2026 去偽存真：AI 全民偵查黑客松競賽
【決賽】命題文件

命題單位
Gogolook
公司介紹
Gogolook（走著瞧股份有限公司）是全球信任科技（TrustTech）領導者，秉持「Build for Trust」的核心理念，致力用 AI 與數據守護每一次溝通。旗艦產品 Whoscall 結合龐大的風險號碼資料庫與智慧辨識技術，協助全球用戶即時辨識陌生來電、過濾騷擾與詐騙，成為數位安全的第一道防線。我們相信，真正有溫度的科技，是讓每個人都能更安心地連結彼此、重建信任。 面對生成式 AI 加速詐騙手法演化，Gogolook 持續推進防詐技術，讓威脅被更早辨識、風險被更快阻斷。我們期待在本次黑客松與優秀團隊共同探索 AI 的正面影響力，從偵測到預防，打造更可信的數位環境，用智慧科技守護社會的每一份善意。
命題類別
詐騙識別防範
命題主題
打造全民防詐識別系統
命題背景
臺灣詐騙已從單點手法演進為「跨渠道、多步驟」攻擊（電話、簡訊、社群、網頁、假冒客服/政府/銀行）。多數受害不是因為不懂詐騙，而是在高壓、低資訊、短時間的情境下，做出錯誤決策。 本競賽目標：產出能被授權、整合、產品化、規模化的防詐方案，協助： ● 消費者：在下一步行動前得到可信的風險判斷與引導 ● 企業：在客服/交易/平台流程中降低被詐騙利用與損失 ● 政府/公部門：提升通報與治理效率，掌握趨勢與風險態勢
決賽命題說明
一、核心任務 請提出一個可落地的「詐騙識別防範」方案，須具工程落地與產品化思維，並於決賽採用主辦單位提供之 AWS 開發環境完成最小可行性產品。 你的方案需解決以下核心問題： 1. 這是不是詐騙？（風險判斷） 2. 為什麼這樣判斷？（可解釋證據） 3. 我下一步該怎麼做才安全？（可執行阻斷/引導） 二、必須交付的 3 大模組 1. 輸入可包含：電話號碼、簡訊、網址 / 網域、內容截圖或文字（投資、交友、購物、客服話術等）、Email、社群、廣告 **2.** 輸出必須包含：

- **Module A**：風險判斷
  - 風險等級（例如：Low/Medium/High 或 0–100）
  - 至少 2 個可驗證的風險訊號（Evidence Signals）
  - 至少涵蓋 1 種「內容型分析」能力，如下：
    - 詐騙文本語意分析（簡訊/對話/廣告文案）或
    - 詐騙圖檔分析（圖片、截圖、海報）或
    - 網址詐騙內容分析（需依照網站內容/畫面/文字特徵判斷），不可僅依賴網址或網域的既有黑白名單。
- **Module B**：可解釋證據
  - 你的系統必須做到「一般民眾看得懂、企業/政府可稽核」，例如：
    - 這個電話/簡訊/網址/網域/內容為何可疑
    - 哪些因素影響風險最大
    - 與哪些已知詐騙模式相似（加分）
- **Module C**：行動引導與阻斷
  - 你的輸出不能只有提醒，必須提供可執行的下一步，協助使用者「真的避開受害」，例如：
    - 停止轉帳、改走官方管道、撥回官方客服、提醒家人
    - 一鍵封鎖 / 一鍵通報 / 一鍵回報證據
    - 長輩或高風險族群友善流程（加分）

三、競賽重點：便利性與有效性

你的方案必須同時滿足：

1. 便利性
- 使用者能以極低成本完成判斷（例如：貼上連結/輸入號碼/上傳截圖）
- 目標是「少步驟、低門檻、快回覆」
- 便利性需包含「高風險族群可用性」考量，例如：長輩模式、低識字友善、低操作成本、清楚的下一步指引與防呆設計。

2. 有效性
- 不只輸出風險分數，還要能改變使用者行為
- 必須包含「原因 + 建議行動」，並能降低受害機率

3. 主動式防詐預警
- 鼓勵發想「主動式防詐」能力，讓防禦跑在詐騙之前，例如：
  - 從回報與資料中自動識別詐騙趨勢與演化模式
  - 即時偵測新型詐騙的早期信號（異常模式）
  - 自動生成防禦策略（用戶推播文案、客服應對建議、內部規則草案）
  - 針對社會熱點事件進行情境化風險推演與詐騙劇本預測

四、成效衡量

提案必須提出量化之可驗證指標，例如：

- 降低受害率或降低「轉帳前未檢查」比例
- 攔截率提升
- 誤判干擾降低
- 判斷時間縮短
- 回報品質提升
- 預警指標（加分）：新型詐騙早期偵測時間、策略生成採用率、趨勢命中率

五、AWS 部署架構設計圖

一張「AWS 架構圖」與服務選型，建議涵蓋：

- 核心必備：計算層、資料層、AI/分析層
- 進階考量：入口與整合、隱私 (最小化、加密、去識別)、資安管理、效能與成本監控

企業數據及資料

＊主辦單位將於 **3/6** 連同組別確認信及以下資料集寄發至您報名填寫之信箱＊

- 號碼查詢 API
- 網頁風險 API
- 網域資訊 API
- 內容風險截圖檢查 API
- 1–2 週高風險電話、網頁、簡訊、社群資料（可用於分析、特徵工程、模型訓練構想或驗證）

決賽交付內容

＊最終交付內容以 **3/26** 競賽現場公告為主＊

1. 目標使用者與場景（消費者/企業/政府，至少選一主軸）
2. 解法概述（你要阻斷哪一類詐騙流程）
3. 三模組設計（風險判斷、可解釋證據、行動引導與阻斷）
4. 使用者流程
5. 風險提示與介面設計（需包含長輩/高風險族群友善版本或說明）
6. AWS 部署架構設計圖
7. 成效衡量
8. Live Demo 網址 / 錄製影片連結
9. GitHub 網站連結

決賽評分標準 (總計 100%)

- （10 %）創意度：三大模組設計、介面設計、使用者體驗的創新性
- （15 %）技術可行性：三大模組的技術架構完整性、AWS 架構設計、Gogolook 資源運用
- （15 %）商業應用性：便利性（低門檻、少步驟、快回覆）、有效性（改變使用者行為、降低受害機率）、高風險族群可用性
- （30 %）主題切合度：完整回答三大核心問題、符合詐騙識別防範主題
- （25 %）完成度：MVP 可實現性、主動式防詐預警、成效衡量完整度
- （5 %）加分項：採用 AWS Kiro

命題文件 聯繫窗口

hackathon@digitimes.com