵件**社交工程(Social Engineering)**:
  - ✓利用電子郵件夾帶病毒、木馬惡意程式或惡意的超連結，以誘人的信件標題使收信者點擊，進而入侵收信者電腦、或盜取使用者資料的手法
  - ✓駭客利用漏洞百出的【人性】，來設計各式各樣的【詐騙手法】

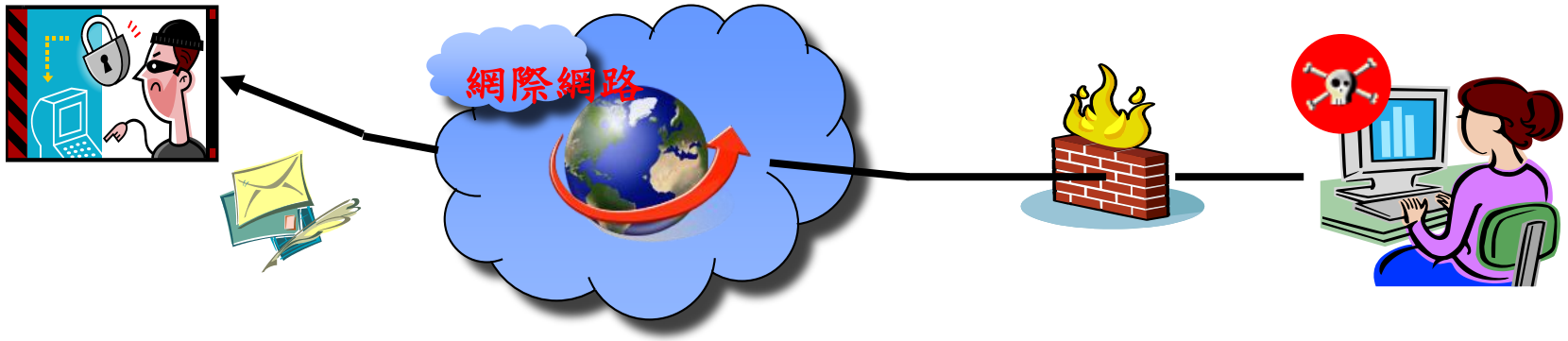


電子郵件社交工程

- **電子郵件社交工程的攻擊手法：**
  - ✓假冒寄件者
  - ✓使用與業務相關或令人感興趣的主旨與內容
  - ✓含有惡意程式的附件或連結(工具、檔案、圖片)
  - ✓利用應用程式之弱點 (包含零時差攻擊)
  - ✓網路釣魚
  - ✓假冒管理者誘騙使用者回覆帳號密碼資訊

電子郵件社交工程

- 電子郵件社交工程攻擊模式:

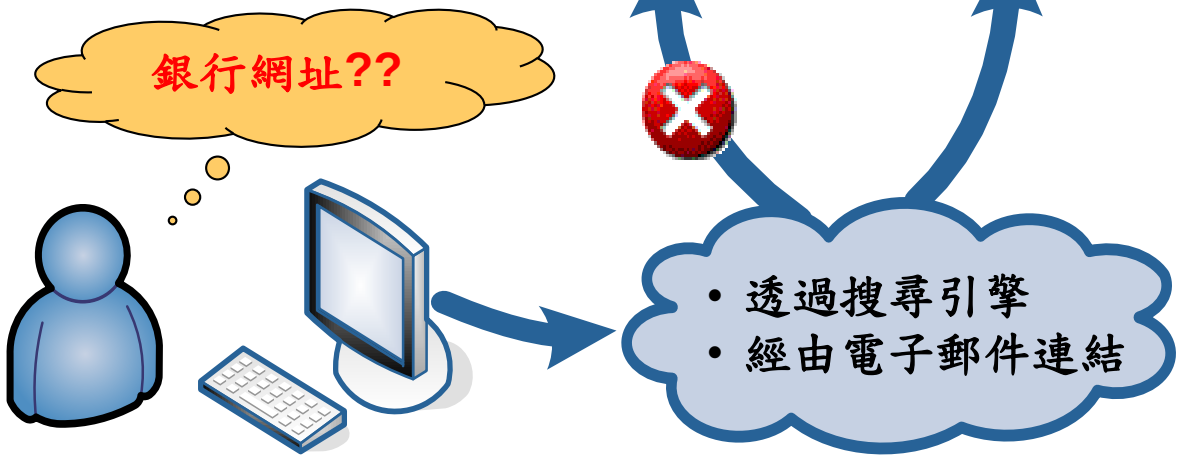


1. 駭客設計攻擊陷阱程式(如特殊Word檔案或惡意連結)
2. 將攻擊程式置入電子郵件中
3. 寄發電子郵件給特定的目標
4. 受害者開啟電子郵件
5. 啟動駭客設計的陷阱，將被植入後門程式
6. 後門程式逆向連接，向遠端駭客報到

電子郵件社交工程

http://www.landbank.com.tw

http://www.1andbank.com.tw 釣魚網頁



例如：

Yahoo奇摩

www.yhaoo.com.tw

臉書

https://faceb00k.com

Google

https://www.g00g1e.com

突然跳出的廣告頁面


www6.imaginativehitech.xyz
忠誠計劃
恭喜Google用戶，您有機會贏得一個Google禮物。
通通都是詐騙！
不要掉入陷阱！
每個 星期一，
挑選10位幸運用戶，送出贊助商提供的獎品。
感謝您對我們的產品和服務的一貫支援。
您可以選擇iP
Air 2 或 Samsung Galaxy S6.
若要獲得中獎機會，您只需要回答以下三個問題。
恭喜，Mob
您是被選中
人之一！你
禮物！
點擊“確定”

電子郵件社交工程常見類型

郵件主旨	郵件寄件者
水電費扣款存款不足，請收到通知7日內補足款項	bank_noties@uniprotect.org.tw
轉知國民旅遊卡相關事項 1100426公告	firstravel@itapei.net.tw
信用卡刷卡異常緊急通知	system_remind@g00g1e.com.tw

✓ 使用讓人感興趣(或恐懼)的主旨與內文

✓ 假冒寄件者

➢ 利用平常工作的業務性質使人不多聯想就點擊

下載假冒LINE電腦版應用程式竟導致個資外洩？

- 近日發現有駭客集團將木馬程式假冒LINE電腦版應用程式展開攻擊。當民眾透過Google搜尋「電腦版Line」等關鍵字，可能會出現假的下載網址，若不慎誤信安裝，電腦就有可能遭植入惡意木馬程式，導致個資外洩或裝置被控制。
- 趨勢科技提出三點建議呼籲：再三留意網址正確性、善用資安工具阻擋查證、確保病毒碼更新，方能即時避免裝置遭受惡意連結或惡意程式侵害。
- 仿造的假網址，例如：「www[.]linec-tw[.]000」，或是「line-chinese[.]000」，「line-tw[.]000」，「windows-line[.]000」等

資料來源https://www.ithome.com.tw/pr/168370 20250413

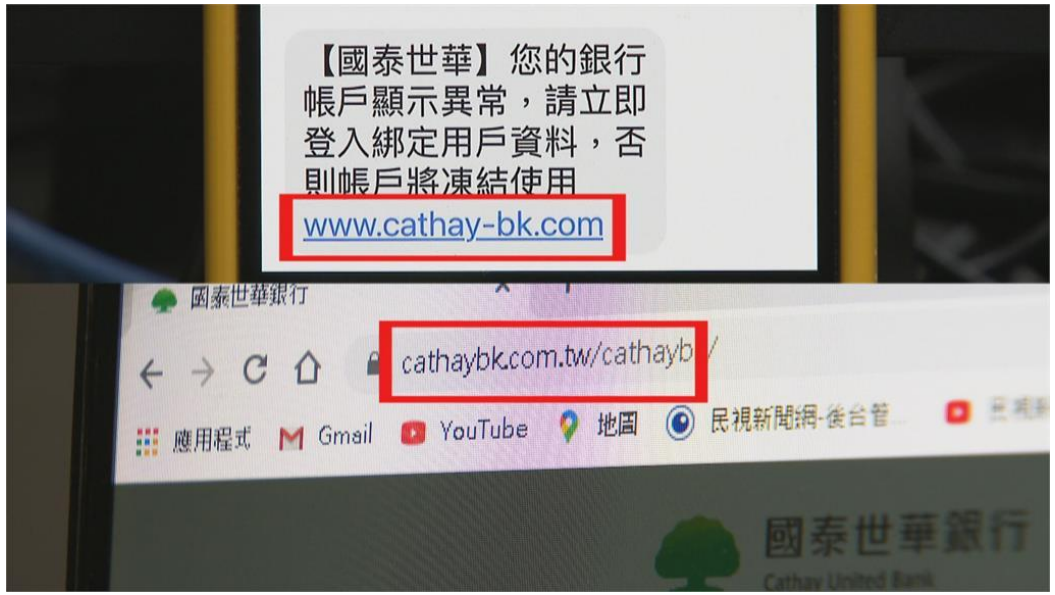
眼見不能為憑，生成式AI好用卻危險

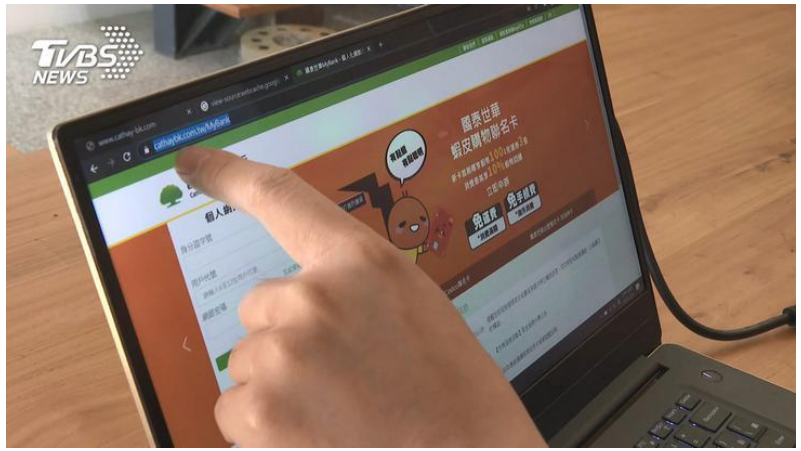
Deep Fake 只要有照片+聲紋即可仿製，如接到打錯電話了，你跟它講幾句，再到FB找人臉，那材料全齊了

快遞包裹已發，請您查收(釣魚簡訊)

資料來源：https://www.police.ntpc.gov.tw/cp-21-64059-1.html

國泰世華釣魚簡訊 3天21人被騙300萬

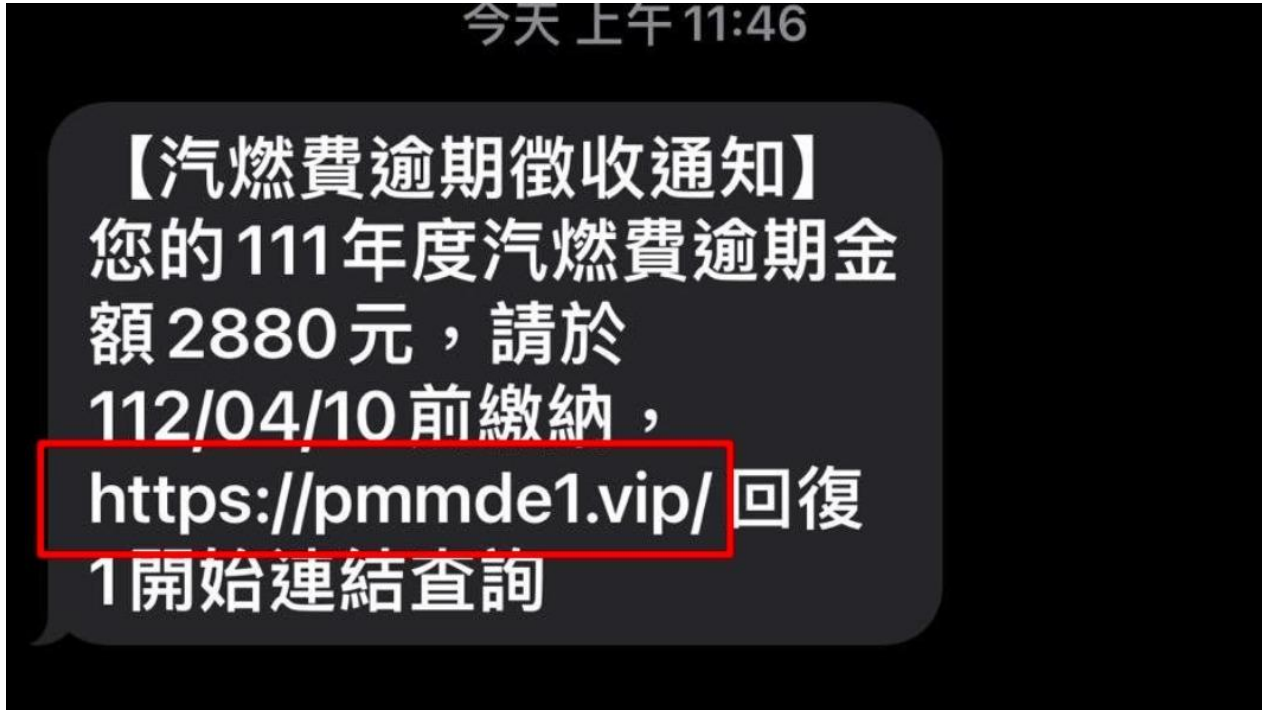


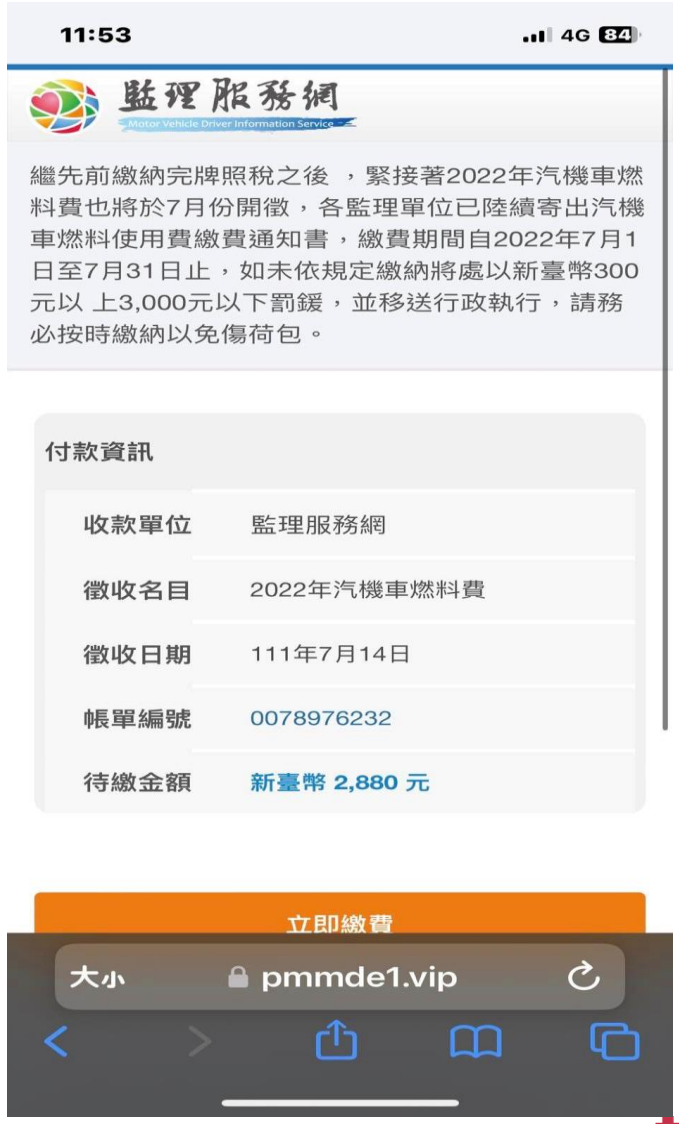


假的國泰銀行網站和正版官網幾乎做的一模一樣，27日到29日短短3天，就有83人檢舉，多達21個人受騙，詐騙金額300多萬，不過目前釣魚網站已經下架。

圖片來源：https://news.tvbs.com.tw/local/1459350
資料來源：https://www.ftvnews.com.tw/news/detail/2021131F04M1

才領6000！手機跳「繳2880元」簡訊





勒索軟體(病毒)攻擊

圖片來源：https://pixabay.com

什麼是勒索軟體

- 綁架電腦裡面的檔案做為人質，要求被害者支付贖金，贖回被加密的檔案
- 使用最高等級的加密技術(RSA-2048或4096)針對使用者的檔案進行加密(包含:Office、PDF、照片、影音檔.....)
- 被加密的檔案由於沒有解密金鑰，因此無法還原

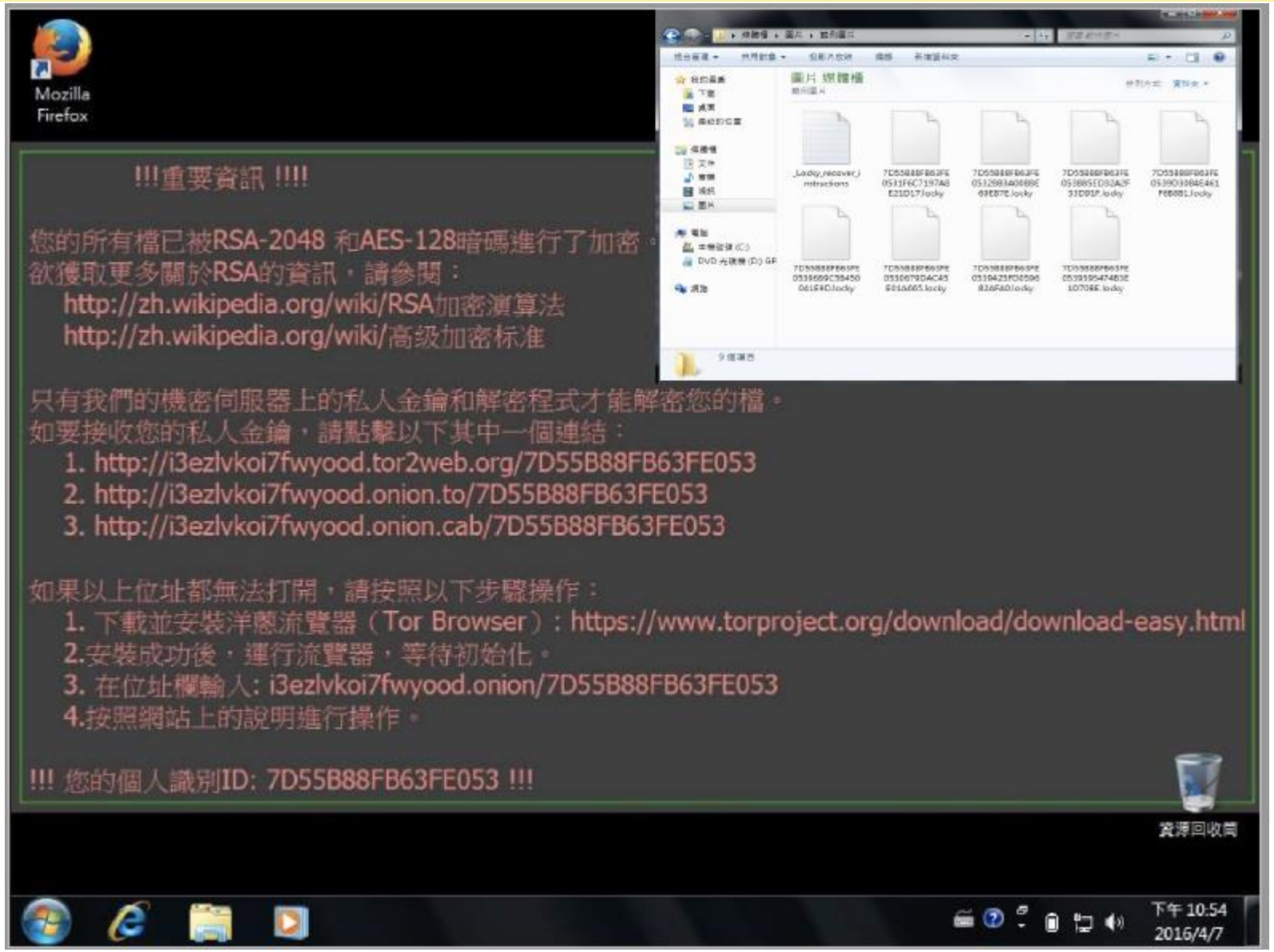
勒索病毒WannaCry

資料來源：iThome 2017/05/14

中了加密勒索軟體時電腦出現的畫面

資料來源：google 圖片

中了加密勒索軟體時電腦出現的畫面



資料來源：google 圖片

病毒與木馬防範

- 7 個常見病毒、木馬、惡意程式的來源:

1. 隨身碟

2. 電子郵件

3.不良內容的網站

4.盜版程式

5.被駭客入侵的網站

6.系統萬年不更新(軟體漏洞)

7.免費、無加密的Wi-Fi

USB隨身碟

圖片來源：取自
Google

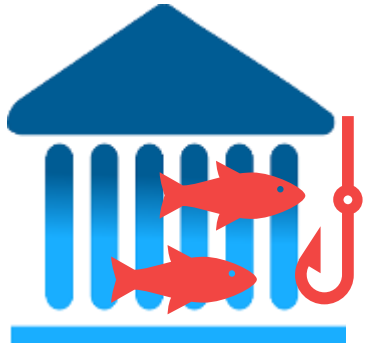
隨身碟實驗

電子郵件

圖片來源： Google

駭客最愛使用的5大Gmail 釣魚郵件

優惠折扣通知



銀行通知

社交網站通知

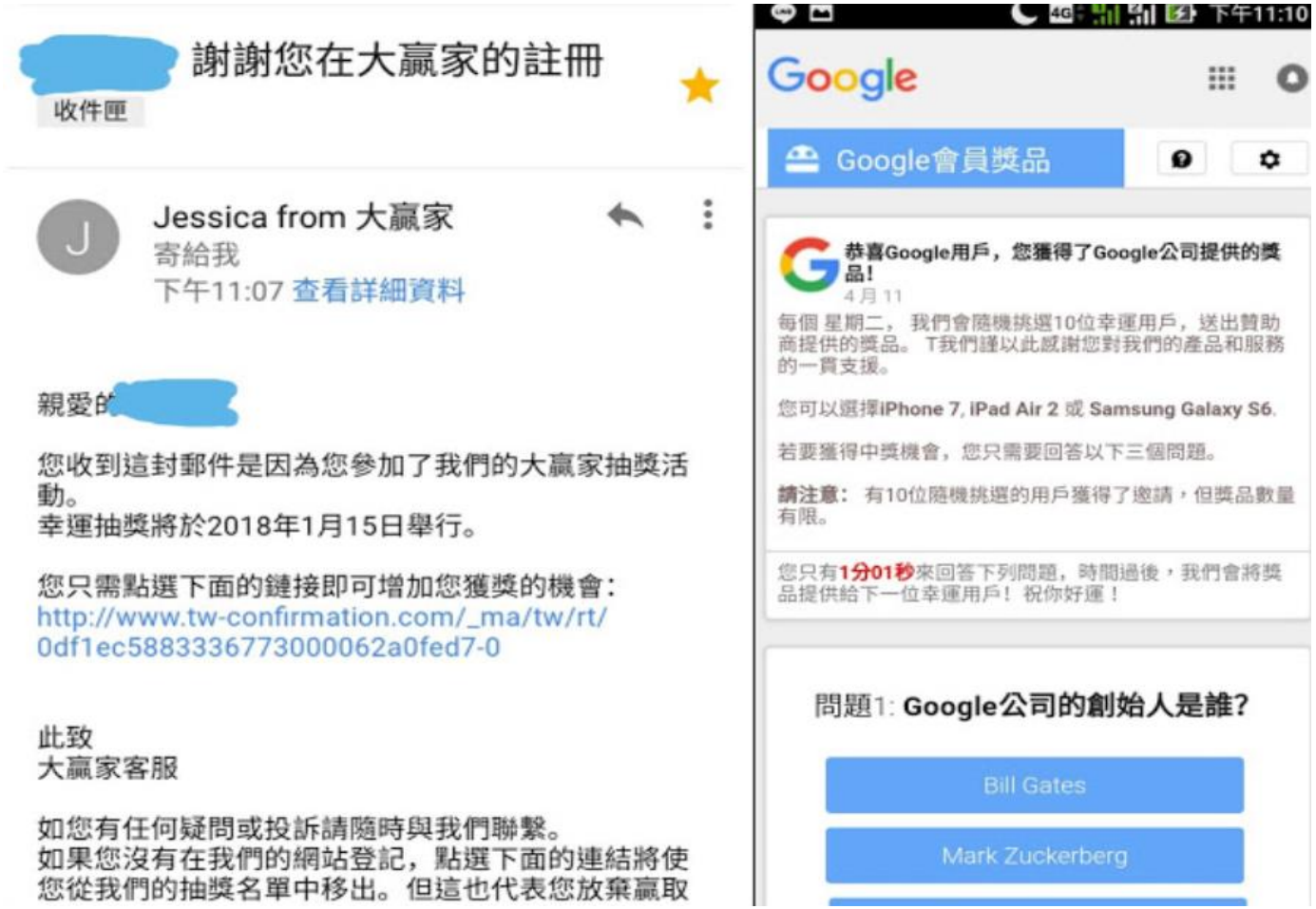
網購訊息通知

中獎通知

資料來源：趨勢科技

社交工程安全防護須知

收到來路不明信件你會怎麼做？



- 確認寄件來源及寄件者
- 確認信件主旨及郵件內容
- 判斷是否跟業務有相關
- 審慎查證寄件人(ex.電話)

非法軟體

資料來源：取自網路

系統、軟體漏洞

資料來源：2017 年 07 月 17 日 BY TREND LABS 趨勢科技全球技術支援與研發中心

Windows、Java、Flash、Chrome、防毒軟體的安全漏洞

資訊安全概念、資安趨勢與案例分析

保障資訊安全的目的

只有經授權的人，才能允許存取資訊

機密性
Confidentiality

上鎖了嗎?

可用性
Availability

被授權者可以想用就用

能正常使用嗎?

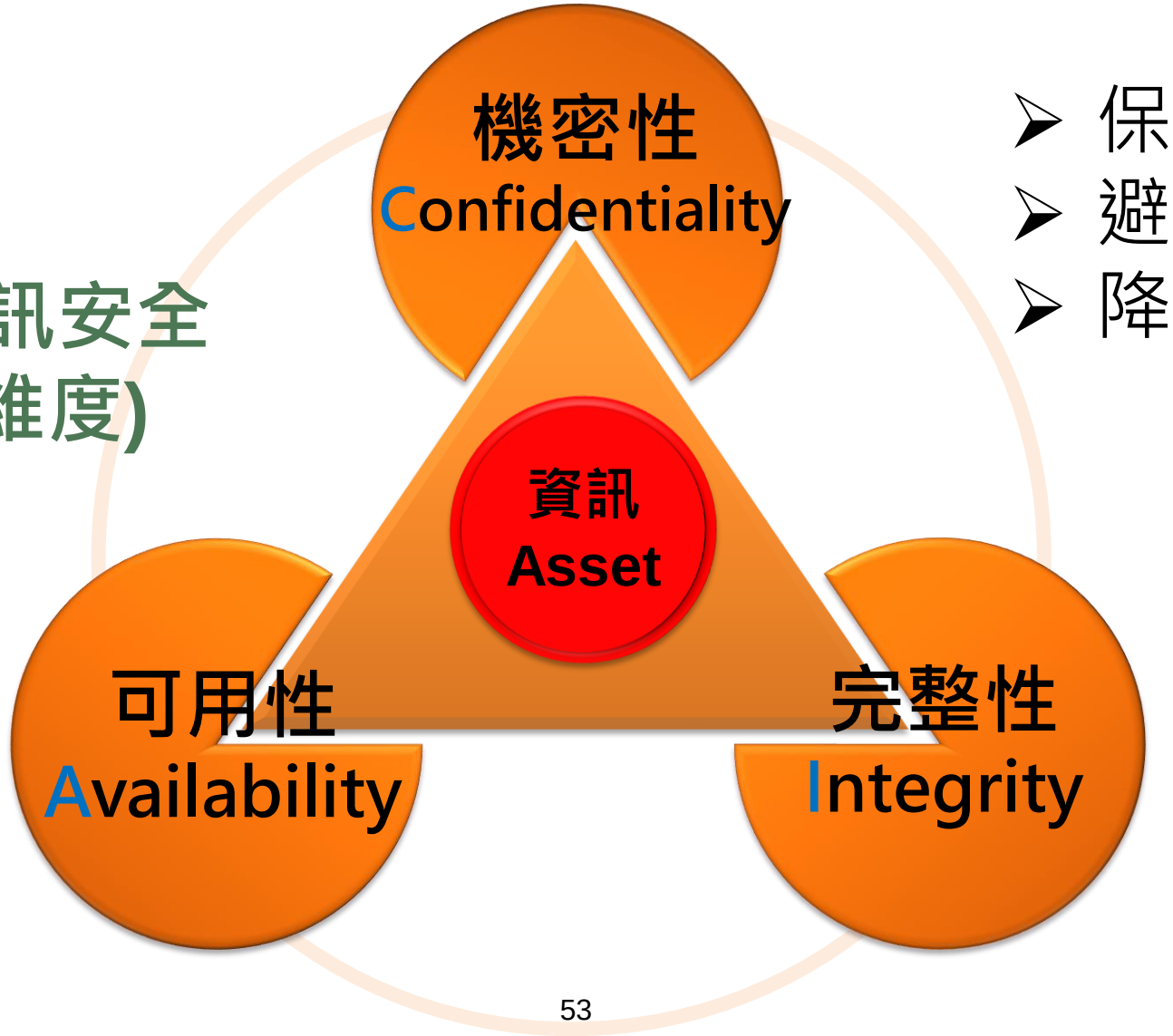
完整性
Integrity

確保資訊在任何階段不會被不當的修改或偽造

有被竄改嗎?

保障資訊安全的目的

常被作為資訊安全
CIA三角(維度)



- 保護資訊資產
- 避免遭受各種威脅
- 降低可能危害

資訊安全基本概念

- 何謂資訊？

  資訊是一種**資產**

✓有**價值**

✓**發生事件時將造成損失**

✓需要被**適當**的**保護**

資訊安全基本概念

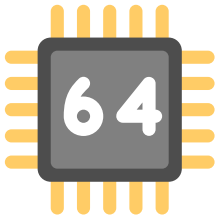
➢何謂資訊？

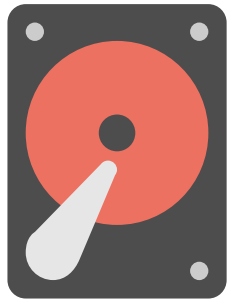
資訊是一種**資產**

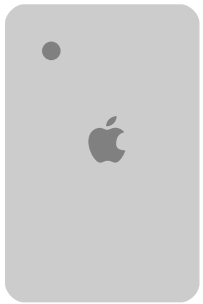
✓有**價值**

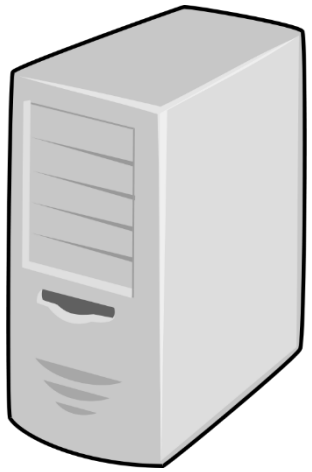
✓**發生事件時將造成損失**

✓需要被**適當**的**保護**









木桶理論

請避免讓自己
成為組織短板

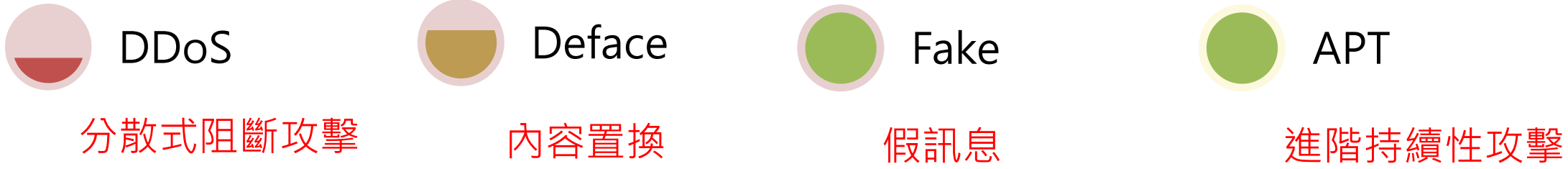
從世界經濟論壇(WEF)展望2025網路安全

資安趨勢趨於複雜的原因

六大影響原因	重點觀察與變化
地緣政治緊張局勢	地緣政治緊張局勢加劇，導致整體環境更加不確定並影響資安策略。	企業更加關切網路間諜活動、智慧財產權竊取的風險。
供應鏈相互依存關係	供應鏈日益複雜與高度依賴下，第三方軟體漏洞與供應鏈攻擊受企業關注。	IT系統過於集中可能引發的風險，隨CrowdStrike事故發生而備受探討。
網路犯罪技術精進	生成式AI助長網路犯罪更精密與更自動化，釣魚攻擊與社交工程攻擊顯著增長，Deepfake技術被廣泛應用於資安詐騙。	網路犯罪即服務成全球犯罪市場的主要商業模式，同時生成式AI降低駭客門檻，擴大攻擊規模
法規要求	全球法規推動資安韌性，但數量增加與變化使企業面臨更高的合規壓力。	不同地區資安法規增加引起法規碎片化的問題，加重企業合規挑戰。
AI與新興科技	企業在應用AI加速競爭力與追求數位轉型時，可能未充分考慮AI相關的資安風險。	企業未能建立強大的資安文化，將更不利於因應AI部署的風險。
網路安全技能缺口	資安技能缺口仍是企業提升韌性的一大挑戰，重視資安人才培訓也要關注職業倦怠風險。	隨著網路安全複雜程度持續提升，資安技能短缺問題也持續擴大，相對是在削弱企業的風險管理能力。

資料來源:世界經濟論壇(WEF)

2025資安預測報告: AI驅動新舊威脅、勒索病毒策略轉型、國家級駭客攻擊未歇



1) AI驅動威脅進化：詐騙手法更加逼真且高效、AI代理成駭客目標

2) 勒索病毒策略轉型，台灣中小型企業成目標

3) APT攻擊持續不斷，供應鏈須納入資安風險管理

4) 擁抱AI變革，展望2025組織資安佈局策略

資料來源:趨勢科技統計期間為2024年1月至11月

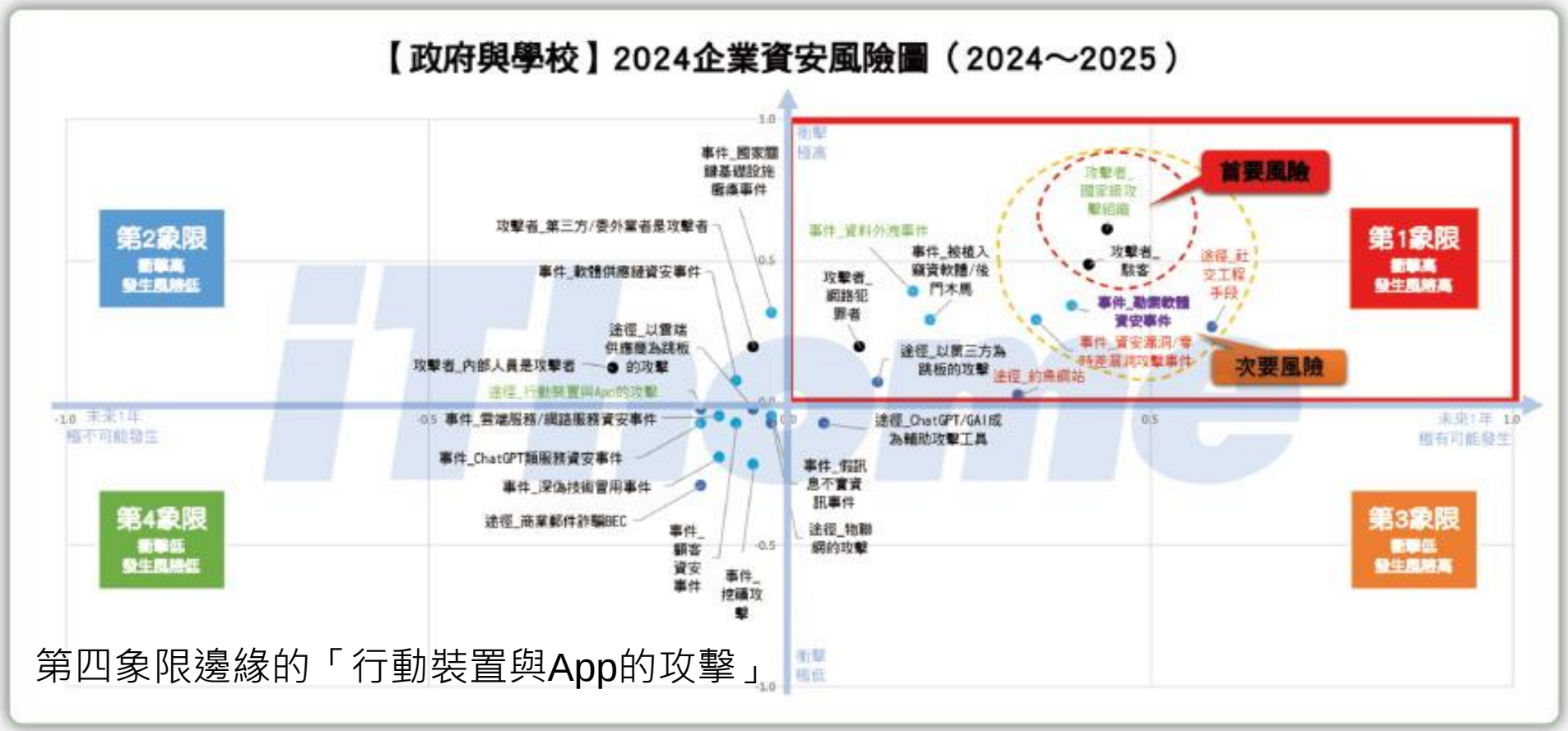
全球短期10大風險排名（2025年至2027年）

1) 錯誤資訊與假訊息（科技風險）
2) 極端氣候事件（環境風險）
3) 國家武裝衝突（地緣政治風險）
4) 社會兩極化（社會風險）
5) 網路間諜活動與戰爭（科技風險）
6) 污染（環境風險）
7) 不平等（社會風險）
8) 非自願移民與流離失所（社會風險）
9) 地緣經濟對抗（地緣政治風險）
10) 人權與公民自由的侵蝕（社會風險）

資料來源：世界經濟論壇，2025年3月

政府學校2025年資安態勢大剖析

國家級攻擊組織和一般駭客都是政府與學校2025年的首要風險，但得留意，前者帶來的衝擊比過去的預期更大，**社交工程手段**、**零時差漏洞衝擊**和**釣魚網站**的發生風險則比去年還要更高。



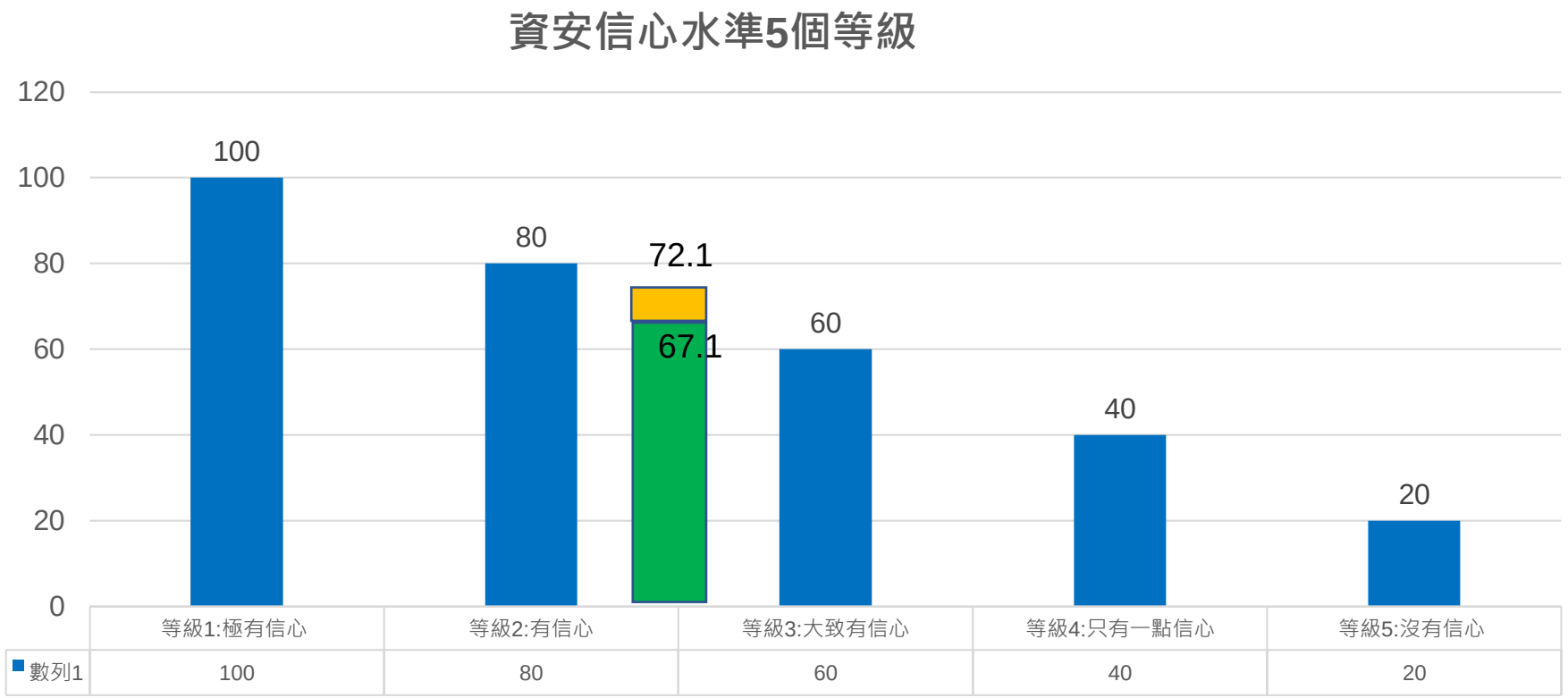
第四象限邊緣的「行動裝置與App的攻擊」

第一象限風險中，釣魚網站威脅、資料外洩事件的衝擊

資料來源:Ithome

政府學校2025年資安態勢大剖析

在這幾年資安即國安政策推動之下，政府學校的資安信心水準在各產業中屬於前段班。若將資安信心水準分成5個等級，極有信心是100分，有信心80，大致有信心60分，只有一點信心40分，沒有信心是20分。以60分（大致有信心）為及格線，整體產業平均是67.1分，政府學校的的信心分數達到72.1分，只有略低於金融業者。



資料來源:Ithome

NIST CSF網路安全框架2.0版的六大面向

網宇安全概念屬性 (NIST CSF):政府學校的資安防護能力哪一項較弱？

政府學校對**識別**能力（69.8分）的信心最低，但這項能力的信心水準也高於一般製造、高科技製造、服務業和醫療業。

- #（Govern）#治理
  對組織環境、風險管理策略、角色與職責與授權，以及政策、監管，還有網路安全供應鏈風險管理。
- #Identify #識別
  建立組織規則以管理系統、人員、資產、資料和功能的網路安全風險。
- #Protect #保護
  建立和實施適當的安全措施以確保重要服務的運行。
- #Detect #偵測
  制定並實施適當的作為以識別網路安全事件的發生。
- #Respond #回應
  對偵測到的網路安全事件，規劃並實施適當的行動。
- #Recover #復原
  制定並實施適當的措施以修復因網路安全事件受損的功能和服務。

圖片來源:Ithome

資安事件案例分享

國內資安事件案例分享

- 2024~2025年國內資安重大事件回顧:

2024/7~8月勒索軟體、網釣攻擊、GitHub遭濫用:

勒索軟體集團Dark Angels成功勒索一家企業7,500萬美元（約24億元）

2024/12月
發布資安重訊的業者有6家，涵蓋紡織業、汽機車製造業、印表機製造業，以及電子零組件業:力鵬、三陽工業、誠研、晟楠、中磊

2025/3月初

彰基醫院:CrazyHunter

2025/03/25
3家臺灣上市公司遭遇資安事故:
1. 喬山:遭CrazyHunter組織攻擊
2. 國揚建設:加密攻擊
3. 居易科技:DDOS

臺灣證券交易所在2024/5月底發布新的規範，要求上市公司發生資安事件，不論是否涉及核心、機密都要發布重訊，後續櫃買中心在7月8日也做出同樣修訂:

1月有3起：京鼎、恩德、伯文。
2月有6起：美琪瑪、富野、瑩碩生技、建準、昶昕、中華電。
3月有1起：華航（發現暗網販售會員資料，但研判為之前個資外洩情事。）
4月有7起：佰研、富野、聯華、聯成、聯合再生、群光、長榮航。
5月有1起：台名

2024/9月數十個臺灣政府機關、企業的網站服務遭受DDoS攻擊:

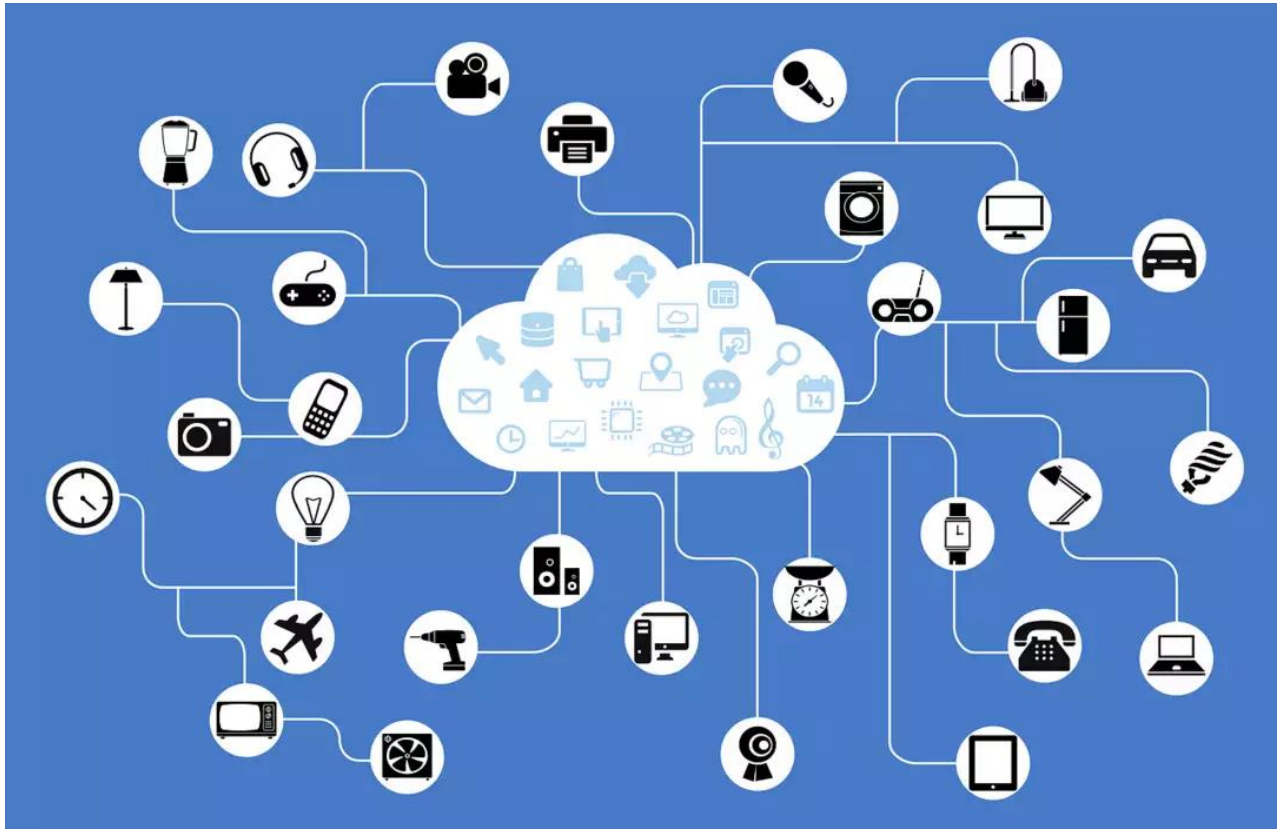
台塑化、緯創、聯電、世芯與多個公家單位(親俄駭客NoName057發動DDOS)

農曆年後多起臺灣上市櫃重大資安事件:11家上市櫃公司發布資安重訊:

1. 印刷電路板（PCB）廠:邑昇、欣興與南亞
2. 美亞鋼管、先進光電、尚立
3. 創見資訊、華城電機、點序科技
4. 友輝光電、新光合成纖維

物聯網裝置帶來的資安威脅

辦公環境而言，通常會有網路交換器、無線路由器、印表機、門禁系統，這些都是能連上公司內部網路的裝置。



圖片來源：https://buzzorange.com/techorange/2019/02/18/iot-data-security/

錄影主機傳出IoT攻擊事件

臺灣可取國際（iCatch）DVR錄影主機傳出IoT攻擊事件，用戶發現設備遭破解後門並陸續被植入木馬，同時對網路骨幹發動DDoS攻擊，許多用戶之後接到中華電信通知，才知道被當跳板。

資料來源：https://www.ithome.com.tw/news/135652

車連網資安事件

Volkswagen

Ford

Mercedez-Benz的GitLab伺服器配置不良，遭研究人員下載逾580個Git儲存庫:一名瑞士軟體工程師Till Kottmann近日向ZDNet爆料，他在德國汽車大廠Mercedez-Benz母公司Daimler AG就地部署的GitLab伺服器上，發現一個配置問題，使他得以下載隸屬該公司的Git儲存庫，內含許多機密資訊，包括一個應用在Mercedes-Benz廂型車上的機載邏輯元件（Onboard Logic Unit，OLU)原始碼。

2020/4/20 → 2020/5/9 → 2020/6/8

不只洩露個資還會影響行車安全！福特和福斯連網車輛傳嚴重漏洞:
汽車與網際網路連接以提供進階功能的情況，如今可說是相當普遍，英國媒體Which?與資安公司Context聯手進行研究找出漏洞，但通報後發現，車商對於相關風險不甚重視，可能會輕忽遭濫用的後果

本田汽車網路疑遭勒索軟體Snake攻擊，部份產線停工:
日本本田 (HONDA)(7267-JP) 在 6 月 8 日遭受網路攻擊，日本國內外工廠的生產及出貨都遭受影響，本田美國及巴西的兩座工廠，汽機車的生產也受到衝擊，雖然美國的汽車工廠已在當地時間 11 日重啟，然而巴西工廠在何時可以恢復也還是未知之數。

資料來源: IThome

能將Tesla直接開走的資安漏洞

研究人員向Tesla通報高階電動車Model X的免鑰匙啟動系統2項安全漏洞，使駭客得以在幾分鐘內解鎖並啟動車子，Tesla已透過軟體更新完成修補。

特斯拉、賓士、BMW都被駭過:「不用200美元，就能偷走要價300萬台幣的特斯拉！」

資料來源：https://www.ithome.com.tw/news/141290

【臺灣史上最大資安事件】台積電產線中毒大當機始末

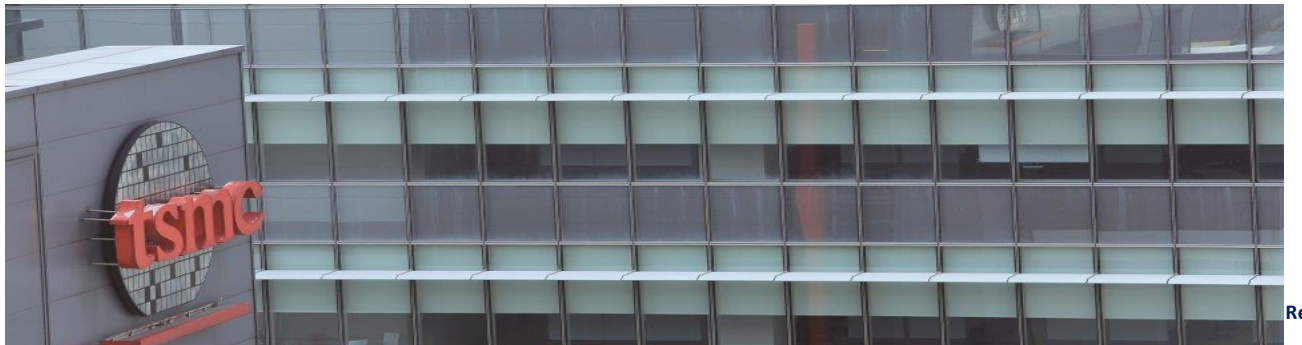
資料來源：iThome 2018/8/10 發表

資安事件案例分享

- 國別: 台灣
- 發生時間: 2018/8
- 產業: 半導體

- 勒索金額:台幣52億元
- 損失金額:
- 勒索軟體: WannaCry

- 事件概況:
  - ✓台積電晶圓廠之所以爆發大規模的病毒感染有兩個關鍵，其一是新機台上線的SOP程序因為人為疏失出錯，導致早已藏匿病毒的機台沒有被防毒軟體擋下
  - ✓加上台積所有臺灣廠區的生產網路全部連結在一起，才會因為一臺機台染上病毒，就造成北中南廠區大規模疫情的嚴重後果

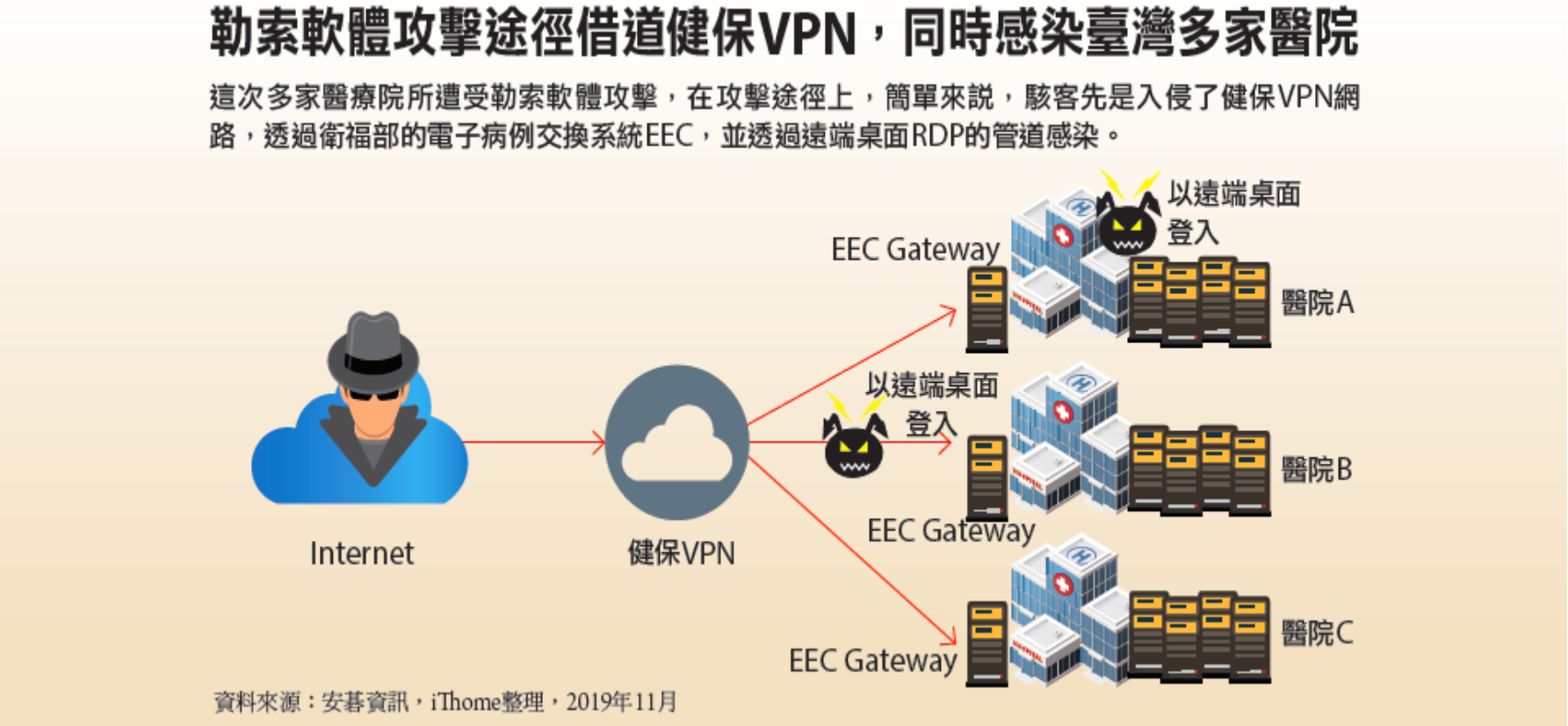


資料來源：iThome 2018/8/10

資安事件案例分享

資料來源：iThome 2018/8/10

鎖定醫療院所進行勒索軟體攻擊-國內



- ✓ 經調查，這次攻擊是從衛服部電子病例交換系統的伺服器（EEC Server）發動，透過健保VPN傳輸，並以EEC Gateway為跳板，早在8月19日就已經植入，隨後入侵並隱藏於院內OT的環控主機，直到28日深夜開始對Windows Server同步發動攻擊

個資事件回顧:健保署2300萬全民個資，基層洩漏長達13年

掌管台灣2300萬人健保資料的健保署，竟傳出職員洩漏民眾個資長達13年！調查局新北市調查處獲報，衛生福利部中央健康保險署已退休葉姓等3名職員，涉嫌外洩健保被保險人個資。

健保署強調，為保障民眾個人資料及隱私權益，健保署在蒐集、處理、利用、銷毀資料時，均以最高標準審視個人資料保護之要求，要求承辦同仁應謹慎自律，嚴守相關法令，亦將持續強化內部查核等防制作為，防杜資料遭非法使用或洩密等不法事件發生。

個資事件案例分享

- 2025/1月:花蓮縣政府涉個資外洩事件 承諾全面檢討與賠償

花蓮縣政府日前舉辦的「113年友好城市參訪—福岡」活動，因活動承辦廠商未妥善控管個資，導致參與者個人資料外洩，包含護照影本及戶籍謄本等敏感資訊，曝光內容高達133頁。此事件遭花蓮縣胡姓議員揭露。

參與參訪活動的人員只需掃描指定的QR碼，即可進入雲端硬碟查看所有報名者的個人資料，甚至包括未選上的報名者資料也未能倖免。他表示，發文前已要求縣府行政研考處通知廠商下架並關閉相關系統，但事件仍已造成嚴重個資外洩。胡議員呼籲縣府主動通知受影響者，並協助有需要的民眾更換護照，相關費用應由縣府或廠商負擔。

個資事件案例分享

- **2024/10月:台灣旅客個資外洩！76萬用戶資料恐遭駭客利用。**
  - ✓ 區塊鏈技術解決方案公司OwlTing因Amazon Web Services (AWS) 儲存空間設定不當，導致大量個人資料暴露於網路上。
  - ✓ 此次外洩的電子郵件地址數量不多，僅約 3,000 筆，主要收集的是電話號碼。外洩記錄的總數接近 900 萬筆。
  - ✓ 外洩資料主要與飯店管理服務相關，包含來自Booking、Expedia等熱門平台的訂房資料。受影響的資訊包括用戶全名、電話號碼、部分電子郵件地址，以及詳細的訂房資訊，如入住日期、房型和付款細節等。
  - ✓ 值得注意的是，92%以上的外洩電話號碼屬於台灣用戶。此外，數千名來自日本、香港、新加坡、馬來西亞、泰國和韓國的用戶資料也在此次事件中遭到洩露。

刑事警察局公共關係室:公布113年第四季高風險業者排名

- 提醒消費者慎防詐騙，發布日期:114-01-27，更新日期:114-02-03
  - ✓ 解除分期付款詐騙案之「高風險業者」為「東南旅遊」及「台灣中油股份有限公司」。

打詐儀錶板連結： https://165dashboard.tw/ 2025/04/26

高風險賣場(1)提高警覺

~~重複扣款、升級ＶＩＰ、操作ＡＴＭ、購買點數、訂單錯誤~~

另外，還有幾家較知名的網購業者，雖然不是年度最嚴重前五，但也值得留意，因為都是2020年初才出現。例如，以前幾個月165反詐騙公布的每周資訊來看，包括東森購物、金石堂網路書局、蝦皮購物、與Gomaji等，警方也都陸續接獲民眾的通報。

資料來源：https://www.ithome.com.tw/news/142240

碩士女教師遭詐騙12萬元

40歲的陳姓女教師擁有碩士高學歷，去年底在某知名購物網站刷卡270元購書，日前接到假冒網站客服及銀行人員來電，表示購物網站員工作業疏失導致她的訂單被設定為連續12期扣款，要求女老師操作ATM解除設定，共匯出12萬元。

資料來源：https://www.ithome.com.tw/news/142240

臺灣宿配網個資外洩

臺灣宿配網坦承日前確實發生資料外洩事件，駭客竊得用戶的姓名與電話，導致曾經使用他們服務的用戶約2千至3千人，都可能會接到的詐騙電話騷擾。

2.8萬存款被盜！專家解釋「用公共WiFi＝裸奔」帳密GG　網友秒懂

日前在深圳從事水果生意的傅先生指，他在華強北附近用手機連上公共Wi-Fi，數分鐘後就收到銀行訊息，顯示帳戶內人民幣6000多元（約台幣2.8萬元）存款遭盜，經媒體披露引發熱烈討論。就有專家呼籲，使用公共Wi-Fi存在不小風險，帳號、密碼面臨的危險程度近乎「裸奔」。

網友在PTT發文，表示直到今天還是有無數民眾愛用公共、免費的Wi-Fi服務，事實上非常危險。他說，大家要有一個簡單的基本概念，「只要掌控封包，使用者所有未加密的資訊都將會開誠布公，一五一十的出現在你面前。」

他舉例，像是PTT平台預設就是明碼傳輸，若用Wi-Fi上網，Wi-Fi提供者可以直接看到使用者的帳號和密碼，「明碼傳輸連一點技術門檻都沒有，連破解都不用破解。」更恐怖的是，就算是已加密的資訊，目前使用SSL2.0的伺服器也幾乎都有辦法破解，「只是運算的時間問題」。

資料來源：https://www.ettoday.net/news/20180221/1116601.htm

個資外流頻發生 資安專家：最好別連公共WIFI

引用來源：https://www.youtube.com/watch?v=MnTg3bwBl8w

大陸129款APP違法蒐集個資

引用來源：YDN　2021/6/13

詐騙網站！陳時中教投資買虛擬貨幣

引用來源： MyGoPen

個人應注意之資安防護事項

新竹縣政府「新進人員資安宣導單」:設備使用-1

1. 辦公環境內必須使用機關提供之資訊設備、網路，及規定之軟體，不得使用個人私有設備及中國廠牌產品，公務設備亦不得連結個人私有手機上網。若有業務上的需求，必須經資訊安全官同意後，列冊管理並定期檢討。
2. 設定開機密碼，啟動螢幕保護程式（於一定時間未使用即自動鎖定電腦，時間不超過15分鐘）或是其他控制措施保護。
3. 離開座位致個人電腦有遭入侵之虞者，應於離開前將螢幕鎖定或關閉電腦。
4. 非因公務需要並經授權，不得攜出辦公處所。
5. 個人使用時應注意避免輸入私密資料。

新竹縣政府「新進人員資安宣導單」:軟體使用-2

1. 安裝所需軟體，安裝前應先確認取得合法授權。
2. 不得散布無合法授權軟體，亦不得將授權軟體轉借或給予未經授權人員使用。
3. 如發現使用非授權軟體，由使用者自負相關法律責任。
4. 不得安裝及使用點對點（Peer-to-Peer, P2P）分享軟體。
5. 即時通訊軟體使用應注意不得傳送公務敏感資料。
6. 傳送公務資訊應有適當保護，例如加密傳送。

新竹縣政府「新進人員資安宣導單」:網路使用-3

1. 不得任意更改個人電腦IP 位址與網路卡。
2. 個人電腦不得安裝數據機或無線、行動網路等相關對外連線設備。
3. 使用無線網路時注意資料傳輸之加密性，避免輸入私密資料。
4. 上班期間不應連結非公務需要之網站，並避免連結惡意網站或釣魚網站，如發現異常連線，請通知資安窗口。

新竹縣政府「新進人員資安宣導單」:機敏個人資料處理網路使用-4

1. 機密檔案不得在網路上傳送，敏感性資料傳送前應先加密。
2. 機敏電子檔案應加密保護，不得存放於分享資料匣或對外公開之系統。
3. 重要檔案定期備份及做回復測試，機敏性資訊之備份媒體應置於上鎖櫃內。
4. 儲存媒體（含硬碟、USB隨身碟、光碟等）廢棄時需格式化或消磁，必要時，須採用實體破壞。
5. 職務異動時電腦設備內業務資料應列入交接或進行適當銷毀或重置，以避免資料遭不當存取使用。
6. 書面文件置於可上鎖之抽屜或櫥櫃，不得留置於會議室、影印機處等公用空間，廢棄時應使用碎紙機絞碎。

新竹縣政府「新進人員資安宣導單」:帳號密碼管理-5

1. 帳號及密碼，應妥善保管，並遵守機關規定，如有外洩疑慮，除儘速更換密碼外，並應通知資安窗口。
2. 不得將密碼張貼在個人電腦或終端機螢幕或其他容易洩漏秘密之場所。
3. 密碼設定不得沿用預設密碼、不得與帳號相同，至少8碼之英數字組成，建議包含特殊字元（如@、#、%等），並避免使用與個人有關之資訊（如生日、身分證字號、單位簡稱、電話號碼、員工代號等）。
4. 密碼應至少每3個月更換一次，變更時，新設密碼不得應原密碼相同。
5. 職務帳號應於職務異動時列入交接，完成交接後新使用者應立即變更密碼。
6. 禁止共用帳號，以區分安全責任；調離職時應立即辦理權限異動或帳號移除。

新竹縣政府「新進人員資安宣導單」:病毒及駭客防範-6

1. 個人電腦應設定自動更新(Windows Update)修補系統漏洞、安裝本中心所提供之防毒軟體並隨時注意病毒碼更新狀態、並關閉USB自動執行設定(Auto Run)，防止駭客藉由USB裝置植入後門程式。
2. 避免從網路自行下載軟體或檔案安裝及使用，或直接點選來路不明之連結，因業務需要者，應選擇自資料來源之官方網站下載、查詢。
3. 於瀏覽器連線外部網站時，對可疑或未經簽署之行動碼(如ActiveX、Java applets等)，應避免直接啟用。

新竹縣政府「新進人員資安宣導單」:防範惡意電子郵件社交工程-7

1. 個人電腦應設定自動更新(Windows Update)修補系統漏洞、安裝本中心所提供之防毒軟體並隨時注意病毒碼更新狀態、並關閉USB自動執行設定(Auto Run)，防止駭客藉由USB裝置植入後門程式。
2. 避免從網路自行下載軟體或檔案安裝及使用，或直接點選來路不明之連結，因業務需要者，應選擇自資料來源之官方網站下載、查詢。
3. 於瀏覽器連線外部網站時，對可疑或未經簽署之行動碼(如ActiveX、Java applets等)，應避免直接啟用。

新竹縣政府「新進人員資安宣導單」:資安通報獎懲-8

1. 主動通報資安事件或可能資安風險者，依規定獎勵。
2. 未遵守機關資安規定，初次予以告誡，若持續發生或勸導不聽者，依規定懲處；若因而發生資安事件，加重處分。
3. 有資安疑慮或異常時，應即時通報資安窗口。

病毒檢測線上服務

- Virus Check(TWCERT/CC台灣電腦網路危機處理暨協調中心提供)
- https://viruscheck.tw/

勿上傳公務或含敏感/個資檔案！

重要資料要備份

- 備份的重要性
  預防重要資料或設備損壞遺失

- 備份的有用性
  3-2-1 備份原則
  -至少**備份三份**。
  -使用**兩種不同的媒體**備份。
  -其中**一份備份要存放異地**。

- **定期檢查備份是否為最新內容且可還原**。

USB使用要謹慎

- 可移除式媒體優點:
  - 體積小，攜帶方便
  - 儲存容量大
  - 便宜
- 可移除式媒體資安威脅:
  - 遺失
  - 洩密
  - 傳播病毒

- **USB使用前應先掃毒，使用完畢即將資料刪除。**
- **建議關閉自動播放媒體選項。**

容易遭到破解的5大密碼類型

1. **只有數字組成、或依照鍵盤順序排列的懶人密碼**
   - 如123456這種只有以數字組成的密碼
   - 依據鍵盤位置，橫向或直向依序輸入的英數字如qwerty、1qaz2wsx

2. **未更換系統提供的預設密碼**
   - 出廠的預設帳號密碼往往可能是admin和password

3. **密碼中含有個人資訊**
   - 如生日、家人（尤其是另一半或寵物）的名字等

4. **直接使用英文字典中的單字當作密碼**
   - 形同有規則的排列方式，容易破解

5. **多個系統和網站都使用同一組密碼**
   - google與加州大學研究發現從黑市買入19億資料中，有25%可以存取受害者google帳號

2020 最糟密碼前20名

1. 123456
2. 123456789
3. picture1
4. password
5. 12345678
6. 111111
7. 123123
8. 12345
9. 1234567890
10. Senha
11. 1234567
12. qwerty
13. abc123
14. Million2
15. 000000
16. 1234
17. iloveyou
18. aaron431
19. password1
20. qqww1122

資料來源：NordPass

密碼安全管理建議

- **密碼長度至少8碼以上。**
- **定期**更換各系統密碼。
- 密碼確實使用**英文大小寫、數字、符號字元等混合在一起使用**。
- 避免多個系統使用同組密碼，以免遭受字典攻擊。
- **善用雙因子/多因子認證(Two-Factor/Multi-Factor Authentication，2FA/MFA）或動態/一次性密碼（One-Time Passwords，OTP）。**

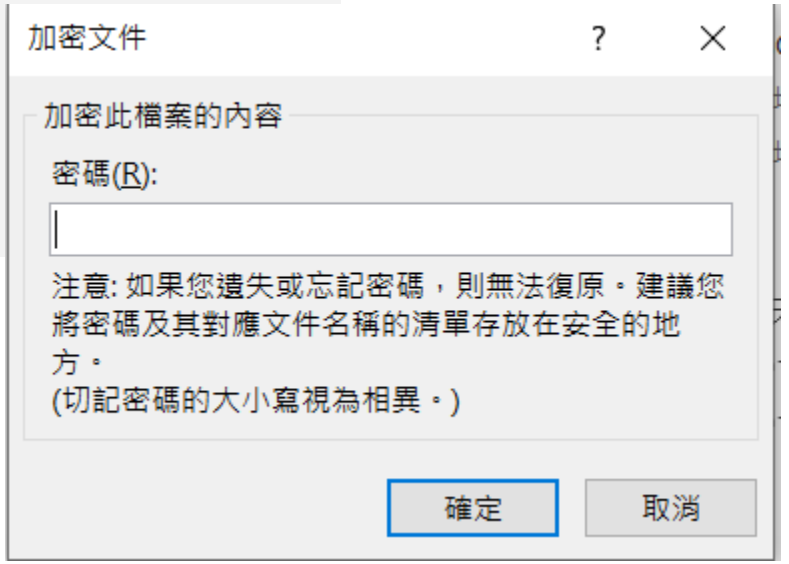
- **避免將密碼書寫於明顯且容易讓他人取得之處。**
- 離開電腦座位時應使用電腦鎖定功能。

電子資料壓縮加解密防護

- 電子檔案壓縮加解密可應用於電子檔案儲存或傳送，以保護資料之機密性、完整性。
- 常用軟體Microsoft Office、Adobe Acrobat、LibreOffice、7-ZIP，均具有檔案加密之功能。

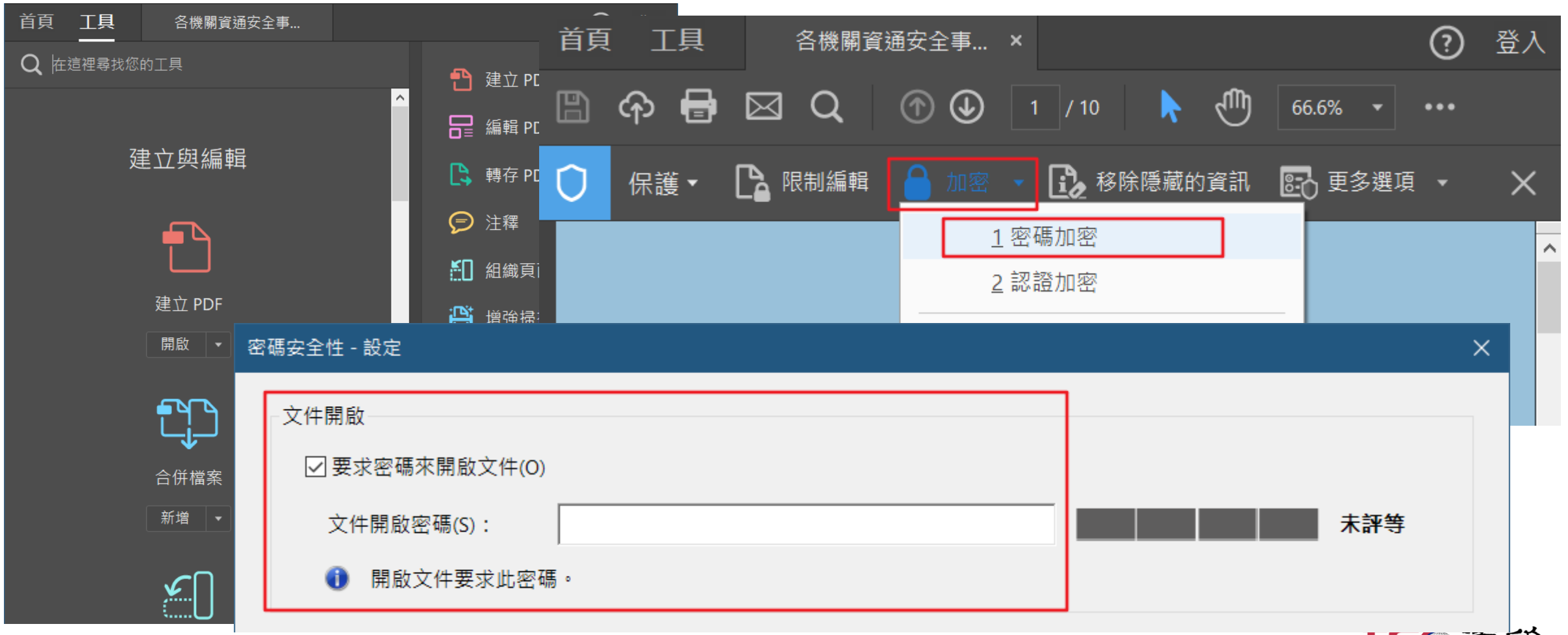
PowerPoint檔案加密

打開需要壓縮的PowerPoint→ 點選左上角的檔案→ 點選資訊 → 保護簡報→以密碼加密→確定



Adobe文件(PDF)加密

打開欲加密PDF → 工具 → 保護 →按加密並選擇密碼加密 →
打勾「要求密碼來開啟文件」 → 輸入密碼



行動資安宣導

如何做好個人的資訊安全管理(1)

- BYOD(Bring Your Own Device) = 自攜型裝置。
- 舉凡筆電、智慧型手機、智慧手錶、藍芽耳機、藍芽音箱...各種可以帶著就走並連上網路使用的設備。

如何做好個人的資訊安全管理(2)

充電器
充電線
無線充電盤
OTG

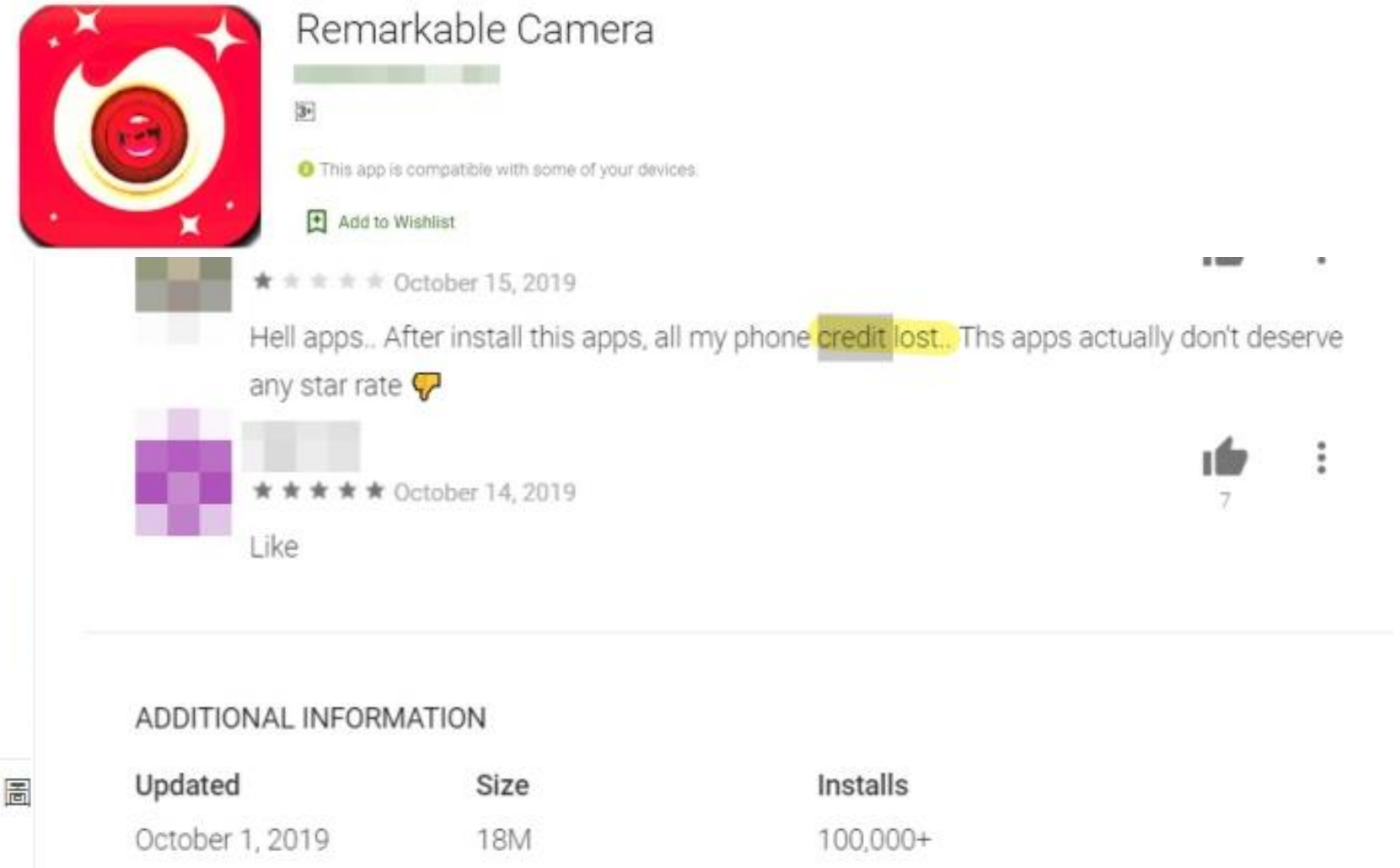
無定期更新
刷ROOT
越獄
非官方韌體

美圖拍照
系統清理
電池管理
免費遊戲
不明來源APP

廣告網站
遊戲網站
影片線上看

如何做好個人的資訊安全管理(3)

▲ 有許多惡意程式暗藏在美顏相機App之中。（圖



▲ 有使用者反應當他安裝App之後，電信預付額度就被異常扣款。

如何做好個人的資訊安全管理(4)

小心公共USB充電站讓惡意程式上身，美政府籲勿使用

美國洛杉磯郡地方檢察院本周就警告，為免感染惡意程式，大眾交通工具的乘客應避免以機場、飯店和其他地方的公用USB充電站為手機或其他裝置充電。在這些充電站充電，可能遭遇名為充電陷阱（juice jacking）的駭客手法，歹徒在充電站或充電線中植入惡意程式，以等待不知情的過路旅客將裝置插上而感染。這會造成裝置被鎖住，或是用戶資料或密碼經由惡意程式傳送到駭客架設的伺服器。

資訊產業很早就注意到USB傳輸線的安全問題。2014年即有德國廠商SRLabs 發現變更可程式化的USB控制晶片，即可將各種USB裝置變成邪惡裝置（BadUSB），隨後並有安全公司發展出將USB線變成人機輸入介面。今年安全研究人員Mike Grover還在USB介面上嵌入了Wi-Fi晶片，以便可在適當的距離內遠端攻擊，竊取裝置資料。

資料來源：https://www.ithome.com.tw/news/134225

如何做好個人的資訊安全管理(5)

✓購買原廠認證的線材及充電設備(MFi、Google、三星認證)

Made for iPod iPhone iPad

蘋果官方查詢網站：https://mfi.apple.com/MFiWeb/getAPS.action

✓快速充電選擇有QC認證或PD認證，無線充電有Qi認證

Qualcomm Quick Charge 3.0

✓選擇有品牌、有商譽的商家購買(高星數評價，留言評價反應好)

✓不使用**來源不明**的線材及充電設備

如何做好個人的資訊安全管理(6)

- **NFC（Near Field Communication）**是一種短距離的高頻無線通訊技術，可以讓裝置進行非接觸式點對點資料傳輸，也允許裝置讀取包含產品資訊的近距離無線通訊 **(NFC)** 標籤。您也可使用此功能來付款或購買車票或活動門票，但須先下載所需的應用程式。

- 例如:Apple Pay、Google Pay、Samsung Pay

- Line Pay、街口支付等為行動支付但非使用NFC而是使用QR Code技術。

如何做好個人的資訊安全管理(7)

- 防止不當利用的五個法則

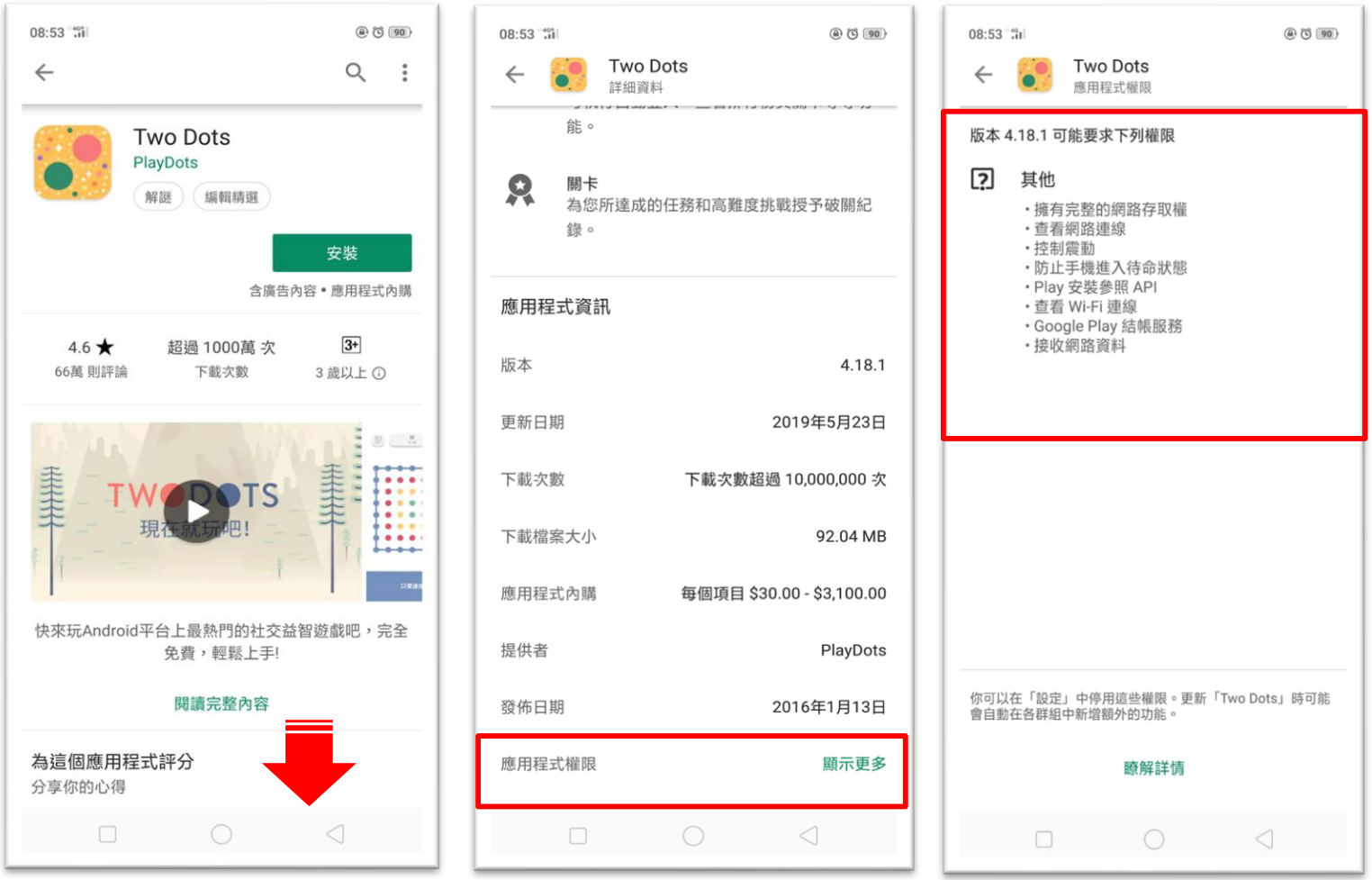
1. 務必開啟螢幕鎖定功能(密碼、指紋、人臉)
2. 能夠高額支付的APP請開啟鎖定功能
3. 開啟「GPS」並給予「尋找裝置」功能權限(其餘APP斟酌)
4. 利用安全的行動支付服務(Apple Pay、Google Pay、Line Pay等)
5. 不使用的支付APP請適時解除安裝

手機APP的隱私存取權限(1)

影片參考：PTS Taiwan. Best of INPUT
https://www.youtube.com/watch?v=HnRsvhUuRgw

手機APP的隱私存取權限(2)

下載前查看應用程式會有哪些權限(Android範例)。



手機APP的隱私存取權限(3)

查看應用程式存取權限(IOS範例)。

手機APP的隱私存取權限(4)

- 下載APP前注意:
  - 確認APP是否為官方所開發
  - 好評價不一定是OK的APP(評價可以洗)
  - 注意APP所需權限(例如:相機照片為何要取用電話及簡訊的權限)
  - 盡可能不點擊廣告或下載廣告內APP

LINE安全防護須知

從帳號主頁檢查盾牌顏色

藍色是認證帳號

綠色是官方帳號，可以放心加入

灰色則是一般帳號，只要「看到灰色就高機率是假的」。

LINE真假訊息求證

LINE官方帳號搜尋:
趨勢科技防詐達人

LINE 訊息查證官方帳號：
@linefactchecker

LINE 訊息查證

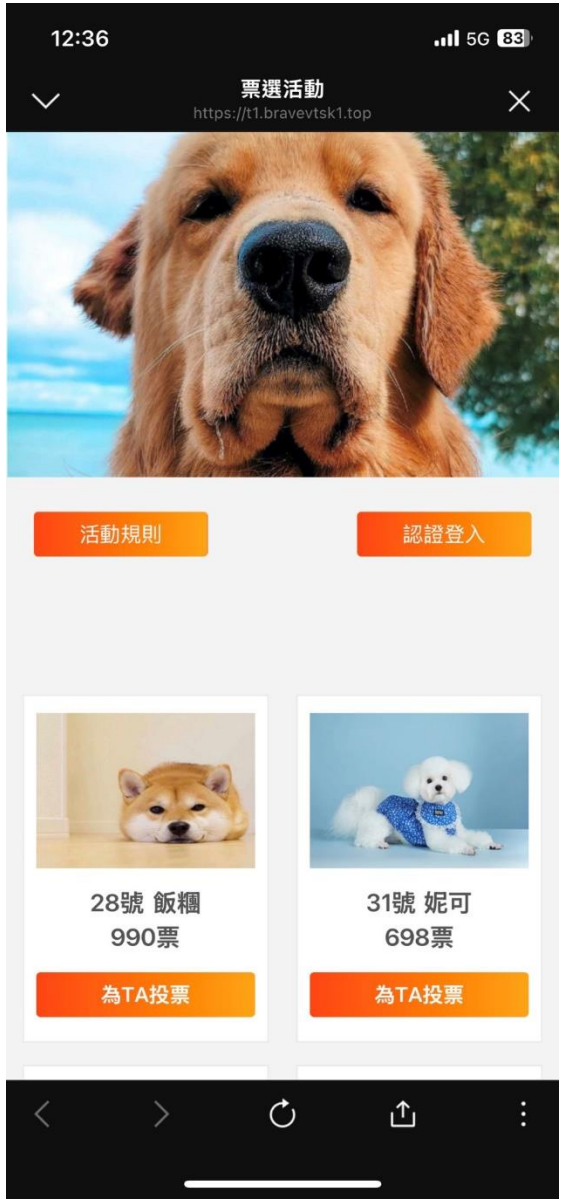
假帳號送貼圖騙個資　LINE教你4招破解

影片參考: https://www.youtube.com/watch?v=sTSDjcMTuYo

LINE阻擋非好友/廣告訊息

- LINE→其他→設定→隱私設定→勾選「阻擋訊息」

LINE詐騙/寵物比賽投票



TSC CAPITAL GROUP
The Bridge to the Asia Pacific Region

Q/A