資拓宏宇國際股份有限公司
International Integrated Systems, Inc.

學校資安認知宣導課程

危險與你的距離

講　師：資拓宏宇資安顧問
日　期：112/6/20

簡報大綱

- 資訊安全發展趨勢與新興議題
- 個資與資安事件案例分析
- 社群網路常見詐騙伎倆
- 社群網路安全使用守則
- 個人資料安全風險

資訊安全發展趨勢與新興議題

全球資通安全威脅趨勢

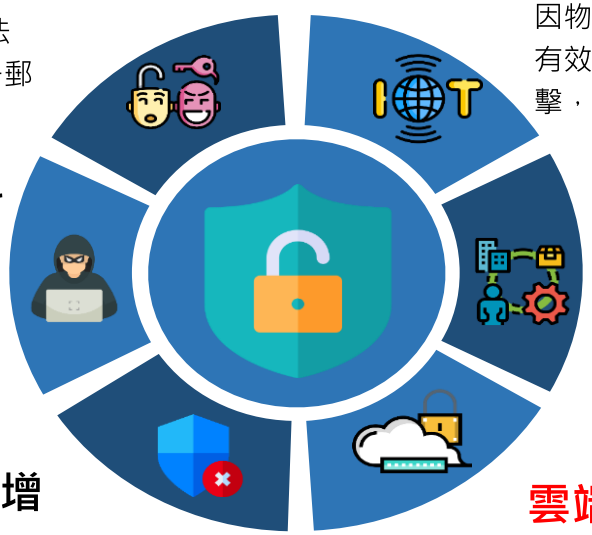
- 綜整111年全球資安威脅報告歸納，全球資安威脅趨勢可分為六大類

社交工程手法層出不窮

依統計，駭客常使用 的攻擊手法為釣魚攻擊其次為各種詐騙電子郵件

萬物聯網資安風險倍增

因物聯網設備普及，多數物聯網裝置缺乏有效控管，長期遭駭客入侵利用於各種攻擊，如DDoS攻擊與殭屍網路



進階持續性攻擊竊取機敏資料

駭客集團鎖定特定組織或國家精心策劃結合多種攻擊手法，包括：社群平台、手機、 Office文件及各式產品漏洞，持續而隱匿地逐步滲透，藉此竊取機敏資料

資安(訊)供應商遭駭客破壞供應鏈安全

供應鏈風險對全球組織影響漸增，供應鏈安全落差使駭客鎖定監控較不嚴謹之設備或供應商，做為入侵管道

漏洞利用攻擊風險激增

據國外調查統計，駭客最愛利用漏洞主要為遠端程式碼執行或提權等權限控管缺陷；另，郵件伺服器(Exchange)產品等重大漏洞也屢遭利用

雲端服務平台遭駭客利用

雲端服務平台可幫助企業組織快速部署提高效率，但也遭駭客利用以掩飾惡意行為

資料來源：111年第2次政府資通安全防護巡迴研討會

政府領域資安威脅趨勢

- 綜整111年政府領域資安威脅偵測與機關通報資訊，主要威脅趨勢有6大面向

社交工程與APT惡意電子郵件仍為主要攻擊手法

遠端服務探測與產品漏洞利用為主要網路威脅

人員資安意識不足導致資料外洩

雲端服務中繼站盛行協助駭客隱匿惡意行為

供應鏈安全遭破壞成為入侵跳板

物聯網衍生應用造成資安風險

資料來源：111年第2次政府資通安全防護巡迴研討會

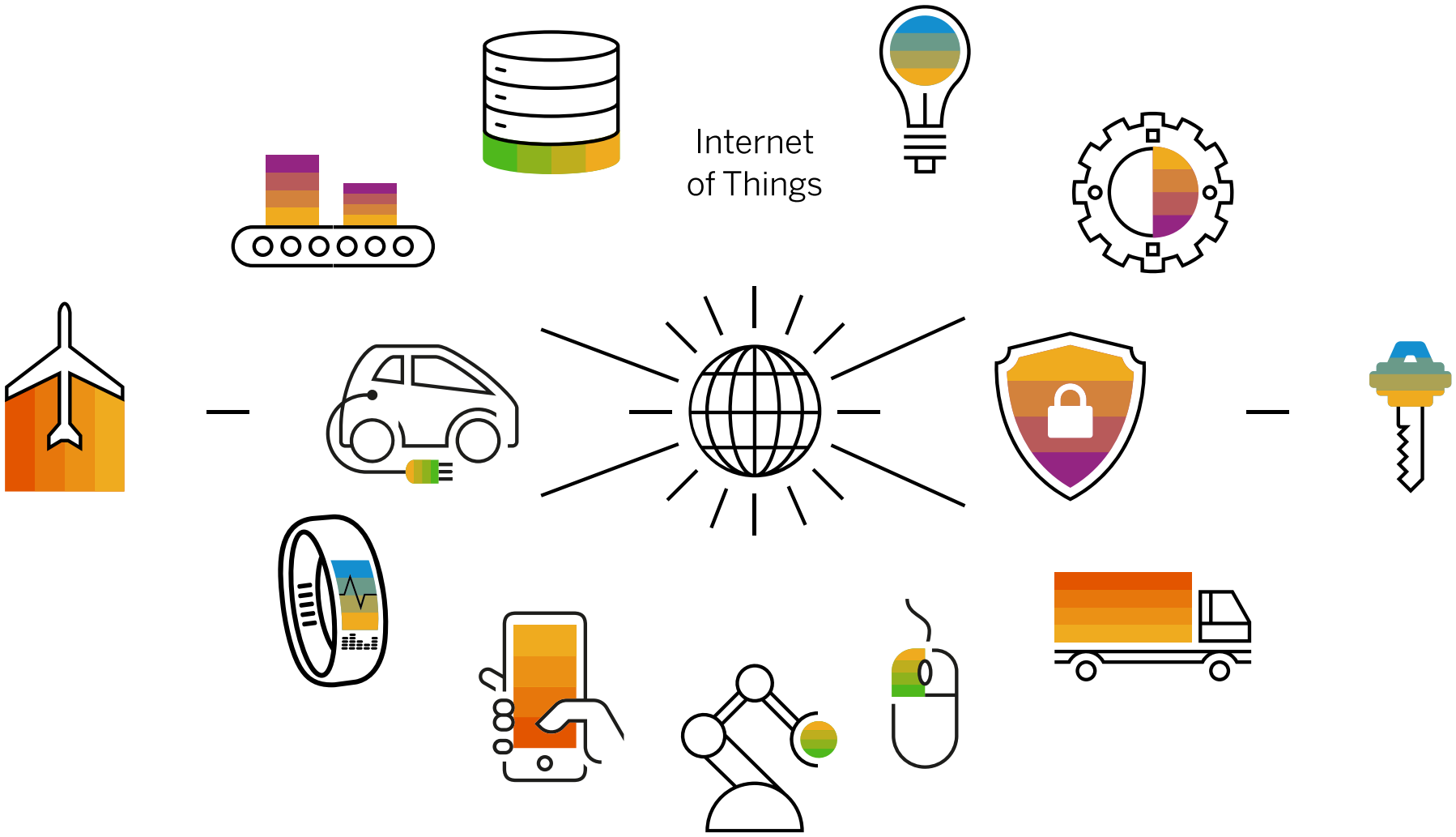
享受便利的IoT代價

物聯網定義

物聯網（英語：Internet of Things，縮寫 IoT）從最廣義的層面而言，物聯網包含**任何可以連線至網際網路的物體或「東西」**然而，現今的物聯網更特指結合了感測器、軟體和其他技術的互連設備，能夠通知使用者或者自動化動作。傳統上，連線能力主要依靠 Wi-Fi 實現，而現在 5G 和其他類型的網路平台，已幾乎具備能隨時隨地處理大型資料集的速度和可靠性。

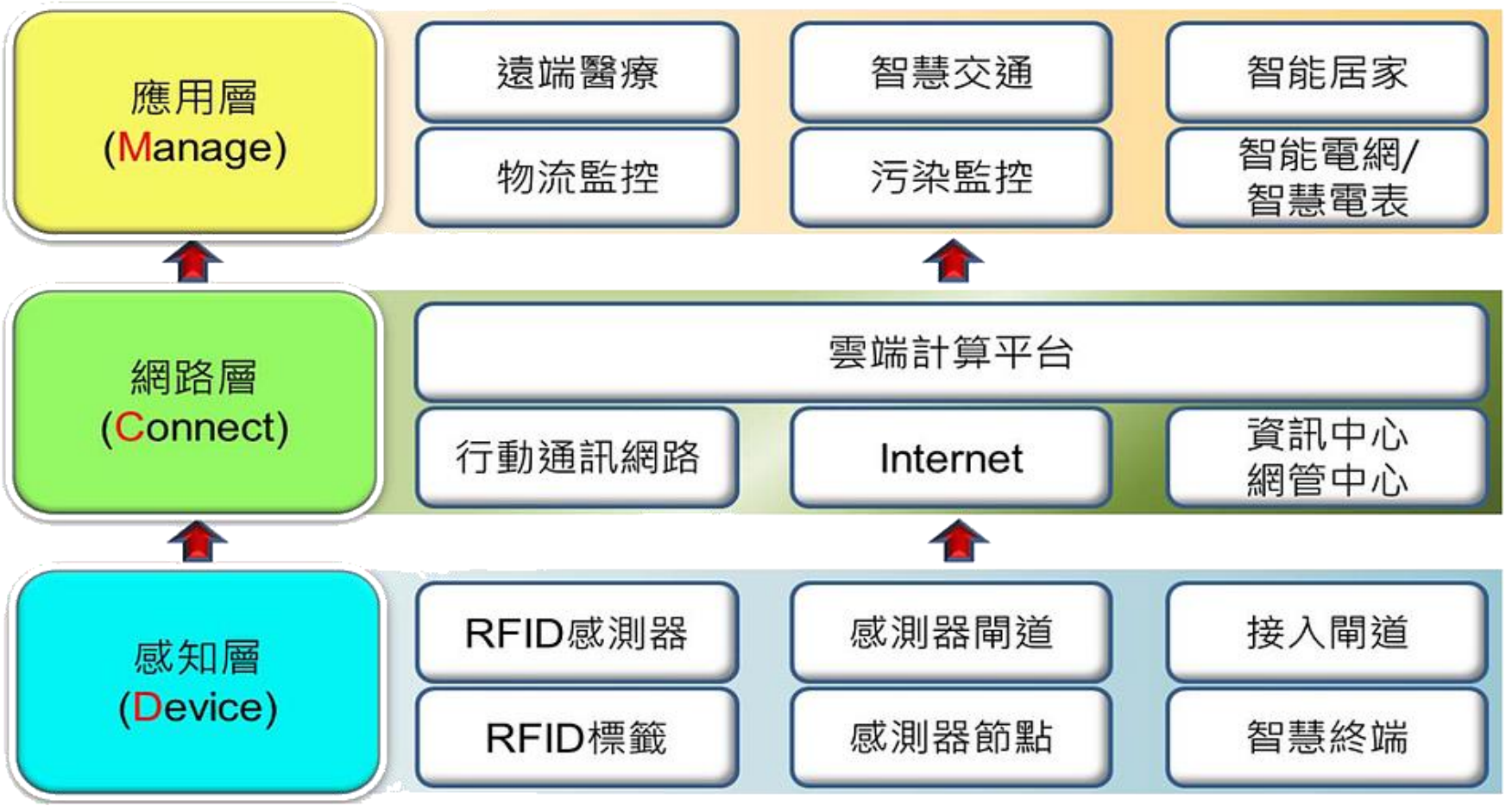
資料來源： https://www.sap.com/taiwan
圖片來源：http://www.hihttps.com

IoT 的應用



資料來源： https://www.sap.com/taiwan

物聯網架構



圖片來源： http://www.leeandli.com/TW/Newsletters/6009.htm

IoT 面臨的資安風險

- **系統更新及漏洞修補不易**：IoT 設備通常會以公板方式客制化生產，且生產數量眾多。
- **安全認證問題**：IoT 設備為能連接網路及控制設備，因此除了有線網路介面外，可能還有像藍芽、無線網卡等介面。
- **遭受非法應用**：當一種 IoT 設備遭到破解入侵後，因 IoT 設備的特性意謂著採取相同設計或硬體的設備皆存在於此風險中。
- **連接埠安全**：IoT 設備通常會內建一些方便管理的功能，這些功能會有特定連接埠。

資料來源：TACERT

監視器畫面"被上網" 疑因中製系統遭駭

資料來源：華視 https://youtu.be/a6s62B-osgk

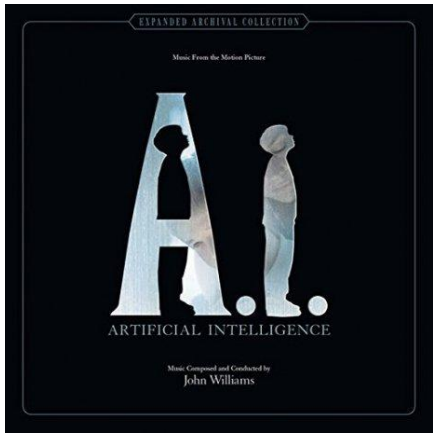
資安專家發現最新監聽技術！

影片來源： https://youtu.be/jhlMveZuYeo

你以為的AI

AI定義

- 人工智慧是打造電腦與機器的科學領域，這些電腦和機器可以進行推論、學習以及採取行動，而這類行動原本需要人類智慧判斷或涉及超出人為分析能力上限的資料規模。
- AI 是一個廣泛版圖，包含許多不同的專業領域，包括電腦科學、資料分析與統計資料、硬體與軟體工程、語言學、神經科學，甚至是哲學和心理學。
- 在業務營運方面，AI 是一組採用機器學習技術和深度學習的技術，可用於資料分析、預測和預報、物件分類、自然語言處理、推薦、智慧資料擷取等。



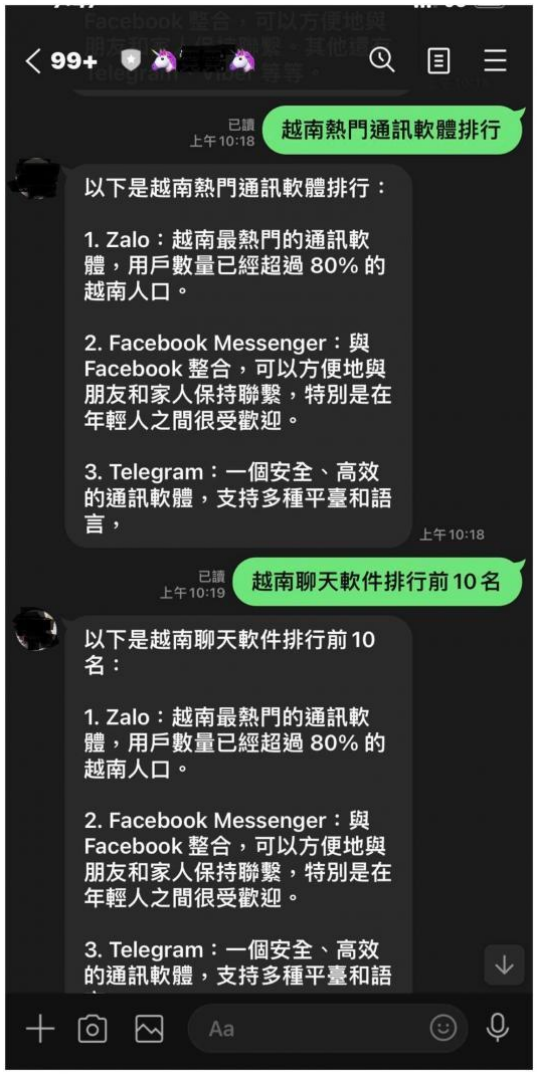
資料來源：https://cloud.google.com
圖片來源：https://tw.bid.yahoo.com

AI人工智慧的應用程式和用途

1. **語音辨識**：自動將語音轉成書面文字。
2. **圖片辨識**：辨別圖片的各個層面並加以分類。
3. **翻譯**：將某個語言的書面或口說文字翻譯成其他語言。
4. **建立預測模型**：探索資料，以高度精細的方式預測特定結果。

資料來源： https://cloud.google.com

AI聊天機器人竟成新詐騙手法 (相關報導)



資料來源：https://newtalk.tw

使用ChatGPT 會有哪些資訊安全風險?

- 使用ChatGPT的一些潛在的資訊安全風險：
  1. 隱私風險：ChatGPT是一種大型語言模型，需要大量數據進行訓練。如果模型接收到包含個人身份識別信息或其他敏感信息的數據，這些信息可能會被存儲和使用，造成隱私風險。
  2. 語言生成風險：ChatGPT可以生成自然語言文本，但可能會生成不當或有害的內容。例如，如果聊天對象要求模型產生令人反感或不當的內容，模型可能會產生此類內容，這樣就會造成風險。
  3. 欺詐風險：使用ChatGPT進行虛假聲明或詐騙是一種風險。模型可以生成與真實文本相似的內容，這可能會被用於詐騙活動。
  4. 安全漏洞風險：如果ChatGPT的軟件實現存在安全漏洞，駭客可能會利用這些漏洞對系統進行攻擊或破壞。
- 總的來說，使用ChatGPT需要仔細考慮資訊安全風險。對於保護個人資料和防止不當用途，必須制定相應的策略和實施相關的安全措施。

ChatGPT App騙取個資盜刷信用卡

資料來源： https://news.pts.org.tw

ChatGPT App騙取個資盜刷信用卡

時間	2023年3月11日
案情	➢ AI聊天機器人ChatGPT從去(2022)年11月推出後，吸引不少民眾使用，也讓詐騙集團發展新的詐騙手法。一旦民眾裝假的ChatGPT APP，裡面隱藏的惡意程式碼會在聊天對話時提供錯誤訊息或做出奇怪回應，也要求使用者填寫信用卡這些資料，目前全台灣已經有20例遭騙。 ➢ 學者表示ChatGPT背後的公司OPEN AI，它的營運模式就是開放了API，也就是應用程式開發介面，讓其他的APP開發商可以去介接它的工具做資訊串接，在這種情況下民眾有很多時候是無從分辨，且App目前在國內並沒有主管機關，因此民眾下載APP前還是得小心查證並參考其他使用者評價，才能避免落入詐騙圈套。
影響	個資外洩、財物損失

資料來源： https://news.pts.org.tw

ChatGPT可能生成電腦病毒！

時間	2023年3月11日
案情	➢ 日本已經有資訊專家發現，人工智慧聊天軟體「ChatGPT」有可能可以生成電腦病毒，呼籲資訊安全界必須注意。 ➢ 專家表示，「ChatGPT」在一般的情況下，是會拒絕生成電腦病毒的指令碼的；不過如果不肖份子，輸入偽裝成開發者的指令，就能夠生成可用於網路犯罪的電腦病毒。 ➢ 日本資安專家「吉川孝志」，就突破了「ChatGPT」「防止惡意使用」的限制，生成了勒索病毒，而且在幾分鐘之內，就能夠完成，相當驚人。
影響	惡意攻擊比例增加、病毒威脅偵測系統恐無法及時發現並阻擋

資料來源： https://today.line.me

個資與資安事件案例分析

國寶高階數位檔案外洩

人為疏失?
制度缺陷?

時間	2022年6月~2023年
案例	➢ 十萬件文物高階圖檔遭駭外流。 ➢ 相關檔案於淘寶網低價販售。 ➢ 2022年6月發現，2023年3月14日補行通報資安事件。 ➢ 承辦人為了加速40萬張6百萬畫素國寶檔案的數位化、盡快達標，求好心切，自己建立一個降檔系統轉換。因為量大在公開系統做作業流程，傳檔過程中引發問題，讓院外的工具軟體擷取到高階圖檔。
影響	● 故宮發律師函要求淘寶網下架商品。 ● 立法委員要求故宮提出相關報告。

資料來源：綜合媒體報導

國寶高階數位檔案外洩(相關報導)

自由藝文 即時 藝起享享 品風格 焦點人物 自由副刊 家庭plus 林榮三文學獎

無心之過比被駭嚴重 立委要求故宮月內提資安報告

2023/03/22 14:21

立院教育文化委員會今（22）日由召委范雲帶隊赴故宮實地考察，院長蕭宗煌親自報告
者凌美雪攝）

〔記者凌美雪／台北報導〕針對故宮近日爆發10萬筆高階圖檔外流事件，立院教育
（22）日由召委范雲帶隊赴故宮實地考察，並就故宮資安防護機制，由故宮進行
件檢討措施及資安防護」說明，以及「圖像調檔系統操作展示」。

對於教文會的實地考察與質詢，故宮院長蕭宗煌開頭即向社會大眾表達歉意，蕭宗
檔外流事件雖是無心之過，但的確造成傷害，故宮已積極展開強化資安訓練、盤點

yahoo! 新聞

新聞眼／故宮喊數位轉型 卻欠基本資安

本報記者陳宛茜

2023年3月15日

故宮十萬件文物高階圖檔遭複製外流，在故宮已非第一次。早在十多年前故宮敲響資安警鐘後，故宮至今沒做任何改善與應變的SOP，連資安人員的培訓、提高危機意識都付諸闕如。故宮多年來多次宣稱要轉型「新故宮」、「數位故宮」，卻連最基本的資安都做不到。

二○一一年，故宮博物院文創行銷處陳姓研究員盜取故宮館藏的「龍藏經」、「富春山居圖」等原檔，送大陸廠商複印後，再以每套十萬元價格轉銷回台。

此事因研究員熟悉故宮授權龍岡公司的複製技術，成立人頭公司將軟體技術轉移給自己，再透過人頭公司接受大陸訂單。這件故宮人「吃裡扒外」的數位國寶偷盜事件當時鬧得驚天動地，如今證明船過水無痕，故宮針對文物數位檔案的複製技術、如何防止宮內人「監守自盜」，沒有任何防範措施。

早在二○○八年，故宮還曾發生一起故宮文物數位影像資料庫的授權風波。當時一間公司協助故宮製作數位影像，條件是與故宮共用智慧財產權五十年。之後該公司將影像授予大陸電視紀錄片使用，遭故宮告上法庭。

一位和故宮合作多年的文創公司負責人說，故宮約在廿年前展開數位之路，但故宮院長沒有一位具數位專業、但也沒打算把故宮的數位化交給專業的人，「故宮數位化」變成為一種好大喜功的口號。

資料來源：綜合媒體報導

航空公司會員個資外洩

人為蓄意?
安全機制不足?

時間	2023年1月
案例	➢ 國外論壇有駭客陸續於1月4日、1月11日對外公布華航會員個資，包含政、商、藝界多位知名人士。 ➢ 疑似資料庫資料外流，華航收到匿名網路勒贖信件。 ➢ 經比對與會員資料庫不盡相同，目前無法確認來源。
影響	● 華航啟動防禦應變機制，報警並依法通報主管機關。 ● 華航通知會員，提醒定期修改密碼，以保障個資安全。 ● 民航局邀集資訊專家對華航進行行政檢查。

資料來源：綜合媒體報導

航空公司會員個資外洩(相關報導)

iThome 新聞 產品&技術 專題 AI Cloud 醫療IT 資安 研討會 社群 IT EXPLAINED 搜尋

國外論壇公開華航會員資料，外洩名單包含賴清德、張忠謀和林志玲

華航會員資料庫遭駭客公開，駭客鼓勵受駭者應該委由消基會提出集體訴訟向華航求償；華航表示全力配合警方調查，呼籲會員定期修改密碼

文/ 黃彥棻 | 2023-01-13 發表

讚 615 分享

A member database from China Airlines (in Taiwan)

by iamtrump - Wednesday January 11, 2023 at 10:32 AM

iamtrump

BreachForums User

MEMBER

Posts: 1
Threads: 1
Joined: Jan 2023
Reputation: 0

Here is the example of data. There are 10 celebrities and politicians contact information.
(The data of another 50 celebrities will be announced next time)
These data come from the member database of China Airlines, including more than 3 million membership data. Most celebrities in Taiwan are their members.
They already knew on Jan. 4, 2023 that the data of 60 people would be released here on Jan. 11, 2023, but they did not make any response .

Hidden Content

member_id,chinese_name,birthday,email,english_name,country_code,phone_number

國外論壇揭露外洩的華航會員資料庫名單，有許多政界、商界和明星的中英文姓名、出生年月日、[illegible]羅一鈞、張忠謀、郭台銘、蔡明忠、蔡明介、王文淵、周玉蔻、謝震武、陳文茜、趙少康、徐熙娣遭到駭客揭露。

iThome IT EXPLAINED WEBINAR 數位轉型攻略

CYBERSEC 2023 臺灣資安大會 5.9 - 5.11 臺北南港展覽二館

ORGANIZED BY iThome

年度資安大展 300+資安品牌 | 資安主題論壇 250+專業議程 | 資安專家演說 國際級資安大師 | CyberLAB 實戰演練攻防戰

個資外洩又一遭。在國外論壇中，[illegible]客同樣以擠牙膏的方式，先後於今[illegible]和50筆，總計60筆包括臺灣知名[illegible]的資料，外洩資料除了華航的會員

自由時報 Liberty Times Net

即時 熱門 政治 軍武 社會 生活 健康 國際 地方 蒐奇 影音 財經 娛樂 體育 3C 評論 藝文 玩咖 食譜 地產 專區 TAIPEI TIMES 求職

更新時間 19:22 新增民航局回應

〔記者鄭瑋奇 / 台北報導〕國外論壇有駭客陸續於1月4日、1月11日對外公布華航會員個資，包含副總統賴清德、台積電創辦人張忠謀、交通部長王國材、外交部長吳釗燮、藝人林志玲、徐若瑄等多位知名政、商界和明星。中華航空表示，近日收到匿名網路勒贖信件後，清查確認疑似外流個資與華航公司資料庫不盡相符，尚無法確認來源，將全力配合警方調查。

中華航空在1月7日已對外說明有收到匿名網路勒贖信件，並第一時間啟動防禦應變措施，報警及依法通報主管機關，同時確認各項資通系統作業正常，未影響航班營運，也無會員資料遭不當使用事件產生；另譴責非法行為，並提醒華夏會員定期修改密碼，以保障個資安全。

不過疑似因為華航並不承認有個資外流引發駭客不滿，持續公布疑似華航會員的個資。華航今日表示，針對近日收到匿名網路勒贖信件，華航已清查確認，疑似外流個資與本公司資料庫不盡相符，尚無法確認來源；華航在接獲匿名網路勒贖信件後，已立即報警及依法通報主管機關，並在第一時間有效採取防禦應變措施，確認各項資通系統作業正常，也配合警方追查事件及釐清原因，並全面性檢視系統安全，確保資安防護，未來將持續嚴格落實個資保護，強化資訊安全。

資料來源：iThome、自由時報

IM.B詐騙事件

社會 時事

imB假債權吸金飆破50億、恐上萬人受害　3處「秘密基地」未曝光！警追查中

記者：社會組｜ 2023-05-16 16:44

imB詐騙 | 秘密基地 | 詐騙 | 宜蘭

警方在宜蘭一處別墅內逮捕曾男和其女友，在屋內發現由40個盒子堆成的「愛馬仕牆」，正深入追查其他秘密基地。（圖／資料照片）

A+ A-

「imB」假債權吸金詐騙案，刑事局本月3日逮捕負責人50歲曾男及其張姓女友後，新聞曝光財損金額不斷飆升，上看50億元，受害人數恐怕逾萬人。誇張的是，曾男原本住在桃園，爆出詐騙案後他跑路到宜蘭，入住友人別墅落網，警方在別墅內查獲「一整牆」愛馬仕和香奈兒，以及數十箱紅酒、洋酒，據了解曾男「狡兔好幾窟」，至少還有3處秘密基地，如同宜蘭別墅藏有名牌包、高價物品，警方正循線追查中。

警方表示，民眾若有資金需求，大多數會向銀行借錢，但有些人可能因信用瑕疵無法向銀行借錢，im即為此類P2P媒合平台，以個人對個人方式，讓有資金需求者透過平台找到願意借錢者，平台賺取手續費、借錢者賺取利息。打著「土地作抵押品」、風險較低，許多受害者因而上鉤決定投資，由於平台年化報酬率約9至12%，1名受害人在臉書「當沖勒戒所」PO文，一開始每個月爽領快13萬，領了兩個月後，投資的1500萬全部打水漂，才驚覺遭詐騙。

真相究竟為何？
讓我們繼續看下去...

個資法修法三讀通過

- 112年5月16日三讀通過。
- 業者若未善盡安全維護義務以致個資外洩，罰鍰將提高至2萬～200萬元，情節重大者、屆期未改正者的罰鍰更高達15萬～1,500萬元。
- 由個人資料保護委員會擔任個資法主管機關。

社群網路常見詐騙伎倆

臉書、IG退流行了？

- 《READr讀+》於2020年12月30日至2021年4月26日針對學生族群社交軟體喜好的調查結果
  - 國高中生最愛的前三名：IG、FB與TikTok，小紅書排第6名。
  - 大學生最愛：IG、FB與Dcard，小紅書排名第10。
- 根據2022年Google Play熱門免費項目排行
  - 小紅書囊括「社交」類與「所有類別」的冠軍
  - 其他熱門社交App分別為Twitter排名第5、Instagram排名第6、Facebook排名第9，「TikTok」是「影音播放與編輯」類的第一名，「所有類別」排名第11。
- 有網友擔心會有文化統戰的問題，但也有人認為，小紅書相當實用，資訊的完整度勝過IG。

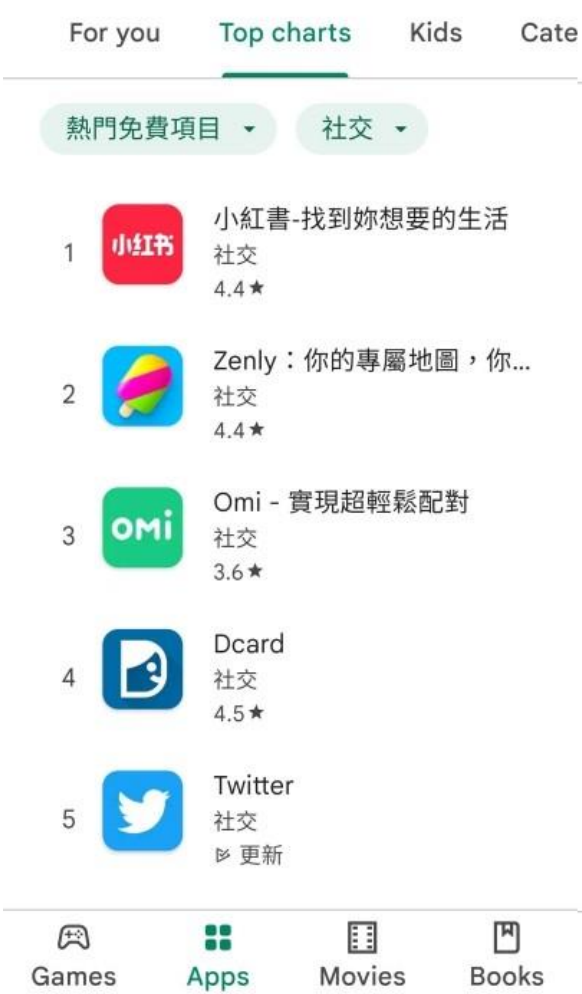
資料來源：風傳媒

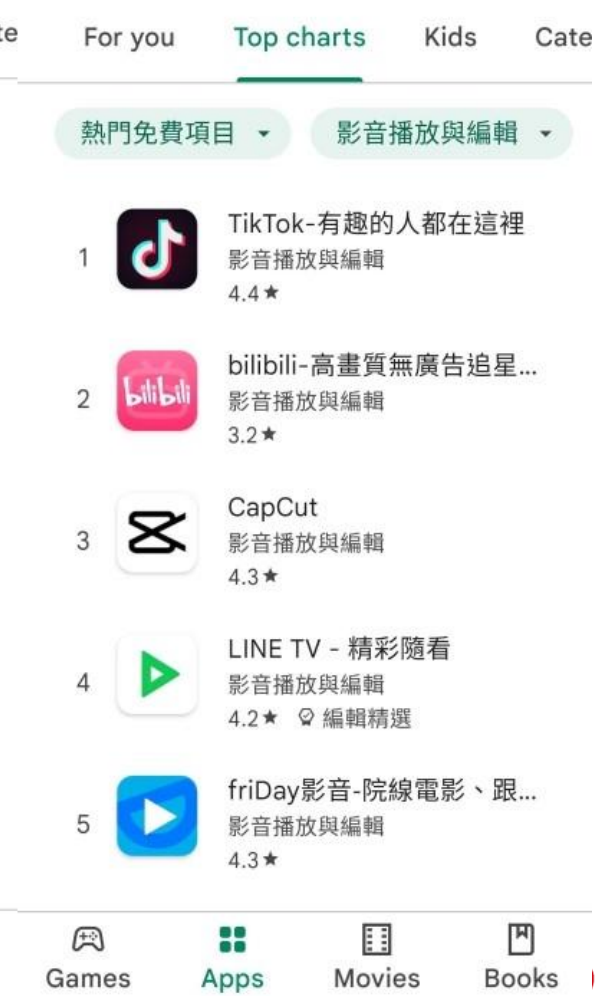
台灣年輕人間爆紅的「小紅書」是什麼？

- 「小紅書」是中國知名的「網路購物」和「社交APP」，人稱「中國版的IG」。電商可PO文，一般人也能分享「好物」。
- 操作與IG差不多，可發文(小紅書稱為筆記)、限時動態(小紅書稱發佈瞬間)、介面也是圖片影音為主，亦有按讚、分享、留言等基本社群功能。
- 可分享美妝、穿搭；也能紀錄生活大小事。可透過「標籤」將自己包裝成網紅。
- 小紅書是中國時下少女追蹤流行資訊必備的搜尋平台。
- 不少人把小紅書當成Google、百度等搜尋引擎。
- 購物或潮流相關問題都先使用小紅書搜尋，或直接使用APP內的「商城」購買商品。
- 台灣00後妹子笑「IG是老阿姨玩的」！
- 很多年輕人都改用小紅書。

資料來源：風傳媒

小紅書、TikTok 排行





資料來源：風傳媒 https://www.storm.mg/lifestyle/4195441

「小紅書」爆紅原因？與IG的差異？

- 小紅書的功能與Instagram相似，例如：
  - 以圖和影音為主的介面呈現
  - 發佈瞬間豐富濾鏡(類似IG story)
  - 發文私訊按讚分享等社群功能
- 與Instagram的差異是：
  - 新註冊用戶可依興趣選擇喜好內容
  - 推薦貼文不侷限單一主題，能自動延伸相似內容
  - 演算法自動推送貼文至手機通知
  - 內建熱門音樂庫、精美影集模板，讓用戶直接套用
  - 以「教程」為主的影片內容，網紅專家一分鐘內「包教包會」

資料來源：風傳媒

「小紅書」畫面範例

資料來源：風傳媒 https://www.storm.mg/lifestyle/3443657

網路上的假訊息

定義	以不實資訊誤導大眾，以帶來政治、經濟、市場、或心理得到成就感和利益的新聞或宣傳，包括通過傳統新聞媒體（印刷和廣播）或線上社群媒體傳播的故意錯誤資訊或惡作劇。
目的	➢ 造成恐慌 ➢ 扭曲事實或掩蓋真相 ➢ 牟取利益(經濟、政治) ➢ 帶風向

是她還是他？

- 利用繪圖軟體的合成功能與網路的匿名性及無限想像空間，網紅圈粉、有心人士進行詐騙與犯罪行為。

資料、圖片來源：奇摩新聞

你以為的 vs 實際上的

圖片來源： 木棉花 、天下雜誌

假消息的特徵

- 太過於誇張、聳動、讓人不禁想點擊的標題，都有可能是惡意的「點擊誘餌」。
- 網址很可疑，魚目混珠。
- 新聞內容出現許多錯字或網站版面編排不正常。
- 很多明顯經過刻意修圖的照片或圖片。
- 沒有附註發布日期。
- 未註明作者、消息來源或相關資料。

如何避免成為假消息的受害者與傳播者

- 提高警覺：不輕信令人嘩然的圖片或文章。
- 查證訊息來源：判斷新聞的可信度。
- 不要只看標題：可能文不對題，要看完內文。
- 留意評論：參考讀者留言以釐清謬誤。
- 注意日期：檢查報導日期，是否舊聞新推。
- 搜尋相片：利用Google圖片搜尋，看看是否舊圖亂用，或文圖不符。
- 有片未必有真相：要判斷片段前後發生甚麼事。
- 調查及統計數據要細心讀：避免統計誤植。
- 小心斷章取義：要審視邏輯，有無扭曲。

訊息辯真偽

收到可疑訊息(新聞、郵件、簡訊...等)，可至『Cofacts 真的假的』網站查詢訊息的真偽。

- **網址**：https://cofacts.tw/
- **Facebook**：https://zh-tw.facebook.com/cofacts.tw/

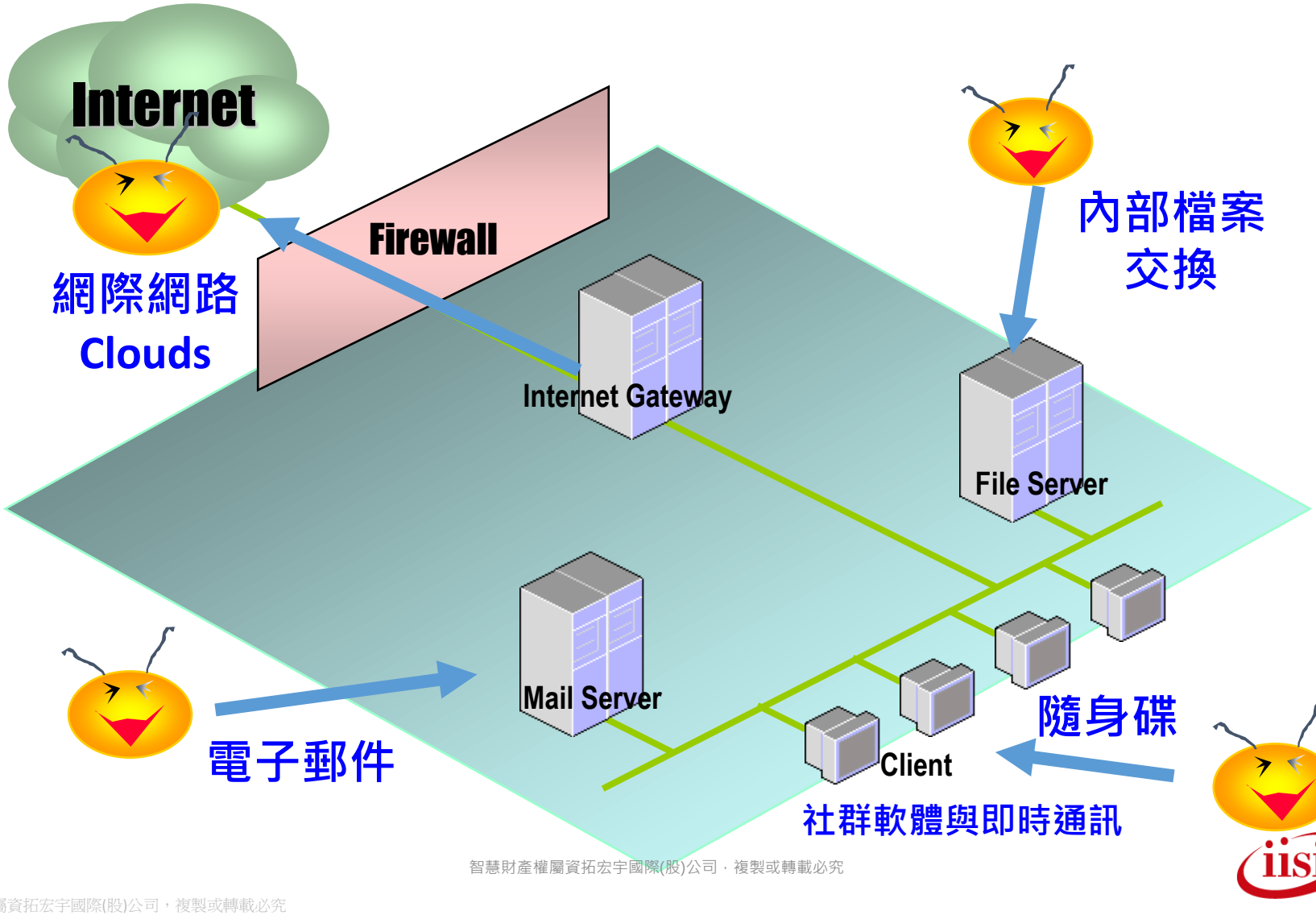
社交工程與網路釣魚

- **網路釣魚(Phishing)**是網路上常見的社交工程
  - 請求某種動作：執行檔案、點選連結、觀看影片，甚至是程式自動執行的功能，如郵件預覽、Script。
  - 在執行某種動作後，受害者的電腦可能就此被操縱，然後再繼續攻擊其它的電腦。
  - 智慧型手機、平板電腦等行動裝置案例愈來愈多
- **詐騙管道**
  - 電子郵件
  - 社群軟體
  - 即時通訊

惡意程式與假消息散播管道

- 社群軟體
  - 如：Line、FB、IG 等軟體使用, 由於使用者眾多, 特別適合利用此平台來散佈病毒與假消息。
- E-mail
  - 開啟了含有病毒的 E-mail 附加檔, 就會中毒。為了避免中毒, 建議您不要隨意開啟 E-mail 裡的附件檔, 甚至是連結的網址。
  - 病毒利用自動散佈病毒信給通訊錄名單中的人, 每一次有人中毒再轉寄此信時, 就會變更新的信件主題和內文。
- 網頁瀏覽與下載檔案
  - 病毒隨著網頁、下載的檔案傳播。特別容易被植入像是木馬程式, 以致個人電腦中的資料被竊取或遺失。
- 儲存媒體
  - 如光碟片、隨身碟等, 只要執行或開啟儲存媒體中的檔案, 病毒便會感染其他的程式, 或常駐在電腦中。
- 內部網路的資料交換
  - 利用一般企業、公司、政府機構、學校、研究單位、軍事單位所架設的區域網路來傳播病毒。

我們的資料保護有哪些破口？



智慧財產權屬資拓宏宇國際(股)公司，複製或轉載必究

社交工程的類型

- 面對面
  - 蒐集資訊或進行各種詐術
  - 金光黨
- 電話詐騙
  - 電信詐騙集團
- 電子傳訊管道
  - 網路詐騙或網路釣魚(Phishing)
  - Email/Line/Skype/QR code/Facebook

常見的網路社交工程手法

- 常見的詐騙與攻擊手法：
  - 假冒為同事或新進員工
  - 假冒廠商、客戶或政府單位
  - 假冒具有權威的人
  - 假冒系統廠商，表示欲提供系統修補程式或更新程式
  - 假冒好心人士，告訴對方如果電腦發生問題可以找他，然後製造問題，讓受害人打電話來求援...等。
  - 使用流行或特定關心的議題
- 社交工程攻擊常鎖定的目標：
  - 一般人員
  - 新進員工或特定業務人員

都有一個假網址

社交工程郵件與訊息的特徵

1. 非正常的發信時間或是認識的人來信但主旨或內容與其習性不符，這時候都應該要提高警覺。
2. 陌生寄件者郵件: 因為此類信件就有可能是偽冒寄件者之偽造的電子郵件(有時會冒充公務機關、微軟、Google等具知名度名稱寄信者，要特別注意)。
3. 來信郵件多包含惡意圖片、連結及附件檔案，檔案格式為ZIP、PDF、EXE、BAT、XLS、DOC等要特別小心。

社群網路安全使用守則

社群軟體安全最佳守則

- 啟用多重因子身分驗證(MFA)。
- 不要在不同平台使用相同密碼。
- 定期更新各平台的安全設定。
- 縮小您的朋友圈範圍以減少未知威脅。
- 關注社群媒體的安全風險。
- 瞭解網路釣魚攻擊的模式。
- 留意您帳戶內的假冒行為。

資料來源：Fortinet https://www.fortinet.com/blog/industry-trends/7-best-practices-for-social-media-security-and-privacy

多重身份驗證

- 多重身份驗證(Multi-Factor Authentication，MFA）需要成功驗證下列3種中的2種身分證明。
- **1.你知道的事物Something you know：知識型驗證**

  它可以是一個密碼、預設的安全問題、或圖形的形式出現，基本上它通常是個「知識因素(knowledge factor)」。
- **2.你持有的事物Something you have：權杖型驗證**

  這可以是一個小型的硬體設備，例如智慧晶片卡或是智慧型手機token。它們能產生獨特的一次性密碼，通常是由使用者手機上的應用程式所產生或被傳送過來的；這種驗證方法被認為是「持有因素 (possession factor)」。

- **3.你本身的特徵Something you are：生物特徵辨識為基礎的驗證**

  這通常需要一個生物特徵辨識器，用來偵測某一個人擁有的身體特徵，例如指紋、虹膜、臉孔、掌紋、筆跡或是聲音。這類的驗證因素定義為「與生擁有因素 (inherence factor)」。

為何要多重驗證?

- 單因素驗證已經過時
  - 密碼容易破解：精巧的密碼破解工具與無比強大的處理器
  - 雲端密碼破解服務（分散式電腦運算的Cloud Cracker）：嘗試300萬次的密碼破解只需不到20分鐘
  - 只要有時間和運算資源，沒有任何一種加密方法是絕對安全的
- 持有因素(智慧晶片卡，手機或硬體token)：
  - 優點：比密碼安全，不易破解
  - 缺點：登入時必須持有，可能遺失
- 與生擁有的因素(生物特徵)
  - 優點：不用記密碼，不用持有物件
  - 缺點：樣本檔損毀或辨識設備精準度不夠

行動載具優缺點

- 透過手機驗證的缺點：
  - 必須手機不離身，否則會有登入麻煩
  - 手機遺失、遭竊或毀損，將導致無法登入
- 透過手機驗證的優點：
  - 提供密碼之外的第二道防線
  - 結合手機生物辨識技術，達多重(3重)驗證之安全性

Google Authenticator

- 進入gmail登入畫面，輸入密碼。(如圖1)
- 打開手機的Google Authenticator 驗證器App，查看驗證碼。(如圖2)
- 將手機顯示的驗證碼輸入gmail兩步驟驗證畫面後，按〔驗證〕登入信箱

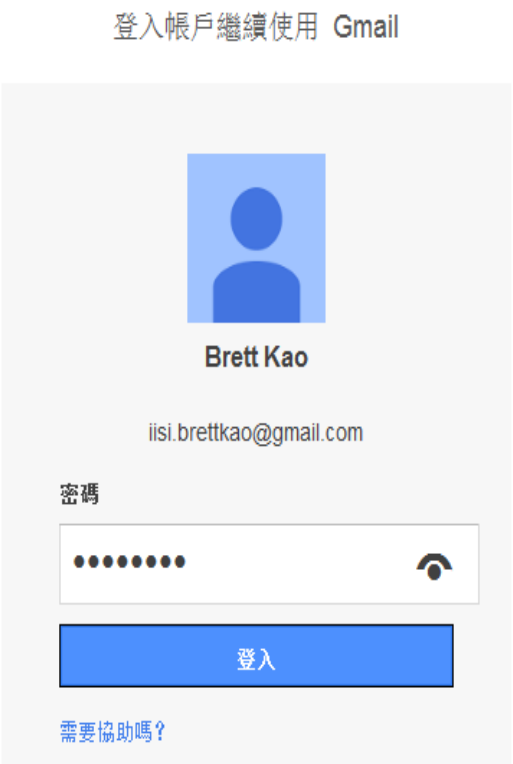


圖1

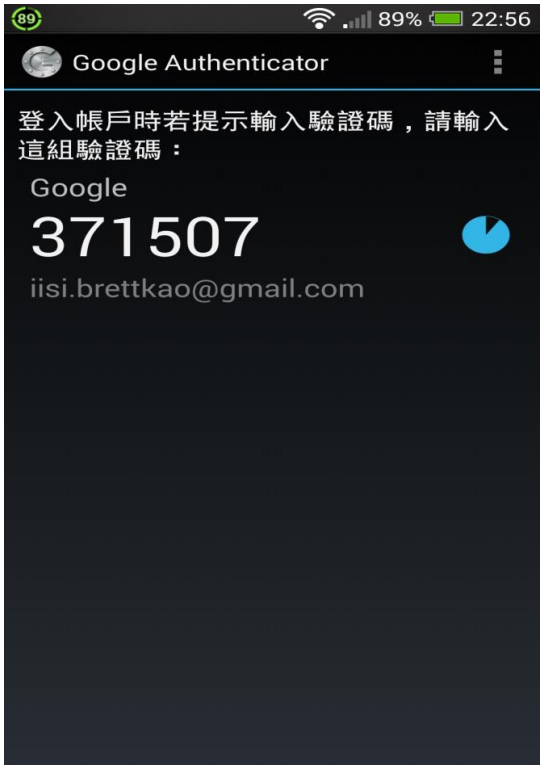


圖2

注意社群軟體的安全設定

Advice from social media platforms

The following guidance is provided by each of the major social media platforms. Click to read detailed information.

- **Facebook**
  Basic privacy settings and tools
- **Twitter**
  How to protect and unprotect your Tweets
- **YouTube**
  Privacy and safety
- **Instagram**
  Privacy settings and information
- **LinkedIn**
  Account and privacy settings overview
- **Snapchat**
  Privacy settings
- **Tiktok**
  Privacy and security settings

資料來源:https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely

社交工程訊息之防範方式—提高警覺

- Q:為何我會收到這封郵件或訊息?
  - 寄件人不認識就不要開啟
- Q:我是否應該收到這封郵件或訊息?
  - 與業務或本身職務無關主旨不要開啟
  - 信件主旨雖與業務有關，但寄件者郵件非公務信箱
- Q:我是否應該開啟這封郵件或訊息?
  - 與業務或本身職務無關
  - 不隨意點選郵件超連結

個人資料安全風險

為什麼一打噴嚏，臉書就出現感冒藥廣告？

- 「我可以試穿這雙nike的7號鞋嗎？」一名顧客問店員。
  - 當晚，臉書就跳出nike的廣告。好，這可能是巧合。
- 「現在市面上最好的體重計是什麼？」一位妻子問他的老公。
  - 5分後，Instagram就出現多款體重計的廣告。
- 「吃點感冒藥吧。」兒子一打噴嚏，媽媽忍不住叮嚀。
  - 當天下午，社群網站跑出什麼廣告，就是感冒藥！

- **我們都被監聽了嗎？**

原文出處：天下雜誌

特定廣告為什麼找上你

廣告商會依據興趣、年齡和地點等因素來定義觸及對象。

我們會向最可能對其商品、服務和公益活動感興趣的用戶顯示廣告。

當廣告商的目標受眾是……

附近的自行車愛好者

- 18 - 35歲
- 女性
- 我商店的20 英里範圍內
- 對騎自行車感興趣
- 手機用戶

我們會向以下用戶顯示廣告……

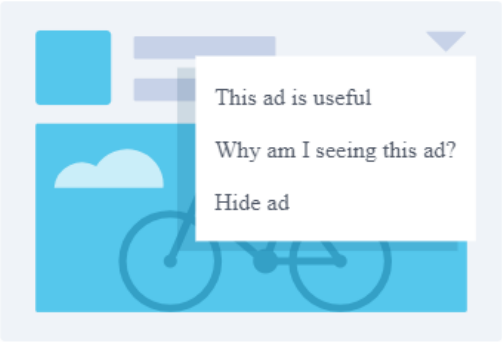
Elena

- 30歲
- 女性
- Menlo Park, CA
- 對騎自行車電影、烹飪有興趣
- iPhone 用戶購車者、玩家

如何自行控制看到的廣告

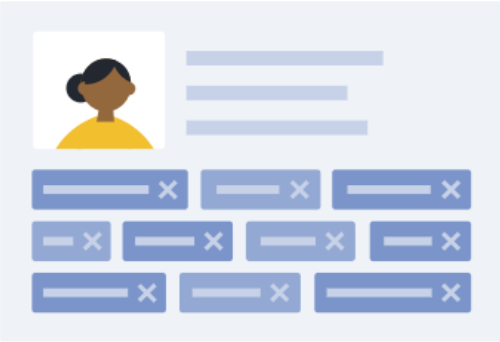
更能夠控制你看到的廣告

你可以審核並編輯廣告偏好設定，以控制你看到的廣告。



直接從廣告提供意見回饋

瞭解詳情



查看並縮小廣告範圍

管理廣告偏好設定

檢查並調整廣告設定

管理廣告設定

Facebook廣告偏好設定

如何避免隱私被蒐集?

- **如果不想被追蹤該怎麼辦？**
  - 放棄在任何商家集點數，放棄成為會員。
  - 用一組與臉書帳號全然不同的email與電話號碼去註冊會員。
- **比購買資料更值錢的是...?**
  - 就是**你的位置資訊**
  - 你到過一家商店，廣告就會提醒你別忘再度光臨。
  - 某一家店就在你附近？優惠券就會跳出來吸引你。
  - 想要限制臉書探查你的位置，臉書APP裡的帳號設定>地點>接著關閉定位服務與紀錄。
- **臉書還用這個方式了解你**
  - **臉書也透過網頁瀏覽歷程了解你**。數百萬個網站和應用程式目前都裝了Facebook Pixel，讓廣告商和臉書摸透你都在網路上幹什麼。這就是為什麼你上了屈臣氏官網後，就會在臉書上看到屈臣氏廣告。Facebook Pixel甚至連你看了什麼產品和文章都知道。
  - 如果想擺脫，可以到**帳號設定>廣告>廣告設定>關閉「依據我使用的網站和應用程式顯示廣告」**。
- **即便你關閉這些設定，也不會改變你看到廣告的數量，但能因此加強網路個資隱私的關聯性與保護。**

原文出處：天下雜誌

減少個資外洩風險(1)

- **刪除個人資料**
  - 許多臉書使用者都知道，編輯頁面資訊容易找到相關同好，例如：你曾經就讀哪個學校？你喜歡哪些品牌與粉絲專頁？這些資訊都可能透過臉書自動登入功能或者第三方應用程式取得。

- **限制分享對象**
  - 禁止臉書以外的搜尋引擎連結到個人資料，讓陌生人無法輕易在網路上搜尋到。

原文出處：聯合新聞網

減少個資外洩風險(2)

- **不要玩心理測驗或遊戲**
  - 很多時候常常會接到一些來路不明的遊戲或心理測驗的邀請，千萬不要傻傻的隨意點選，因為它通常都會蒐集你的個資，尤其是看到臉書的提醒「XXX想取得以下的資訊」時，更是要警覺。

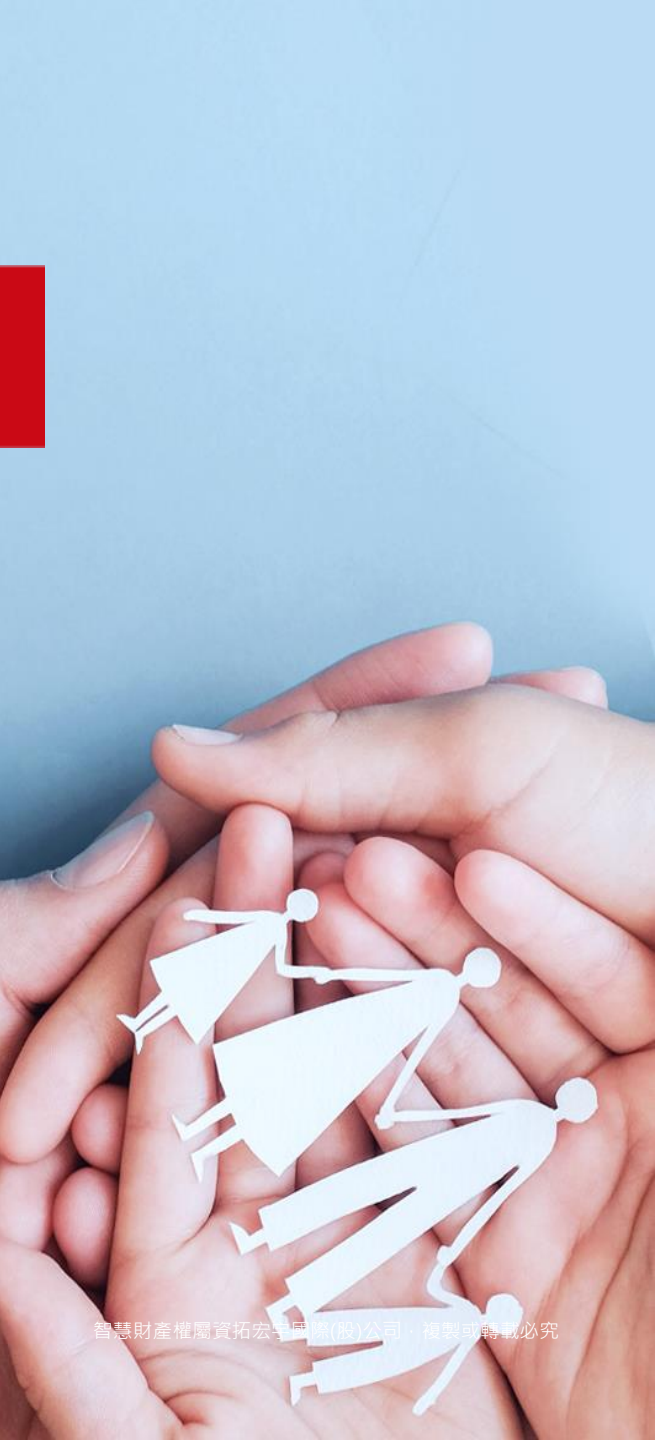
- **限制廣告偏好**
  - 避免一些不必要的騷擾。最好的方法就是在「廣告設定」的欄位拒絕臉書針對用戶興趣顯示廣告，讓廣告商無法獲取個資。

原文出處：聯合新聞網

減少個資外洩風險(3)

- **解除可疑的第三方應用程式連結**
  - 人們常常不經意授權一些應用程式（APP）使用臉書資訊，但你知道有時候貪圖這些方便，就有個資外洩的風險。請適時刪除一些不必要或根本沒在使用的應用程式，防止被他人不當利用。

原文出處：聯合新聞網



總結

時時警覺可保安全無虞

- 使用資通設備須注意安全，避免個資外洩。
- 發現問題應依循組織紀律與程序處理，切勿隱瞞。
- 作業系統與應用軟體應注意更新與防毒。
- 妥善保護自己與他人的個資以增加防禦力。
- 資通安全，人人有責。

智慧財產權屬資拓宏宇國際(股)公司，複製或轉載必究

- 敬請指教 -

資拓宏宇國際股份有限公司
International Integrated Systems, Inc.
公司總部：22041 新北市板橋區縣民大道二段7號6樓
電話：(02)8969-1969　　傳真：(02)8969-3359