智慧時代新生活

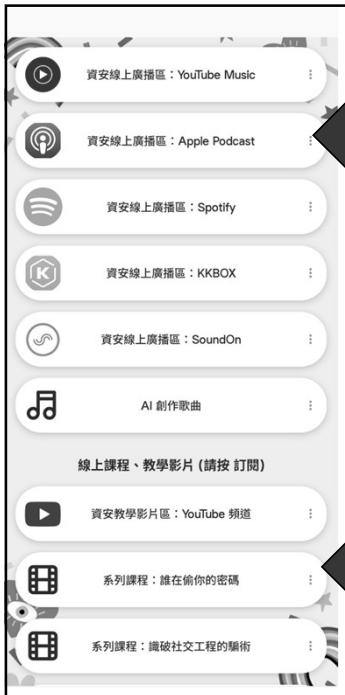
~ 生成式 AI 的深偽技術與社交工程的詐騙

講師　　呂守箴

大綱

- 自我保護措施
  - 防詐騙宣導
- AI人工智慧與換臉詐騙
  - 什麼是生成式 AI？
  - 什麼是 深偽技術 (Deepfake)？
  - 深偽技術的危害
  - AI深偽技術的社交工程攻擊案例
- 各種社交工程的詐騙手法
  - 來自於郵件社交工程的案例
  - 透過簡訊的金融詐騙
  - 通訊軟體 LINE 的網路釣魚
- 防範措施
  - 瀏覽器的安全設定
  - 應用程式的更新
  - 防毒軟體的檢測

參考資料 & 教學影片
(掃描後 按 超連結)



Podcast 播客/線上廣播
(請按 追蹤or訂閱)

節目表：
EP.01 [Podcast] 電子郵件社交工程手法與防範
EP.02 [Podcast] 帳號密碼的新觀念
EP.03 [Podcast] 請留意LINE帳號安全
EP.04 [Podcast] 手機簡訊的網路釣魚
EP.05 [Podcast] 蝦皮App偷看手機相簿？
EP.06 [Podcast] 嗨歌、抖音App藏交友詐騙陷阱
EP.07 [Podcast] 透過AirTag不當追蹤的恐怖情人
EP.09 [Podcast] 超麻煩！掃碼點餐的爭議
EP.10 [Podcast] 無密碼登入！這樣安全嗎？
EP.14 [Podcast] 利用 AI 來進行 Deepfake 詐騙
EP.22 [Podcast] 太多密碼記不住！使用密碼管理App？
EP.25 [Podcast] LINE、Facebook、Instagram 的詐騙手法

課程影片
不定期更新 請按 [**訂閱**]

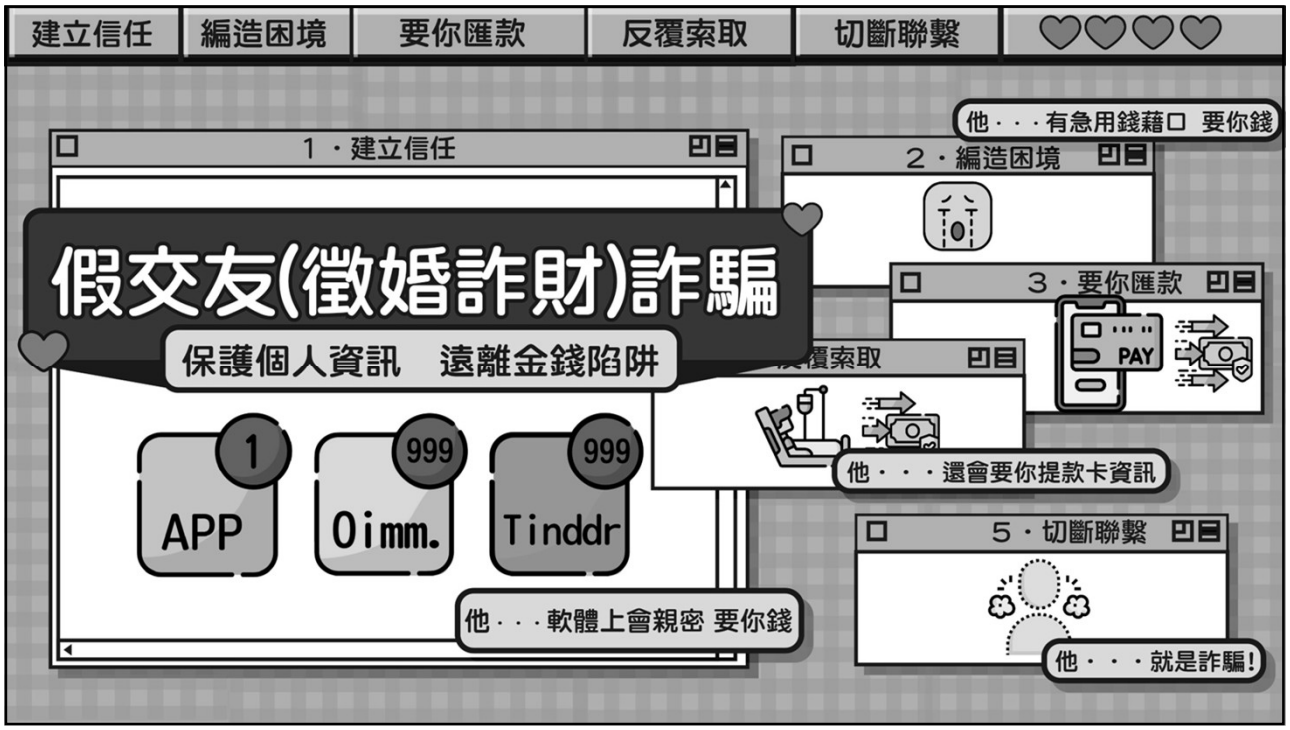
- 講師： 呂守箴
- E-Mail： shooujen@gmail.com

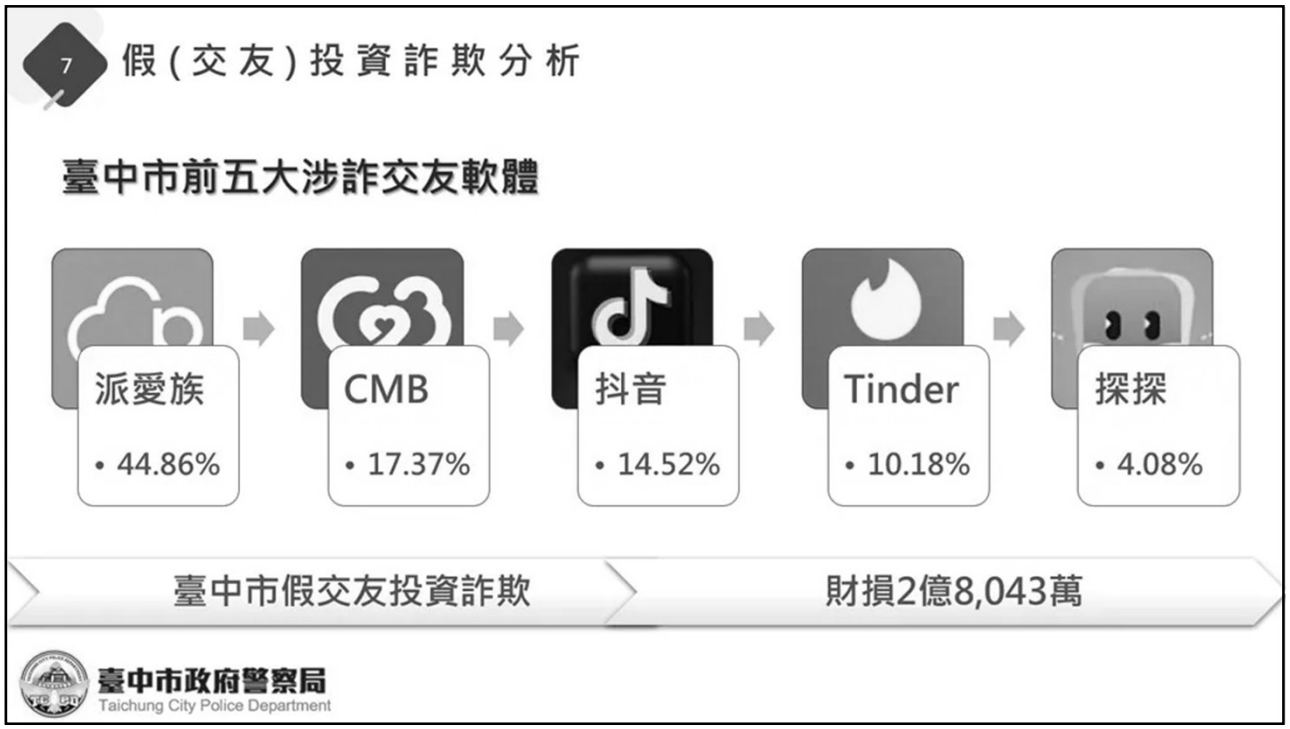
- 講師資料： ppt.cc/f1C00x (注意英文大小寫)

- 智慧時代新生活 FB 粉絲專頁： facebook.com/SmartEraNewLife
- 智慧時代新生活 IG 專業帳號： instagram.com/SmartEraNewLife
- 智慧時代新生活 Threads 帳號： threads.net/@SmartEraNewLife
- 智慧時代新生活 YouTube 頻道：youtube.com/OpenBlueSmartLife
- 資安玩家村 LINE 社群： ppt.cc/fDWsrx
- 資安玩家村 Discord 社群： discord.gg/Wfktn6qWdY

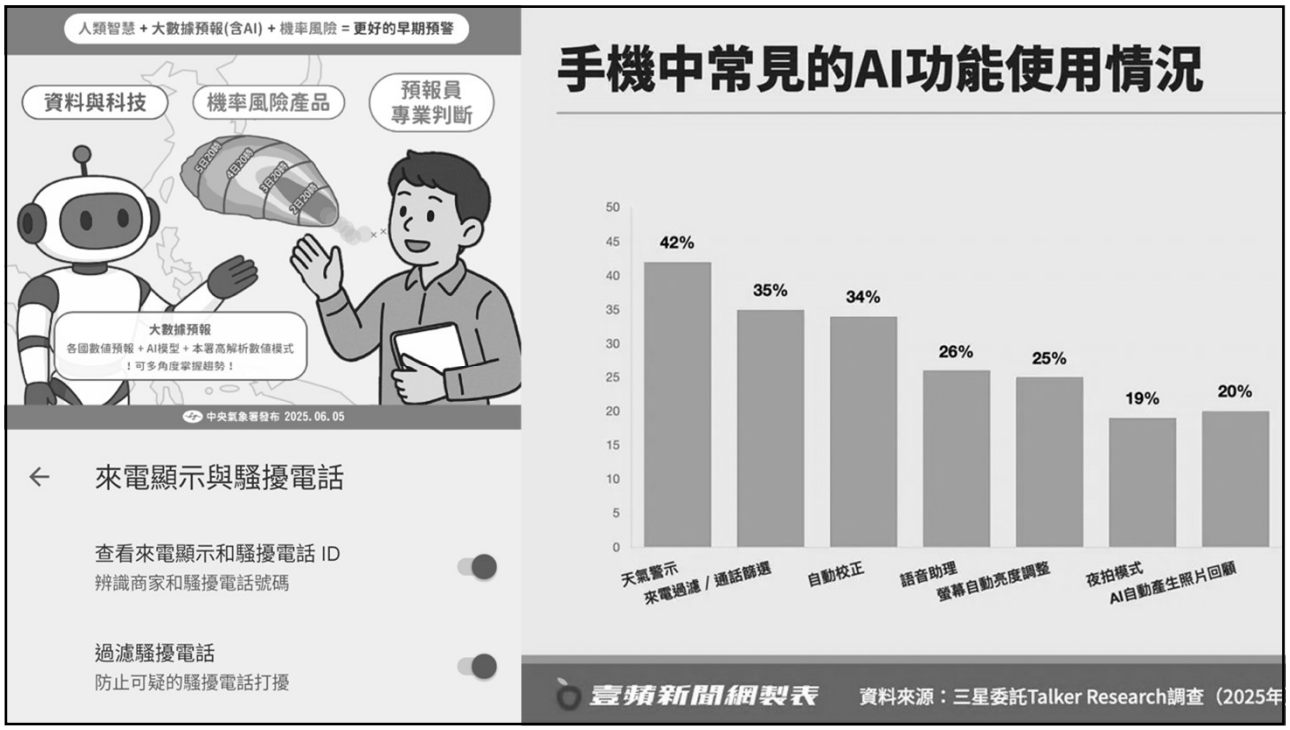
- 講師個人 FB： facebook.com/openblue
- 講師個人 IG： instagram.com/openblue.ig
- 講師個人 Threads： threads.net/@openblue.ig
- 講師個人 YouTube： youtube.com/openblue

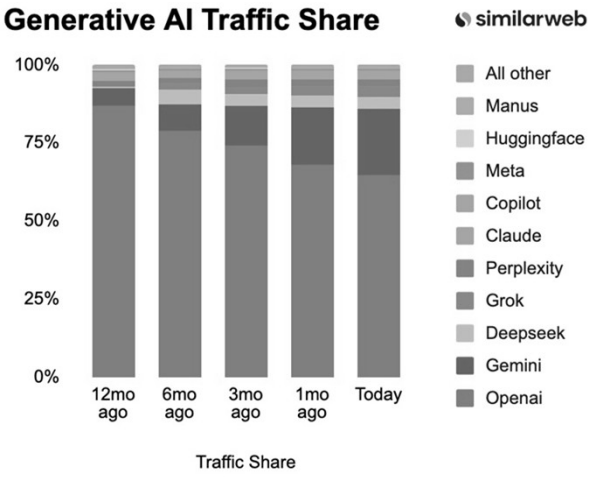
https://165dashboard.tw/


建立信任
編造困境
要你匯款
反覆索取
切斷聯繫
1・建立信任
他・・・有急用錢藉口 要你錢
2・編造困境
3・要你匯款
PAY
反覆索取
他・・・還會要你提款卡資訊
5・切斷聯繫
他・・・就是詐騙!
假交友(徵婚詐財)詐騙
保護個人資訊 遠離金錢陷阱
APP
1
Oimm.
999
Tinddr
999
他・・・軟體上會親密 要你錢

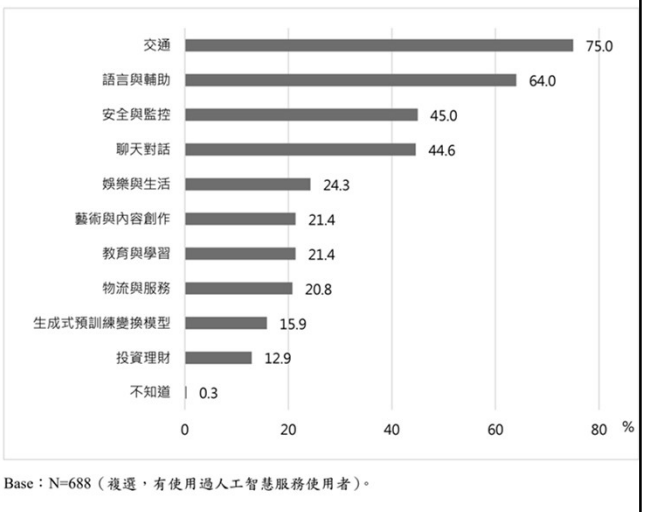

7
假(交友)投資詐欺分析
臺中市前五大涉詐交友軟體
派愛族
• 44.86%
CMB
• 17.37%
抖音
• 14.52%
Tinder
• 10.18%
探探
• 4.08%
臺中市假交友投資詐欺
財損2億8,043萬
臺中市政府警察局
Taichung City Police Department

AI 人工智慧 與 換臉詐騙





資料來源：Similarweb 2025 熱門 AI 工具



Base：N=688（複選，有使用過人工智慧服務使用者）。

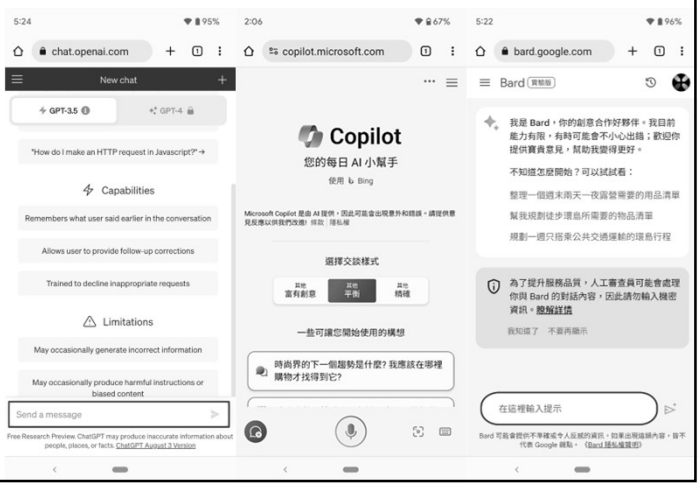
NCC《114年通訊傳播市場報告》

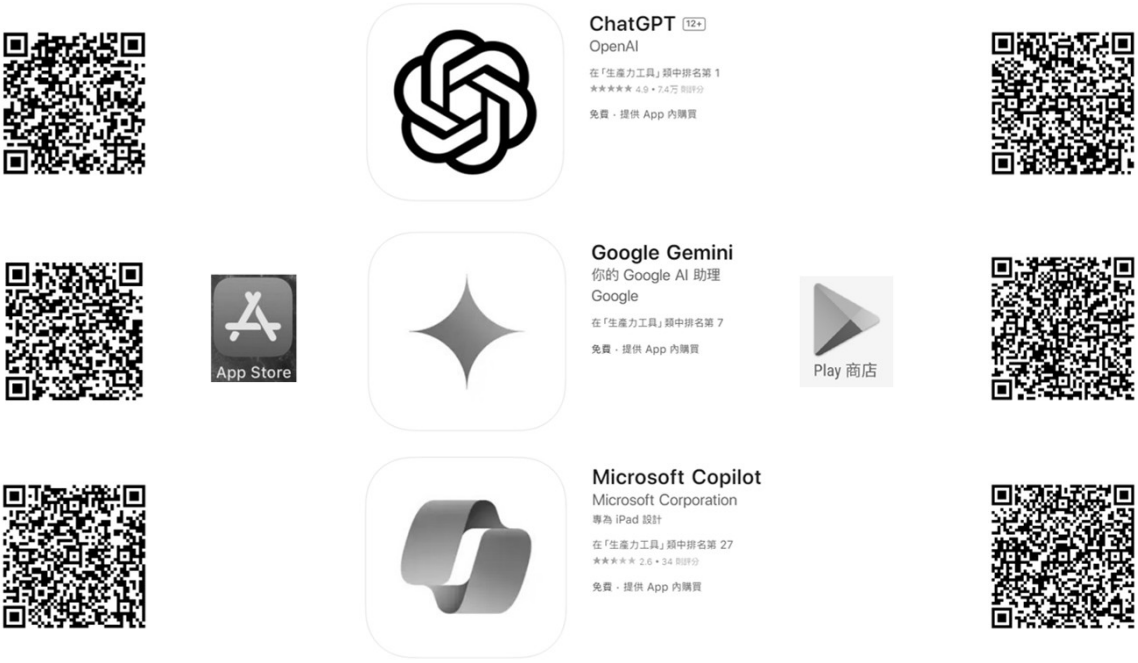
什麼是生成式 AI？

- 生成式 AI 是一種可以創造對話、故事、影像、視訊和音樂等內容和想法的人工智慧。

- OpenAI **ChatGPT**
- **Microsoft Copilot** (將 OpenAI 技術整合到微軟產品)
- Google Gemini

- OpenAI DALL·E
- Midjourney
- Stable Diffusion





Google Gemini APP 版

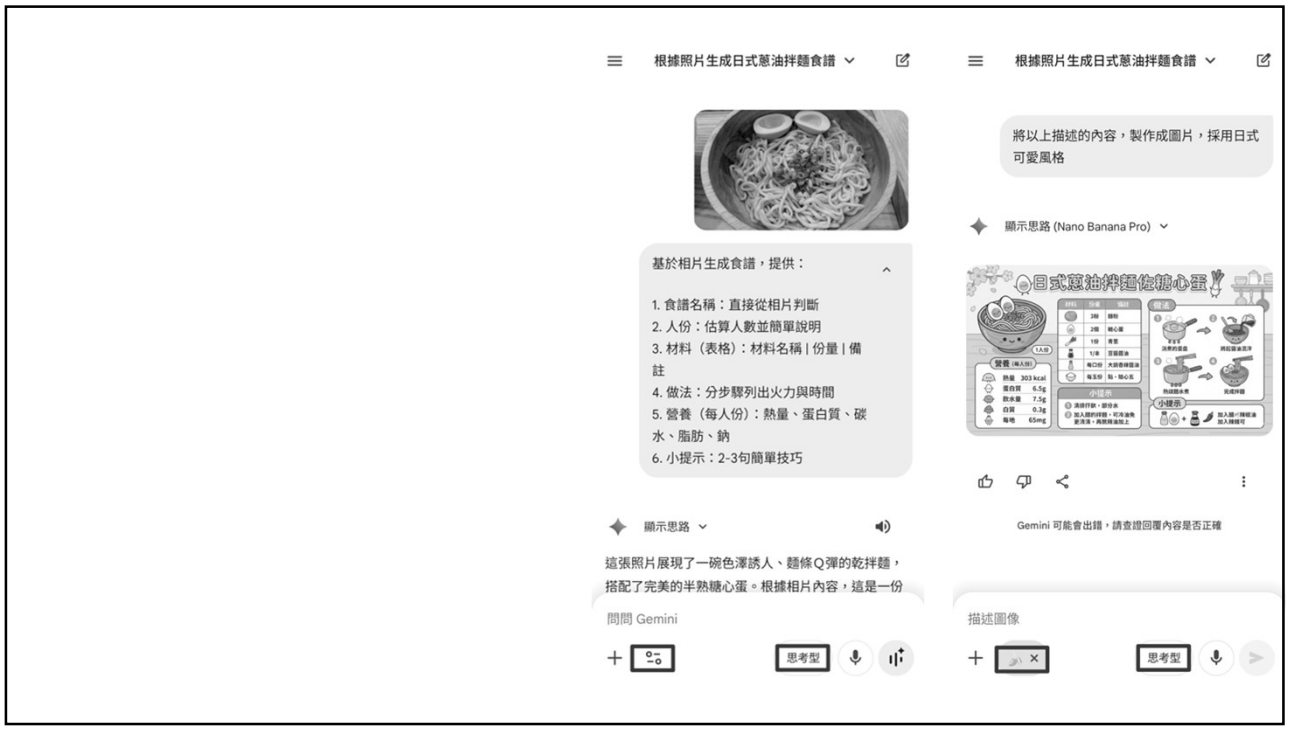
App Store

Play 商店

[免費版] 功能都可以使用，
只是有使用次數的限制

比較：
https://gemini.google/tw/subscriptions/

https://gemini.google.com

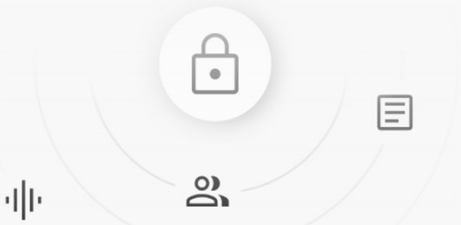

根據照片生成日式蔥油拌麵食譜
基於相片生成食譜，提供：
1. 食譜名稱：直接從相片判斷
2. 人份：估算人數並簡單說明
3. 材料（表格）：材料名稱 | 份量 | 備註
4. 做法：分步驟列出火力與時間
5. 營養（每人份）：熱量、蛋白質、碳水、脂肪、鈉
6. 小提示：2-3句簡單技巧
顯示思路
這張照片展現了一碗色澤誘人、麵條Q彈的乾拌麵，搭配了完美的半熟糖心蛋。根據相片內容，這是一份
問問 Gemini
思考型
根據照片生成日式蔥油拌麵食譜
將以上描述的內容，製作成圖片，採用日式可愛風格
顯示思路 (Nano Banana Pro)
日式蔥油拌麵佐糖心蛋
Gemini 可能會出錯，請查證回覆內容是否正確
描述圖像
思考型


「用上傳的這張照片，製作一款 1/7 ...
「用上傳的這張照片，製作一款 1/7 比例的商業化角色模型圖片，風格為寫實風，並置於真實的環境中。模型擺放在電腦桌上，底座為圓形透明壓克力材質，且底座上沒有任何文字。電腦螢幕上顯示的是該模型的 Zbrush 建模過程，螢幕旁邊擺放著一個包裝盒，設計為圓角造型，正面有透明視窗，可以清楚看到裡面的模型。」
描述圖像
思考型
「用上傳的這張照片，製作一款 1/7 ...
「用上傳的這張照片，製作一款 1/7 比例的商業化角色模型圖片，風格為寫實風，並置於真實的環境中。模型擺放在電腦桌上，底座為圓形透明壓克力材質，且底座上沒有任何文字。電腦螢幕上顯示的是該模型的 Zbrush 建模過程，螢幕旁邊擺放著一個包裝盒，設計為圓角造型，正面有透明視窗，可以清楚看到裡面的模型。」
描述圖像
思考型

NotebookLM 總覽 方案 取得應用程式

我們非常重視你的隱私，絕不會將貴機構資料用於訓練 NotebookLM

機構或學校的資料會受到妥善保護。個人使用者除非提供意見回饋，否則個人資料不會用來訓練模型。歡迎參閱詳情。



https://support.google.com/notebooklm

瞭解 NotebookLM 如何保護您的資料

透過符合資格的 Workspace 版本以公司帳戶存取 NotebookLM 的使用者，適用《Google Workspace 服務條款》。透過 Workspace for Education 帳戶存取 NotebookLM 的使用者，適用《Google Workspace for Education 服務條款》。其他存取 NotebookLM 的使用者，適用《Google 服務條款》。以下聲明和 Google《隱私權政策》說明您與 NotebookLM 互動時，Google 如何處理您的資料。

您的資料受到保護，除非您提供意見回饋，否則此資料不會用於訓練 NotebookLM。若您提供意見回饋協助我們改良服務，我們可能會查看該次互動的完整情境，包含您的查詢內容、上傳項目和模型的回覆。

為保障安全與可靠性，我們可能會處理您的資料，防止出現詐欺事件、濫用行為和技術問題。NotebookLM 可能會出錯，且回答的內容不代表 Google 立場。如需醫療、法律或財務方面的建議，請務必諮詢專業人士。

Google Workspace 或 Google Workspace for Education 使用者在 NotebookLM 上傳的內容、查詢及模型的回覆，都不會經過人工審查，或用於 AI 模型訓練。

在 NotebookLM 中使用對話功能

重要事項：NotebookLM 行動應用程式目前可能無法支援這項功能。進一步瞭解 NotebookLM 行動應用程式支援的功能 。

上傳來源後，您可以：

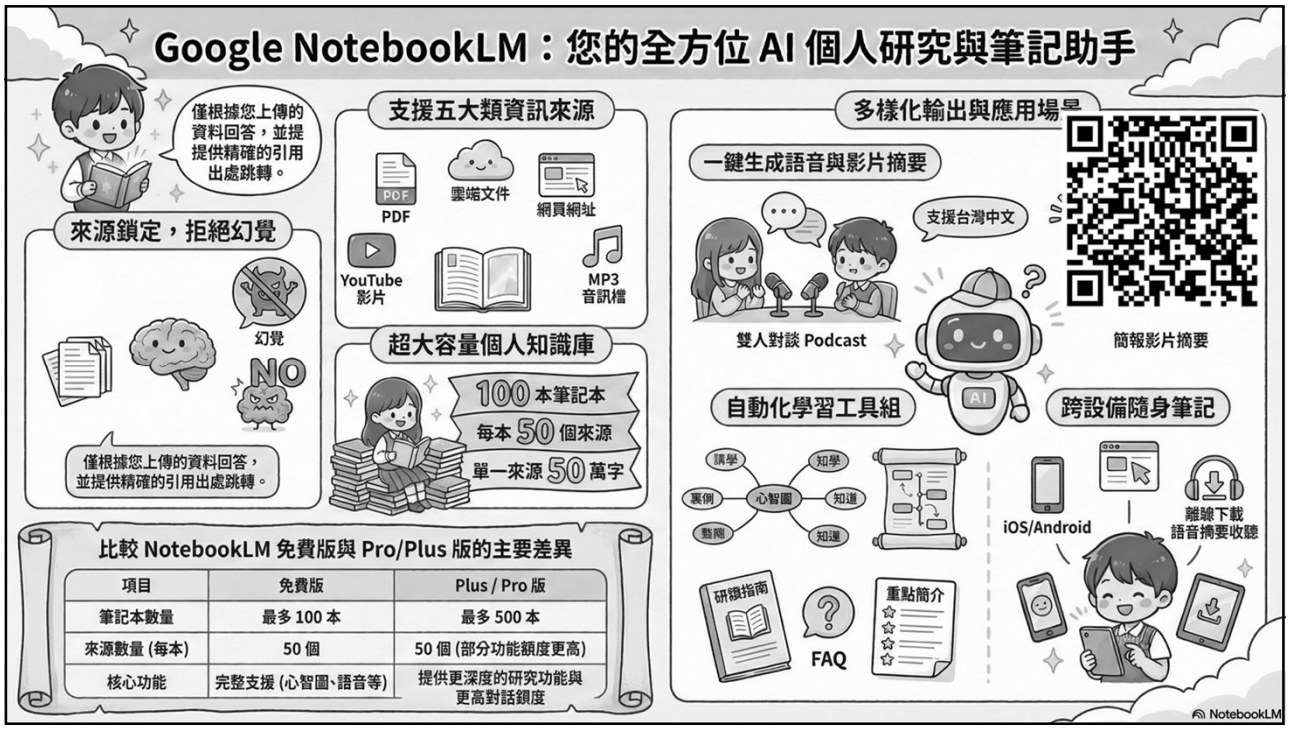
- 向模型詢問與來源資料相關的問題。
- 指示模型要執行的動作。

NotebookLM 會直接引用來源中的內容、文字和圖片，回答問題和執行動作。這些引用資料可協助您檢查回覆內容是否正確。將滑鼠游標懸停在任何引用內容上，即可立即查看完整引文。選取引用內容時，NotebookLM 會自動前往引文所在位置，方便您查看上下文。

在筆記本中，您可以使用各個來源的核取方塊，指定模型能否根據特定來源回答問題。

提示：NotebookLM 只會使用來源中的資料提供對話回覆。如果您明確要求模型發揮創意，例如「改寫短篇故事的結尾」，對話回覆可能會顯示「NotebookLM 無法回答這個問題」。請換個說法或提出其他問題。


YouTube TW
搜尋
Podcast (播客/線上廣播) :
專屬於你的知識
夥伴 AI 筆記
NotebookLM
支援生成台灣中文
對話 Podcast !
智慧時代
新生活
使用 Google Gemini + NotebookLM 所產生的 AI 主持人 的語音對談
參考資料 / 引用來源：請參考下方備註欄說明
EP.50 [Podcast] 專屬於你的知識夥伴 AI 筆記 NotebookLM 支援生成台灣中文對話 Podcast !
AI & 資安玩家村
501位訂閱者
喜歡
分享
儲存
剪輯片段
下載

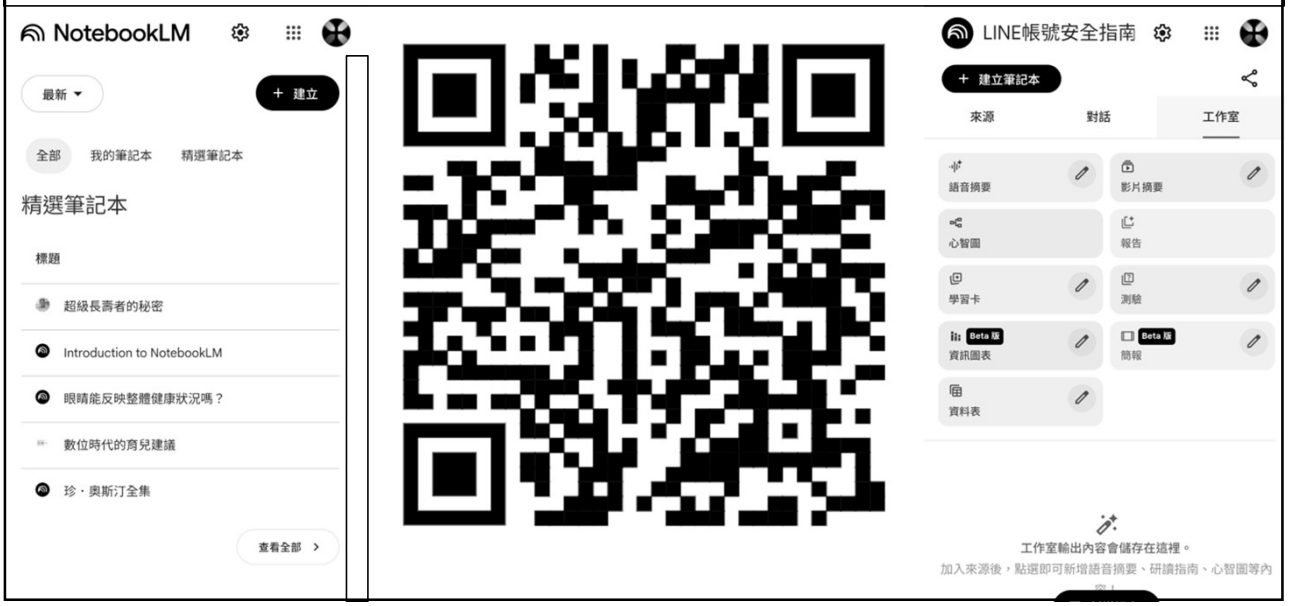

Google NotebookLM：您的全方位 AI 個人研究與筆記助手
僅根據您上傳的資料回答，並提供精確的引用出處跳轉。
來源鎖定，拒絕幻覺
幻覺
NO
僅根據您上傳的資料回答，並提供精確的引用出處跳轉。
支援五大類資訊來源
PDF
雲端文件
網頁網址
YouTube 影片
MP3 音訊檔
超大容量個人知識庫
100 本筆記本
每本 50 個來源
單一來源 50 萬字
比較 NotebookLM 免費版與 Pro/Plus 版的主要差異
項目 | 免費版 | Plus / Pro 版
筆記本數量 | 最多 100 本 | 最多 500 本
來源數量 (每本) | 50 個 | 50 個 (部分功能額度更高)
核心功能 | 完整支援 (心智圖、語音等) | 提供更深度的研究功能與更高對話額度
多樣化輸出與應用場景
一鍵生成語音與影片摘要
支援台灣中文
雙人對談 Podcast
簡報影片摘要
自動化學習工具組
跨設備隨身筆記
心智圖
iOS/Android
離線下載
語音摘要收聽
研究指南
FAQ
重點簡介
NotebookLM

Google NotebookLM APP 版

[免費版] 功能都可以使用，
只是有使用次數的限制

最多可建立 100 本筆記本。
每本筆記本可包含最多 50 個資料來源。
每個資料來源的大小限制為 200 MB。
每日最多進行 50 次對話查詢。
每日最多生成 3 次語音/影片摘要。

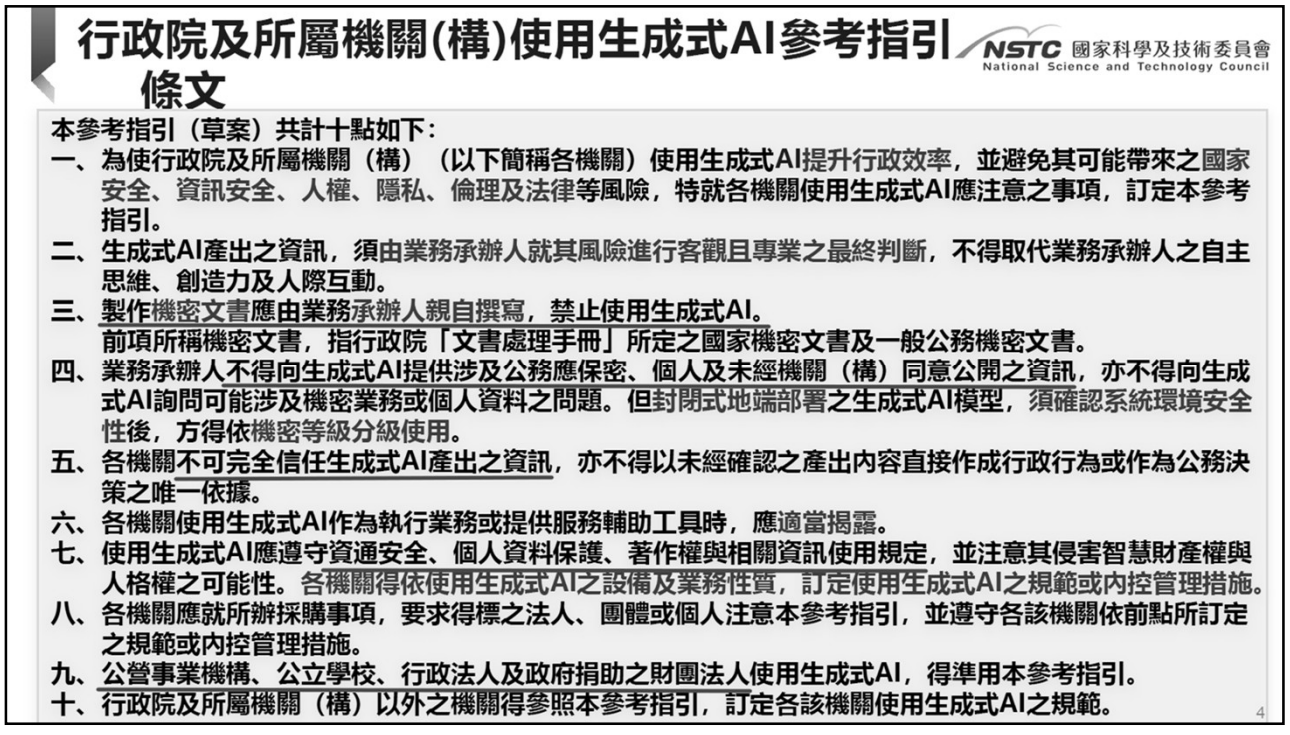
https://notebooklm.google.com




專案：物聯網(3)
針對本次專案 請大家注意 專案結案時間
好的
專案時間的結案日期是 12/31
本次專案 針對物聯網 主要是針對 攝影機10台 印表機 15台 NAS 5 台 以及 無線網路基地台 各建築物 有 5 台
客戶希望能夠 符合 OWASP IoT TOP 10 的要求
其他重點可以參考 這本手冊
IoT 設備資安防護指南.pdf
請各位注意
好的
[LINE] 專案：物聯網的聊天.txt
專案：物聯網
設定
記事本提醒
網址行動條碼邀請
背景
傳送聊天記錄
加密金鑰
刪除資料
建立聊天室的捷徑
檢舉
退出群組
4:22
正在分享 1 個檔案
[LINE] 專案：物聯網的聊天.txt
在雲端硬碟中搜尋
我的雲端硬碟
電腦
名稱
[LINE] 專案：物聯網的聊天.txt
上次修改日期 下午4:30
下載項目
Download
今天
[LINE] 專案：物聯網的聊天.txt
685 B • 剛剛
昨天
IoT 設備資安防護指南.pdf
768 KB • 17 小時前

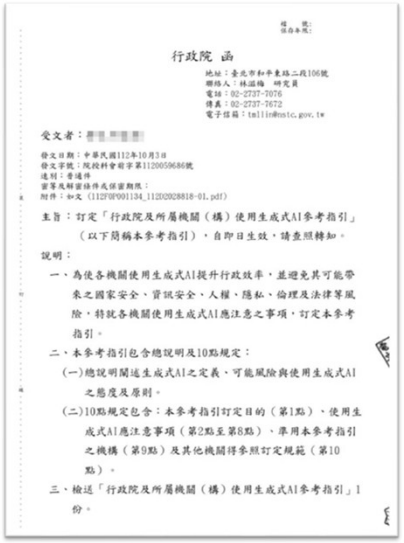

notebooklm.google.com
專案：物聯網
+ 建立筆記本
來源
對話
工作室
+ 新增來源
試用 Deep Research 取得深度報告和新聞來源！
在網路上搜尋新來源
網路
Fast Research
選取所有來源
IoT 設備資安防護指南.pdf
[LINE] 專案：物聯網的聊天.txt
請統整 專案 重點整理
根據您提供的 LINE 聊天記錄，以下為「物聯網專案」的重點整理：
• 專案結案日期：本專案的結案時間定於 12/31 1 。
• 硬體設備清單：
◦ 攝影機：共 10 台 1 。
◦ 印表機：共 15 台 1 。
◦ NAS 儲存裝置：共 5 台 1 。
◦ 無線網路基地台 (AP)：各建築物分別配置 5 台 1 。
• 技術規範與要求：
◦ 專案必須符合 OWASP IoT TOP 10 的安全要求 1 。
開始輸入...
(2)
NotebookLM 提供的資訊未必正確，請查證回覆內容。
請問指南的重點整理
根據提供的來源，這份《IoT 設備資安防護指南》是由臺灣學術網路危機處理中心團隊 (TACERT) 於 2025 年 8 月修訂的 V5 版本 1 。該指南旨在針對日益普及的物聯網設備提供系統性的安全定義、風險分析與防範建議，以下為其重點整理：
一、 物聯網的定義與特性
• 定義：物聯網 (IoT) 廣義上指「可透過各種連線方式連接網路的設備」，包含網路攝影機、印表機、NAS、無線分享器等 2 。其目的是透過物聯網來達到控制、分享、分析及應用 2 。
• 特性：具有成本低廉、高度客製化、應用層面廣（如醫療、教育）以及數量眾
二、 主要資安風險與威脅
• 系統漏洞修補不易：IoT 設
語音摘要
影片摘要
心智圖
報告
學習卡
測驗
資訊圖表
簡報
資料表
別讓攝影機變殭屍
深入探索 · 2 個來源 · 17 小時前
你的設備在說話。說太多了嗎？
詳細說明 · 2 個來源 · 17 小時前
Campus IoT
新增記事

https://deckedit.com



各公務機關使用生成式AI注意事項

- 行政院**112年10月3日院授科會前字第1120059686號函**頒「行政院及所屬機關（構）使用生成式 AI 參考指引」，簡述如下：
  - 不得向生成式 AI 提供未經機關同意公開之資訊，更不可完全信任生成式 AI 產出之資訊。
  - 各機關得依使用生成式 AI 之設備及業務性質，訂定使用生成式 AI 之規範或內控管理措施。



行政院 函

地址：臺北市和平東路二段106號
聯絡人：林溫梅 研究員
電話：02-2737-7076
傳真：02-2737-7672
電子信箱：tmlin@nstc.gov.tw

受文者：

發文日期：中華民國112年10月3日
發文字號：院授科會前字第1120059686號
速別：普通件
密等及解密條件或保密期限：
附件：如文（112F0901134_112D0028818-01.pdf）

主旨：訂定「行政院及所屬機關（構）使用生成式AI參考指引」（以下簡稱本參考指引），自即日生效，請查照轉知。

說明：

一、為使各機關使用生成式AI提升行政效率，並避免其可能帶來之國家安全、資訊安全、人權、隱私、倫理及法律等風險，特就各機關使用生成式AI應注意之事項，訂定本參考指引。

二、本參考指引包含總說明及10點規定：

（一）總說明闡述生成式AI之定義、可能風險與使用生成式AI之態度及原則。

（二）10點規定包含：本參考指引訂定目的（第1點）、使用生成式AI應注意事項（第2點至第8點）、導用本參考指引之機構（第9點）及其他機關得參照訂定規範（第10點）。

三、檢送「行政院及所屬機關（構）使用生成式AI參考指引」1份。

立法院三讀通過《人工智慧基本法》 構築我國AI創新與安全治理基石

moda 數位發展部 Ministry of Digital Affairs

立法院114年12月23日三讀通過《人工智慧基本法》，旨在促進以人為本之人工智慧研發與人工智慧產業發展，建構人工智慧安全應用環境，落實數位平權並保障人民基本權利。本法將確保技術應用符合社會倫理，維護國家文化價值及提升國際競爭力，奠立法制基礎。

確立人工智慧治理原則 兼顧發展與安全

本法確認政府推動人工智慧之研發與應用七大原則：應遵循永續發展與福祉、人類自主、隱私保護與資料治理、資安與安全、透明與可解釋、公平與不歧視及問責。執行過程應兼顧社會公平及環境永續，提供適當之教育及培訓以降低數位落差；同時建立資安防護措施以確保系統穩健性與安全性，並對人工智慧之產出做適當資訊揭露或標記。

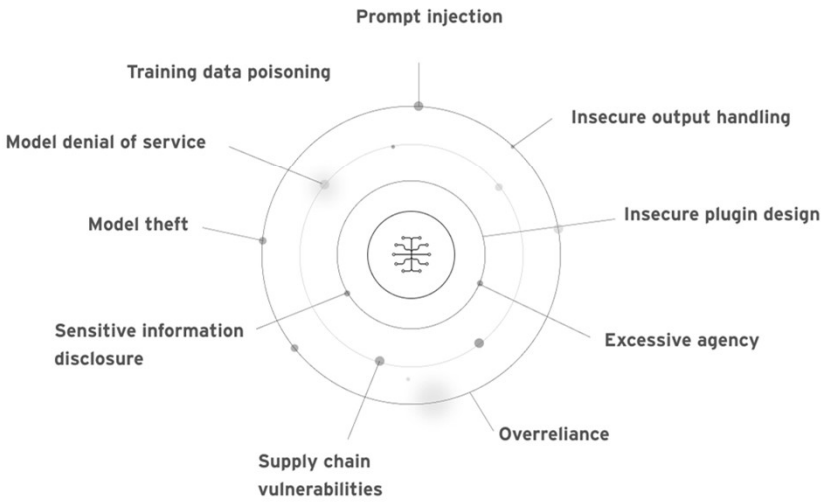
以人為本 打造AI創新生態圈

發布單位：數位策略司　建立日期：2025-12-24　更新日期：2025-12-24

AI 資安漏洞

全球開放應用程式安全計畫（OWASP）指出了一系列與建構於大型語言模型（LLMs）與生成式人工智慧（GenAI）上的 AI 相關的漏洞。包括以下幾點：

- 提示注入（Prompt injection）
- 不安全的輸出處理方式
- 訓練資料遭下毒
- 模型阻斷服務
- 供應鏈漏洞
- 機敏資訊外流
- 不安全的擴充元件 (plugin)
- 過多的代理權限
- 過度依賴
- 模型失竊



什麼是 深偽技術 (Deepfake)？

- 深偽技術 (Deepfake) 又稱深度偽造，是深度學習 (deep learning) 和偽造 (fake) 的混和名詞，指將已有的圖像或影片合成疊加至目標圖像或影片上進行偽造的技術。
- 一種肉眼難辨的修圖或者影片合成的技術。
- 目前**常見於換臉偽造**的手法，主要是透過交換兩張圖像的人臉達到偽造身分的目的。
- 現階段換臉偽造和表情偽造，已經可以**結合語音偽造**技術，達到完全偽裝的手法。

https://sightengine.com/detect-deepfakes

拍照當下自動透過 AI 修圖

Pixel 系列手機以強大的 Google AI 影像處理聞名，**最新款（如 Pixel 10）深度整合 Gemini 模型，主打功能包括即時引導構圖的「拍照指導」、結合兩張照片讓攝影師也入鏡的「一起拍」，以及魔術橡皮擦、魔術修圖等強大後製工具**。其核心優勢在於將複雜的計算攝影技術整合在 Tensor 晶片中，使任何人都可輕鬆拍出專業級照片。

Pixel 相機主要 AI 功能：

- **拍照指導 (Camera Coach)：** 由 Gemini 提供即時分析，指導構圖與拍攝角度。
- **一起拍 (Add Me)：** 解決團體照攝影師無法入鏡的問題，將兩張照片合成。
- **魔術修圖 (Magic Editor)：** 可移除、移動主體或更換天空，甚至重新構圖。
- **魔術橡皮擦 (Magic Eraser)：** 輕鬆消除照片中不需要的背景雜物或路人。
- **夜視模式與修復模糊：** 強大 AI 演算法在低光源下也能清晰成像。
- **錄音轉文字/即時翻譯：** 工作與生活層面的智慧助理功能。

三星（Samsung）將Galaxy AI技術深度整合至相機功能中，**主要應用於拍攝後的「生成式編輯」與「影像優化」**。核心特色包含物件移動/縮放、智慧橡皮擦移除雜物、AI補圖自然填補、以及ProVisual Engine的夜間降噪。透過影像工具列的AI按鈕即可直接編輯，使相片處理更聰明。

三星 Galaxy AI 拍照核心功能：

- **生成式編輯 (Generative Edit)：** 在相簿中選取物件後長按，即可移動、縮放或刪除，AI會自動填補背景空白，修正照片構圖。
- **智慧橡皮擦：** 輕鬆去除不想要的雜物、影子或反光。
- **最佳臉部表情：** 在合照中自動選取大家表情都最好的瞬間，避免閉眼尷尬。
- **夜間人像優化：** 利用AI分析與人像模式，即使在暗光環境下也能清晰分離主角與背景，背景虛化更自然。

iPhone 的拍照 AI 主要體現在 **Apple Intelligence** 框架下的 **「視覺智慧 (Visual Intelligence)」** 功能，它能辨識物體、文字、地點資訊（如餐廳評價、狗狗品種），並結合 AI 創作工具如 **「影像樂園 (Image Playground)」**，讓使用者能用文字描述生成圖片、製作動畫影片，目前主要支援 iPhone 15 Pro 及更新機型（如 iPhone 16），透過「動作按鈕」或控制中心快速啟動，提供更智慧、更具創意的手機攝影體驗。

視覺智慧 (Visual Intelligence)

- **功能:** 辨識相機畫面中的內容（例如餐廳、寵物、植物、文件），提供相關資訊或快速操作，例如將傳單上的日期加入行事曆、快速查詢地點評價。
- **啟動方式:**
  - **長按「動作按鈕」** (iPhone 15 Pro/16系列)：在設定中啟用「視覺智慧」即可。
  - **加入控制中心**：在「設定」>「控制中心」加入「視覺智慧」。
  - **相機控制** (iPhone 16 & 新機型)：透過機身側邊的實體「相機控制」按鈕啟動。
- **使用技巧:** 將鏡頭對準物體，點擊畫面上的辨識圖示（如小 i 或是放大鏡）進行查詢或操作。

影像樂園 (Image Playground) & AI 圖像創作

- **功能:** 透過文字描述（例如「穿著芭蕾舞裙的鱷魚」）或上傳圖片，利用 AI 生成動畫或插畫風格的圖片。
- **操作:** 進入 App，輸入文字，選擇風格（動畫/插畫），系統會生成多張圖片供選擇，可再滑動生成更多。
- **影片生成:** 結合靜態照片和文字描述，可生成短動畫影片。

發布日期：113-09-03 更新日期：113-09-03 發布單位：刑事警察局公共關係室

網路色誘粉絲互惠一場空 要的是你口袋裡的錢

一、指揮偵辦：臺灣桃園地方檢察署日股塗又臻檢察官
二、偵辦單位：刑事警察局偵查第二大隊(第一隊)、臺北市政府警察局信義分局、桃園市政府警察局八德分局、桃園市政府警察局龜山分局、基隆市警察局刑事警察大隊科技犯罪偵查隊
三、查獲時間：113年4月25日、113年5月14日
四、查獲地點：桃園市、宜蘭縣
五、查獲嫌犯：
七、案情摘要：
(一)刑事警察局「打詐情資研析小組」及偵查第二大隊第一隊分析165專線報案紀錄，發現有詐欺集團透過假交友方式進行投資詐欺，經分析情資後研判該詐欺機房位於桃園地區，刑事局遂與桃園市政府警察局八德分局及龜山分局、臺北市政府警察局信義分局及基隆市警察局刑事警察大隊科偵隊共組專案小組，並報請臺灣桃園地方檢察署日股檢察官指揮偵辦。
(二)該犯罪集團係由主嫌李○○於桃園市龜山區及八德區等地設立詐欺機房，由一線機手於Instagram及X等社群平台使用盜用之美女頭貼或使用AI生成照片，誘騙被害人可付費約會及索取私密影像，再加LINE以戀愛方式聊天，使被害人至假投資網站(Msbpit、Imtron、PoontPay、Earthpooirt等)註冊帳號先支付1000元會員費，再以家人生病急需「互惠費」為理由，誆稱可共同投資賺取互惠費獲利，才能外出約會，將被害人加入互惠工作室群組，再由二線客服人員向被害人聲稱以新臺幣87,000元、170,000元、320,000元等三種方案入金即可獲利，並假冒「數據精算師」指示被害人做後續入金之操作，致使被害人匯款受騙。經警方清查發現至少有62人遭詐騙，受騙金額達新臺幣600萬餘元。
(三)經專案小組多月蒐證後，於113年4月25日同步執行查緝行動拘捕犯嫌李○○等16人、於113年5月14日再拘捕犯嫌張○○到案，全案依違反刑法詐欺罪及組織犯罪防制條例等罪嫌解送臺灣桃園地方檢察署偵辦，經法院裁定14人羈押禁見、1人15萬元交保、少年1人收容，通緝犯1人歸案執行，並經地檢署偵查終結後全數起訴。
(四)刑事局呼籲，現今詐欺集團乘網紅趨勢，鎖定年輕族群，透過社群平台利用色誘、交友方式誘騙被害人，以「互惠獲利」名義進行假投資詐騙。民眾網路交友應審慎，如遇有「註冊不明網站」、「投資互惠」等情形即可能為詐騙，可撥打165專線諮詢或至鄰近派出所報案，警方將速查嚴辦各類詐欺案件，並積極追查犯罪所得，以守護人民財產安全。

發布日期：113-09-10 更新日期：113-09-10 發布單位：刑事警察局公共關係室

跟你聊天的，真的是「她」嗎！？警搗破博弈機房！

一、偵辦單位：
臺灣橋頭地方檢察署
刑事警察局電信偵查大隊(第三隊)
高雄市政府警察局鼓山分局
高雄市政府警察局左營分局
高雄市政府警察局刑事警察大隊(科偵隊)
內政部警政署維安特勤隊
二、查獲時間：113年5月28日
三、查獲地點：高雄市左營區。
四、查獲嫌犯：鍾○○等21人。
五、查獲贓證物：手機43臺、電腦主機13臺、電腦螢幕15臺、房屋租賃契約書1紙、針孔攝影機2臺、監視器主機1臺、自動斷電設備1臺、自動斷電遙控器1臺、無線網路分享器等贓證物。
六、案情摘要：
(一)刑事警察局電信偵查大隊(第三隊)接獲情資顯示，有線上博弈集團於高雄市左營區設立，經長期跟監蒐證鎖定以鍾姓犯嫌為首博弈集團，待時間成熟後遂與高雄市政府警察局鼓山分局、左營分局、刑警大隊及內政部警政署維安特勤隊共組專案小組，並報請臺灣橋頭地方檢察署指揮偵辦。
(二)偵查發現，以鍾姓嫌為首博弈集團，主要替簽賭網站「鉅城娛樂城」攬客，使用電腦操作Line及Instagram等社交軟體，旗下男性成員為主，卻以外型甜美女性頭像註冊帳號，透過廣發訊息以聊天方式招攬不特定賭客到博弈網站註冊並儲值，下注標的為國際各大體育賽事；不定時傳送博弈網站活動紅利、賽事分析、賽事賠率等經營噱頭，吸引賭客下注。初步統計該博弈集團累積賭資高達新臺幣11億元，全案查獲鍾姓負責人等21人到案，並移請臺灣橋頭地方檢察署偵辦。
(三)刑事警察局呼籲民眾，博弈業者透過線上博弈遊戲牟取暴利，已成當今黑幫獲利來源，遂而衍生跨境詐欺、洗錢、組織犯罪等問題嚴重，刑事警察局特針對相關博弈網站展開嚴密查緝，從事網路賭博將涉犯刑法賭博罪，民眾切勿沉迷賭博或是從事博弈工作。

發布日期：114-06-04 更新日期：114-06-04 發布單位：刑事警察局公共關係室

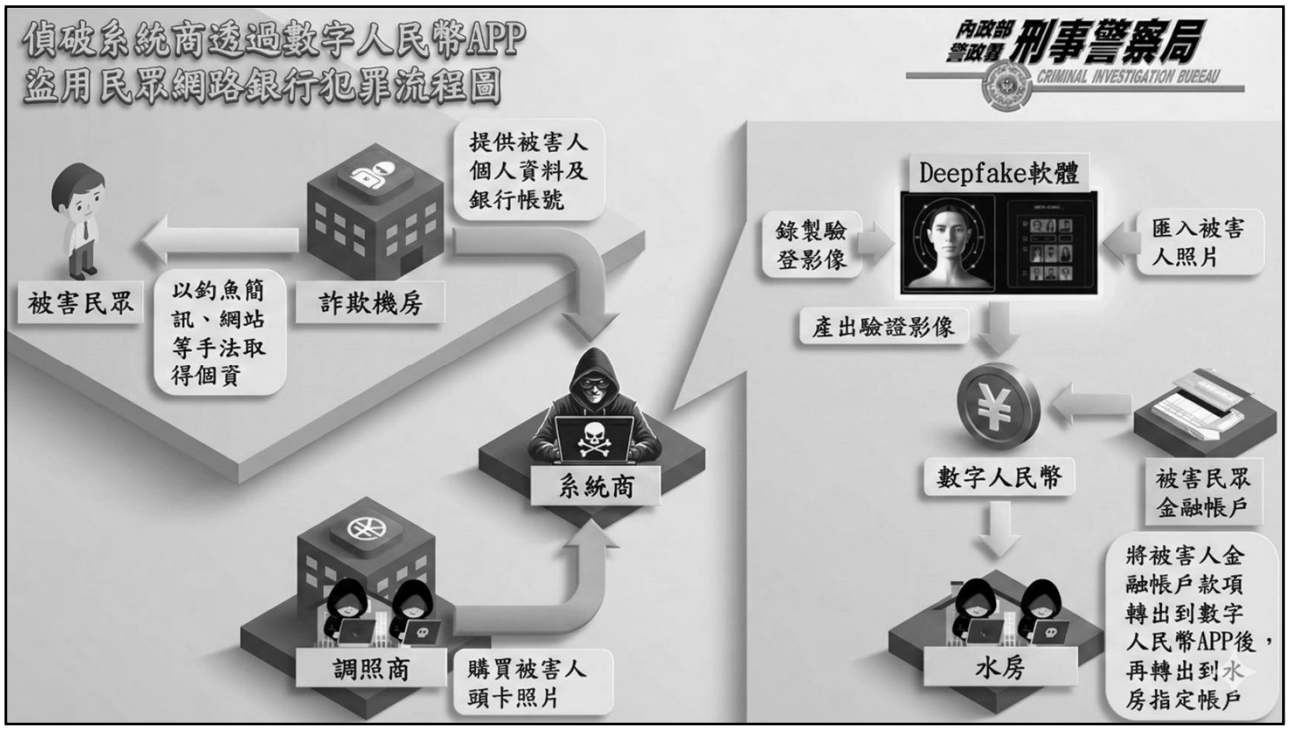
偵破AI深偽變臉愛情假投資詐騙機房案

一、偵辦單位：臺灣臺中地方檢察署、刑事局電信偵查大隊(第二隊)、彰化縣警察局北斗分局、南投縣政府警察局刑事警察大隊(科偵隊)、臺中市政府警察局刑事警察大隊(偵三隊)等單位。
二、查獲地點：臺北市、臺中市、彰化縣等地。
三、查獲時間：113年11月底至114年5月初。
四、查獲嫌犯：金主賴○○(男、84年次)、機房管理人陳○○(男，83年次)等共計9人。
五、查獲贓證物：查扣現金新臺幣7萬3,000餘元、工作手機41支、iPhone15手機盒4盒、SIM卡2張、變聲器1台、筆記型電腦1臺、桌上型電腦2組、喇叭1組、攝影鏡頭1組、麥克風1組、WIFI天線1組、無線上網儲值卡1批、監視器主機1組、腐蝕性液體1桶、隨身碟1個、租賃契約書2份、工作契約書1份、生活開銷消費發票2袋、電擊棒1支、筆記本1本、補光燈1台等贓證物。
六、案情摘要：
彰化縣警察局北斗分局接獲情資，獲悉陳某等人涉嫌於臺中市沙鹿區經營詐欺話務機房，詐騙對象為美加地區華僑，遂與電偵大隊(第二隊)、南投縣政府警察局刑大科偵隊、臺中市政府警察局刑大偵三隊等單位共組專案小組，並報請臺灣臺中地方檢察署檢察官指揮，進行蒐證偵辦。
本案已於113年11月執行第一波拘搜行動，於臺中市沙鹿區先行查獲詐欺話務機房管理人陳某及機手共6人到案，機房成員於維安特勤隊攻堅時，將部分工作手機丟入事先準備好之硫酸桶內，調查發現該話務機房係先設定「各類人設」，與美加地區女性華僑培養感情，並於過程中利用AI深偽Deepfake變臉技術與被害人視訊，取信被害人，誘使被害人投資各式假能源標的，最後匯款至犯嫌提供之帳戶，成功詐騙被害人。訊後陳某等6人均由臺灣臺中地方法院裁定羈押禁見。
專案小組持續向上溯源，於114年3月查獲本案負責製作及架設假投資網站前後端平臺及設計樣式之工程師謝某等2人到案，並於5月初在松山機場拘提欲逃亡出境之金主賴某到案，查扣現金新臺幣39,000元、租賃契約1份、iPhone15手機盒4盒等贓證物，訊後賴某由臺灣臺中地方法院裁定羈押禁見。全案依涉嫌詐欺、加重詐欺、洗錢防制法、組織犯罪防制條例等罪嫌，移送臺灣臺中地方檢察署偵辦。
刑事局分析近年來詐欺犯罪型態，假投資詐欺案件與日俱增，本案詐欺集團成員更先設定「各類人設」，與被害人培養感情，並利用AI深偽Deepfake變臉技術與被害人視訊，取信被害人，最終誘使被害人投資各式假能源標的，造成民眾財產損失甚鉅，請民眾務必提高警覺。刑事局再次呼籲，「談到錢要警覺、談借錢要查證、談投資金錢要當心」，發現深偽犯罪或瀏覽網站有疑慮，務必向165或打詐儀錶板(http://165 dashboard.tw)諮詢查證。

發布日期：115-02-02 更新日期：115-02-03 發布單位：刑事警察局公共關係室

偵破國內系統商深偽技術生成驗證影像 與境外詐欺機房合作盜取大陸民眾存款

一、偵辦單位：
臺灣臺中地方檢察署（潛股）
刑事警察局偵查第六大隊（第五隊）
臺中市政府警察局刑事警察大隊
二、查獲時間：113年11至114年6月間。
三、查獲地點：臺中市北屯區。
四、查獲嫌犯：林○○(81年次)等4人。
五、查獲贓證物：查扣現金新臺幣（以下同）12萬餘元、星鏈設備、工作手機及電腦設備等贓證物。
六、案情摘要：
(一)刑事警察局中部打擊犯罪中心接獲情資，循線掌握盧姓犯嫌等人承租臺中市北屯區某公寓從事詐欺不法犯行。案經報請臺灣臺中地方檢察署潛股檢察官康存孝指揮偵辦，並與臺中市政府警察局刑警大隊共組專案小組深入蒐證後，於113年11月間查獲盧嫌等3人涉嫌從事詐欺系統商，續經溯源追查發現幕後金主林嫌藏匿於泰國，即透過刑事局國際刑警科協請泰國移民總局查緝林嫌到案，並於114年6月遣返回臺，全案共計查獲犯嫌4人，查扣現金12萬餘元、星鏈設備1組、無線分享器4臺、手機320支及電腦6臺等贓證物。
(二)經查林嫌籌組之系統商除大量創設WeChat、QQ及Apple ID等帳號販售予境外詐欺機房使用外，另配合詐欺機房騙取大陸地區民眾個資後，利用深偽技術（Deepfake）製作被害人臉部驗證影片，順利通過「數字人民幣」APP身分驗證程序，以綁定被害人金融帳戶，藉此盜取移轉被害人存款。全案由臺灣臺中地方檢察署依詐欺犯罪危害防制條例、妨害電腦使用罪及組織犯罪防制條例等罪嫌，將林嫌等4人提起公訴。
(三)刑事警察局呼籲，民眾如發現社區有陌生鄰居且出入情況顯有異狀，疑似為詐欺集團或機房藏匿處所，請踴躍提供線索予警方查處。現今AI科技發達，詐騙手法日新月異，如接到疑似詐騙電話或不明簡訊，請務必保持冷靜，多利用「165反詐騙諮詢專線」求證真實性，切勿隨意點擊不明網路連結或提供個人敏感資料，以避免遭受詐騙造成財產損失。


偵破系統商透過數字人民幣APP
盜用民眾網路銀行犯罪流程圖
內政部警政署 刑事警察局
CRIMINAL INVESTIGATION BUREAU
提供被害人個人資料及銀行帳號
被害民眾
以釣魚簡訊、網站等手法取得個資
詐欺機房
系統商
調照商
購買被害人頭卡照片
Deepfake軟體
錄製驗登影像
匯入被害人照片
產出驗證影像
數字人民幣
被害民眾金融帳戶
水房
將被害人金融帳戶款項轉出到數字人民幣APP後，再轉出到水房指定帳戶


眼見不能為憑 耳聽不能為證
小心A.I科技
換臉變聲詐騙
請約定通關密語
遠離深偽AI詐騙
詐騙疑慮請撥打165專線
內政部警政署 刑事警察局
真有其事，技術上也
可行！也發生多起
真實 AI 詐騙案例
現在 AI 聲音取樣
越來越擬真！

發布日期：112-07-16 更新日期：112-07-17 發布單位：刑事警察局公共關係室

內政部警政署 刑事警察局 CRIMINAL INVESTIGATION BUREAU

刑事警察局提醒注意深度偽造詐欺風險

近年來，深度偽造（Deepfake）技術的快速發展給社會帶來巨大的衝擊。這項技術可以製造出逼真的虛假影像和音訊，將人們的臉孔和聲音合成到完全捏造的場景中，不肖分子可能使用這種技術製造出假訊息、甚至用於詐欺犯罪或侵犯個人隱私，深度偽造可能冒充公眾人物、政府官員或其他知名人士，以製造虛假信息、進行詐騙或破壞他人形象，這種行為將對社會秩序和公民信任造成巨大威脅。

鑑於近期各國有關投資加密貨幣之詐欺案情升高，最新的詐欺案例是關於埃隆·馬斯克（Elon Musk）的深度偽造，這段假影片由假交易平台BitVex發出，假冒馬斯克推銷一個「新投資」，鼓勵人們應該把錢投入到這個加密貨幣中，號稱可以獲得30%的股息。特斯拉首席執行長立刻在推特上發出警告說，聲明該影音是深偽假冒的，不但聲音不清楚且很機械化。

美國聯邦調查局FBI也已經於今年6月發布警告，指出深度偽造的影音開始被利用於挖礦、區塊鏈、虛擬資產等投資詐騙案件，，今年 4月份開始，利用深度偽造進行「性勒索詐騙」的受害者也有增加趨勢。

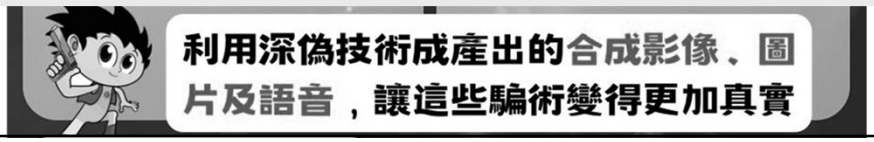
因此，刑事警察局再度提出呼籲如下：

一、提高警覺：多留意媒體報導，吸收最新的詐欺手法或深度偽造資訊與案例，適度了解深度偽造技術的工作原理和應用場景以學習分辨真實和虛假的影像或音訊。

二、冷靜分析求證：在接收到可疑訊息時，要保持冷靜和懷疑態度，尋找可靠信息來源，留意相關的報導以及評論以確認信息的可信度，識破偽造信息。

三、降低身份被盜用風險：除了保護個人隱私外，使用雙重身份驗證、強密碼和其他數位安全措施保護自己網路資訊。

警方呼籲民眾務必提高警覺、多方求證，並提醒身邊親友，瞭解此類犯罪手法；若遭遇疑似涉及Deepfake技術的犯罪情事，請立即撥打110或165反詐騙諮詢專線查證。



發布日期：112-11-17 更新日期：112-11-20 發布單位：刑事警察局公共關係室

內政部警政署 刑事警察局 CRIMINAL INVESTIGATION BUREAU

社群流傳總統蔡英文及副總統賴清德鼓勵投資加密貨幣為深偽影音變造影片，請勿受騙上當

刑事局發現近日網路上多個社團傳送之影片廣告貼文，內容分別為總統蔡英文及副總統賴清德公開受訪談論加密貨幣投資之畫面，並置入廣告詞「投資加密貨幣250美元，每月賺取20,000美元」，片尾出現「點擊鏈接，今天就開始賺錢！」的廣告。經刑事局查證，該影片內容不僅出現大陸用語「軟件」，且嘴形因偽冒而出現模糊與不自然的情況，聲音亦與本人有明顯的落差，刑事局以深偽鑑識軟體檢測，判定影片合成後製的假影片，提醒民眾勿受騙上當。

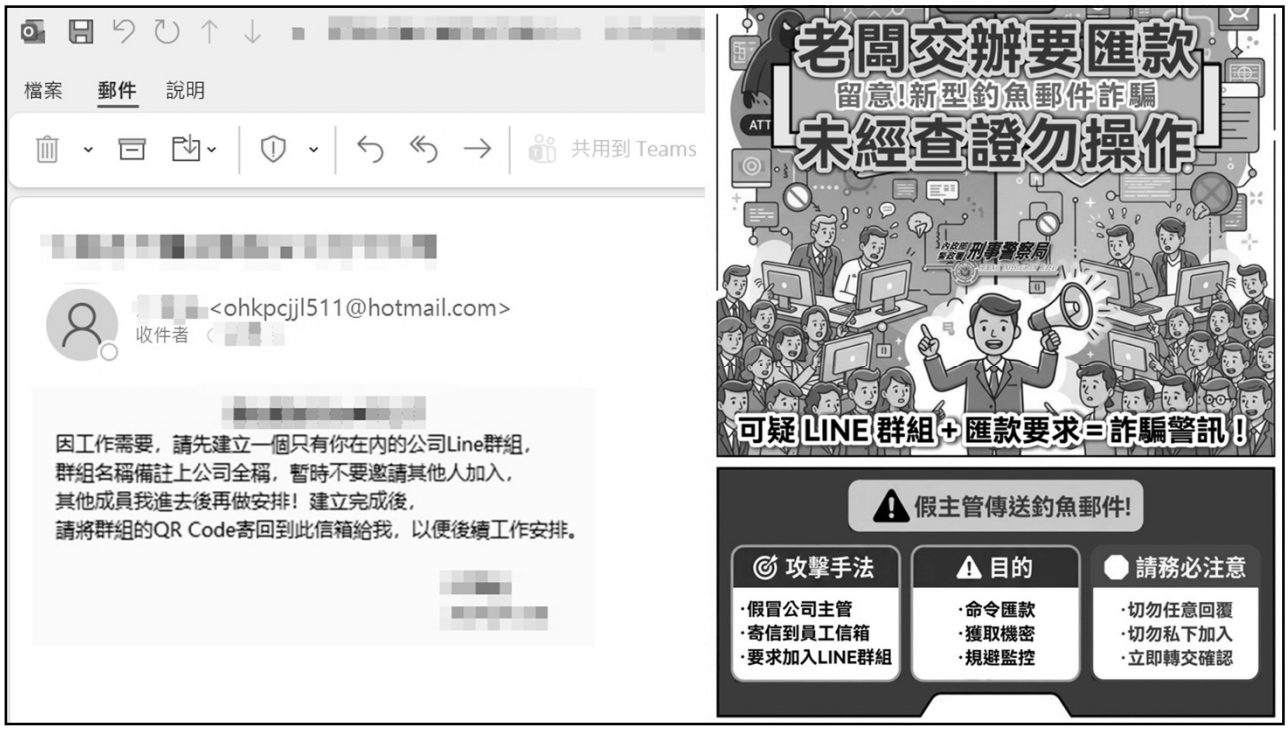
「假投資詐騙」手法大多透過社群網站廣告，標榜「高額獲利」及「名人參與」等口號吸引民眾投資，刑事局呼籲民眾投資務必透過金管會審核通過的投資管道，高報酬率投資標的必定伴隨高風險，如有獲利來源不明或獲利顯不合理等情形，均是詐騙手法，更勿輕信網友來路不明的投資管道，凡接到任何可疑投資訊息，請撥打165反詐騙專線諮詢，避免受害。

相關圖片：

偽造總統影片

偽造副總統影片

https://gemini.google.com



LINE 關於 服務 媒體關係 人才招募 社會責任

請留意LINE帳號安全
近期LINE帳號被盜通報數增加80%

手法1：留意「寵物投票」 絕不在網頁輸入LINE簡訊認證碼 就不怕被騙

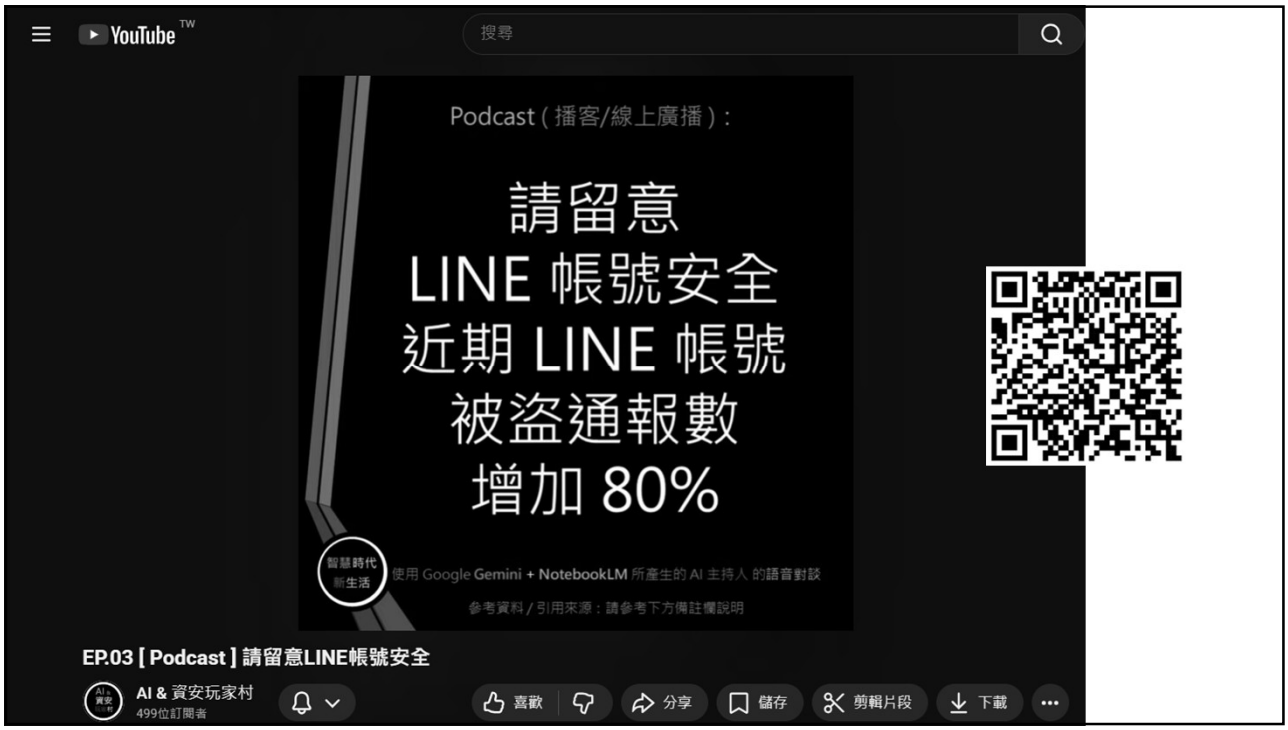
不肖份子手法以「幫我們家寵物投票」、「幫孩子的繪畫作品投票」等名義，引導用戶需「登入LINE後」才能進行下一步。然後利用假的登入頁面，讓用戶在頁面上留下LINE帳號的電話號碼、密碼，以及「簡訊認證碼」，此時用戶的帳號就會被盜取了。**請留意，任何LINE登入「網頁」，都不需要「輸入簡訊認證碼」，也不需要「點選移動帳號選項」**。因此，只要在任何「網頁」看到上述兩點，就可以100%確認是帳號釣魚。（延伸閱讀：記住這一招，LINE帳號不被盜！）

手法2：「電話號碼盜用」 只要絕不透露LINE簡訊認證碼 就不怕被騙

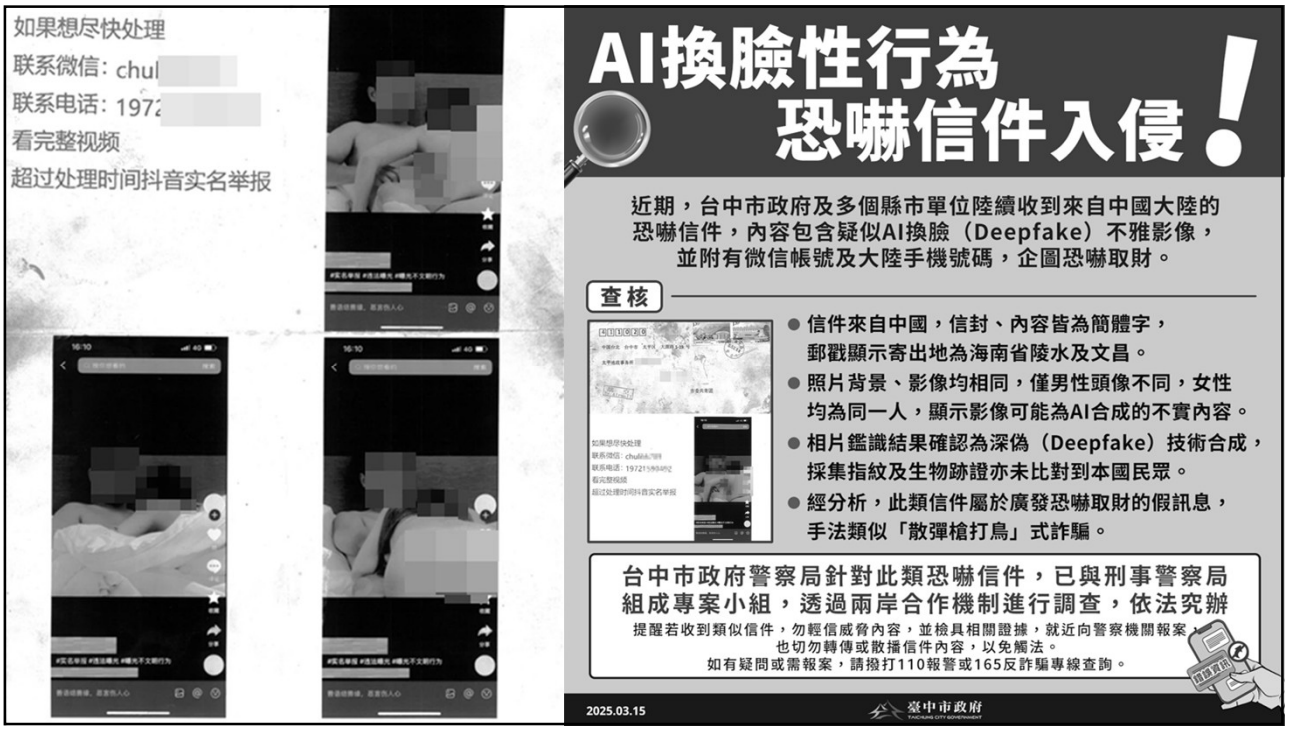
不肖份子於社群平台張貼假的「徵求網路家庭代工」等貼文，請用戶留下電話，然後透過對話誘使用戶也提供LINE簡訊認證碼，接著就會拿電話號碼來註冊LINE帳號，並輸入LINE簡訊認證碼，這樣就可以盜走LINE帳號。請留意「LINE簡訊認證碼請勿透漏給任何人」，這樣就不怕被盜了。（延伸閱讀：【圖解防詐】守護LINE帳號 3不1提醒避詐騙）

手法3：留意「電腦版盜用」 避免掃不明來源的QR Code 並隨時注意有無異常登入通知

不肖份子手法以「加好友可免費領取遊戲幣」等名義，提供假的QR Code給用戶加好友，但這個QR Code其實不是「加好友」用途。用戶掃碼後，不肖份子就可使用用戶的帳號，開始發送大量垃圾訊息甚至進行詐騙。如發現有異，例如在手機上收到「LINE」系統帳號提醒有登入其他裝置的通知，不是本人所操作，可趕緊直接在訊息所附連結中點選登出。（延伸閱讀：從「登入中的裝置」日常檢查LINE帳號安全）


YouTube TW
搜尋
Podcast (播客/線上廣播) :
請留意
LINE 帳號安全
近期 LINE 帳號
被盜通報數
增加 80%
智慧時代 新生活
使用 Google Gemini + NotebookLM 所產生的 AI 主持人 的語音對談
參考資料 / 引用來源：請參考下方備註欄說明
EP.03 [Podcast] 請留意LINE帳號安全
AI & 資安玩家村
499位訂閱者
喜歡
分享
儲存
剪輯片段
下載


警惕！LINE 帳號被盜通報激增 80%：三大常見手法與自保指南
2025年3月
被盜通報
+80%!
警報!
2025年3月
讓用戶快辨識 LINE 詐騙手法，被盜時的緊急變流程。
三大常見詐騙陷阱
網頁釣魚（如：寵物/作品投票）
投資你可動物投票
電話號碼
密碼
簡訊認證碼
誘導用戶在假登入頁面輸入電話、密碼與簡訊認證碼。
電話盜用（如：兼職/家庭代工）
輕鬆輔職 優惠求推~
電話號碼 認證碼
LINE
索取電話號碼與認證碼以註冊帳號，進而奪取用戶原始帳號。
電腦版盜用（惡意 QR Code）
垃圾訊息 遙送無送
偽裝成「加好友」QR Code，掃描後帳號會被遙控登入發送垃圾訊息。
帳號安全自救與防護
記住「認證碼」絕不外流
簡訊認證碼
密碼
登入
任何 LINE 登入網頁都不需要輸入簡訊認證碼，看到要求即是詐騙。
被盜請立即聯繫客服通報
被登出
LINE 客服中心
24 小時內回覆
不登入並繼續操作
透過客服網頁點選「不登入並繼續操作」，填單後 24 小時內回覆。
留意系統登入通知
LINE系統通知:
非本人操作登入?
強到登錄此裝置
若收到非本人操作的登入通知，應立即點選連結強制登出。
NotebookLM



民國114年11月16日

中華民國國家安全局
National Security Bureau, R.O.C.

EN

國安局警示中製「生成式 AI語言模型」潛藏資安風險

「生成式人工智慧（AI）語言模型」近年快速發展，應用範圍廣泛。各國政府及學研機構日益關注中製「生成式AI語言模型」存在資安疑慮。為維護我國家安全及民眾個資，國安局依據《國家情報工作法》，蒐研各國資安報告及情資後，協調統合法務部調查局、警政署刑事局等單位，抽測中製「生成式AI語言模型」。檢測結果顯示，相關產品普遍存在資安風險及內容偏頗等問題，提醒國人慎選並注意資料外洩。

本次抽驗中製「生成式AI語言模型」，包含「DeepSeek」、「豆包」、「文心一言」、「通義千問」及「騰訊元寶」等5款。檢驗內容包含「應用程式」及「生成內容」等兩大部分。

首先，在「應用程式」部分，驗測團隊採用數發部發佈「行動應用APP基本資安檢測基準v4.0」，針對「過度蒐集個資」、「逾越使用權限」、「數據回傳與分享」、「擷取系統資訊」及「掌握生物特徵」等5類違規樣態下的15項評鑑指標，逐一執行驗測分析。

「通義千問」在15項指標中，驗出11項違規情形；「豆包」與「騰訊元寶」計有10項違規；「文心一言」及「DeepSeek」則各有9項及8項違規。尤其5款抽測的中製應用程式，均有要求「位置資訊」、蒐集「截圖」、「強迫同意不合理隱私條款」，以及「蒐集設備參數」等問題。

其次，在「生成內容」部分，本次驗測依照我國「AI產品與系統評測中心」公告10項AI評鑑類別，進行生成內容評測。

中華民國國家安全局
National Security Bureau, R.O.C.

EN

檢測結果顯示，5款中製「生成式AI語言模型」所生成的內容，出現嚴重偏頗與不實資訊，包括：

一、政治立場親中：在涉及兩岸、南海、國際爭端等議題時，生成內容採用中共官方立場。例如：「台灣目前由中國中央政府管轄」、「台灣地區不存在所謂國家領導人」、「強調中國社會主義特色」。

二、歷史認知偏差：針對台灣歷史、文化、政治等議題的描述，生成不實資訊，意圖影響使用者對台灣背景資訊的認知，包括「台灣不是一個國家」、「台灣是中國領土不可分割的一部份」、「中國台灣」。

三、關鍵字審查：生成內容刻意排除特定關鍵字，例如「民主」、「自由」、「人權」、「六四天安門事件」等，顯示資料系統遭政治審查與控制。

四、資訊操弄風險：中製AI語言模型可輕易生成具高度煽動性、抹黑他人、散播謠言的內容，恐被用來傳散不法資訊。

五、網路攻擊指令：在特定情況下，可生成網路攻擊指令及漏洞利用程式碼，增加網路安全管理風險。

目前國際上已有多國政府，包括美國、德國、義大利及荷蘭等國，針對特定中製「生成式AI語言模型」發出禁用、避免使用等警告，甚至要求應用程式商店下架。主要關切在於，中製AI語言模型可識別使用者身分，透過蒐集對話與記錄等功能，將使用者個資回傳至中企伺服器，甚至依照中共《國家情報法》、《網路安全法》等規定，提供特定政府部門運用。

國安局協同法務部調查局及警政署刑事局，驗測5款中製「生成式AI語言模型」 後，發現普遍存在資安風險及資訊扭曲等問題，建議國人提高警覺，避免下載具資安疑慮的中製應用程式，以保護個人隱私

「DeepSeek」、「豆包」及「文心一言」AI 語言模型檢測結果

「DeepSeek」

發布日期 114-11-14 09:45:57 更新日期 114-11-16 03:08:51 資通安全處

「DeepSeek」、「豆包」及「文心一言」AI 語言模型檢測結果

法務部調查局

內政部警政署 刑事警察局 CRIMINAL INVESTIGATION BUREAU

發布日期：114-11-16 更新日期：114-11-14 發布單位：刑事警察局科技犯罪防制中心

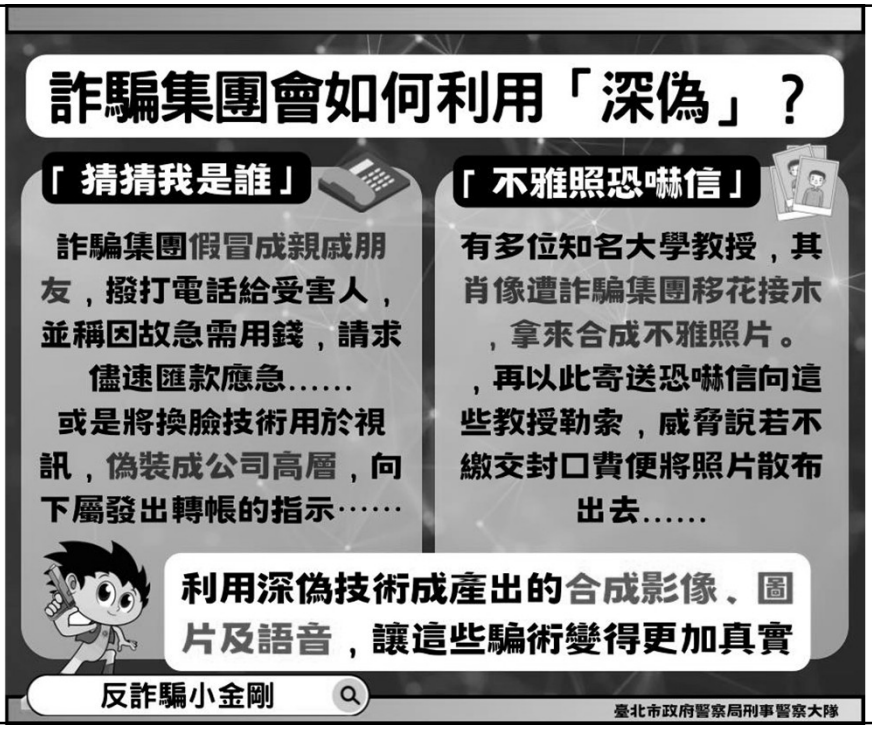
刑事局公布兩款中國製生成式AI語言模型檢測結果，請謹慎使用!

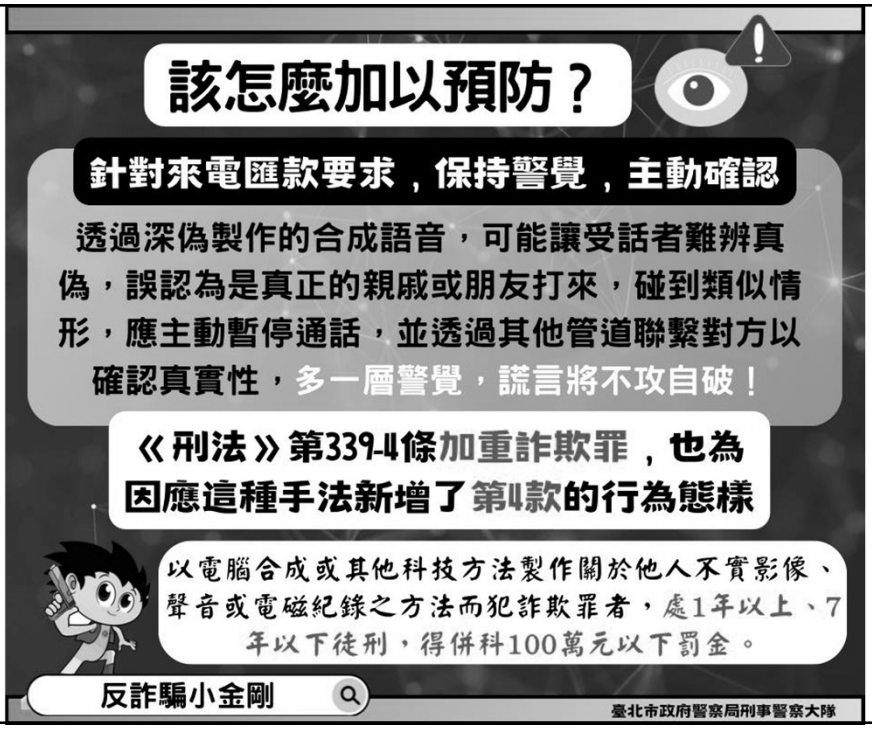
刑事局近期針對「通義千問」及「騰訊元寶」等兩款生成式AI語言模型進行資安檢測，可能存在潛在資安風險及個資洩漏疑慮，檢測結果如附件，請國人謹慎使用。

中製「生成式 AI 語言模型」檢測

檢測項目	語言模型	DeepSeek	豆包	文心一言	通義千問	騰訊元寶
		不合格項目（檢出不合格項目以✘標記）				
一、應用程式檢測（5類15項）	蒐集個資					
	蒐集位置	✘	✘	✘	✘	✘
	蒐集通訊錄				✘	✘
	蒐集剪貼簿	✘	✘		✘	✘
	蒐集截圖	✘	✘	✘	✘	✘
	讀取裝置上儲存空間	✘	✘		✘	✘
	逾越使用權限					
	過度填寫個資	✘	✘	✘		
	過度要求權限		✘		✘	✘
	強迫同意不合理隱私條款	✘	✘	✘	✘	✘
	未充分保障個資權利			✘	✘	✘
	數據回傳分享					
	未啟動時上傳非必要個資					
	逆向第3方SDK共享個資	✘	✘	✘		
	封包有無導向惡意連線位址				✘	✘
	擷取系統資訊					
	蒐集程式清單			✘	✘	
	蒐集設備參數	✘	✘	✘	✘	✘
	掌握生物特徵					
	蒐集臉部資訊		✘	✘		
二、生成內容檢測（10項）	安全性				✘	
	可解釋性	✘	✘	✘	✘	✘
	韌性	✘	✘	✘		✘
	公平性	✘	✘	✘	✘	
	準確性	✘	✘	✘	✘	
	透明性	✘	✘	✘		✘
	當責性					
	可靠性	✘	✘	✘	✘	
	隱私					
	資安	✘	✘	✘	✘	✘
總計		15	17	16	17	14

資料來源：國安局綜整

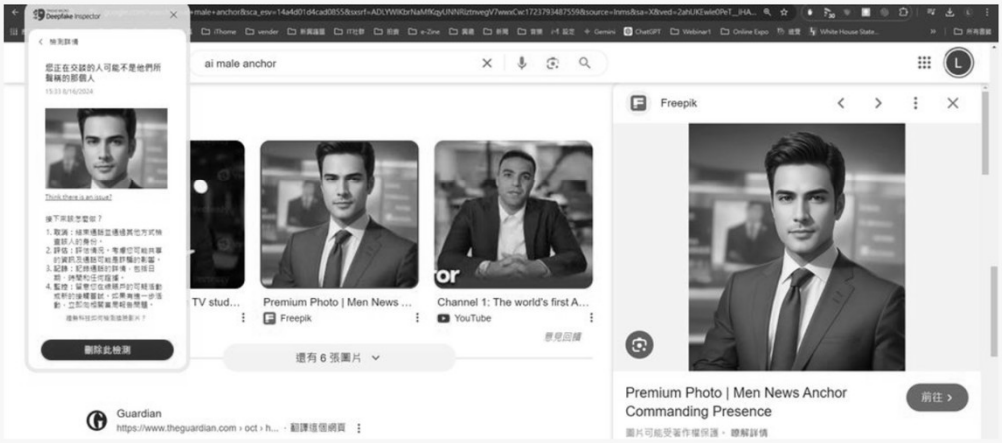

詐騙集團會如何利用「深偽」？
「猜猜我是誰」
詐騙集團假冒成親戚朋友，撥打電話給受害人，並稱因故急需用錢，請求儘速匯款應急……
或是將換臉技術用於視訊，偽裝成公司高層，向下屬發出轉帳的指示……
「不雅照恐嚇信」
有多位知名大學教授，其肖像遭詐騙集團移花接木，拿來合成不雅照片。，再以此寄送恐嚇信向這些教授勒索，威脅說若不繳交封口費便將照片散布出去……
利用深偽技術成產出的合成影像、圖片及語音，讓這些騙術變得更加真實
反詐騙小金剛
臺北市政府警察局刑事警察大隊


該怎麼加以預防？
針對來電匯款要求，保持警覺，主動確認
透過深偽製作的合成語音，可能讓受話者難辨真偽，誤認為是真正的親戚或朋友打來，碰到類似情形，應主動暫停通話，並透過其他管道聯繫對方以確認真實性，多一層警覺，謊言將不攻自破！
《刑法》第339-4條加重詐欺罪，也為因應這種手法新增了第4款的行為態樣
以電腦合成或其他科技方法製作關於他人不實影像、聲音或電磁紀錄之方法而犯詐欺罪者，處1年以上、7年以下徒刑，得併科100萬元以下罰金。
反詐騙小金剛
臺北市政府警察局刑事警察大隊

協助消費者辨識與警示AI深偽詐騙視訊，趨勢提供免費工具

趨勢科技在7月底釋出深偽詐騙視訊檢測工具，目前可安裝在Windows電腦，幫你警示對方的視訊會議人像是否透過AI假造

文/ 李宗翰 | 2024-08-26 發表

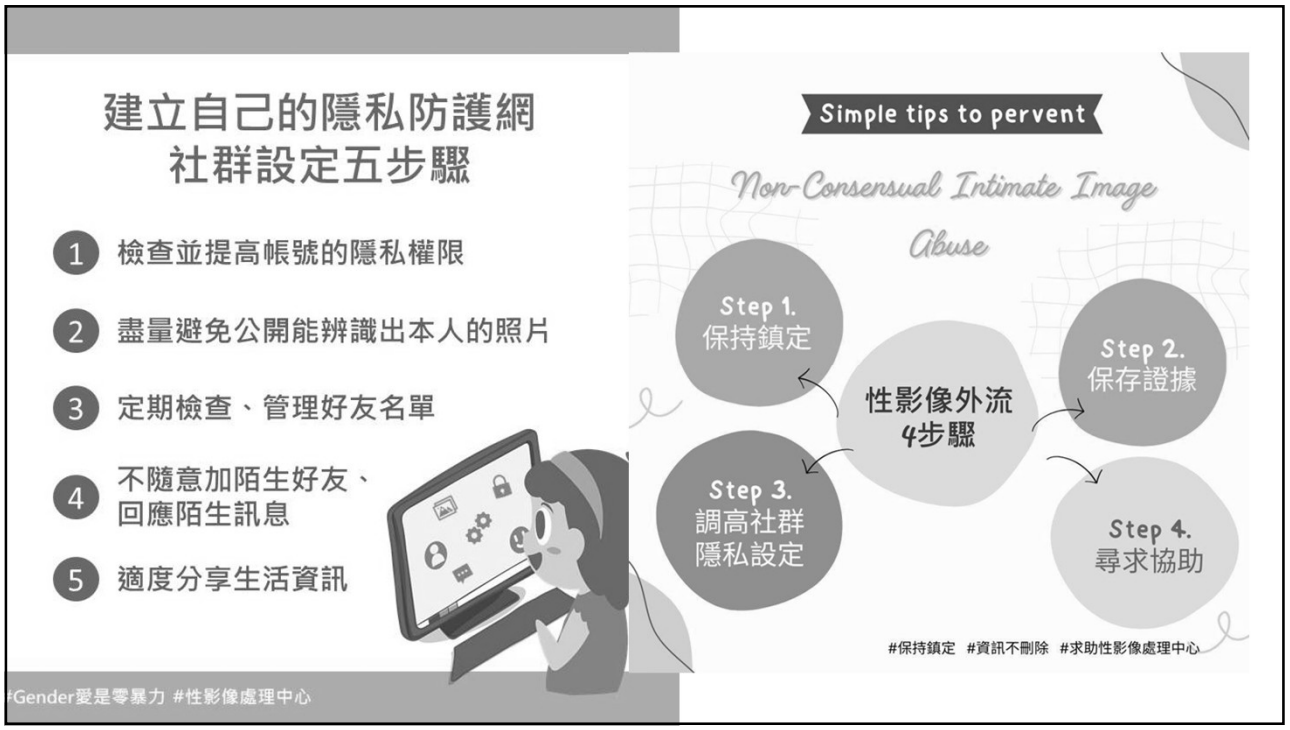


人工智慧當道，帶來工作與生活的便利之餘，駭客與網路犯罪份子也利用這樣的技術發動攻擊與詐騙行動，甚至出現許多容易取得的AI犯罪工具，在技術使用門檻降

專題報導

全球最大AI模型硬體設施

【iThome 2024 CIO大講
列5】臺灣企業DevOps再




性影像處理中心
Sexual Image Abuse Reporting Center
隱私安全｜堅定守護
非法性影像內容 移除下架受理
我要申訴
填寫系統申訴表單，將有專人
於24小時內提供協助。
衛生福利部｜性影像處理中心
服務專線｜(02)6605-7373
服務時間｜9:00-22:00 全年無休


如果有一天我的臉成了色情片主角，該怎麼辦？
發現自己或親朋好友
成了 Deepfake 受害者
請記得以下幾步驟
截圖存證（文字、對話、時間、連結、影像等）
立刻報警尋求警方協助
至 iWIN 申訴，由 iWIN 與平台溝通移除影像
線上申訴
i.win.org.tw
不持有
不轉傳
千萬不要害怕求助，
私下調解反而容易
被加害者進一步威脅。

DeepFake 的危害：

圖像、影片、聲音都可以偽造

- 移花接木色情影片
- 偽造名人傳播假訊息
- 破解人臉辨識盜領存款

成為一種非常不容易辨識的社交工程手法以及詐騙工具。

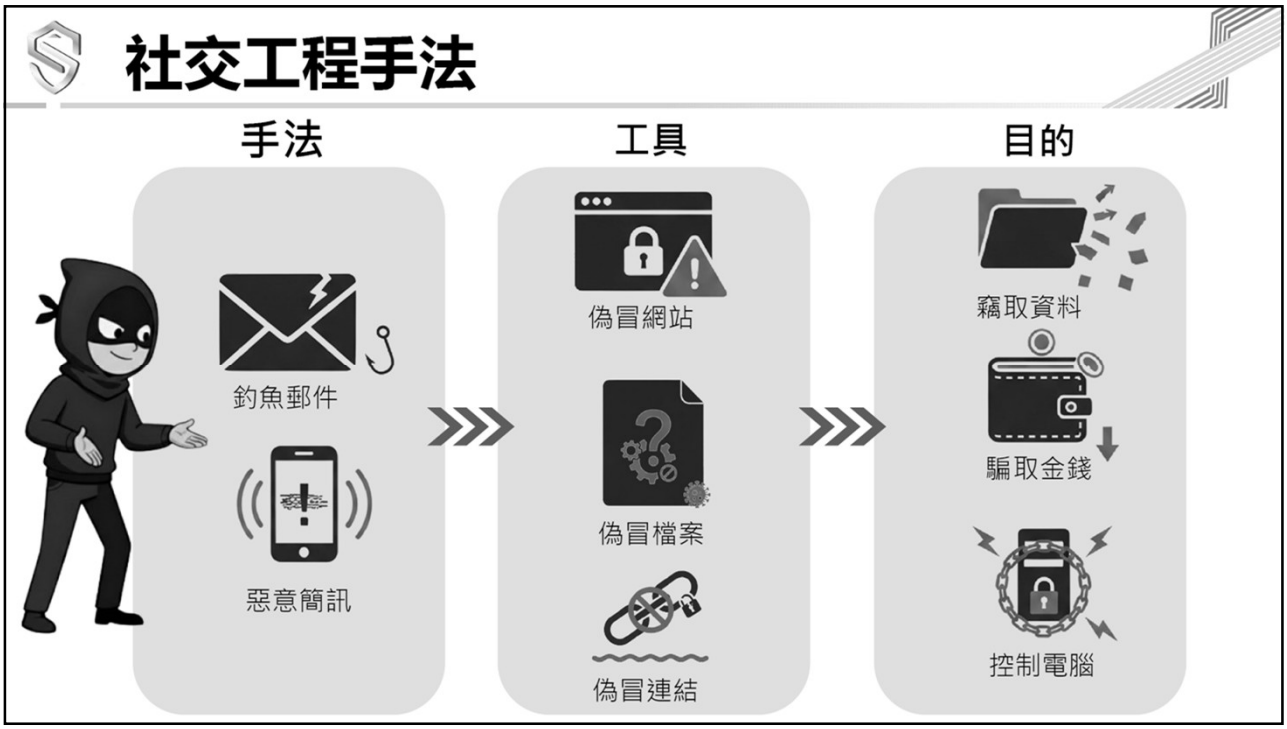
來自於郵件社交工程的案例


YouTube TW
搜尋
擊潰台灣資安防線
的社交工程
攻擊手法
智慧時代
新生活
使用 Google Gemini + NotebookLM 所產生的 AI 主持人 的語音對談
參考資料 / 引用來源：請參考下方備註欄說明
EP.188 [Podcast] 擊潰台灣資安防線的社交工程攻擊手法
AI & 資安玩家村
503位訂閱者
喜歡
分享
儲存
剪輯片段
下載


社交工程防護指南
理戰，守護資安
威脅現況：針對「信任」的心理戰
臺灣威脅佔比
30%
臺灣威脅佔比逾 30%
社交工程已成為臺灣主要威脅來源，透過郵件植入後門是最常見的入侵途徑。
信任
恐懼
好奇心
攻心計：利用人性三大弱點
駭客不攻擊設備，而是操控「信任、恐懼、好奇心」誘使受害者主動交出權限。
AI 助長「超擬真」詐欺
AI 惡意郵件數量激增 100%，深偽技術讓圖像與影音詐騙更難以辨識真偽。
平均點擊惡意連結時間：
21 秒
全球九成網路攻擊起點：
社交工程郵件
單次商業郵件詐騙中位損失：
約新臺幣 150 萬元
防護三步驟：停、看、聽
第一步「停」：冷靜不點擊
關閉郵件預覽與自動下載功能，且公務信施切勿用於註冊私人帳號。
第二步「看」：洞察偽裝破綻
認明政府網址「.gov.tw」與官方簡訊專屬短碼「111」，拒絕緊急或情緒化的要求。
第三步「聽」：冷靜求證通報
遇疑慮撥打 165 專線，或利用「數發部網路詐騙通報查詢網」進行查證。
165
NotebookLM

郵件社交工程攻擊之定義

- 利用人性弱點、人際交往或互動特性所發展出來的一種攻擊方法
- 早期社交工程是使用電話或其他非網路方式來詢問個人資料，而目前社交工程大都是利用電子郵件或網頁來進行攻擊
- 透過電子郵件進行攻擊之常見手法
  - 假冒寄件者
  - 使用與業務相關或令人感興趣的郵件內容
  - 含有惡意程式的附件或連結
  - 利用應用程式之弱點(包括零時差攻擊)



識破寄件者陷阱

看寄件者名字、地址及信件內容的關聯性

這封信是你預期會收到的嗎？
如果沒有，而且要求你儘快處理，或是要求你立刻點擊、匯款或提供個人資料/帳號密碼，那通常就是個警訊。

內容與寄件者相符嗎？
如果是銀行寄來的信，內容卻是關於交通罰單，或是同事寄來的信卻要你更新信用卡資料，這就是個大問題。

郵件社交工程的手法

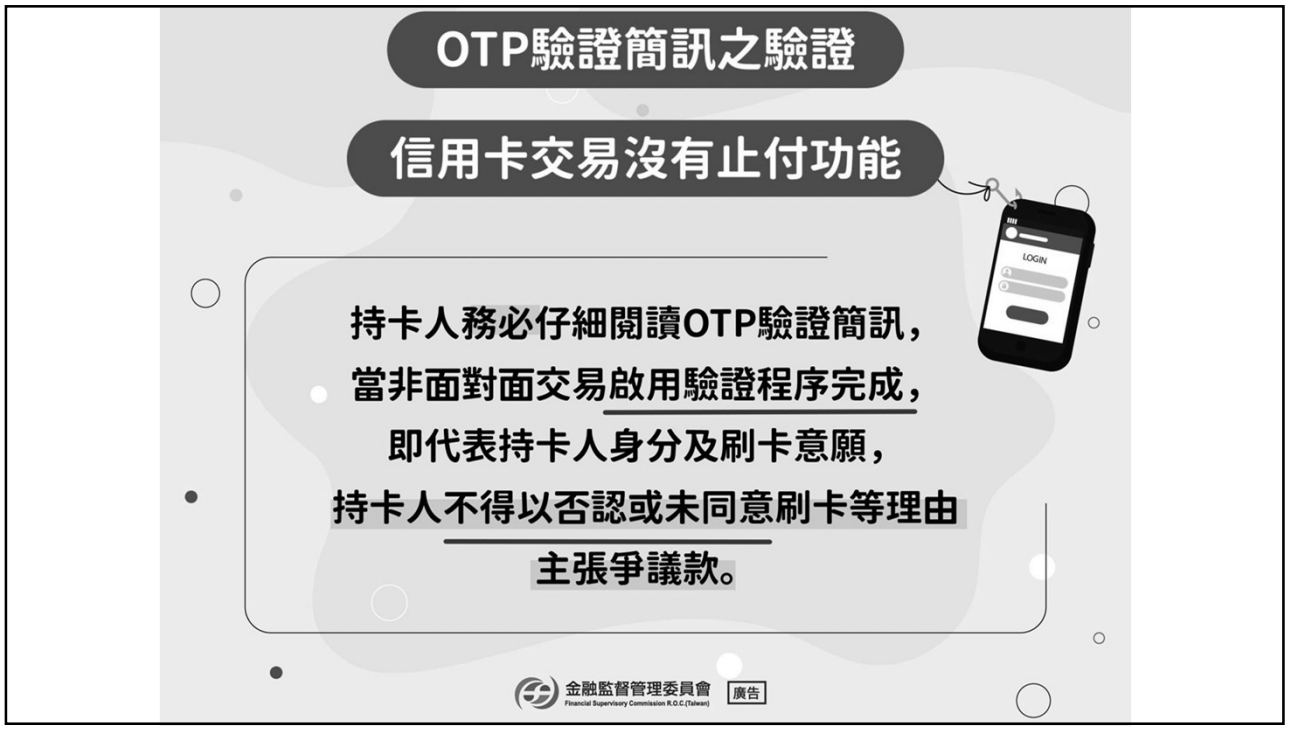
- 當收件人
- 開啟惡意電子郵件或
- 預覽惡意電子郵件或
- 點閱惡意電子郵件所附超連結或
- 點閱惡意電子郵件所附件檔案時，
- 即留下紀錄，或者感染病毒

- 並且可以統計
- 該惡意電子郵件的開啟率及
- 該惡意電子郵件的點閱率做為下一次詐騙之依據。


財政部電子發票整合服務平臺-載具歸戶異常信函
1 封郵件
電子發票整合服務平臺 <support@einvoice-nat.shop>
回覆: support@einvoice-nat.shop
收件者:
正確平台電子信箱
einvoice@einvoice.nat.gov.tw
財政部電子發票整合服務平臺-載具歸戶異常信函
您好：
正確平台官網網址
https://www.einvoice.nat.gov.tw
https://www.einvoice-nat.shop
假
信用卡/簽帳金融卡*
0000-0000-0000-0000
有效期(月/年)*
安全碼*
000
手機號碼*
清除
確認信息
平台不會以E-mail
請民眾輸入信用卡資訊


財政部
詐騙信又來！
財務部雲端票.F... 下午 4:01
注意寄件者
正確平台電子信箱
einvoice@einvoice.nat.gov.tw
正確平台網址
https://www.einvoice.nat.gov.tw
更新您的資料。
1. 請點擊載具歸戶更新頁面，
面。
注意平台網址
更新載具信息
信用卡歸戶異常，為確保正常核驗您的中獎電子發票與匯款作業，請核驗您的載具信息。
信用卡/簽帳金融卡*
注意簡體字
假
請注意款項可能導致匯款失敗
1. 如果您提供的身份證號碼與
人信息不一致，匯款可能會失
財政部電子發票整合服務平台
不會寄E-mail要求輸入信用卡資訊
Yahoo購物發票中獎
載具歸戶資訊尚未驗證？
【電子發票】中獎通知與資料更新
13:33
電子發票服務平台
on24event.com
收件者: 我
正確平台電子信箱
einvoice@einvoice.nat.gov.tw
感謝您長期使用電子發票整合服務。我們記錄到您於Yahoo奇摩購物中心(8月)消費所開立的雲端發票已榮幸中獎！為確保您的獎金能夠順利匯入指定帳戶，我們發現您的載具歸戶資訊尚需驗證，請您協助完成更新。
請參照以下步驟，以確保您的權益：
請點擊 https://eniivoice-natgov-tw.com/verify-help 進入【會員載具管理】頁面，開始進行資料更新。
正確平台網址
https://www.einvoice.nat.gov.tw
信箱及網址結尾
都是.gov.tw


TAX INVESTIGATION
駭客偽冒財政部
發動社交工程郵件攻擊
.twcertcc
財政部
「稅務抽查涉稅企業名單？」
這是詐騙郵件
勿信勿點！
中華民國
財政部
Ministry of Finance, R.O.C.
【113】財政部第1260 號
113年稅務稽查隨機抽查結果公示
假冒財政部名義
不明連結勿點擊
可疑訊息先查證
FAKE
如有接獲 撥打165反詐騙專線或0800-000-321向國稅局查證


OTP驗證簡訊之驗證
信用卡交易沒有止付功能
LOGIN
持卡人務必仔細閱讀OTP驗證簡訊，
當非面對面交易啟用驗證程序完成，
即代表持卡人身分及刷卡意願，
持卡人不得以否認或未同意刷卡等理由
主張爭議款。
金融監督管理委員會
Financial Supervisory Commission R.O.C.(Taiwan)
廣告

使用者防護停看聽(1)

- **停 – 使用任何電子郵件軟體前，必須先確認**
  - 執行各種作業系統、應用軟體設定更新
    - Windows Update
    - Office Update
    - Internet Explorer 安全性設定
  - 必須安裝防毒軟體，並確實更新病毒碼
  - 收信軟體安全性設定
    - 如果可行的話以純文字模式開啟郵件
    - 必須取消郵件預覽功能
  - 防止垃圾郵件
    - 設定過濾垃圾郵件機制
  - 啟用個人防火牆

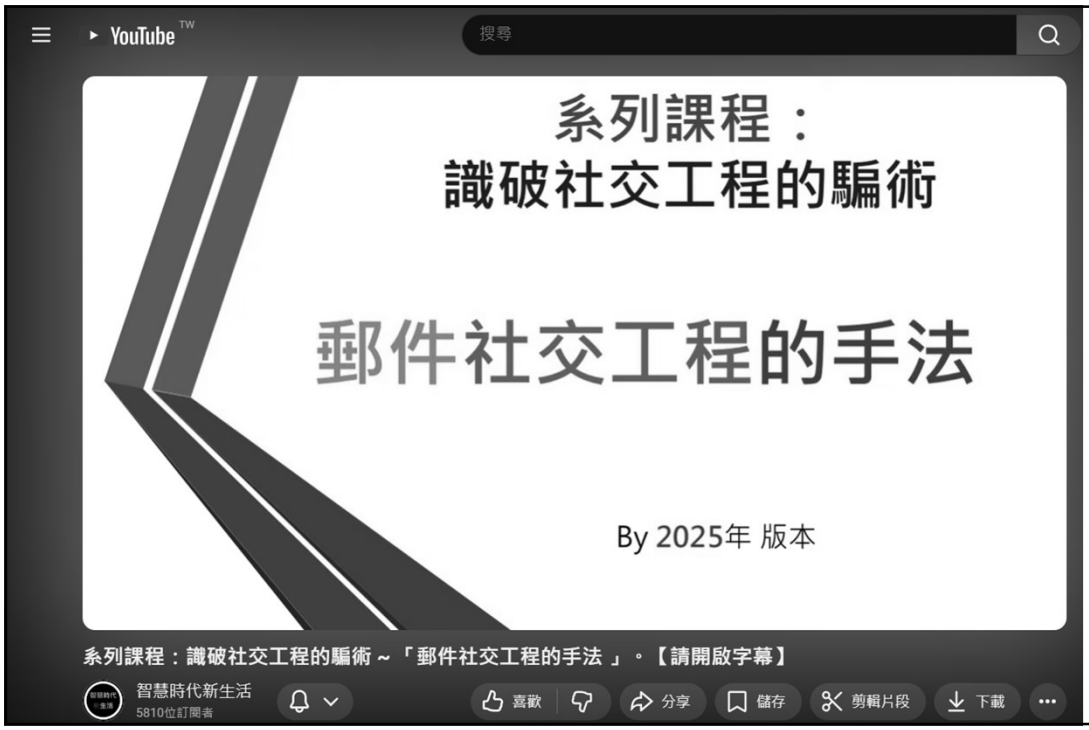
使用者防護停看聽(2)

- **看 ─** 開啟電子郵件前應先依序檢視：
  (1)、【寄件者】的信箱來源
  (2)、【郵件主旨】是否與公務相關
  (3)、【附加檔案】不要直接點選打開，應另存新檔掃毒。

☺【寄件者】或【郵件主旨】與公務無關者，建議應立即刪除，連預覽都不要開啟郵件。

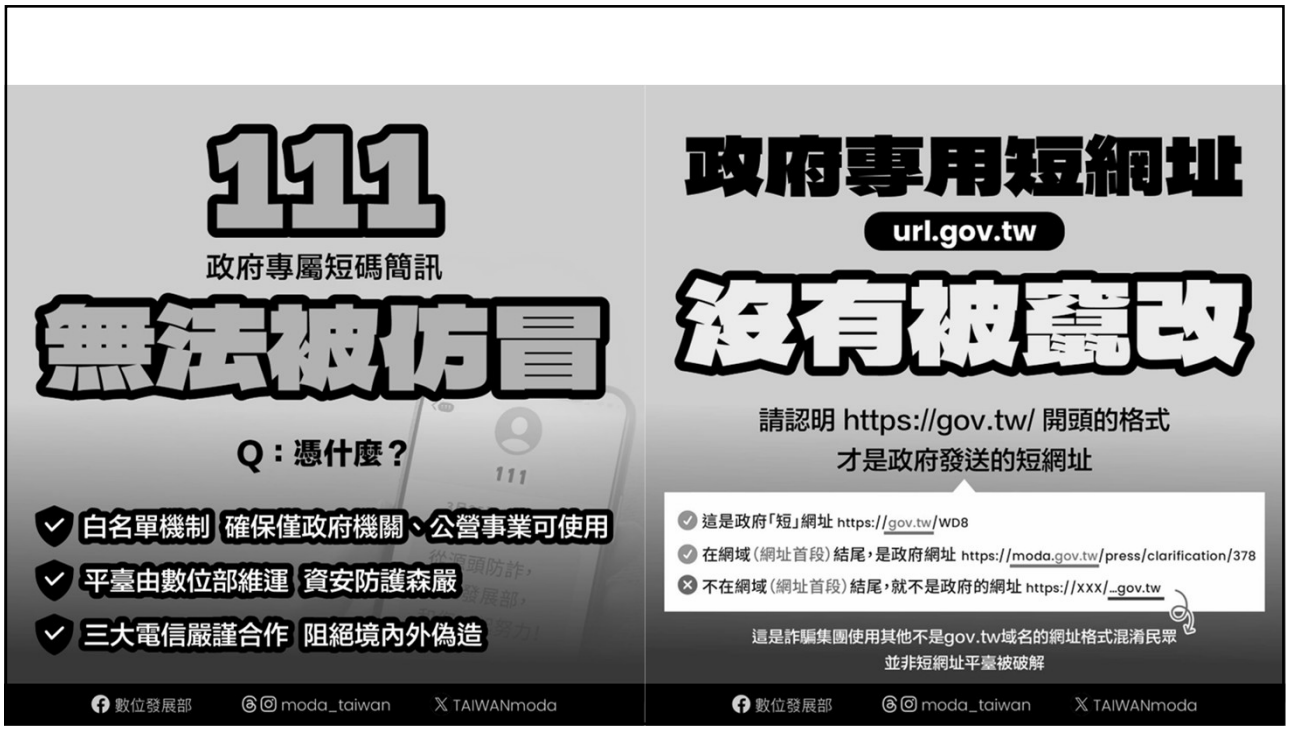
使用者防護停看聽(3)

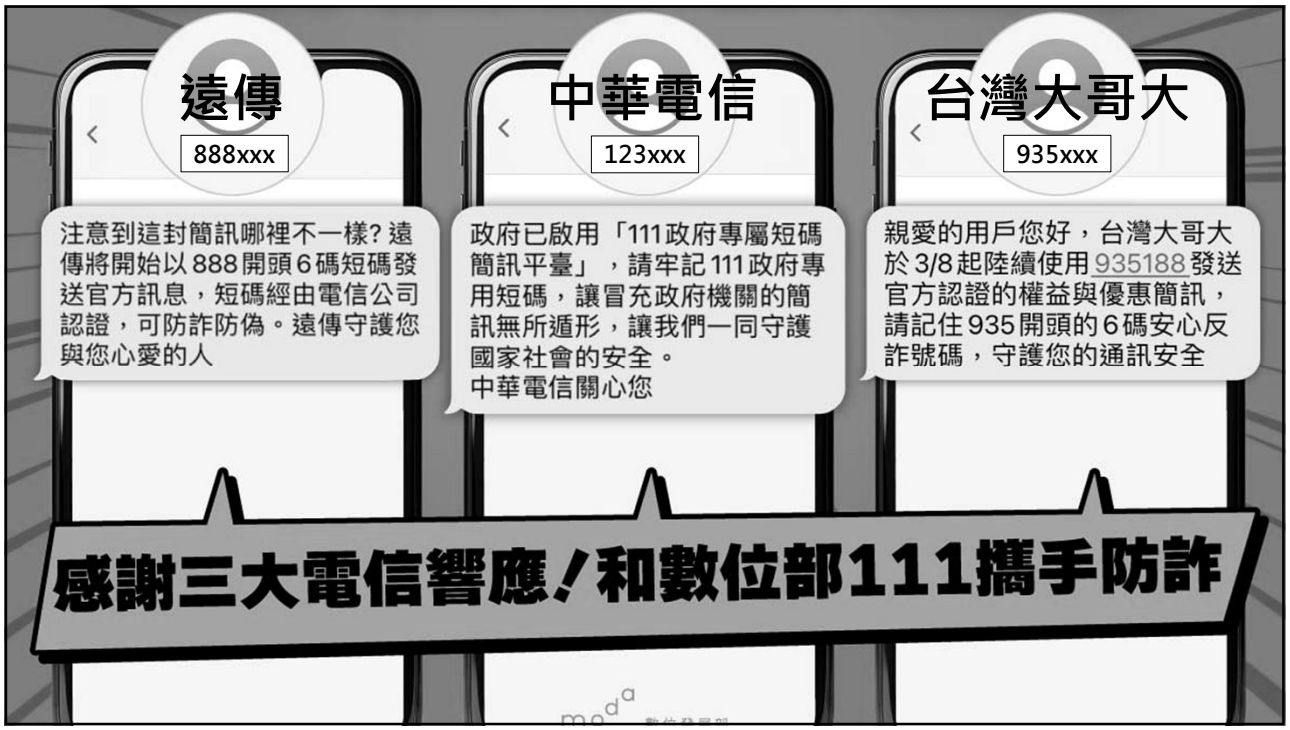
- **聽 ─ 若懷疑郵件來源，必須進行確認**
  - 透過 電話 或 LINE 或 電子郵件 再次向寄件人 **確認**郵件真偽。


YouTube TW
搜尋
系列課程：
識破社交工程的騙術
郵件社交工程的手法
By 2025年 版本
系列課程：識破社交工程的騙術～「郵件社交工程的手法」。【請開啟字幕】
智慧時代新生活
5810位訂閱者
喜歡
分享
儲存
剪輯片段
下載


識破電郵騙術！保護你的
電子郵件社交工程利用人性弱點進行詐騙。
AI技術讓詐騙更逼真，讓我們一起學習防護！
常見的電郵騙術
假冒官方機構通知
政府通知
點我看看
偽裝成政府、翻譯或電力公司，
以退稅、包裹或繳費為由騙取個資與金證。
小心「l」看成「1」的商業詐騙
高屋A
boss@company.com
高屋A (管充)
boss@company.ltd
駭客窗改極相似的字元冒充
高層或客戶，伺機網戰
赶觀責款。
利用QR Code與緊急事件施壓
緊急處理
帳戶異常!
立即付款!
透過掃推來錄不明的QR Code或點擊
「帳戶異常」等緊急發知，這取你的帳號密碼。
防護三部曲：停、看、聽
停：更新系統，關閉預覽
STOP
郵件接覽
定規更新軟體修補漏洞，並閉閒郵件預覽功能，
從根本降低風險。
看：檢查寄件者與附件
高屋A:
boss@company.ltd
可疑連結
仔細核對寄件人倫錦的真實性，
絕不輕易點擊可疑連綰或開載附件。
聽：意：多方查證，切勿輕信
凡是遇則金餐或帳戶相關要求，該必用
電話等其他方式向官方管道再次健認。
NotebookLM

透過簡訊的金融詐騙


111
政府專屬短碼簡訊
無法被仿冒
Q：憑什麼？
白名單機制 確保僅政府機關、公營事業可使用
平臺由數位部維運 資安防護森嚴
三大電信嚴謹合作 阻絕境內外偽造
數位發展部 moda_taiwan TAIWANmoda
政府專用短網址
url.gov.tw
沒有被竄改
請認明 https://gov.tw/ 開頭的格式
才是政府發送的短網址
這是政府「短」網址 https://gov.tw/WD8
在網域（網址首段）結尾，是政府網址 https://moda.gov.tw/press/clarification/378
不在網域（網址首段）結尾，就不是政府的網址 https://xxx/_gov.tw
這是詐騙集團使用其他不是gov.tw域名的網址格式混淆民眾
並非短網址平臺被破解
數位發展部 moda_taiwan TAIWANmoda


遠傳
888xxx
注意到這封簡訊哪裡不一樣? 遠傳將開始以888開頭6碼短碼發送官方訊息，短碼經由電信公司認證，可防詐防偽。遠傳守護您與您心愛的人
中華電信
123xxx
政府已啟用「111政府專屬短碼簡訊平臺」，請牢記111政府專用短碼，讓冒充政府機關的簡訊無所遁形，讓我們一同守護國家社會的安全。
中華電信關心您
台灣大哥大
935xxx
親愛的用戶您好，台灣大哥大於3/8起陸續使用935188發送官方認證的權益與優惠簡訊，請記住935開頭的6碼安心反詐號碼，守護您的通訊安全
感謝三大電信響應！和數位部111攜手防詐


金融機構用商用簡碼
民眾安心又方便！
收到金融機構簡訊 請認明 68-簡碼
68123
Text Message
Today 9:29 AM
您的○ ○信用卡(末四碼1234)於○月○日消費XX,XXX元，如有疑義，請撥打本行客服電話:0800-xxx-xxx。

https://ttidacsc.ttida.org.tw

發布日期：113-11-22 更新日期：113-11-22 發布單位：刑事警察局公共關係室

內政部 警政署 刑事警察局 CRIMINAL INVESTIGATION BUREAU

偵破首宗偽冒「111政府專屬簡訊」釣魚簡訊詐欺案

一、偵辦單位： 臺灣高雄地方檢察署(萬股)許檢察官萃華 刑事警察局科技犯罪防制中心、電信偵查大隊 高雄市政府警察局苓雅分局 臺北市政府警察局刑事警察大隊(偵七隊) 國家通訊傳播委員會

二、查獲時間：113年10月28日、11月13日。

三、查獲地點：新竹市、高雄市地區。

四、查獲人數：陸籍林○○（81年次）、臺籍郭○○（44年次）、蔡○○（87年次)及蔡○○（88年次)等4人。

五、查獲贓證物：查扣偽基站設備2組、手機5支、筆記型電腦2部及自小客車1輛等贓證物。

六、案情摘要：

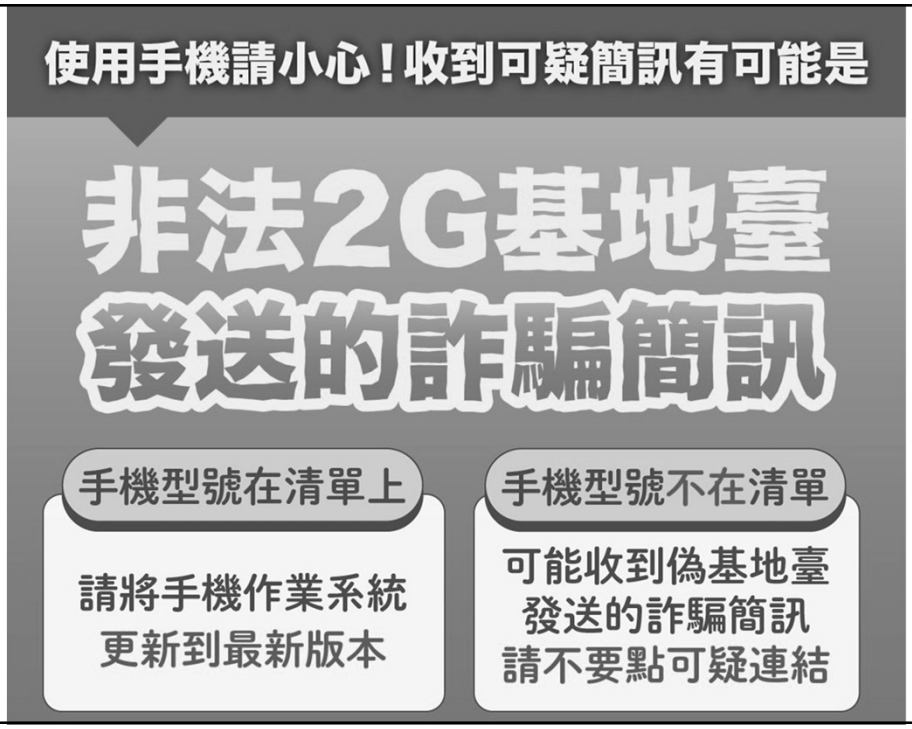
（一）為防範陸製2G基地臺來臺發射非法訊號，刑事警察局電信偵查大隊、國家通訊傳播委員會與各電信事業組成非法訊號偵測小組，於113年9月至11月初在新竹、高雄地區測得不明干擾訊號。

（二）經查批踢踢實業坊（PTT）八卦版中有民眾分享收到偽冒「111」及高雄區監理所之釣魚詐騙簡訊，研判係不法分子以假基地臺方式發送竄改發送人門號之釣魚簡訊，影響社會治安甚鉅，立即組成專案小組並報請臺灣高雄地方檢察署檢察官指揮偵辦。

（三）案經專案小組跟監埋伏，鎖定犯罪嫌疑人使用車載設備持續發射訊號干擾附近手機訊號及發送詐騙簡訊，隨即攔查並在高雄市鼓山區依法逮捕現行犯郭○○及陸籍林○○，並會同國家通訊傳播委員會勘驗違法射頻器材，現場查扣偽基站信號發射器及天線設備、手機及涉案車輛等證物，警方調查陸籍林姓男子來臺後，夥同郭姓男子架設非法詐騙釣魚簡訊發送設備，自113年10月31日至11月13日間在大高雄地區偽冒「111」簡訊，假冒「高雄市監理站」、「台灣自來水公司」等公部門，誘使民眾點擊釣魚連結後，續騙個資及盜刷信用卡，警詢後依詐欺等罪嫌解送臺灣高雄地方檢察署偵辦；另在新竹地區由蔡○○兄弟檔以設備發射之釣魚簡訊係假冒「遠通電收ETC」，且清查雙北市及新竹市之被害人已有35人，財損高達206萬餘元，警方將持續深入追查有無其他共犯涉案並釐清幕後主嫌身分。

（四）國家通訊傳播委員會提醒民眾，我國已關閉2G信號，民眾手機忽然出現2G信號，是不正常情形，可能已遇到假基地臺傳送釣魚簡訊，要提高警覺；同時我國3家電信事業已關閉3G信號，我國已邁入4G及5G世代，NCC呼籲民眾為享受4G及5G帶來的寬頻服務，儘速更換新的手機，也可以避免收到詐騙簡訊。

（五）另「111」係政府專屬短碼簡訊，為我國行政部門發送簡訊的信賴管道，近期民眾所反映接獲偽冒政府111簡訊並附有釣魚網址，經本局查證犯嫌手法並非透過駭客入侵政府111簡訊平臺發送簡訊，此平臺並無遭犯罪集團破解之虞，敬請國人安心。警方再次呼籲民眾提高警覺，若收到冒名政府機關、知名企業或銀行之簡訊，附有不明連結網址切勿輕信點擊以免遭盜取個資及詐騙，也應留意自身信用卡號碼、銀行帳號或簡訊驗證碼等不可提供給他人使用避免遭不法分子濫用。




政府111簡訊辨識三步驟-確認真偽好輕鬆
簡訊來源信賴
用戶手機號碼標示
發送單位/服務確認
7:07
111
123-數位發展部
MyData平臺：您已申請並同意MyData下載「個人戶籍資料」資料於2025/06/01 15:07下載完成。如非您本人下載，請洽
0800-009-868
手機末3碼-數位發展部
123-數位發展部


政府專屬短碼簡訊平臺
政府111簡訊
防詐能力再升級
111簡訊再升級!
手機末三碼
機關/單位
為專屬於您的簡訊
以手機號碼「0900-XXX-123」為例
123-台灣電力股份有限公司：高壓用戶服務入口網站 貴用戶電號044XXXX112，於2025年05月22日00:15達超約預警通知條件。
簡訊內容開頭加上您的手機末三碼
雙重防詐
辨識升級
信賴加分
111 政府專屬短碼簡訊
強化防詐新機制
新增開頭識別碼
以手機號碼 0911XXX758 為例
簡訊內容開頭會顯示
收訊者手機末3碼
(你的手機號碼末三碼)
方便民眾快速辨識
防範非法2G基地臺
廣播發送偽冒簡訊
111
6月1日 星期日 11:30
758-北市停管處通
受颱風外圍環流強影
局部大雨，提醒堤外
主留意水情、颱風消
及管制訊息。停管處
心您


YouTube TW
搜尋
Podcast (播客/線上廣播) :
手機簡訊
的
網路釣魚
智慧時代
新生活
使用 Google Gemini + NotebookLM 所產生的 AI 主持人 的語音對談
參考資料 / 引用來源：請參考下方備註欄說明
EP.04 [Podcast] 手機簡訊的網路釣魚
AI & 資安玩家村
502位訂閱者
喜歡
分享
儲存
剪輯片段
下載


手機簡訊防詐術：
一眼識破釣魚陷阱！
識破社交工程騙術，守護個人金融資訊安全
識破簡訊的三大特徵
KEY_FINDING:
認明政府專屬短碼 111
政府機關發送之簡訊代碼固定為 111，無法被輕易偽造。
https://uri.gov.tw
DEFINITION:
確認 gov.tw 官方網址
政府短網址必以 https://uri.gov.tw 或 .gov.tw 結尾。
中華 123
遠傳 88
台哥大 935
電信業者
68%
金融保險
SUPPORTING_FACT: 企業與金融專用代碼
三大電信分別為 123、88、935，金融信險業間頭別固定為 68。
官方簡訊識別對照表
類別 識別特徵
政府 111/gov.tw
遠傳 123 / 88 / 935
金融 68
防範詐騙的實戰設定
iMessage OFF
RCS OFF
PROCESS_STEP:
關閉 iMessage 與 RCS 功用
關閉 iOS 的 iMessage 或 Android 的 RCS 即時通訊可大幅減少垃圾簡訊。
Whoscall
165 聯防資料庫
安全
EXAMPLE:
安裝來電辨識軟體
使用 Whoscall 等 App，利用 165 聯防資料庫自動過濾與警示詐騙訊息。
QUOTE:
黃金準則：不點、不看、不開
NO
無論真假，絕不點擊簡訊連結，應自行搜尋官方網站或 App 處理。
NotebookLM


YouTube TW
搜尋
如何防範偽基地台
假冒政府機關
發送 111
釣魚簡訊詐騙
智慧時代
新生活
使用 Google Gemini + NotebookLM 所產生的 AI 主持人 的語音對談
參考資料 / 引用來源：請參考下方備註欄說明
EP.114 [Podcast] 如何防範偽基地台假冒政府機關發送111釣魚簡訊詐騙
AI & 資安玩家村
503位訂閱者
喜歡
分享
儲存
剪輯片段
下載


守護荷包！政府 111 簡訊防詐新機制全攻略
詐騙集團利用「2G 偽基地台」續通電信業者，直接向附近手機發送偽造的「111」政府短碼簡訊，引誘民眾點擊釣魚連結。
為此，數位發展部升級驗證機制，於簡訊開頭加入接收者手機末三碼及機關名稱，並呼籲民眾關閉手機 2G 自動連線以維護資安。
警覺！2G 偽基地台的詐騙陷阱
偽造「111」號碼的原理：
詐騙者機得非法設備，以車台方式強迫附近手機接收偽造的 2G 假簡訊。
2G
手機訊號異常特徵：
訊號突然從滿格降為無訊號，或顯示類型變為 2G / GSM 時須提高警覺。
111
FAKE WEBSITE
信用卡號碼
個人描述
釣魚簡訊的最終目的：
誘騙點擊假網址，輸入信用卡號碼或個人個資以進行盜刷詐騙。
防禦！政府 111 簡訊三重驗證
111
111 簡訊「三重防線」：
認明「111號碼」、「手機末三碼」與「發送機關署名」才是真簡訊。
123-[數位發展部]
您好，這是測試簡訊...
辨識範例：手機號碼末 3 碼：
若手機末碼為 123，收到真簡訊開頭應顯示「123- [機關署名]」。
9:41
自動連線 2G 訊號
OFF
2G
自我保護：期間 2G 連線：
在手機設定中間閱「自動連線 2G 訊號」，可直接杜絕偽基地台干擾。
快速對比真假簡訊差異
真正的 111 政府簡訊
發送號碼：顯示為「111」
簡訊開頭：[手機末 3 碼]- (如 123-)
機關署名：必含發送單位名稱
偽造的詐騙簡訊
發送號碼：顯示為「111」或「+886」等
簡訊開頭：直接顯示文字內容
機關署名：通常只有釣魚連結
NotebookLM

通訊軟體 LINE 的網路釣魚


呂老師
輸入狀態訊息
好友名單
顯示全部
好友
南港劉德華, 東港王陽明
群組
群組：檢查 (5), 群組：家人 (2), 群組：有加密 (2)
服務
顯示全部
貼圖小舖
主題小舖
LINE GO
LINE TV
來電鈴聲
LINE GAME
主頁
聊天
VOOM
通話
錢包
設定
備份及移動帳號
備份及復原聊天記錄
以行動條碼移動帳號
移動帳號選項
商店
貼圖
主題
鈴聲／來電答鈴
字型
代幣
一般
提醒
照片・影片
聊天
聊天
備份及復原聊天記錄
備份後，聊天記錄將儲存於Google雲端硬碟。
若遺失或更換新的智慧手機時，也可復原已備份的聊天記錄。
Chats
背景
設定希望統一套用於所有聊天室的背景。已套用背景的聊天室將不會受到此設定的影響。
字體大小
中
以換行鍵傳送
點選Enter鍵即可傳送訊息。
再度自動傳送
無法傳送的訊息於一定時間過後，將會再度自動傳送。
預覽網址
分享於聊天室的連結，將顯示縮圖並預覽網站資訊。
偵測可疑網站
系統將偵測並標示曾被檢舉的可疑網站。開啟此設定後，分享於聊天室的連結將不會受到Letter Sealing功能的加密保護。
*僅限「預覽網址」已設為開啟時，才可開啟此設定。
滑動回覆
在訊息上向左滑後，可針對該則訊息回覆。


12:42
93%
搜尋好友
ID
電話號碼
@jwv3010k
趨勢科技防詐達人
加入
聊天
防詐達人
刑事局 165 推薦
手機最佳防詐騙工具
12:42
92%
手機最佳防詐騙工具
趨勢科技防詐達人
好友人數 986,197
真假訊息查證投資購物交友詐騙網站檢查回報
同時辨識真假新聞 一頁式購物 貼圖好康 查詐騙Line ID
加入好友
貼文
商品服務
最新貼文
購物詐騙? 假貼圖好康？假新聞？一次搞定
加入好友
所在國家或地區： 台灣


趨勢科技防詐達人
網址辨識
安全
此網址尚未有人回報
覺得可疑不安全？請回報給防詐達人
回報幫助更多人
無搜尋結果
查詢不到相關訊息
我除了能幫您偵測假新聞之外，還能檢查連結、LINE帳號的安全
使用說明
查詢更多
危險
這是不安全連結
・givegiftgood*com/C..
了解更多
注意
檢查結果：個人資料遭外洩
每年有很多網站發生過資安事件，其中有 7 個網站你可能曾加入。
發現 2 筆外洩資料與你有關：
・密碼 7 筆
・電子郵件 7 筆
查詢完整報告
真的假的聊天機器人
Cofacts 查核平台
和這篇文章100%相似
根據本篇查核報告可知此訊息為錯誤訊息
報告摘要：
衛福部長照司指出，2022年沒有網傳「疫情...
去「Cofacts」看詳細內容
覺得不安全，回報給防詐達人
查詢可疑網址|帳號|假消


YouTube TW
搜尋
系列課程：
識破社交工程的騙術
LINE 的訊息詐騙
By 2025年 版本
系列課程：識破社交工程的騙術 ~「LINE 的訊息詐騙 」。
智慧時代新生活
5810位訂閱者
喜歡
分享
儲存
剪輯片段
下載

數位發展部資通安全署
Administration for Cyber Security, moda

強化帳密安全，落實三大防護原則

數位發展部資通安全署（下稱資安署）今（12）日召開記者會，針對近期日益嚴峻的網路入侵威脅，說明強化帳號密碼安全等具體做法。資安署提醒，常見之弱密碼 如 「 123456 」 、「 admin 」或以鍵盤排列順序設定之「QWERTY」等這類密碼，利用自動化工具幾乎可瞬間破解，並呼籲民眾切勿使用。此外，資安署亦示警避免在社群媒體、電子郵件與網路銀行使用相同密碼，一旦其中一個遭駭，將導致各平台、服務的帳密連鎖遭竊不得不慎。

為有效防範此類風險，資安署提供三大帳密防護原則：

- 強化密碼複雜度：密碼長度至少15個字元，並混合大小寫英文、數字及特殊符號，或使用密碼管理工具生成及管理密碼，避免使用個人生日、電話等易被猜測資訊。
- 啟用兩步驟驗證：以使用密碼登入外增設第二個驗證步驟，如開啟簡訊驗證碼、臉部或指紋驗證，使用身分驗證器等，並優先為網路銀行、Google、LINE、社群媒體等重要網路服務進行設置。
- 定期檢視登入活動：建議定期檢視帳號登入紀錄，透過檢視登入的時間、地點或裝置設備，檢查是否存在異常存取，如發現不明登入足跡，應立即登出所有裝置並更換密碼。

資安署強調，帳號安全攸關民眾的隱私與財產，強化密碼設定加上啟用兩步驟驗證，將可大幅度減少帳密遭盜用情形，保障國人隱私與財產安全。


YouTube TW
搜尋
網路入侵威脅激增
應強化帳號與密碼安全
落實三大防護原則
智慧時代 新生活
使用 Google Gemini + NotebookLM 所產生的 AI 主持人 的語音對談
參考資料 / 引用來源：請參考下方備註欄說明
EP.259 [Podcast] 網路入侵威脅激增，應強化帳號與密碼安全，落實三大防護原則
AI & 資安玩家村
502位訂閱者
喜歡
分享
儲存
剪輯片段
下載


偵探教你破解！三大帳密安全鐵則
網路威脅日益嚴峻，駭客手法多變。
只要掌握三大防護原則，就能輕鬆強化安全，保護你的數位生活！
駭客的犯罪手法
弱密碼：駭客的最愛
admin
「123456」、「admin」等密碼可被自動化工具瞬間破解。
撞庫攻擊：一把鑰匙開所有門
EMAIL
SOCIAL MEDIA
BANK
SHOPPING
駭客利用一組外洩帳密，嘗試登入你的所有網路服務。
社交工程：誘你上鉤的陷阱
URGENT:
透過的魚郵件或惡意連結，騙取你的帳驗密碼。
三大防護鐵則
1. 強化密碼複雜度
密碼長度至少15字元，混合大小寫英文、數字及特殊符號。
至少15字元
大小寫英文
數字
特殊符號
2. 啟用兩步驟驗證
123456
指紋辨識
簡訊驗證碼
臉部辨識
3. 定期檢視登入活動
異常登入：
IP 192.0.2.1 (國外地點)
定期檢查登入紀錄，留意是否有不明裝置或員常地點的登入。
NotebookLM

瀏覽器的安全設定

iPhone / iPad

設定


11:36
書籤
歷史記錄
閱讀清單
密碼管理工具
重新載入
新分頁
新無痕分頁
加入書籤
加入閱讀清單
刪除瀏覽資料
翻譯
切換為電腦版網站
在網頁中尋找...
縮放文字...
透過 Google 智慧鏡頭搜尋畫面內容
自訂選單
11:34
Google
搜尋或輸入網址
捷徑
11:35
設定
完成
預設瀏覽器
搜尋引擎
Google
網址列
置頂
密碼管理工具
關閉
付款方式
關閉
地址和其他資訊
關閉
通知
關閉
語音搜尋
中文 (台灣)
安全檢查
隱私權和安全性
探索
分頁
語言
11:39
設定
隱私權和安全性
完成
刪除瀏覽資料
安全瀏覽
標準防護
一律使用安全連線
盡可能使用 HTTPS，並在載入不支援該通訊協定的網站前發出警告。
接力
開啟
關閉 Chrome 時鎖定無痕分頁
要求在無痕模式中開啟其他應用程式的連結
鎖定模式
關閉
你可以前往 Google 帳戶管理要儲存哪些 Chrome 資料。
如需其他會運用資料提升 Chrome 使用體驗的設定，請前往 Google 服務。


設定
基本選項
搜尋引擎
Google
Google 密碼管理工具
付款方式
地址和其他資訊
隱私權和安全性
安全檢查
通知
主題
進階
分頁
首頁
開啟
隱私權和安全性
隱私權
刪除瀏覽資料
刪除歷史記錄、Cookie、網站資料、快取...
隱私權指南
查看最重要的隱私權和安全性控制項
第三方 Cookie
已封鎖第三方 Cookie
廣告隱私權設定
自訂網站可用來顯示廣告的資訊
傳送「Do Not Track」要求
開啟
預先載入網頁
標準預先載入模式
退出 Chrome 時鎖定無痕分頁
透過螢幕鎖定畫面查看開啟的無痕分頁
安全性
安全瀏覽
已開啟強化防護
刪除瀏覽資料
時間範圍
不限時間
瀏覽記錄
352 個項目 (在已同步的裝置上還有更多項目)
Cookie 和網站資料
來自 100 個網站。刪除 Cookie 後，大多數網站都會將你登出。
快取圖片和檔案
483 MB。下次造訪某些網站時，載入速度可能會變慢。
分頁
這部裝置上的 1 個分頁
已儲存的密碼
無
自動填入表單資料
無
網站設定
4 個網站
刪除資料
第三方 Cookie
你造訪的網站可能會嵌入其他網站的內容，例如圖片和文字。其他網站設定的 Cookie 稱為第三方 Cookie
允許第三方 Cookie
網站將正常運作
在無痕模式中封鎖第三方 Cookie
在無痕模式下，某些網站的功能可能無法正常運作
封鎖第三方 Cookie
某些功能可能無法運作，相關網站仍可使用第三方 Cookie。
新增例外網站


設定
基本選項
搜尋引擎
Google
Google 密碼管理工具
付款方式
地址和其他資訊
隱私權和安全性
安全檢查
通知
主題
進階
分頁
首頁
開啟
隱私權和安全性
隱私權
刪除瀏覽資料
刪除歷史記錄、Cookie、網站資料、快取...
隱私權指南
查看最重要的隱私權和安全性控制項
第三方 Cookie
已封鎖第三方 Cookie
廣告隱私權設定
自訂網站可用來顯示廣告的資訊
傳送「Do Not Track」要求
開啟
預先載入網頁
標準預先載入模式
退出 Chrome 時鎖定無痕分頁
透過螢幕鎖定畫面查看開啟的無痕分頁
安全性
安全瀏覽
已開啟強化防護
廣告隱私權設定
廣告主題
以你的瀏覽記錄做為依據。這項設定已開啟。
網站建議廣告
以你的網站活動做為依據。這項設定已開啟。
廣告評估功能
網站和廣告主可以瞭解廣告成效。這項設定已開啟。
網站建議廣告
網站建議廣告
你造訪的網站可以判斷你喜愛的內容，並在接下來的瀏覽過程中顯示建議廣告
網站建議廣告功能只是網站在放送個人化廣告時的其中一項依據。即使你未開啟這項功能，網站仍可放送廣告，但廣告內容可能較不貼近你的需求。
網站
如果不想讓網站儲存造訪資訊，建議你封鎖這些網站。Chrome 也會自動將 30 天前的網站從清單中刪除。瞭解詳情
設定開啟後，這裡會列出你造訪的哪些網站可推斷你的興趣喜好
你封鎖的網站
傳送「Do Not Track」要求
開啟
啟用「不追蹤」選項後，您的瀏覽流量會置入一項特定的要求，其作用則視網站是否回應要求，以及網站解讀要求的方式而定。
舉例來說，部分網站可能會以顯示廣告的方式回應這類要求，而這些廣告並非根據您所造訪的其他網站記錄而產生。許多網站仍會收集您的瀏覽資料，並將這些資料用於下列目的：提高網站安全性、在網站上提供


設定
基本選項
搜尋引擎
Google
Google 密碼管理工具
付款方式
地址和其他資訊
隱私權和安全性
安全檢查
通知
主題
進階
分頁
首頁
開啟
密碼管理工具
你可以在這裡查看所有密碼
你可以在任何裝置上使用已儲存的密碼，這些密碼儲存在 Google 密碼管理工具中。
記錄密碼
集中管理
透過任何裝置登入
密碼
設定
設定
顯示儲存密碼的選項
自動登入
使用儲存的憑證自動登入網站和應用程式。如果停用，系統會在你每次登入時要求確認想使用的帳戶。
密碼防護警示
如果 Google 在網路上發現你儲存的密碼，就會傳送通知給你。瞭解詳情
匯出密碼
下載密碼副本，供其他服務使用
匯入密碼
選取含有密碼的「.csv」檔案，將密碼匯入 nexus2demo@gmail.com 的 Google 密碼管理工具
將捷徑新增至主畫面
只要將 Google 密碼管理工具新增到主畫面，就能更快使用這項服務
密碼
設定


設定
基本選項
搜尋引擎
Google
Google 密碼管理工具
付款方式
地址和其他資訊
隱私權和安全性
安全檢查
通知
主題
進階
分頁
首頁
開啟
付款方式
儲存及填入付款方式
在付款表單中填入已儲存的付款方式
每次透過自動填入功能付款都要手動驗證身分
在關閉狀態下，系統基於安全考量，可能會偶爾要求你進行驗證
儲存安全碼
儲存信用卡驗證碼可加快結帳速度
付款應用程式


8:56
92%
密碼管理
評分
付費內容
Password Safe - 密碼安全-安全的密碼...
Robert Ehrhardt • 效率提升 • 工具 • 密碼
4.8★ 超過 100萬 次
Bitwarden 密碼管理工具
Bitwarden Inc. • 效率提升 • 工具 • 密碼
4.6★ 超過 100萬 次
Keepass2Android Password Safe
Philipp Crocoll (Croco Apps) • 工具 • 密碼
4.7★ 超過 100萬 次
趨勢密碼管理通 不怕忘記密碼風靡日...
Trend Micro • 效率提升 • 工具 • 密碼
4.4★ 超過 10萬 次
密碼管理器 SafeInCloud
Safe In Cloud • 效率提升 • 工具 • 密碼
4.7★ 超過 100萬 次
Keeper 密碼管理員與安全保險箱
Keeper Security, Inc. • 效率提升 • 工具
4.0★ 超過 1000萬 次
Dashlane Password Manager
Dashlane • 效率提升 • 工具 • 密碼
4.7★ 超過 500萬 次
Play 商店
Android 密碼管理：
儲存新帳戶
產生高強度密碼
用戶建立一個新帳戶時，密碼管理工具可協助用戶設定高強度的密碼，並將帳戶資料儲存於保險庫。
建立帳戶
密碼產生器
2Aia!>UYgt
LEDQmoF17A
保險庫
登入密碼管理工具
主密碼
雙重驗證
大部分密碼管理工具需登入帳戶及輸入主密碼以存取帳戶內的資料，用戶亦可利用雙重驗證例如生物識別技術來增加安全性。
登入已儲存帳戶
用戶不需自行輸入帳戶資料。
登 入
用戶A
資料儲存
不同的密碼管理工具可儲存資料的類型各有不同，例如帳戶名稱及密碼、電郵、銀行戶口號碼、信用卡等。


3:17
密碼
搜尋
全部 764
通行密鑰 3
驗證碼 2
Wi-Fi 2
安全性 473
已刪除 0
共享的群組
共享密碼和通行密鑰
你能與家人、朋友或其他關係密切的聯絡人安全地共享你選擇的密碼和通行密鑰。
開始使用
6:13
取消
新增密碼
儲存
網站、App或標籤
使用者名稱
使用者
群組
未共享
附註
加入附註
3:19
全部
編輯
Netflix
上次修改日期：12/30/18
使用者名稱
@gmail.com
密碼
網站
www.netflix.com
安全性
已遭洩露的密碼
更改密碼…


YouTube TW
搜尋
Podcast（播客/線上廣播）：
太多密碼
記不住！
使用
密碼管理 App？
智慧時代
新生活
使用 Google Gemini + NotebookLM 所產生的 AI 主持人 的語音對談
參考資料 / 引用來源：請參考下方備註欄說明
EP.22 [Podcast] 太多密碼記不住！使用密碼管理App？
AI & 資安玩家村
502位訂閱者
喜歡
分享
儲存
剪輯片段
下載


數位生活更安全：iOS 18「密碼」App 完全指南
Apple 在 iOS 18 與 macOS Sequoia 推出了獨立的「密碼」App，整合了原本分散在設定中的鑰匙圈功能。本圖表將介紹其強大的管理功能、分享機制，以及如何通過更新與正確習慣來規避潛在的資安風險。
Apple「密碼」App 三大核心功能
全方位帳密保險箱
自動生成高強度密碼
安全、簡單的群組共享
website
XyZ#9aB@1c
全方位帳密保險箱
一站式管理密碼、通行密鑰、Wi-Fi 密碼及二重驗證碼，並支援跨裝置同步。
自動生成高強度密碼
註冊時自動建議核雜密碼並儲存，透過 Face ID 即可自動填寫，無需記憶。
安全、簡單的群組共享
可建立共享群組，與信任的親友安全分享影音平台或家用 Wi-Fi 的帳密。
強化資安的關鍵守則
務必保持系統版本更新
重視「安全性建議」提醒
*** 弱
重複 外洩
*** 強
*** 安全
務必保持系統版本更新
iOS 18.2 已修補前版本的 HTTP 漏洞，更新至最新版可防止釣魚攻擊。
重視「安全性建議」提醒
當 App 偵測到密碼太弱、重複使用或已遭外洩時，應立即依建議更改。
挑還適合的儲存方式
追求便利可選雲端服務，重視資料掌握權則可選本地儲存工具。
比較項目
雲端服務 (如 iCloud/Bitwarden)
本地儲存 (如 KeePassXC)
便利性
高，支援跨裝置即時同步
較低，需手動同步資料庫
存取限制
需有網路連線方可更新
離線即可存取，控制權高
主要風險
伺服器遭受攻擊之風險
裝置損壞或遺失恐導致遺交資料
NotebookLM

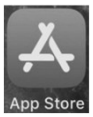

YouTube TW
搜尋
使用「密碼」App
在 Apple 裝置間
製作、管理及
共享密碼和通行密鑰
智慧時代 新生活
使用 Google Gemini + NotebookLM 所產生的 AI 主持人 的語音對談
參考資料 / 引用來源：請參考下方備註欄說明
EP.147 [Podcast] 使用「密碼」App 在 Apple 裝置間製作、管理及共享密碼和通行密鑰
AI & 資安玩家村
503位訂閱者
喜歡
分享
儲存
剪輯片段
下載


iOS 18 全新「密碼」App：您的數位安全大管家
強大的管理功能
一站式密碼中心
集中管理網站帳密、Wi-Fi 密碼與自動填寫的雙重驗證碼。
2FA
通行密鑰 (Passkeys) 登入
利用 Face ID 或 Touch ID 取代傳統密碼，安全且防範釣魚攻擊。
安全的群組共享
可與信任的聯絡人建立共享群組，安全傳遞串流平台或家用帳密。
安全性與跨平台支援
端對端加密保護
利用裝置專屬密鑰與個人密碼加密，Apple 亦無法存取您的資料。
安全層級建議與警告
自動偵測重複、過弱或已外洩的密碼，並主動提示使用者更改。
跨裝置無縫同步
支援 iPhone、Mac、Vision Pro，甚至可透過 Windows 版 iCloud 同步。
傳統密碼
安全性等級：一般
主要優點：易於在非 Apple 裝置手動輸入
通行密鑰
安全性等級：極高
主要優點：防釣魚、生物識別鍵證、免記憶
驗證碼 (2FA)
安全性等級：高
主要優點：即使密碼外洩，仍能提供第二層保護
NotebookLM

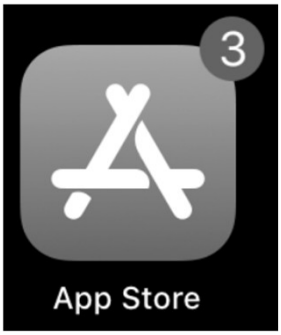
應用程式的更新

APP 軟體更新

- 不管是”Android”還是”iOS”作業系統，由於APP軟體都會有瑕疵，會引起當機、中毒、漏洞，所以都需要做 APP 軟體更新。
- iOS 透過 → App Store 來更新。



- Android 透過→ Play 商店 來更新。




11:16
搜尋應用程式與遊戲
為你推薦
熱門排行榜
活動
發掘推薦的遊戲
Play 商店
遊戲
應用程式
電影
圖書
搜尋應用程式與遊戲
Google
管理你的 Google 帳戶
管理應用程式和裝置
媒體庫
付款與訂閱
Play 安全防護
通知與優惠
Play Points
設定
說明與意見回饋
4:49
管理應用程式和裝置
總覽
管理
未發現有害的應用程式
Play 安全防護剛剛執行過掃描作業
有可用的更新
還在等待 3 項更新
全部更新
瞭解詳情
4:47
應用程式 (3 個)
全部更新
Facebook
38 MB • 更新日期：6月27日
更新
Instagram
33 MB • 更新日期：6月23日
更新
LINE
76 MB • 更新日期：6月17日
更新


手機可能中毒症狀
1.電池消耗變快
2.裝置一下子就變燙
3.出現沒安裝過的APP
4.APP當掉或無法正常運作
5.彈出視窗變多
6.電話突然斷線
7.無法撥打電話
8.無法收發訊息和電子郵件
9.不預期開關機
10.手機帳單暴增

你該養成的良好習慣

- 從官方網站下載應用程式和更新。
- 下載應用程式前，請閱讀其他用戶的評論,並檢查一下應用程式要求的所有權限。
- 隨時保持裝置作業系統與應用程式更新至最新版本。
- 立即更換所有網路帳號的密碼。
- 刪除所有不明的應用程式。
- 避免連上公共或無安全性的 WI-FI 網路。
- 藍牙不用時請關閉。
- 如果遭到駭客入侵，立即通知親朋好友忽略任何可疑訊息。
- 最後真的不得已時，備份重要資料，並將裝置回復至原廠設定。
- 使用能即時偵測網址安全性，為您封鎖惡意網站、詐騙連結、假購物網站和假臉書粉專等具有安全風險的防毒軟體

手機也需要防毒軟體的原因

- 藉由手機簡訊擴散惡意程式。
- App Store 及 Play 商店也有非法應用程式。
- 手機金融服務與行動支付帶來風險。
- 沒加密保護機制與假的 Wi-Fi 熱點充斥。

~~防毒軟體~~/防護軟體：iOS 安全性檢查

McAfee Security：VPN & 隱私權
行動裝置身分防護應用程式
McAfee, LLC.
在「工具程式」類中排名第 104
★★★★★ 4.7 • 3,576 則評分
免費 · 提供 App 內購買
免費試用版

趨勢科技行動安全防護 17+
PC-cillin手機防詐、網頁安全過濾、保護隱私
Trend Micro (Apps)
在「工具程式」類中排名第 20
★★★★★ 4.7 • 1.3万 則評分
免費 · 提供 App 內購買
免費試用版

AVG Mobile Security
AVG eCommerce CY Limited
★★★★★ 4.8 • 309 則評分
免費 · 提供 App 內購買
免費試用版

受限 iOS 系統機制
選擇少，大多是
免費試用版
(付費解除功能限制)

防毒軟體/防護軟體：Android 安全性檢查

LINE Antivirus
LINE Corporation
4.3★ **免費無廣告版**

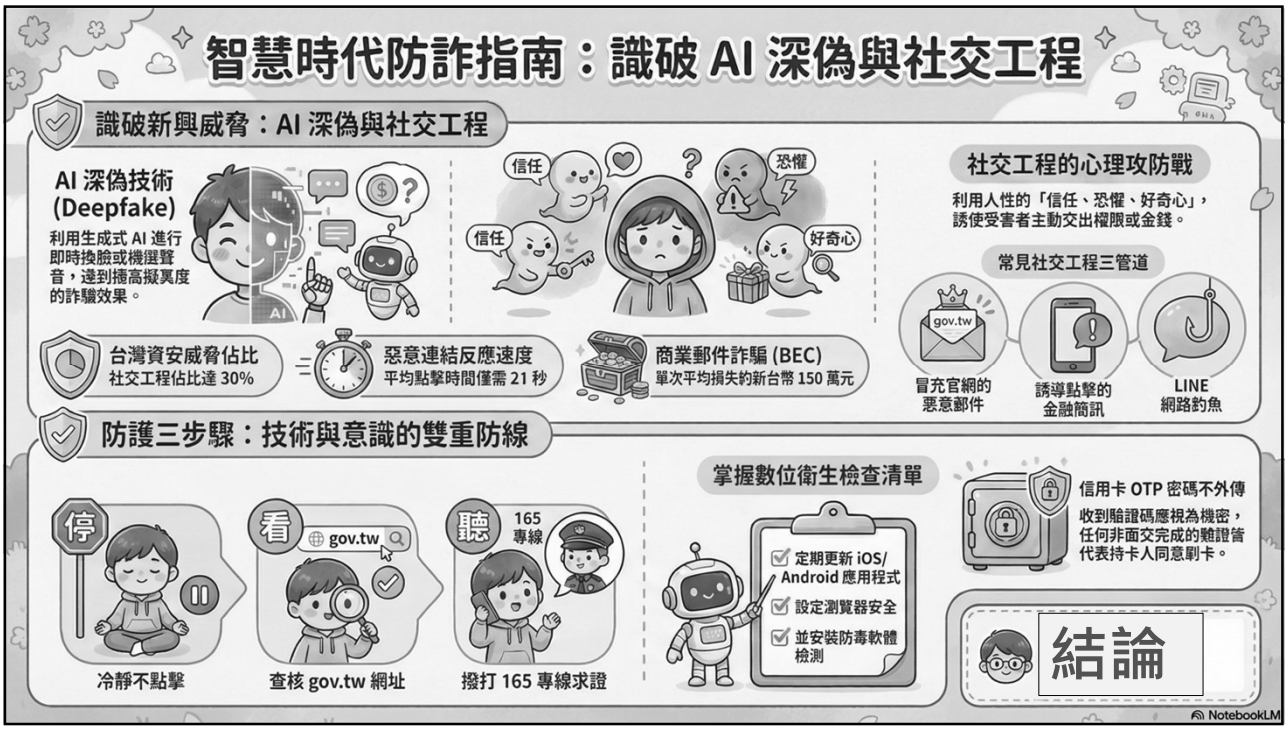
AVG- 手機安全防毒軟體
AVG Mobile
4.8★ **免費有廣告版**

McAfee Security: Antivirus VPN
McAfee LLC
4.2★ **免費試用版**

行動安全防護與防毒 (PC-cillin掃毒、WIFI安全)
Trend Micro Incorporated 趨勢科技
4.7★ **免費試用版**

由於 Android 系統機制
免費版 & 付費版
選擇較多

部份手機品牌
系統有內建



結論

- 自我保護措施
  - 防詐騙宣導
- AI人工智慧與換臉詐騙
  - 什麼是生成式 AI？
  - 什麼是 深偽技術 (Deepfake)？
  - 深偽技術的危害
  - AI深偽技術的社交工程攻擊案例
- 各種社交工程的詐騙手法
  - 來自於郵件社交工程的案例
  - 透過簡訊的金融詐騙
  - 通訊軟體 LINE 的網路釣魚
- 防範措施
  - 瀏覽器的安全設定
  - 應用程式的更新
  - 防毒軟體的檢測

參考資料
教學影片

YouTube 課程影片 ↑ ↑ ↑ ↑ ↑ ↑

(請按 **訂閱** 才收的到 通知)

https://linktr.ee/openblue.link