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

當今數位資訊，
AI取代你了嗎？

演講日期：113年06月21日

演　講　人：譚升翔

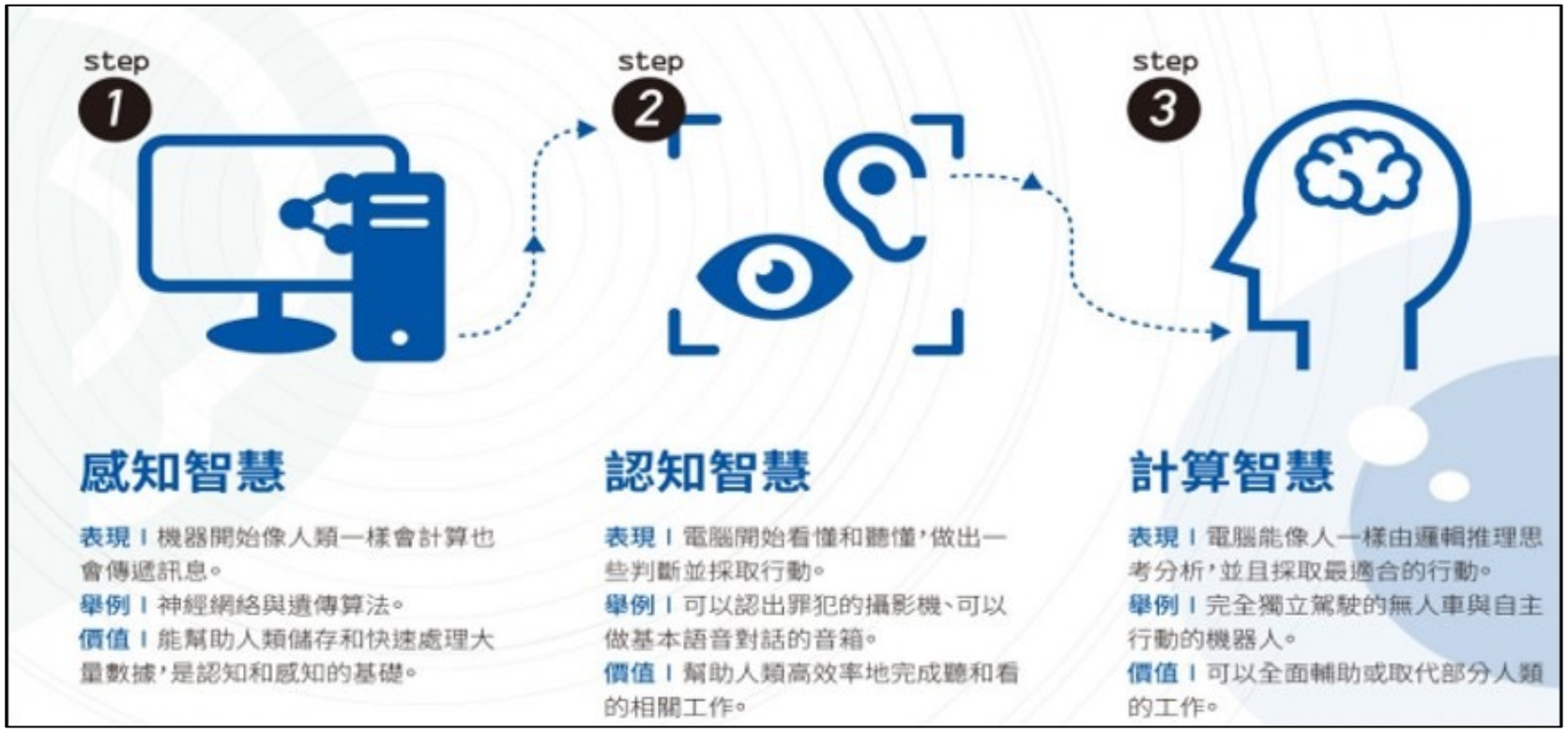
大綱

1. AI如何自動化與智能化
2. AI創新生活型態和商業模式
3. AI的影響與威脅
4. 預防重於治療
5. 社交工程須知

AI如何自動化與智能化

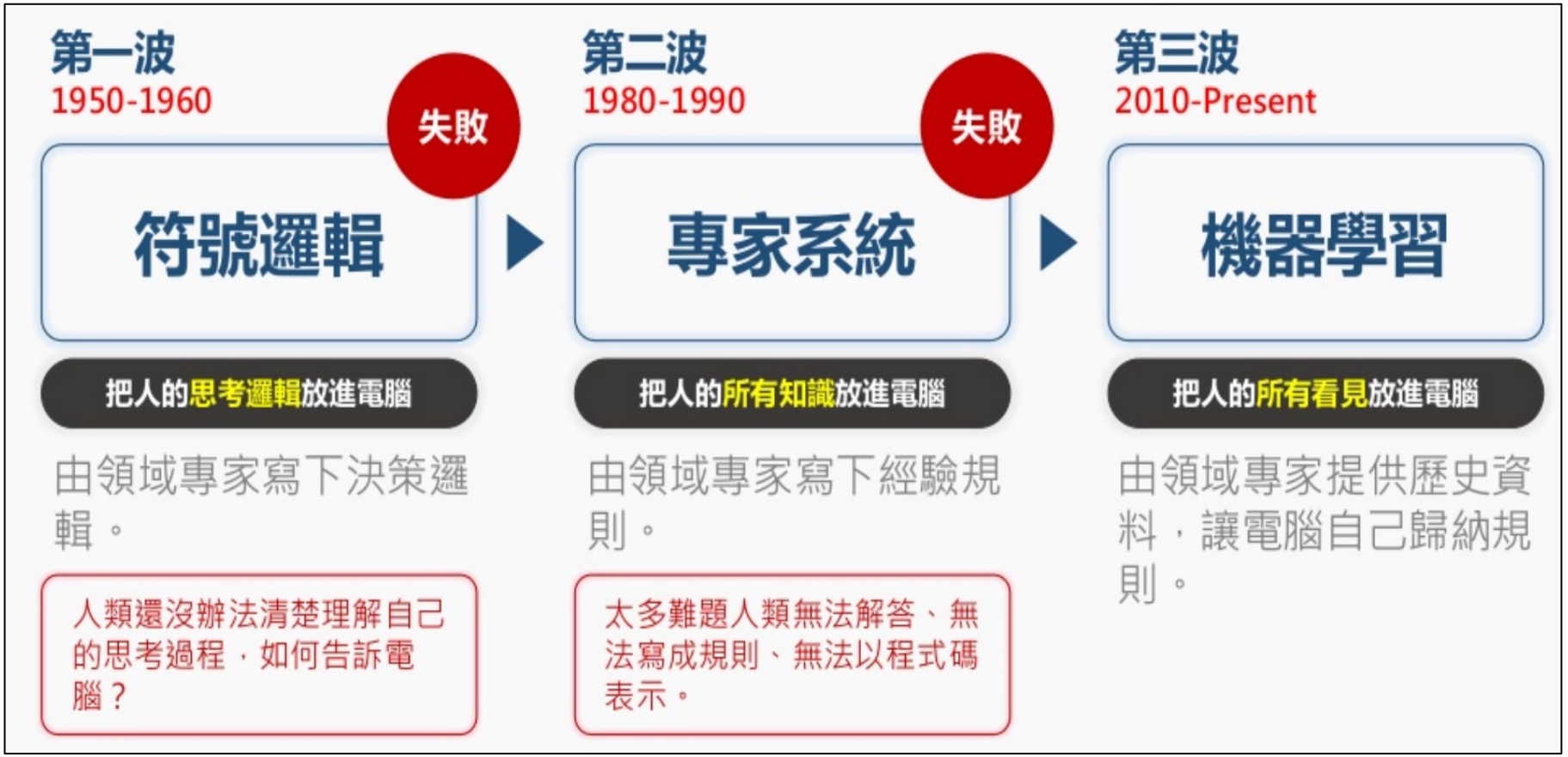
人工智慧發展階段

- **人工智慧**（Artificial Intelligence；縮寫：AI），是指以人工方式來實現人類所具有之智慧的技術。



資料來源：數位時代

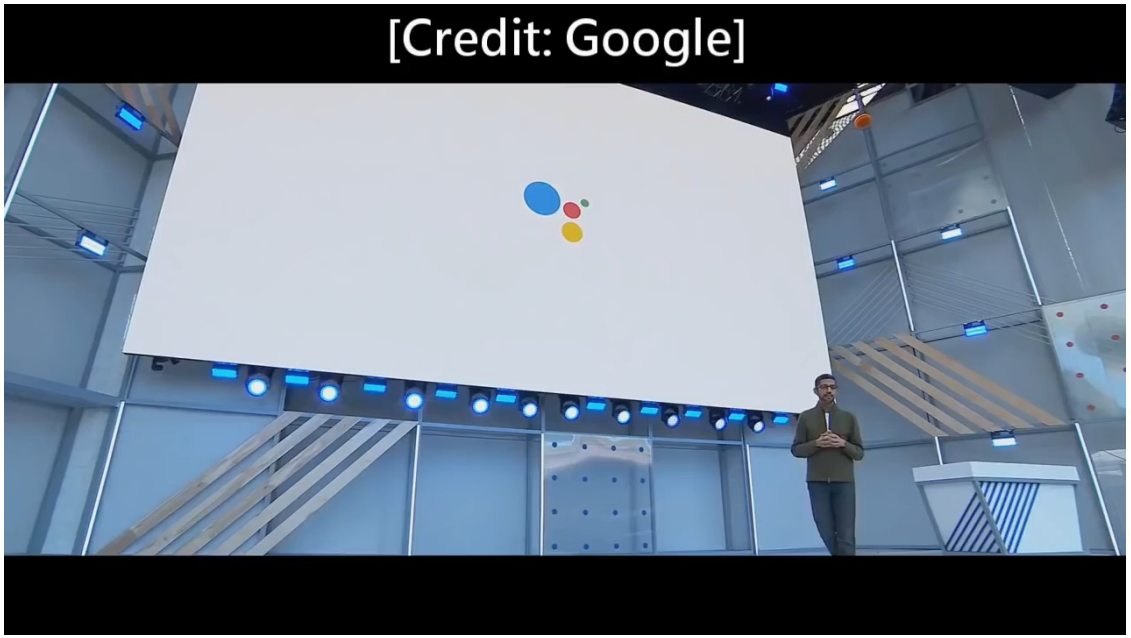
人工智慧發展簡史



資料來源：「人工智慧在台灣」

正逐步實現的人工智慧

- 機器人公民
  - 2017年10月，索菲亞成為沙烏地阿拉伯公民，這是世界上第一個獲得國籍的機器人。
- Google 語音助理進化



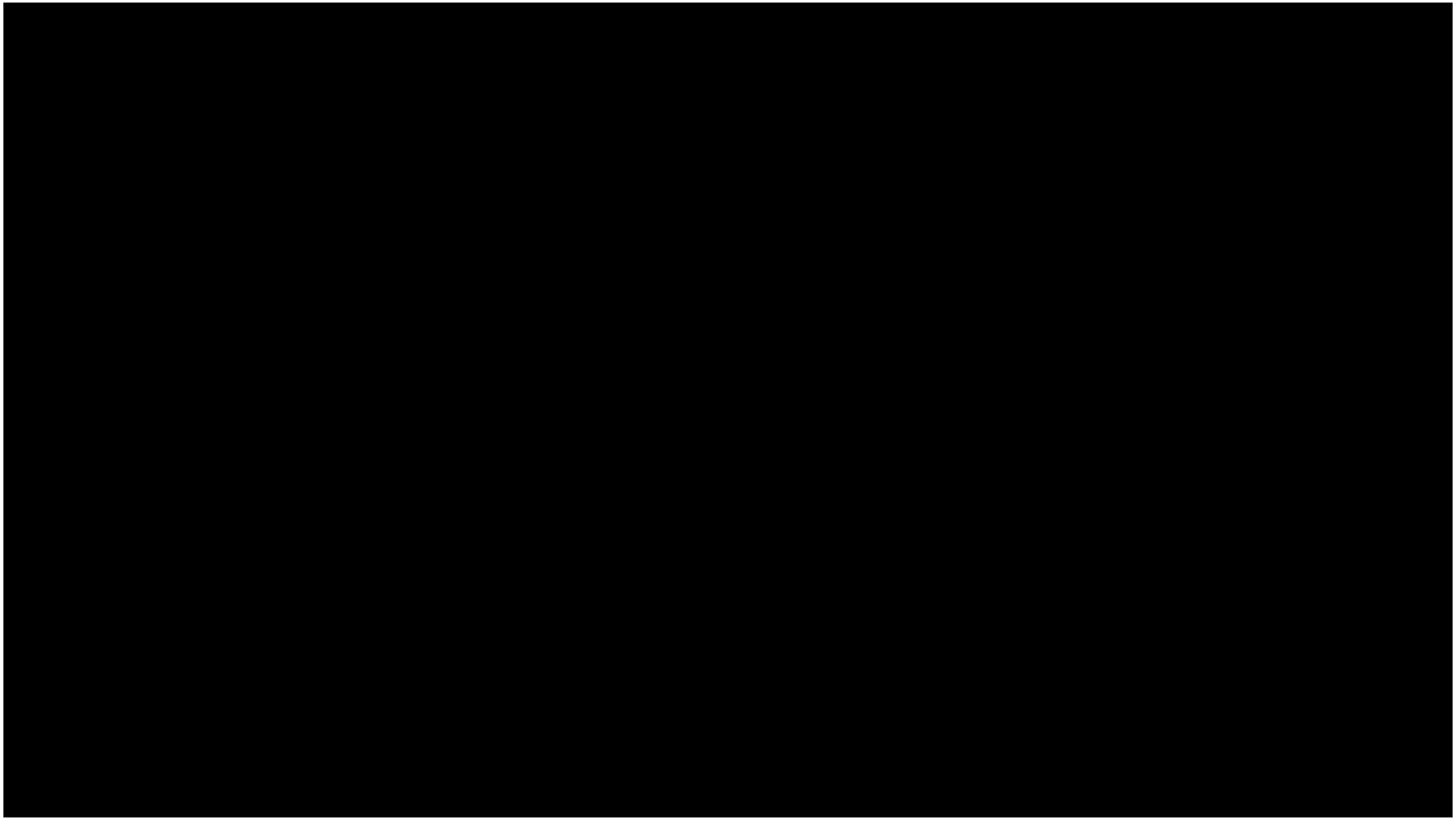
資料來源：數位時代 影片來源：https://youtu.be/007WVm2-1qQ

人工智慧的實際應用-資訊安全

- 現在的垃圾郵件發送者越來越精明，並且已經從純文字訊息演變成使用附件檔或其他作法。
- 讓機器能夠學習去識別和封鎖垃圾郵件
- 啟用機器學習的防禦措施可以經由每封新垃圾郵件來更加了解當前的垃圾郵件流程和方法。
- 結合了機器學習及其他保護技術，研究人員發現可以有效地識別並封鎖95%的垃圾郵件。

AI創新生活型態和商業模式

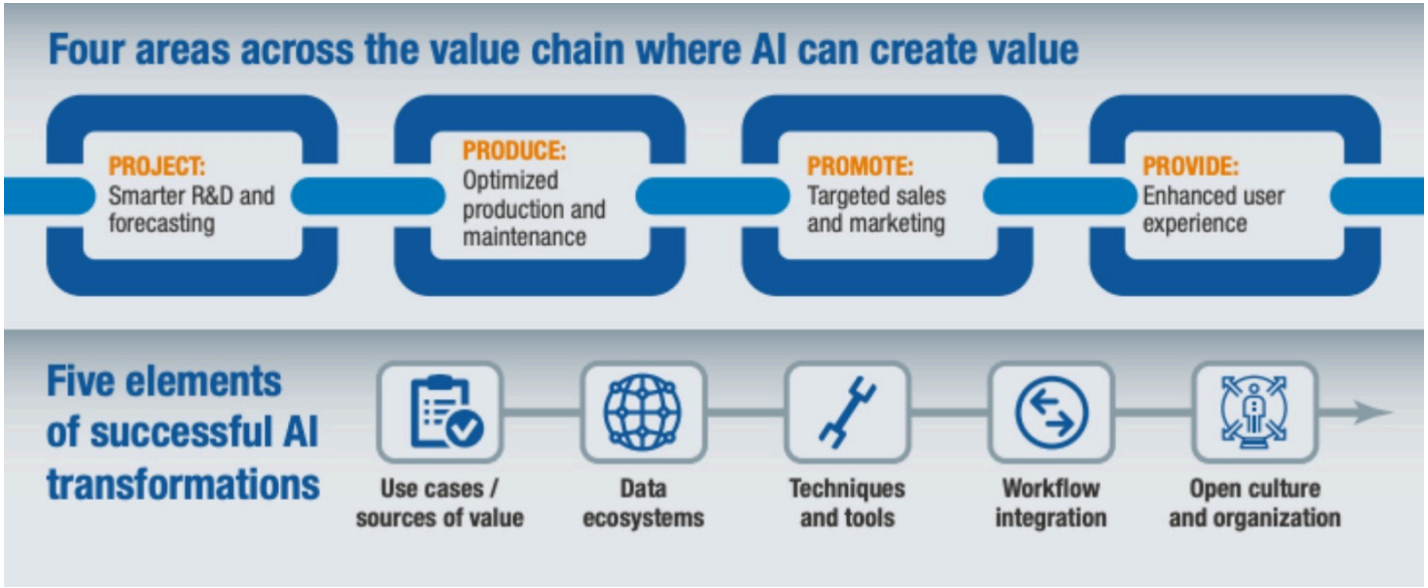
西元2030年時



資料來源：Youtube https://www.youtube.com/watch?v=1Gt2KY_9B9k&t=94s

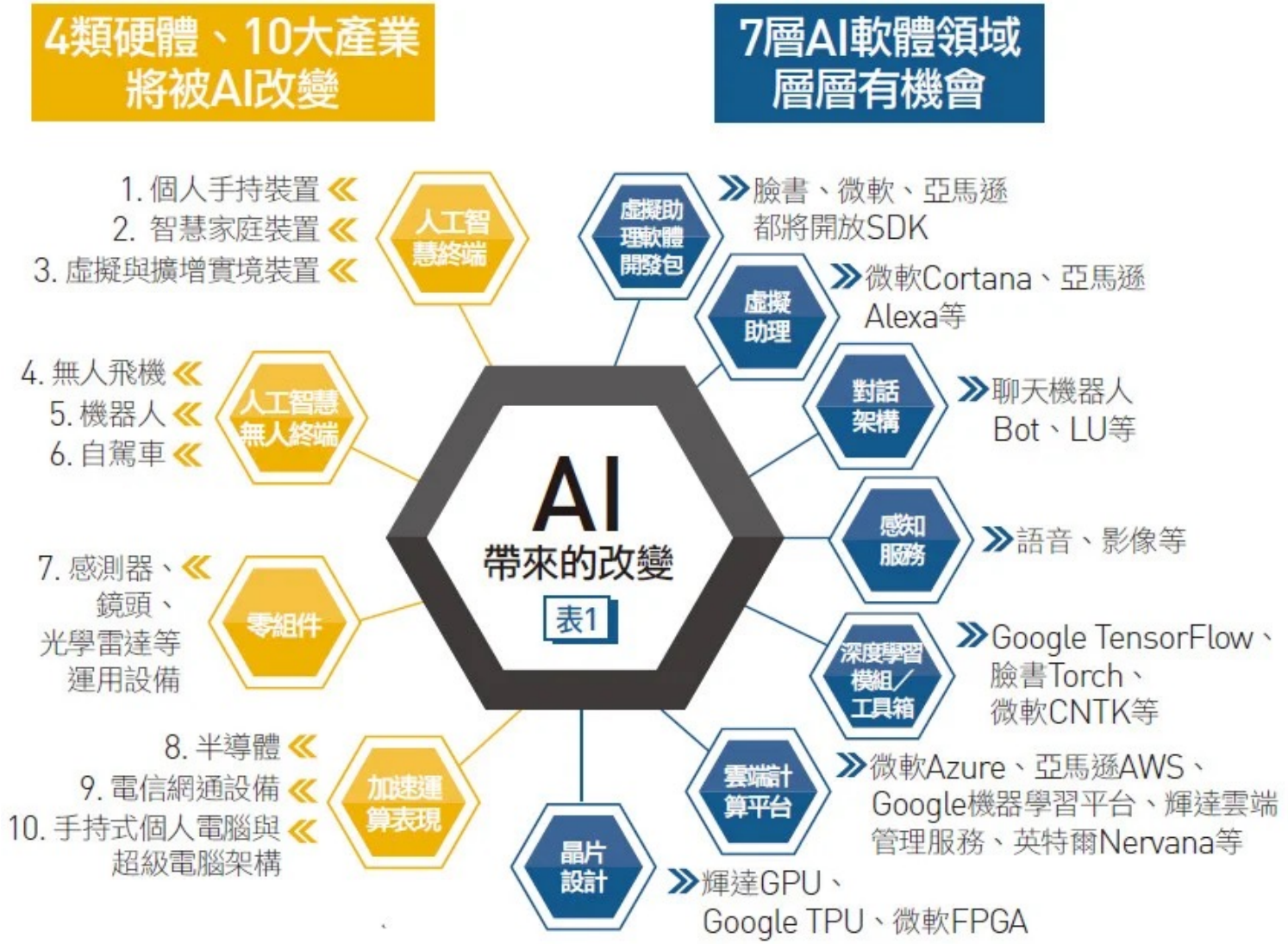
人工智慧AI有哪些應用？

- 2017年，管理顧問公司麥肯錫（McKinsey & Company）將人工智慧的應用場景分成四大面向：
- Project（計畫）：準確地預測與規劃，完成最佳生產計畫。
- Produce（生產）：維持高品質、高效率的生產流程。
- Promote（行銷）：精準目標銷售與市場分析。
- Provide（供給）：提高客戶滿意度，帶動永續經營。



資料來源：https://futurecity.cw.com.tw/article/2228

AI發展帶來產業的重大改變



資料來源：【天下雜誌-封面故事】AI全面啟動-台灣不能錯過的第四次工業革命

人工智慧AI應用

應用	說明
醫療	AI科技在醫療健康產業中，已開始協助臨床決策、疾病判斷，進一步跨入預防醫學、精準醫療等領域；除了**減少醫護工作負擔、降低出錯率**，也克服人類無法解決的醫療挑戰。
交通	台灣交通的人工智慧應用，已發展到**自駕車、車流計算、路況安全預警、路網優化**等領域。
生活	生活中，常見智慧音箱及**手機AI助理運用的語音辨識功能**；Netflix、**YouTube為你推薦的影音演算法**；AI客服辨識客戶想法，提出個人化回覆……AI人工智慧應用早已無所不在，持續為你改善生活品質。
能源科技	將太陽能產生的電力用在校園用電，配合蓄電池與電動車充電樁設備，讓校園具備削峰填谷，調節尖峰用電的能力。**經過AI演算法調校，成功協助校園降低尖峰用電約30%的用電量，拓展綠電自發自用的可能性。**

資料來源： https://futurecity.cw.com.tw/article/2228

智慧醫療-AI一秒判讀新冠肺炎X光

- 影片來源：https://youtu.be/jcQ37yuB7Xs?feature=shared

生活醫療-身邊無所不在的AI

- AI 的身影已經慢慢出現在我們的生活中
  - 手機助理語音辨識功能
  - 社群網路上的廣告投放
  - 串流影音網站的推薦（如YouTube推薦影片、Spotify精選）
  - Google Map 最佳路線規劃
  - 掃地機器人
  - Chatbot(聊天機器人)

資料來源：TVBS NEWS 影片來源：https://www.youtube.com/watch?v=L2wmAzDf0LQ

AI的影響與威脅

AI的潛在風險

- **資源分配極度不均**
  人類的「既有專業」將輕易地被機器快速複製，造成經濟階層結構性的調整並形成技術性的失業。
- **資訊壟斷**
  「足夠且有用的數據」將是人工智慧的最大關鍵之一，各領域領先者會大量的對關鍵數據建立屏障來產生區隔，而使一般使用者取得數據的成本愈來愈高，造成資訊壟斷風險。
- **未來無隱私**
  麥肯錫預估2025年將會有1兆種類的物件相互聯網，這表示在物聯網趨勢下，未來我們的周遭可能全是資訊收集器，而在人工智慧技術的涵蓋下，這些資訊收集器可能都具有自主思考的功能並自行判斷所需的時機來開啟感測器。無論未來隱私權的防治可做到何種地步，人工智慧與萬物聯網的綜效一開始就將隱私權相關風險推進到一個很高的級數。
- **社會疏離**
  各種虛擬實境與人工智慧技術讓這虛擬世界更為真實，進而催生出更多上述的依賴群聚，造成真實社會間人際關係互動更疏離的現象。
- **無自主權**
  人工智慧已經進化到可以判斷出我們常看且想看的資訊，讓我們得到的訊息越來越趨單一化，導致人類在各領域無自主思考的風險

資料來源：https://iknow.stpi.narl.org.tw/Post/Read.aspx?PostID=14069

當AI遇上安全問題

資料來源：CIO Taiwan

俄國最大叫車軟體遭駭，造成鬧區交通大亂!

資料來源：iThome https://www.ithome.com.tw/news/152880

俄國最大叫車軟體遭駭，造成鬧區交通大亂!

時間	2022年9月5日
案情	➢ 俄羅斯最大叫車軟體Yandex Taxi遭駭，大量計程車同時被叫到同一個地方，造成莫斯科鬧區交通大亂。 ➢ 當地媒體上周報導，俄羅斯最大計程車Yandex Taxi的叫車App遭不明人士駭入，把所有計程車同時叫到莫斯科車水馬龍的大街Kutuzov Prospect上同一目的地，大量計程車造成的壅塞令莫斯科市交通大亂。
影響	➢ 首都交通受影響。

資料來源：iThome https://www.ithome.com.tw/news/152880

車用資安防衛戰開打!

- **駭入電動車**

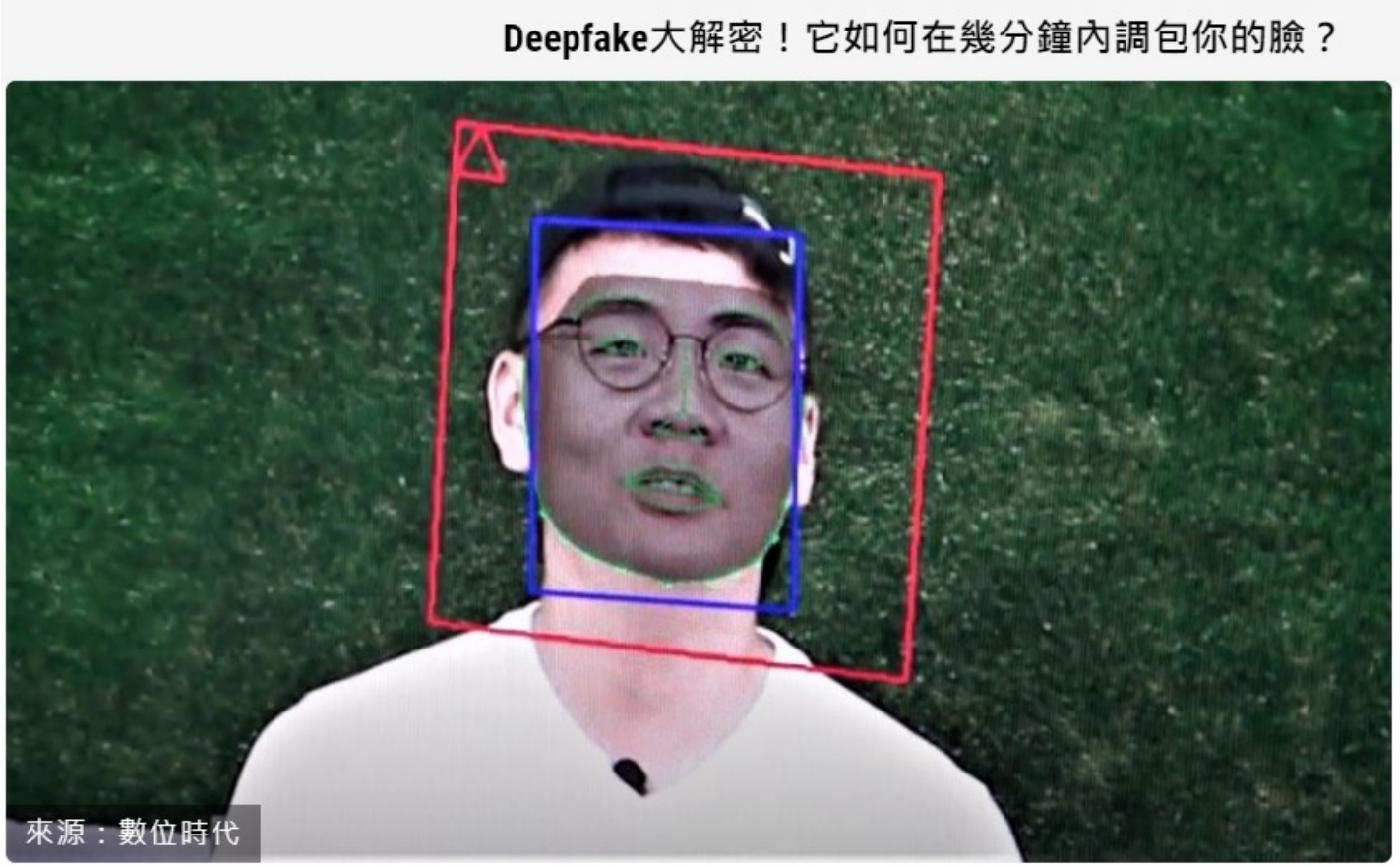
  2022年初，**一名19歲的德國少年透過Tesla第三方開源軟體(TeslaMate)中的一項漏洞，成功駭進13個國家的25輛Tesla電動車，遠端操控車輛**，包括關閉車輛哨兵模式、開關車門、車頭燈、車內音響、鳴笛、透過駭入車鑰匙軟體以取得車主電子信箱。不僅如此，有外媒指出，由於Tesla網路儀表板中的一項安全漏洞，使得駭客可自由接取系統資訊、使用車主從未修改過的預設密碼，加上車主的錯誤配置，導致逾百輛TeslaMate儀表板資訊暴露於公開網路之中，包括該車輛行經路線、充電位置、目前所在地點、行駛速度等，直接暴露於無形的風險之中。

- **各大車廠曾遭駭**

  根據趨勢科技研究報告指出，自2015年起，各大車廠包括Tesla、BMW、凌志(Lexus)、三菱(Mitsubishi)、福斯(Volkswagen)等在內，皆發生不只一件遠端攻擊事件，且預估未來3~5年內，全球連網車總數將達7億輛之多的市場前景之下，資安事件預期將不減反增。

資料來源：http://www.digitimes.com.tw/

網紅小玉用Deepfake換臉製作不雅片



透過既有的Deepfacelab等Deepfake生成軟體，AI會自動分析影片中的人臉，讓使用者不用深厚的程式撰寫能力，也能製造出Deepfake影片。

資料來源：數位時代 https://www.bnext.com.tw/article/57260/deepfake-ai-deep-learning

網紅小玉用Deepfake換臉製作不雅片

時間	2022 年 12 月
案情	➢ 網紅「小玉」朱O宸與助理莊O睿利用Deepfake（人工智慧深偽技術），把高雄市議員黃O、空服員的臉，「換臉」至色情片牟利，自109年7月起至110年10月共牟利新台幣1,300餘萬元，新北地院近期判賠受害者黃O、空服員等各新台幣100萬元。 ➢ 不只是黃O，就連立法委員高O瑜、「雞排妹」鄭O純也是受害者。黃O指出，感謝法官還給受害者公道，寒冬中給受害者一些安慰。不過更迫切的仍是數位性暴力的修法，包括懲處、防範及補救下架機制，但願不會再有人因為性影像的威脅和流傳而擔心受怕。
影響	個人隱私受到侵犯

資料來源：數位時代 https://www.bnext.com.tw/article/57260/deepfake-ai-deep-learning

眼見耳聞不再為憑... AI聲音、表情都能複製

時間	2023年8月
案情	➢ 台灣AI語音詐騙　甜美女聲誘騙投資：「您好，我們是理財調查小組...」甜美的女聲，邀請加入投資社團，其實電話那頭沒有真人，全都是預錄好的語音訊息，利用AI語音辨識系統即時回話。 ➢ 美國AI語音詐欺大量發生！7成受害者難辨真假：「媽！救救我，我被抓走了。」美國有一名母親珍妮佛，接到一通陌生電話，話筒卻傳來15歲女兒的哭聲，喊著自己被綁架了。
影響	➢ 婦人因此遭騙走2000萬元。 ➢ 個人名譽受損。

資料來源：https://www.businesstoday.com.tw/article/category/183012/post/202308160072/

駭客也愛用 AI！帶來資安大挑戰

- **AI 可以用來偵測電腦本身尋找系統和軟體弱點的模式**，駭客便能利用這些新發現的弱點。透過 AI，網路犯罪分子可以在公司網絡中長時間處於休眠狀態而不被發現，在此期間，他們可以對企業的關鍵基礎設施設置後門。並且可以**竊聽會議、提取數據、散播惡意軟體、創建特權帳戶以訪問其他系統和或安裝勒索軟體**。
- 搭配上竊取到的個資和一些公開的社群媒體貼文的資訊後，駭客便能**透過 AI 來發送大量網路釣魚信件**。許多資安專家注意到：**AI 生成的網路釣魚郵件相較人工製作的郵件，有更高的開信率**。
- **AI 也能用來設計不斷變化的惡意軟體，來避免自動防禦工具的檢測**。不斷變化的惡意軟件簽名可以幫助駭客規避防火牆等靜態防禦，同樣的，也可以潛伏在系統內部收集數據、觀察用戶行為，直到準備好啟動另一階段的攻擊或用較不容易被發現的方式來發送訊息。

資料來源：TechOrange https://buzzorange.com/techorange/2022/10/25/cyber-security-ai-hacker/

預防重於治療

SANS發佈2023年最危險的5種新興攻擊技術

技術	說明	特性
對抗性AI攻擊	對抗性攻擊是指**利用AI模型中的不足和漏洞，破壞AI模型用來學習的資料**，並生成能夠欺騙模型的對抗樣本。這些樣本看起來與正常資料非常相似，但是卻能夠導致模型產生錯誤的輸出結果。	威脅分子通過操縱AI工具，可以更方便地識別複雜應用系統中存在的安全性漏洞。**組織需要部署縱深化防禦的安全模式，提供層次化保護、自動化檢測和回應操作，並支持更有效的事件處理流程**。
利用ChatGPT的社交工程攻擊	ChatGPT可以非常真實流暢地模仿人類寫作，這個特點使其有可能成為一種強大的網路釣魚和社會工程工具，特別是當威脅分子需要進行跨語種的欺詐攻擊時，**ChatGPT可能被用來更有效地分發惡意軟體**。	企業組織比以往任何時候都更容易受到傷害，只需誤點擊一個惡意檔，就可能使整個公司面臨風險。在這種更嚴峻的攻擊面管理挑戰下，**需要組織自上而下宣導網路謹慎文化，以確保員工能夠提前認識到與ChatGPT相關的攻擊**。

資料來源：https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=10441

SANS發佈2023年最危險的5種新興攻擊技術

技術	說明	特性
SEO優化攻擊	SEO搜尋引擎優化技術已經被廣大網站運營者廣泛使用，但它同樣可以被網路攻擊者所使用，**使得非法欺詐網站的訪問量大幅提高，從而提升攻擊活動的成功率**。	攻擊者利用SEO關鍵字誘騙受害者訪問欺騙網站、下載惡意檔，**通過漏洞利用實現遠端用戶訪問，還會使用一些技巧保護惡意樣本長期潛伏**。為了應對SEO優化攻擊，企業組織需要**實施更有針對性的安全意識培訓計畫**。
惡意廣告利用攻擊	與利用SEO優化技術來擴大惡意網站的訪問類似，**攻擊者還在利用付費的廣告搜索技術，來提升欺詐網站的搜尋引擎展示效果**。	**透過惡意廣告利用，可以人為地提高某些非法惡意網站搜索排名，從而誤導受害者**。以一款名為Blender的免費3D圖形軟體的模仿廣告為例。當使用者搜索這個關鍵字時，排在最上部的三個網站連結都指向了惡意的欺詐網站，直到第四個結果，用戶才能進到真正合法的軟體網站。而那些非法的惡意網站看起來和真正的Blender官網幾乎完全相同，一般用戶很難分別其真偽。

資料來源：https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=10441

SANS發佈2023年最危險的5種新興攻擊技術

技術	說明	特性
軟體供應鏈攻擊	現代軟體系統的底層程式碼中超過90%都是開源的，這意味著幾乎所有軟體的研發與應用都存在著一條供應鏈，包括各種元件的引用，以及在軟體設計、開發、測試、部署和維護期間所涉及的各種環節，**安全性漏洞隨時可能出現，因此在企業軟體供應鏈中可能導致安全風險的因素也非常複雜。**	軟體供應鏈攻擊已經成為現代企業組織必須高度重視的最危險攻擊方式之一。2022年的LastPass漏洞事件就是最好的證明，攻擊者會利用協力廠商軟體漏洞繞過現有控制措施並訪問特權環境。對於各大行業的企業組織而言，LastPass漏洞攻擊再次強調了要與協力廠商軟體供應商保持緊密合作的重要性，以便實現整體的安全架構、分享威脅情報，並熟悉不斷發展的攻擊技術。**企業組織在解決軟體供應鏈安全問題時，需要基於軟體應用的全生命週期來考慮，監控和保護其中的每個環節。**

資料來源：https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=10441

資安與個資 - AI 人工智慧是敵是友?

- AI
  - AI人工智慧應用的領域。
  - 有了AI，人類工作不保？
  - AI 可否有自主權及夢想？
  - AI 人工智慧專法。
  - AI 機器人相不可為真實存在的人(不論自然人或非自然人)。
- 資安與個資
  - 系統最高權限由主管持有，不可共用帳號。
  - 未經授權不可存取系統。
  - 員工離職即停用或刪除帳號及權限。
  - 系統原始碼需做檢視與弱點掃瞄。
  - 未經個資當事人同意，不得處理、利用當事人個資。
  - 存放機敏資料之伺服器，實作網段區隔及實體隔離。
  - 使用 USB 前先掃毒。
  - 社交平台注意隱私權設定，勿將帳號或貼文設為公開。

別相信任何人-零信任原則

- **明確驗證**

  所有可用的資料點一律都必須進行驗證和授權，包括使用者識別、位置、裝置健康情況、服務或工作負載、資料分類和異常。

- **使用最低的特殊權限存取**

  任何身分試圖存取資源時，都必須以增強式驗證來辨明身分，以確保存取符合該身分的規則與型態，最低特殊權限存取的原則也必須落實。

- **預設已有安全缺口**

  透過對網路、使用者、裝置和應用程式的認知來分割存取權，縮小外洩的波及範圍並防止橫向移動。此外，所有驗證工作階段皆為端對端加密，並使用分析功能來取得可見度，進而驅動威脅偵測和改善防禦能力。

資料來源：ITHOME https://www.ithome.com.tw/pr/137091

在日常中使用零信任模式

- 不隨意相信其他人事物
  - 使用公共的電腦或是公開的網路的時候
  - 收到一封 email
- 確保帳號與裝置的安全性
  - 常見的方式：
  - 確保更新都有適時的被安裝
  - 有安裝該有的防毒軟體
  - 開啟裝置加密
  - 開啟遺失搜尋
- 持續監控
- 最低權限標準

智慧科技與保護安全的省思

- **智慧裝置辨識功能**

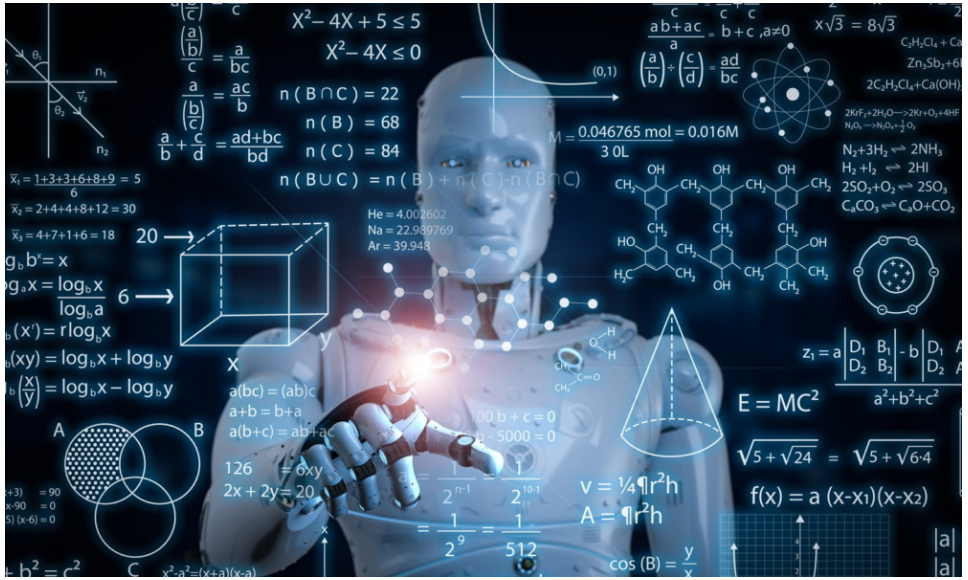
  帳號密碼外生物辨識等方式越來越盛行，透過設備收集、分析與交換，並確實存取使用者個人數據，如識別指紋、聲紋、臉部特徵等其他生物特徵資訊的身份驗證方式。

  - **登入裝置前必須經過「通關方式」**，正確無誤後即根據此帳號建立的使用環境與習慣，提供裝置的功能服務。
  - **如果個人生理特徵資訊如果遭竊，對大眾的傷害應也不低於身份證字號的流出，更應慎重思考保護機制**。

- 廠商與使用者應考量這些關於個人生理特徵的資訊，**須被記錄在無法入侵的安全裝置中**。

審慎因應新興科技衍生的資安議題

- 人工智慧與元宇宙的時代要更加小心資訊的流動。
- 安全與便利之間的取捨須加以權衡，三思而行。
- 勿過度依賴科技與智慧裝置，以維自身安全。
- 吸取最新的資訊安全防護知識與觀念，利己利人。



社交工程須知

什麼是社交工程(Social Engineering)？

- 社交工程(Social Engineering)是一種攻擊者**利用與人互動和操弄來達到目的的技術**。通常涉及說服受害者為了攻擊者的金錢或資訊利益而危害自身安全或破壞安全最佳作法。駭客經常會用社交工程來偽裝自己及動機，通常是冒充成可信任的對象。
- 歸根究底，**重點是要去影響、入侵人心**－**而非系統**。這類攻擊通常都依賴於**人們的善良本性或對負面情況的恐懼**。社交工程很受攻擊者的受歡迎，因為**利用人性要比利用網路或軟體漏洞要來的更加容易**。

資料來源：https://blog.trendmicro.com.tw/?p=75788

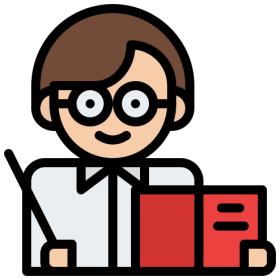
誤點率高的十個網路釣魚主題類型

排名	類型	案例主旨
1	熱門韓劇、最新影片	駭客跟你一樣愛的電影：A.I. 創世者、浴血任務4
2	滿足偷窺慾	喝醉酒女孩影、片連結臉書個人檔案檢視器
3	與工作相關公文	人事部門收到的個人簡歷
4	全民關心度高的議題	二代健保補充保險費扣繳辦法說明、總統大選民調
5	恐懼心理	你因觸犯法規電腦遭鎖定，必須支付罰款才能解除鎖定

排名	類型	案例主旨
6	貪小便宜	拍賣網站的 iPhone 15 Pro特價超便宜?!
7	新產品或服務	iPhone 15 郵件,隨蘋果發表會同步亮相
8	名人相關	打開名人相片(木馬尾隨而來、殭屍大軍伺機招募)
9	新功能	好奇誰取消關注你的 Twitter? IG? 臉書?
10	熱門新聞事件	「失蹤的馬航真的在印度降落了!!」

如何保護自己免於社交工程攻擊？

1. 保持作業系統和網路安全**軟體更新**。
2. **使用2FA（雙重認證）身份驗證**和密碼管理工具。
3. **不要開啟來歷不明的電子郵件**或附件。
4. 將垃圾郵件過濾器層級設定為高。
5. **刪除並忽略對財務資訊或密碼的請求**。
6. 如果你在**互動過程中產生懷疑，請保持冷靜**，三思而後行。
7. 小心自己在社群媒體上分享的內容 – **善用你的隱私權設定**。
8. **每一個人都應該了解組織資安政策**。



- 敬請指教 -

資拓宏宇永遠與您一起創新前進

always innovative always IISI

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