

AI陷阱： 青年解碼行動

議題手冊

AI



Let's Talk
青年好政

目錄

壹、Let' s Talk 活動說明	01
貳、活動資訊	02
參、活動目的	03
肆、活動流程	04
伍、討論方式	05
陸、審議式民主	06
柒、團隊介紹	07
捌、議題說明	12
玖、AI 詐騙政策現況與分析	17
拾、參考資料	28

壹、Let' sTalk 活動說明



未來公民社會發展取決於青年「公民能力」，尤其青年賦權（youth empowerment）更是國內、外民主國家制定青年政策趨勢，教育部青年發展署（以下簡稱青年署）主辦，為鼓勵青年參與公共事務，自 107 年推動以青年為主體之「青年好政系列-Let' sTalk」計畫，培力青年具備審議知能，鼓勵青年參與 Talk 活動，捲動青年將對議題想法融入政府施政；109-113 年 Talk 計畫更配合行政院「臺灣開放政府國家行動方案」，持續擴散青年政策參與行動力，以利青年在未來公民社會中，扮演更積極角色。

114 年青年署配合「國家希望工程」施政目標，新辦「推動青年參與公共事務深化計畫」（以下簡稱深化計畫），補助地方政府建構青年參與在地公共事務治理、實驗與交流平臺。Talk 計畫將視地方政府推動情形，另行鼓勵青年團隊就當前重要政策或議題（如國家希望工程八大施政目標、行政院重大青年政策等）發起青年自主討論。亦將賡續配搭相關培訓，俾討論過程符合審議民主精神；另導入公私協力精神，透過公部門部會與青年齊力協作，共創具體、可行之政策建議。

「Let' sTalk」計畫每年會選擇一個具有公共性和時效性的議題，作為討論的核心主題。每個參與的青年團隊將負責策劃並執行一系列的討論活動，邀請來自不同領域的青年參與，透過多元觀點的交流，深入探討該議題。今年的主題為「AI 創新-青年在 AI 浪潮下如何發展？」。反映了科技進步與青年發展之間的緊密關聯，並希望能激發青年對未來科技和職業發展的關注。參考「知情討論」、「多元對話」及「積極聆聽」之審議民主精神規劃 Talk 討論，可自由選擇合適之討論模式，並提供參與者增進議題認識與提出議題建議的機會。提供參與者一個平等、開放的空間，讓每個人都有機會發表意見、提出問題並共同討論，並將討論結果轉化為具體可行的政策方案，推動青年在公共事務中扮演更加重要的角色。

AI陷阱： 青年解碼行動



AI技術日新月異，詐騙手法也不斷進化！
你知道聲音可以被複製、身份可以被「換臉」？
一起揭開AI詐騙的真相，學會破解關鍵！

報名連結

破解數位詐騙，守護你我未來



聯繫：明新科技大學 行銷系 彭同學
電話：03-5593142 #3514
信箱：mina910918@gmail.com

日期 | 2025.07.23 (三)
時間 | 09:00 - 16:30
地點 | 明新科技大學 管院101教室
(新竹縣新豐鄉新興路1號)

Let's Talk
青年好政

輔導 |  教育部青年發展署
主辦 |  Must明新科技大學
 竹青AI特工隊

參、活動目的

本次「Let's Talk」活動旨在提高年輕人對 AI 詐騙風險的認知，並幫助青年掌握辨識、預防及應對 AI 詐騙的能力。希望透過深入的討論和專家講座的分享，使參與者能夠了解 AI 詐騙的具體形式及其對個人和社會的影響，並學習如何有效防範新風險。將幫助青年更好地了解 AI 技術的潛在危機，提高數位素養和資安意識，從而在 AI 時代中保護自己免受詐騙侵害。

另一大目的是增強年輕一代的批判性思維和問題解決能力，尤其是在面對日益複雜的數位環境時。藉由實踐討論、案例分析和專家指導，幫助青年發展出對於 AI 生成內容的辨識能力，並能夠從多個角度審視信息的真實性，避免輕信來自網路的虛假信息。



此外，本次活動也將作為一個平台，讓參與者能夠與其他領域的專家學者以及社會各界的青年互動交流，促進跨領域的合作與社群連結。其中，參與者不僅能夠獲得有價值的資訊和建議，還能與其他青年共同討論如何在數位社會中建立起更為堅實的防護機制，從而提升整體社會對 AI 詐騙的防範能力。

最終，希冀本次活動能夠產出具體的政策建議和防範對策，並將其提交給相關部門和機構，促進政府和民間的合作，為未來的詐騙防治工作提供支持。同時，讓更多的青年認識到 AI 詐騙的嚴重性，並積極參與到詐騙防治的行動中，成為數位社會安全的守護者。

在 AI 時代中創建一個更加安全、透明的數位環境，減少詐騙案件的發生，保障公民的數位權益。

肆、活動流程

時間	流程	進行方式
08:45~09:00 (15mins)	報到	於報導台領取名牌手冊
09:00~09:30 (30mins)	開場/主講人介紹	大場主持人引言
09:30~10:30 (60mins)	AI 詐騙防治全攻略	議題分享-林妤芬律師
10:30~10:40 (10mins)	中場休息	喝水/上廁所/休息
10:40~11:40 (60mins)	生成式 AI：未來已來	議題分享-李國憲律師
11:40~12:20 (40mins)	午餐時間	享用在地午餐
12:20~12:30 (20mins)	議題說明、講解規則	大場主持人
12:30~12:35 (20mins)	休息五分鐘	喝水/上廁所/休息
12:35~13:35 (60mins)	分組討論(一)	盤點 AI 詐騙
13:35~14:35 (60mins)	分組討論(二)	確認防止 AI 詐騙之困境
14:35~14:45 (10mins)	中場休息 分組	換桌休息
14:45~15:45 (60mins)	分組討論(三)	應對詐騙之方案對策
15:45~16:20 (35mins)	分享	各桌派代表分享心得
16:20~16:30 (10mins)	大合照	開心回家

講師簡報



AI 詐騙防治全攻略



生成式 AI：未來已來

伍、討論方式

本次活動以「變形世界咖啡館」，採不換桌方式進行，學員們的背景、經驗和想法都不同，可以透過小組討論，接觸到不同專業以及不同生活經驗的人一同來討論，更促進多元觀點的交流，亦能夠提升學習參與度和增加互動性，讓學生主動參與和自由表達，每一個參與者不僅是演講者，更是聆聽者，也能夠同時培養 AI 時代必備的關鍵能力像是溝通與團隊合作能力、批判性思維與問題解決能力、創新思維與適應力。

世界咖啡館(The World Café)是將人群分為數個小組(桌子)，並使參與討論的個人頻繁更換討論組(桌子)並被新討論組的「組長」介紹給其他組員。為了促進討論的進行，討論的環境被賦予一種咖啡廳的氣氛。在某些場合，為了使每個人都有發言的機會，會場會保留一定程度的正式性。其他時候，討論可以在各個個人之間同時進行，使其某種意義上成為名副其實的「咖啡館」。除了聽與說以外，討論者亦被鼓勵在桌子上寫字甚至塗鴉，以方便後來的討論者了解之前的討論內容。儘管一開始的討論問題是定好的，但其討論結果並不是事先商討決定的。集體討論可以改變討論者的觀念並且促進集體意識和集體行動的形成是世界咖啡館的引申主旨。

世界咖啡館的七個設計原則：

- **設定背景：**明確展開對話的目的與廣泛範圍
- **創造一個熱情好客的空間：**確保溫馨的環境和心理安全，從而培養個人舒適度和相互尊重
- **探索重要議題：**將集體注意力集中在吸引協作參與的強大議題上
- **鼓勵大家貢獻：**透過全員參與、互相付出，活躍「我」與「我們」的關係
- **交叉傳播並連結不同的觀點：**透過有意增加觀點之間聯繫的多樣性和密度，同時保留對核心問題的共同關注
- **一起傾聽重要議題的作法、見解和更深層的問題：**以培養思想連貫性而不失去個人貢獻的方式集中共同注意力
- **收穫和分享集體發現：**使集體知識和見解可見並可操作

陸、審議式民主

審議式民主 (Deliberative Democracy) 是一種強調公共討論與理性對話的民主理論與實踐方式。此模式的核心在於公民透過理性且尊重他人觀點的討論，來達成共識並做出政策決策。審議式民主不僅重視選舉或投票結果，更強調在政策形成過程中，所有相關利益方的意見都能被充分討論與考慮。

- **理性討論：**審議式民主強調公民在討論過程中應該依據理性論據，而非情感或利益立場來表達自己的觀點。討論應該聚焦於事實、證據以及對公共利益的深刻理解。
- **平等參與：**每個人都應該有平等的機會參與討論，無論其社會背景、政治立場或個人利益如何。在過程中，強調公平對待每一位參與者的聲音，並促進多元意見的交流。
- **包容性：**審議式民主強調所有利益相關者的參與，尤其是那些在傳統政治過程中可能被邊緣化的群體。確保了討論的全面性與決策的合法性。
- **共識建構：**審議式民主的目標不是單純地進行投票，而是透過討論達成某種共識或達到最大的協議。這種過程要求參與者不僅僅關注自身的利益，而是要為了公共利益作出妥協和調整。
- **透明與問責：**審議過程應該是公開的，並且在結束後，決策者應該向公眾解釋決策背後的理由與過程，確保整個決策過程是透明且可問責的。

審議式民主的實踐：

在現實中，審議式民主通常表現為市民大會、公共論壇、議題研討會等形式，這些平台為市民提供了討論和影響公共政策的機會。例如，選舉之外的公共討論、社會議題的市民集會、政府政策的審議等都屬於審議式民主的實踐。

是一種深度重視公共討論和理性對話的民主形式，它鼓勵多元意見的交流與妥協，並將公共政策的制定過程更為開放和透明，讓所有公民都能夠在決策中發揮重要作用。

柒、團隊介紹

(一) 主持人介紹／桌長／業師介紹

姓名	職稱	公參經歷/現職
沈軍廷	業師	現職 • 中華學生事務學會秘書長 • 青年好政-Let's Talk」計畫審議業師及 112 年青年署審議培訓基礎訓桌長 • 第 3 屆桃園市政府青年諮詢委員 • 111年彰化縣政府文化局「彰化縣青年公民文化會議」審議主持人 • 110 年平鎮區公所「石門大圳步道景觀臺參與式規劃工作坊」分組審議主持人 • 109年第1屆全國青年諮詢委員論壇桌長 • 109年楊梅區公所「打造永寧新公園參與式規劃分組」審議主持人 • 107 年桃園市衛生局「長照護鄰社區互助公民參與計畫公民地方論壇」桌長 • 107年桃園市衛生局 公民參與試辦計畫：如何維持身體健康，打造健康體位區域會議」桌長
黃璫葳	大場主持人	現職 • 明新科技大學行銷系專案經理 • 捻花惹草應用所 主理人 • 新竹縣青年諮詢委員 審議或公共事務參與經歷： • 天下雜誌微笑台灣 青年專訪計畫主持人 • 113 年 寶山區域型社區營造計畫 • 113 年 中華開發金地方創生行動 • 112 年 國發會獎勵青年投入地方創生 • 112 年 新竹縣政府微笑公民計畫 • 111-112 年 農業部農村水保署青年回鄉計畫 • 111 年 信義房屋全民社造行動 • 111 年 新竹縣政府青年創業競賽專案執行 • 113 年 國發會青年培力工作站 活動企劃 • 113 年 連江縣 SBIR 計畫 專案經理 • 113 年 大學社會責任實踐(USR)明新科大 專案經理 • 113 年 服務業創新研發計畫 SIIR 專案經理 • 112 年 農業部食農教育計畫 食農教育講師

		• 111 年 教育部青發署北區青聚點 專案 • 110 年 區域特色農遊創新商品獎勵共學計畫 專案 • 110 年 OTOP 城鄉特色產業專案輔導 藝術設計
戴育宏	桌長	現職 • 新竹縣冰壺協會 理事長 • 新竹縣青年諮詢委員 審議或公共事務參與經歷： • 新竹縣教育局青年諮詢委員
彭子庭	桌長	現職： 明新科技大學 行銷與流通管理系/四年級審議或公共事務參與經歷： • 參與農業部食農教育計畫(學校組) • 參與永續發展與社會實踐深碗課程 • 第三期 USR 計畫 兼職助理
林紫晏	桌長	現職： 高雄科技大學 人力資源發展系/碩一 審議或公共事務參與經歷： • 參與農業部食農教育計畫(學校組) • 參與永續發展與社會實踐深碗課程 • 第三期 USR 計畫 兼職助理
古昀仙	桌長	現職： 瓶蓋工廠台北製造所(集思國際會議顧問有限公司南港營業所)/副理 審議或公共事務參與經歷： 107-109年度桃園市政府青年事務局第二屆青諮委員 102-114年度教育部青發署審議桌長主持人

(二) 議題分享人介紹

姓名	職稱	公參經歷/現職
李國憲	講師	現職： 亞洲物聯網聯盟執行長 大佳雲端科技公司總經理 亞物永續創新投資公司執行長 相關經歷： 開源人工智慧促進協會 理監事會/前秘書長 致理科大資管/多媒體設計學系/外貿學院兼任講師 實踐大學國貿學系兼任講師 JS 淇譽電子科技股份有限公司協理/營運長

		NOKIA 全球採購 ODM 專案經理 Acer 手持智慧總處品牌管理暨產品行銷處長 Arima 華冠通訊 智慧手機產品部處長 HTC 宏達電 行銷業務部資深經理 DBTel 大霸電子 業務與專案課長 萬海航運 第一任深圳駐外代表 國立中央大學企業管理學系博士生 芬蘭國立阿爾托大學 EMBA（赫爾辛基經濟學院） 與議題之關聯： 出版書《生成式 AI：未來已來》 青年沙龍：與新世代的對話 新竹場 國憲老師擁有超過 30 年的科技業管理經驗，並且是知名 AI 領域作家，致力於推廣 AI 教育，提供社會與青年對於打擊 AI 詐騙犯罪的相關應對。
林好芬	講師	現職： • 弘準國際法律事務所主持律師 • 外商公司法律顧問 • 政府機關法律顧問 • 新竹縣議員法律諮詢律師法律 • 扶助基金會新竹分會扶助律師 相關經歷： • 協合國際法律事務所實習律師 • 遠東萬佳法律事務所律師 • 宏鑑法律事務所律師 • 弘準國際法律事務所主持律師 • 法律扶助基金會扶助律師 • 新竹市社區關懷法律服務協會理事長 • 參與全台最大土地徵收桃園航空城案之律師團 • 參與柏克萊市政府與美國加州 EAST BAY COMMUNITY LAW CENTER (NGO) • 關於居住正義之社會政策推動

(三) 執行團隊介紹

姓名	經歷/現職
張哲維	現職： 明新科技大學行銷與流通管理系 助理教授明新科技大學校務企劃中心 主任 審議或公共事務參與經歷： 擔任諮詢/顧問/理監事/期刊編審委員/政府單位計畫案/競賽審查委員/校外口試委員 計畫主持人 「跨越醫療產業的鴻溝：從使用者觀點建構全通路醫療服務接受模型與創新擴散策略」國科會計畫 「Egoism or Altruism? Exploring Factors Driving Performance in Placemaking」研討會論文 •委辦連江縣113年度地方型 SBIR 計畫勞務委託案-擴充 •寶山鄉社區營造與新住民藝文推廣委託專業服務案 •113年馬祖新興遊憩活動規劃案 •112年度新竹青年新創基地營運計畫勞務採購案勞務採購案後續擴充 •112年社區營造及村落文化專輔中心採購案二、 議題相關經歷： •期刊論文Hung, S. W., Chang, C. W., & Chen, S. Y. (2023). Beyond a bunch of reviews: The quality and quantity of electronic word-of-mouth. <i>Information & Management</i>, 60(3), 103777.(共同第一作者) (SSCI, 5-year Impact Factor: 10.2) 國科會管二學門推薦期刊。 - Lo, S. F., Lu, W. M., Chang, C. W., Hung, S. W., & Yang, L. L.(2023). An efficiency-driven approach for global ecological industrial parks. <i>Journal of Cleaner Production</i>, 424, 138837. (SCI, 5-year Impact Factor: 10.2) 國科會區域研究及地理學門推薦期刊。 - Hung, S. W., Chang, C. W., Ma, Y. C. (2021). A new reality: Exploring continuance intention to use mobile augmented reality for entertainment purposes. <i>Technology in Society</i>, 67, 101757. (SSCI, impact score: 4.75, ranking it 10 out of 110 in Social Sciences, Interdisciplinary) - Wang, A. P., Chang, C. W., Tsai, J. M., & Hung, S. W. (2021). A performance evaluation of Major League Baseball teams: An integrated social

	network and data envelopment analysis. Managerial and Decision Economics. Doi: http://doi.org/10.1002/mde.3316 (SSCI) •Chang, C. W., Shiu-Wan Hung., Min-Jhih Cheng., Yi-Chen Lee & Cheng-Hong Cheng (2021). For Every Plus There is A Minus: Acceptance and Resistance of Information Technology Users' Behavior. Journal of Business Administration, 46(2), 61-100. (EconLit) Hung, S. W., Lee, C. C., Chang, C. W., & Jian, J. H. (2023). 身歷其境的擴增實境美妝產品購買意願. 資訊管理學報, 30(3), 315-345. (TSSCI) Chang, C. C., Chang, C. W., Hung, S. W., Jian, J. H., & Chang, Y.W. (2023). 生技產業兩階段研發效率分析. 中原企管評論, 21(1), 89-111. •產學案主持人 影像模組光路優化暨智慧影像辨識演算法開發及機聯網稼動率提升策略與資安防護驗證 農遊 o2o 平台商業模式建置與演算技術
宋曼菱	現職： 明新科技大學 行銷與流通管理系/三年級 審議或公共事務參與經歷： •參與農業部食農教育計畫(學校組) •參與永續發展與社會實踐深碗課程 •第三期 USR 計畫 兼職助理



捌、議題說明

隨著資通訊技術的飛速發展，人工智慧（AI）正逐步滲透到我們日常生活的方方面面，帶來了前所未有的便捷與效能。從智慧型手機的語音助手、智能家居設備到各行各業的自動化流程，AI 技術的應用無處不在。然而，隨著這些技術的發展，詐騙手法也在日益精進，尤其是以 AI 為基礎的詐騙行為，已經成為當前數位時代的嚴峻挑戰。

AI 技術尤其是深偽技術（Deepfake）、語音模擬（如 AI 生成語音）以及虛假身份生成等，給詐騙集團提供了全新的工具，讓這些犯罪手段變得更加精密且難以識別。詐騙集團利用這些技術來創建仿真的人物影像或語音，模擬真實人物的行為和語氣，使受害者在網路求職、金融交易、社交平台或在線購物時，難以察覺真假。例如，詐騙者可能會利用 AI 技術來製作一段看似由知名企業代表發出的真實求職邀請，或用偽造的語音模仿熟人要求轉帳，進而進行詐騙。這些行為利用了「社交工程」技巧，即通過操控人性的心理弱點來達到詐騙目的，使得即便是技術背景較為熟悉的人也可能中招。

這種依賴 AI 的詐騙形式帶來的危害，不僅限於個人財產的損失，還涉及到敏感個人資料的外洩。隨著 AI 在金融、求職和社交等領域的應用日益增多，消費者和使用者的個人資料無聲無息地流入了無數不法分子的手中，形成了潛在的數據安全隱患。這不僅影響了單個人的財務安全，更對社會整體的信任體系造成了威脅。事實上，當人們對科技產生疑慮，尤其是對 AI 技術的信任動搖時，社會整體的信任結構可能會受到影響，從而引發更大範圍的社會問題。

年輕一代特別容易成為這些 AI 詐騙的目標。這些年輕人通常對新技術有較高的接受度，並且在網路上活躍，參與網路社交、網上購物、求職或創業等活動，因此他們的個人資料更容易成為不法分子的攻擊對象。然而，年輕人通常缺乏足夠的資安防範意識和數位素養，使得他們在面對日益精密的詐騙行為時，容易掉入陷阱。

隨著詐騙手法的進化，如何在 AI 技術的浪潮中保護自己，成為了當今社會必須正視的重要問題。從提升數位素養到加強資安防護，這不僅是每一個個體的責任，更是整個社會應該共同關注的議題。只有通過有效的教育和技術防範，才能減少 AI 詐騙的發生，保護社會成員免受損害，並維護社會的穩定與發展。

一、導言：我們為什麼要討論「AI 詐騙」？

在人工智慧技術飛速進展的時代，我們的生活越來越依賴各種數位工具與線上溝通方式。AI 的便利性無庸置疑，它能幫助我們撰寫文章、翻譯語言、模擬聲音甚至創造虛擬人像，為工作與生活帶來前所未有的效率與創意。然而，當這些技術落入不法之手，原本用來服務人類的工具，卻可能成為欺騙與操縱的利器。

AI 詐騙，正是這股趨勢中最值得我們警覺的風險之一。現在的詐騙手法早已不再侷限於假電話、簡訊釣魚或假投資網站，而是進化為結合「深偽技術」(deepfake) 與「語音合成」的高仿真手段。有人曾在接到一通「親人來電」後，在短短幾分鐘內便匯出了畢生積蓄；也有企業員工被「上司的語音指令」誤導，將款項轉至詐騙帳戶而損失慘重。這些案例讓我們意識到，AI 詐騙不僅更具迷惑性、針對性，還更快速、更難防範。

在台灣，AI 詐騙案件正迅速攀升。根據刑事局統計，2023 年全年受理詐騙案超過 4 萬 3,000 件，其中涉及語音模擬與假影像的案例日益增多。例如 2023 年 5 月，某科技公司高層誤信由 AI 生成的董事長影片，導致匯款新台幣 1,100 萬元；2024 年起，更有大量利用親友語音的 LINE 通話詐騙事件，許多民眾因情急未察，即誤信上當。

● AI 詐騙的社會影響與案例：

根據警政署刑事警察局《112 年詐欺犯罪分析報告》，2023 年全台詐騙案高達 43,360 件，損失金額逾新台幣 76 億元，其中 AI 相關詐騙雖尚未佔據主流，但成長速度驚人。例如：

2023 年 4 月，新北市一名大學生收到自稱父親的 Line 語音訊息要求緊急匯款。警方事後發現該語音由 AI 生成，聲音與說話方式與其父高度相似。

2024 年 3 月，台中一間中小企業接獲「老闆」語音電話要求支付貨款，財務主管因信任對方聲音而轉帳 300 萬元，後經查為 AI 仿聲詐騙。

2024 年 6 月，桃園某企業主向警方報案，指其助理遭詐團假冒主管發送 Zoom 會議連結，實為惡意釣魚程式，損失商業資料與個資數百筆。

詐團利用生成式 AI 模擬公眾人物（如藝人、政治人物）製作「投資推薦」影片，在 Facebook、YouTube 上投放廣告，誘使民眾點擊連結並投資虛假平台。

社群媒體已成為 AI 詐騙快速擴散的重要渠道。根據 Meta 與台灣事實查核中心於 2024 年上半年的合作報告指出，已有超過 300 部深偽影片被下架，其中三分之一涉及假冒公眾人物的投資詐騙或錯假資訊擴散。這些案例凸顯出 AI 詐騙的兩大特性：高度擬真與擴散力驚人。只要取得一小段聲音或影像樣本，詐騙集團就能快速製作出「看起來很真」的假身分，並透過社群平台進行大規模傳播，導致大量用戶受騙或誤信。

這類詐騙事件不只造成金錢損失，更讓許多民眾對 AI 技術產生不安，甚至懷疑整體網路資訊的可信度，嚴重動搖民主社會中最基本的公共信任。AI 詐騙的本質，已不只是技術層面的犯罪升級，更是對資訊真實性、公民安全與社會信任系統的深層挑戰。

面對這樣的新型威脅，我們該如何應對？我們能否在追求科技創新與守護社會安全之間，找到一個有效且可行的平衡點？本手冊將引導你深入了解 AI 詐騙的現況與危機，並一同思考從教育制度、法規政策、科技設計與社會應變機制中，我們可以做出哪些具體行動。

二、議題背景說明：AI 技術與詐騙型態的演變

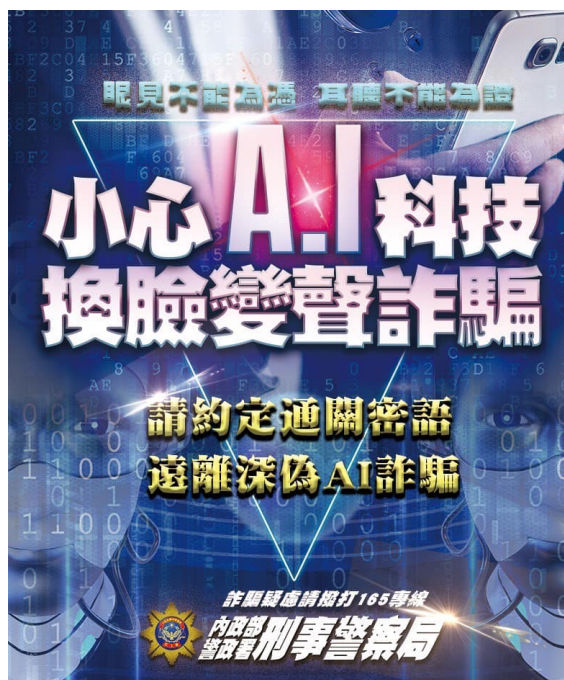
（一）什麼是 AI 詐騙？

AI 詐騙泛指運用人工智慧技術執行詐騙行為，與傳統詐騙方式相比，這類手法更具仿真性、隱蔽性與迷惑性。透過語音模擬、影像合成、虛擬對話等技術，詐騙者能製造出真假難辨的情境，使受害者難以察覺異常，進而落入陷阱。主要手法包括：

- 語音深偽 (Voice Deepfake)：AI 即可合成高度擬真的聲音。詐騙者冒充親友或主管進行語音通話，藉由急迫性話術要求轉帳或提供個資，讓受害者在情急下無法分辨真偽。
- 合成影像 (Deepfake Video)：利用深度學習模型合成虛假的人物說話或行動影片，常用於假冒名人、主管、機關人員，以詐財或操控輿論。

- AI 聊天機器人詐騙 (Scam Bots)：結合自然語言模型與自動對話系統，假冒客服或交友對象，誘導使用者點擊釣魚連結或陷入投資詐騙圈套。

資料來源：Europol (2023)。「Facing Reality? Law Enforcement and the Challenge of Deepfakes」；金融監督管理委員會 (2024 年 3 月) 新聞稿《防範生成式 AI 詐騙 提升金融防詐安全》。



(二) 詐騙型態如何演變？

隨著科技不斷進步，詐騙手法也從早期依賴人際話術的「傳統詐騙」，逐步進化為結合網路工具與數位平台的「網路詐騙」，直到如今利用人工智慧進行聲音模仿、影像合成與自動對話的「AI 詐騙」。手法越來越精密，辨識難度也越來越高，對社會造成更廣泛的影響與挑戰，目前詐騙演變趨勢：

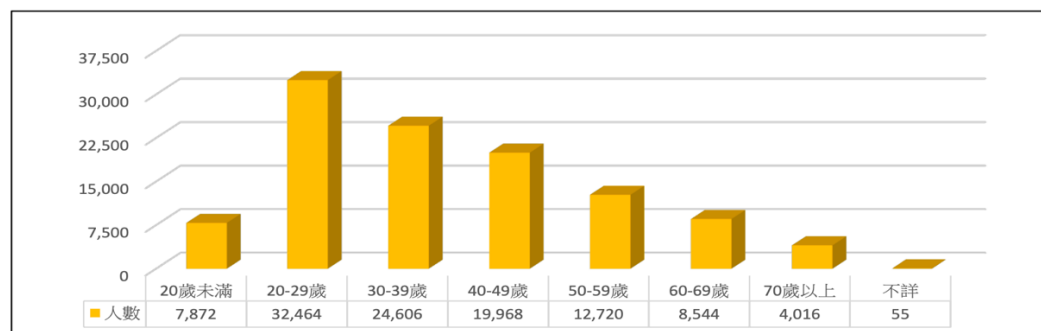
- 科技化與數位化：詐騙手法日益依賴高科技工具，例如使用 AI 模擬聲音、製作仿冒網站、或透過社群媒體平台進行釣魚詐騙與假訊息擴散。
- 跨境化與隱匿化：詐騙集團藉由 VPN、加密通訊與假 IP 等技術，實現跨國操作與身分隱藏，增加執法單位追查難度。
- 人性化與情境化：詐騙話術更加貼近人性，常以信任感、親密關係或急迫情境為誘因，例如愛情詐騙、冒充親友求助、假冒公部門通知等。

- 產業化與組織化：現代詐騙集團已形成產業鏈，內部分工明確，包括話術設計、技術支援、人頭帳戶、虛假客服等角色，進行系統化詐騙操作。
- 不斷創新：詐騙集團會根據時事及科技發展，不斷研發新的詐騙手法，例如利用生成式 AI 進行詐騙、假冒各單位發放補助等。

(三) 為什麼現在要關注 AI 詐騙？

面對層出不窮的 AI 詐騙事件，我們不僅需要認識其技術手法，更應深入理解這種現象背後所代表的社會警訊。AI 詐騙之所以應受到高度關注，並非僅因其個別危害性，更因其已成為跨領域、系統性且持續擴張的數位威脅。從技術應用、生活場景到制度治理，AI 詐騙正對個人安全與社會信任結構產生深遠影響。以下從三個層面說明其急迫性與嚴重性：

- 當代性：AI 詐騙已經進入日常生活
 - 不再是未來想像，而是「現在進行式」的真實威脅。
 - 社群平台、即時通訊工具與生成式 AI 普及化，使一般民眾更容易接觸甚至不自覺散播偽造資訊。
 - 從假冒客服、假投資廣告到偽造聲音、影片，AI 詐騙形式快速多元化。
- 危險性：擬真度高、辨識困難
 - 僅需數秒的聲音或影像樣本，AI 即可合成高擬真內容。
 - 過去常用的辨識策略（如語氣判斷、文字錯誤）已逐漸無效，傳統防詐機制面臨挑戰。
 - 許多受害者在完全無警覺的情況下上當受騙，顯示防範難度已大幅上升。
- 社會影響：侵蝕信任、擴大風險
 - 民眾對網路資訊、媒體內容與數位身分的信任度下降。
 - 假訊息可能操縱輿論、干預選舉，威脅民主社會之正常運作。
 - 青年與數位常用者風險更高，若不加強教育與保護，數位落差將進一步擴大。



113 年 1 月至 11 月全般詐欺犯罪被害人年齡統計

玖、AI 詐騙政策現況與分析

一、政策整體架構與推動背景

隨著人工智慧（AI）技術迅速演進，詐騙手法也同步升級，特別是透過 深偽技術（deepfake）製作仿真語音與影像，或藉由 AI 模型自動生成詐騙訊息與對話，對國內資安與民眾信任造成嚴重威脅。

為了因應這類新型態犯罪，台灣政府自 2023 年起推動「新世代打擊詐欺策略行動綱領」，並於同年升級為 1.5 版，建構以「識詐、堵詐、阻詐、懲詐」為主軸的防詐架構。2024 年更進一步推動綱領 2.0 版，擴大跨部會合作與科技應用，並於 113 年 7 月通過「打詐新四法」，包括新制定《詐欺犯罪危害防制條例》，以及修訂《通訊保障及監察法》、《洗錢防制法》與《刑事訴訟法》，強化執法與監管效能。同年 11 月，行政院正式通過「打詐綱領 2.0 版」行動計畫，涵蓋 114 至 115 年度，並新增了「防詐」作為核心，全面強化數位經濟產業治理下的反詐策略轉型。



二、現況政策措施分析

為因應詐騙犯罪手法不斷演進，並與「打詐新 4 法」相輔相成，政府推動研修「新世代打擊詐欺策略行動綱領」2.0 版，重行檢討各項策略、行動方案及具體措施，並調整架構，除行政院打擊詐欺辦公室轉型為打擊詐欺指揮中心，肩負「府院通報、部會協調及社會溝通」之任務，更新增「防詐」面向，由數位發展部擔任統籌機關，強化數位經濟產業治理。

打詐綱領 2.0 版，延續跨部會合作機制，以「運用 AI 防制、深化跨境合作、監管關鍵產業、加強被害保護」為規劃重點，設立「強化防詐意識、減少發生數、降低財損數」3 項目標，從「識詐、堵詐、防詐、阻詐、懲詐」5 大面向著手，跨部會推動「厚植防詐知能、落實源頭(電信、網路、金融)管理、刨根溯源查緝」等相關工作，並與金融機構、虛擬資產服務提供、電信事業、網路廣告平臺、第三方支付服務、電商及網路連線遊戲等 7 大防詐關鍵產業公私協力，以收抑制詐欺犯罪危害之效，保障民眾財產安全。



(一) 識詐（宣導教育面）→防詐騙：

教育部、內政部、法務部、NCC 及警政署協同學校、銀行、社群平台等單位，針對不同年齡與使用習慣族群推動識詐宣導。強化金融機構「關懷提問」制度，針對 ATM 或臨櫃操作中出現可疑交易時，由行員即時詢問與介入。執行「全民識詐」行動計畫，透過電視廣告、防詐影片、網路社群行銷等多管齊下，提升風險警覺與識別能力。

提升全民防詐意識，降低因資訊落差、焦慮心理或錯誤信任而導致的詐騙受害風險。將識詐能力系統性納入數位素養與媒體識讀教育，特別針對青少年族群強化日常辨識能力。

政府統計顯示，2023 年相關宣導活動觸及人次達 3.3 億。銀行據點協助阻止詐騙案件近 5 萬件，攔阻潛在財損金額近新台幣 60 億元。

- 目前政策回應：政府認為識詐宣導有助於建立第一道防線，是預防犯罪的重要環節。而學界指出，單靠認知教育恐難應對變化迅速的詐騙手法，建議搭配平台管理與技術防詐機制。民眾反映目前宣導內容與實際詐騙情境落差大，建議增加即時更新案例與互動式模擬教學。

（二）堵詐（電信服務面）→截詐訊：

與各大電信業者合作，導入境外來電辨識與警示系統，並推動「簡訊發送實名制」，防止詐騙集團冒名發送不明訊息。整合 NCC（國家通訊傳播委員會）、警政署與平台業者，建立詐騙網址與假帳號的黑名單資料庫，並要求社群平台下架可疑內容。推動「簡訊發送業者登錄管理制度」，控管詐騙訊息的技術散播源頭。

從電信與網路通訊源頭攔截詐騙內容，減少詐騙訊息傳播途徑。提升民眾對可疑來電與簡訊的辨識能力，降低接觸與受騙風險。2023 年 NCC 與警政署合作攔阻超過 9,000 則詐騙網站連結與假廣告。各大電信業者導入境外來電顯示系統，有效降低「假親人」與「假官員」來電受騙機率。

- 目前政策回應：然學者指出，這類政策需要技術密集投入與資通法規支持，且跨境合作仍是盲點。民眾抱怨實務上詐騙簡訊與語音依然猖獗，顯示堵詐機制尚未完全有效。

（三）防詐（數位經濟面）→淨網路：

金管會與數位部推動「廣告主實名制」，要求 Facebook、Google 等平台驗證投放者身分。並開發 AI 偵測工具，24 小時自動巡查假投資廣告、虛假帳號與假粉專。金融機構強化交易風險偵測模型，配合凍結可疑資金流向。

近年要求數位平台承擔「中介責任」，遏止詐騙廣告散播。預防民眾因錯信平台內容而受騙。政府表示已成功下架超過 6 萬件疑似詐騙廣告和逾 2 萬筆可疑帳戶遭平台封鎖或凍結處理。

- 目前政策回應：學界強烈建議制定「數位中介服務法」，明確規範平台責任與資訊揭露義務。民間科技業者支持建立自律公約，並主張公私協作提升風險模型效率。民眾對平台廣告失真感到不安，認為「驗證標章」制度有助重建信任。

(四) 阻詐（贓款流向面）→擋金流：

建立詐騙風險預警系統，與電信業者、社群平台合作即時阻斷可疑連線與帳號行為。擴大金融機構「異常交易通報」義務，針對短時間大量轉帳、人頭帳戶異動進行即時攔阻。推動公私部門協作平台（如 LINE、Meta、Google），共同建立 AI 詐騙內容下架與帳號凍結機制。

強化第一線攔阻能力，在金流與訊流層面減少詐騙成功機會。建立全民防詐意識，從科技、教育到制度全面提升防護網。截至 2023 年底，國內金融機構攔阻高風險轉帳超過新台幣 27 億元。多家社群平台啟動 AI 詐騙偵測模組，協助下架超過千筆深偽廣告與假帳號。

- 目前政策回應：民間團體呼籲強化社群平台責任，並制定更明確的「防詐演算法規範」。金融界指出技術防詐需與使用者教育並行，否則仍可能遭精密詐騙繞過。

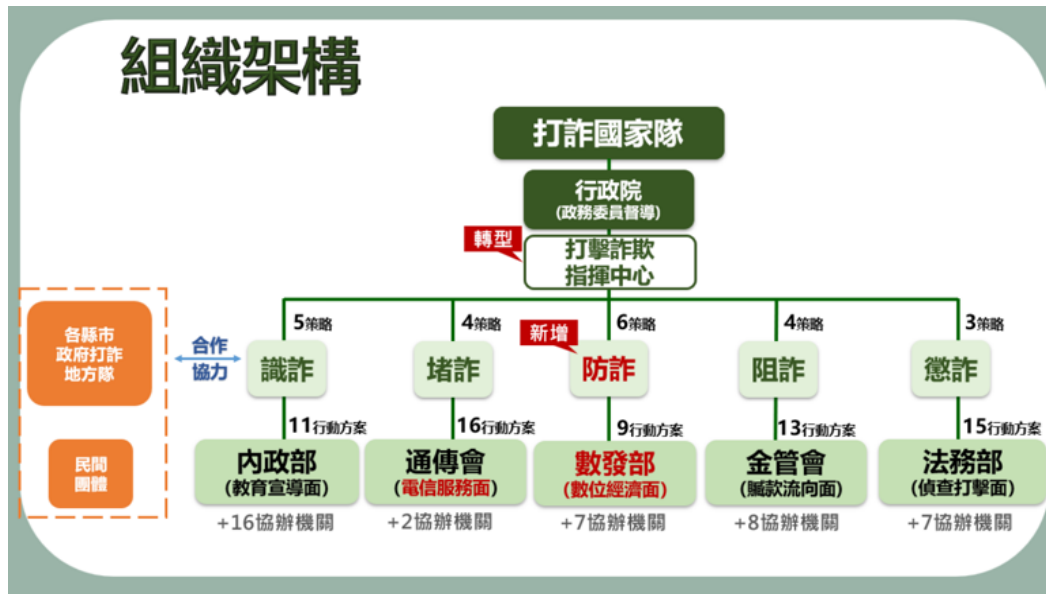
(五) 懲詐（偵查打擊面）→清集團：

推動「打詐五法」修正，擴大共犯認定、加重詐騙集團首謀刑責。成立「打詐國家隊」，整合法務部調查局、警政署、金融監理單位聯合辦案。引入科技工具如數位取證、加密貨幣追蹤技術輔助破案。

強化對詐騙組織的高壓打擊。提高犯罪成本，壓制人頭帳戶與人力招募。2023 年破獲詐騙集團案件超過 1,900 件，查扣犯罪所得近 40 億元。多起詐團跨境合作案件由我國主導發起偵辦。

- 目前政策回應：學界認為，刑責強化具威嚇效果，但必須配合源頭治理與跨境協定。民眾希望能公開詐騙集團名單與手法，增加透明度與警示作用。

三、政府與民間現行對策概述



面向	策略	統籌機關	分項指標
識詐 宣導教育	1. 分齡分眾防詐宣導 2. 落實金融機構關懷提問、及時攔阻 3. 加強網路推播能量 4. 多元管道擴大觸及(強化跨部會合作) 5. 建立正確法治觀念	內政部	1. 每年非網路及網路宣導資訊觸及人次 5,000 萬人次。 2. 每年全般攔阻金額新臺幣 100 億元 3. 每年發送防詐簡訊 1 億 4,000 萬則 4. 各部會每年執行跨部會合作宣導 4 場次；對應族群宣導 2 場次。 5. 加強法治觀念教育(含青少年法治教育宣導)，目標值每年辦理 500 場次活動。
堵詐 電信服務	1. 防杜境外詐騙來話 2. 遏止人頭門號 3. 攔阻惡意簡訊 4. 強化電信事業於涉詐網域及網址之聯防	通傳會	1. 每年攔阻境外涉詐來話 600 萬通(採滾動修正)。 2. 每年限制或停止人頭門號(含非本國籍預付卡)使用至少 2,000 門(採滾動修正)。 3. 每年主動分析篩檢商業簡訊 25 萬件，避免傳送涉詐內容(採滾動修正) 4. 電信事業每年配合攔阻詐騙網域 3 萬件(採滾動修正)。
防詐	1. 防制網路詐騙廣告		1. 每年通報可疑網路詐騙訊息 6 萬件(採滾動修正)。

數位經濟	2. 遏止詐騙網站	數發部	2.每年配合攔阻詐騙網域 3 萬件(採滾動修正)。
	3. 建立政府專屬短碼簡訊發送機制		3.每年發送 2,000 萬則政府專屬短碼簡訊。
	4. 加強電商業者資安維護		4.每年至少辦理 10 家次電商個資行政檢查。
	5. 防制第三方支付詐騙		5.每年至少辦理防制洗錢聯防查核 30 家業者。
	6. 防制遊戲點數成為詐騙工具		6.每年辦理跨部會遊戲點數防詐聯席會議至少 6 場次。
阻詐 贓款流向	1. 防制人頭帳戶進行詐騙	金管會	1.全體金融機構(100%)完成建置「疑涉詐騙境內金融帳戶預警機制」。
	2. 防制信用卡詐騙		2.全體信用卡業務機構及簽帳金融卡發卡機構(100%)加入財團法人聯合信用卡處理中心(下稱聯卡中心)建置之「信用卡
	3.強化虛擬資產服務提供業者洗錢防制及詐欺防制管理		詐欺犯罪防制電子化通報平臺」。
	4. 防制貨到付款、一頁式詐騙		3. 虛擬資產服務提供業者全體(100%)完成建置「疑涉詐騙之異常交易警示機制」。
懲詐 偵查打擊	1. 瓦解電信網路詐欺集團	法務部	4.加強向快遞專區通關之報關業者(100%)宣導慎選上下游業者,以及每月查核貨運公司有無依規定檢查要求託運人於包裹上應註明受貨人、託運人等資訊,並提升每年度「受理件數」與「完成退貨退款件數」之比率 4%。
	2.強化查緝跨境詐欺犯罪能量,遏止境外犯罪		1.每年電信詐騙案件查獲集團數提高 5%。
	3. 落實及強化詐欺犯罪被害人之保護		2.推動駐外法務秘書、警務秘書及移民秘書與駐在國有關機關就打擊跨境詐欺案件或合作機制進行聯繫、晤談或情資交換等(含海峽兩岸共同打擊犯罪及司法互助協議相關執行),每年合計不少於 500 次。
			3.每年查扣犯罪不法所得提高 3%。

四、民間參與與社會創新

詐騙手法層出不窮，從假投資、假親友到社群詐騙手段日益精密。面對複雜多變的威脅，趨勢科技與刑事局今宣布深化逾十年的合作夥伴關係，正式啟動「全民防詐守護戰」計畫。雙方除了持續同步更新詐騙電話、詐騙網址與假 LINE ID 等關鍵涉詐資料外，更將展開兩階段防詐升級行動，包含三個月免費「AI 防詐達人」App 試用活動及橫跨數位平台的聯名宣導，全面升級公私協力的防詐模式。

即日起至 8 月 31 日止，至刑事警察局「165 LINE 官方帳號」、「165 全民防騙網」活動頁面，即可獲得「AI 防詐達人」App 免費三個月試用方案的專屬下載連結，另閱覽「165 打詐儀錶板」至活動頁面 (<https://trend-tw.com/tmc90-165form>) 輸入當日受理案件數及個人資料，還有機會獲得緝毒犬主題贈品與六折優惠券，期望藉此提升民眾識詐、防詐與應對能力。

民間機構參與	對策/行動
MyGoPen、真的假的	協助查核詐騙內容與假訊息，並提供 LINE BOT 即時查核
趨勢科技	結合AI詐騙預測模型、詐騙行為模式分析、刑事局165聯防，實現即時預警與主動防護
台灣事實查核中心	推出生成式 AI 詐騙專題，教育民眾如何分辨深偽影片
中華民國資訊安全學會	建議建立「AI 詐騙國安監測雷達」，類似防疫指揮系統的資訊共享機制

五、多元觀點彙整：公民如何看待 AI 詐騙？

AI 詐騙所涉及的不僅是犯罪問題，更牽涉公民的資訊素養、數位倫理與國家治理策略。以下彙整出現行社會中幾種主要觀點：

(一)強化個人辨識力是根本對策

支持者認為，AI 工具再怎麼進步，若每位公民都能具備基本的媒體識讀與數位辨識能力，詐騙就難以成功。他們主張政府應將防詐教育納入義務教育與長者教育體系，從源頭建立資訊防詐能力。

參考資料：Media Literacy Council (2023)；教育部《資通安全與媒體素養白皮書》(2022)。

(二)平台與企業要負起把關責任

此觀點強調技術提供者與社群媒體平台的倫理責任，例如：應標示深偽內容、過濾不實資訊來源，甚至限制高風險 AI 工具的開放應用。此觀點也質疑目前平台經濟導致獲利優先於安全。

參考資料：AlgorithmWatch (2023)《AI and Accountability in Platform Governance》；Digital Futures Commission (2022)。

(三)政府應立法與跨部會整合反詐行動

有些人主張僅靠個人防範效果有限，應由政府進行科技法制改革、跨國合作並授權警政系統有更高查緝能力。同時呼籲政府建立詐騙警示平台，與電信、金融業協作監控異常交易。

參考資料：行政院資通安全處 (2024)；聯合國毒品和犯罪問題辦公室 (UNODC, 2023)。

(四)過度防範會壓抑創新與言論自由

一部分科技與人權倡議者提醒：若對 AI 生成內容強力控管，可能影響正當創作與技術發展空間，甚至衍生濫用監控與審查權力的風險。他們建議以「風險比例原則」設計法律機制，而非全面封鎖。

參考資料：Electronic Frontier Foundation (EFF, 2023)；Mozilla Foundation (2022)《Regulating AI: The Balance Between Innovation and Oversight》。

六、AI 詐騙的主要議題與價值衝突

- 科技發展與安全監管的平衡：AI 語音與影像合成技術快速進步，是否應限制或延緩公開？

價值衝突		
技術開放促進創新	或	限制技術以防止濫用
資訊自由與隱私		公共安全與社會秩序

例證：2023 年，Meta 與 OpenAI 皆遭批評其生成式 AI 工具可輕易被詐騙者利用，台灣政府亦有呼籲國際平台落實風險控管（NCC，2023）。

- 政府介入與個人責任的界線：政府應該到什麼程度介入防詐？該由個人或家庭自行防範，還是仰賴制度保障？

價值衝突		
政府責任	或	個人自由
全民防詐		過度監控

例證：臺灣警政署 2024 年推動「打詐專責隊」，並結合金融機構進行即時攔阻，但也有民團擔憂侵犯隱私與言論自由（民間司改會，2024）。

- 技術應用與數位落差：不同世代與社會群體對 AI 詐騙的認知程度差異，是否會加劇弱勢受害？

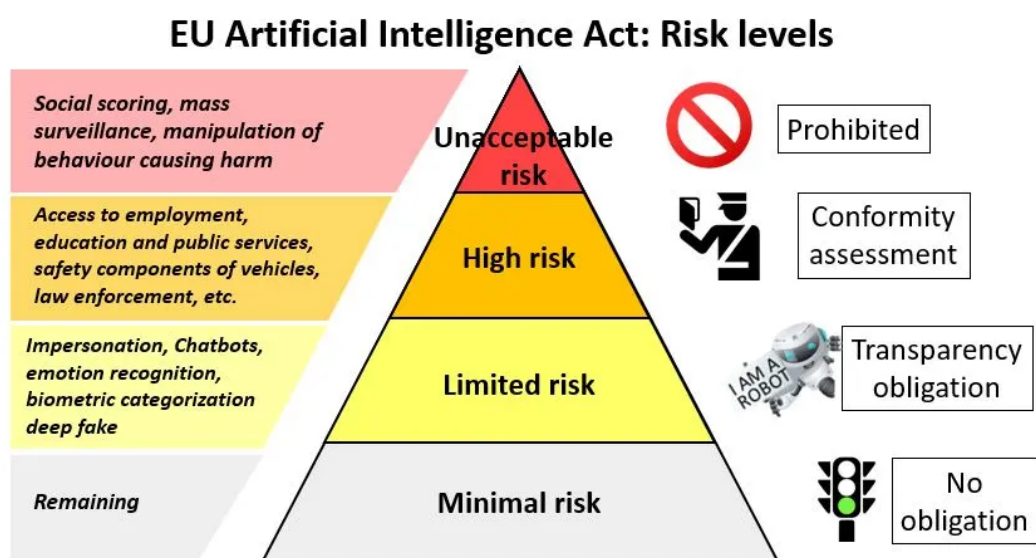
價值衝突		
數位機會平等	或	資訊落差擴大
AI 應用普及		保護資訊弱勢者

例證：長者在使用手機與社群時常因警覺性不足成為受害者。根據高雄市社會局 2023 年統計，65 歲以上長者佔通報詐騙案件的 35%。



七、國際法規與趨勢參考

- 歐盟《AI 法案》(AI Act, 2024 年正式通過)
 - ✓ 分級管理：將 AI 系統依照風險分為 4 類，詐騙屬「高風險用途」。
 - ✓ 內容要求：對深偽 (deepfake) 影片與音訊，要求「明確標示」。
 - ✓ 對企業規範：平台若未善盡 AI 內容審查義務，最高可罰其全球營業額的 7%。
- 美國 AI 治理政策與執法動向
 - ✓ 2023 年白宮發布《AI 權利法案藍圖》(Blueprint for an AI Bill of Rights)
 - ✓ 主張「人們應知道自己正在與 AI 互動」。
 - ✓ 強調 AI 不應被用於誘騙、操弄認知或侵害個資。
 - ✓ FTC (聯邦貿易委員會) 已對數家 AI 公司展開調查：如聲音模擬技術被用於詐騙銀行客服或老人。
- 新加坡《人工智慧治理與倫理準則》(Model AI Governance Framework)
 - ✓ 要求 AI 開發者須進行「詐騙濫用風險評估」與透明通報。
 - ✓ 推出 AI Verify 測試框架，協助企業驗證其 AI 系統風險，強化可信賴性。
- 日本通訊詐欺防制政策 (總務省、警察廳主導)
 - ✓ 採「預防接觸+金融管制+警企合作」三管齊下模式。
 - ✓ 規定電信商若發現異常通話模式，須立即通知用戶與當地警察。
 - ✓ 並推動成立 生成 AI 詐騙通報平台，即時揭露已知詐騙模式與範本。



八、我們有哪些可能的選擇與考量？

可能選擇	預期好處	可能風險
建立 AI 內容強制標示制度	提高辨識力、預防誤信	增加業者成本、侵犯創作自由
要求平台與電信業者設防詐責任	更有效封堵詐騙入口	恐造成過度監控與資訊過濾
推動全民 AI 媒體素養教育	提升社會防詐韌性	成效慢、成本高
投資 AI 詐騙偵測與警政科技	快速因應進化詐騙手法	須小心誤判與偵查濫權
建立跨國 AI 詐騙資訊共享機制	打擊跨境詐騙集團	涉及資訊安全與外交協商難度

九、中華民國刑法詐騙罰則

因網路資訊科技及人工智慧技術之運用快速發展，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，可能真假難辨，易於流傳。詐騙集團之犯罪手法亦推陳出新，為取信被害人而以上開方法施以詐欺行為，易使被害人陷於錯誤，且可能造成廣大民眾受騙，其侵害社會法益程度及影響層面均較普通詐欺行為嚴重，有加重處罰之必要，爰於第一項增訂第四款加重處罰事由。

■ 中華民國刑法第 339-4 條

犯第三百三十九條詐欺罪而有下列情形之一者，處一年以上七年以下有期徒刑，得併科一百萬元以下罰金：

一、冒用政府機關或公務員名義犯之。

二、三人以上共同犯之。

三、以廣播電視、電子通訊、網際網路或其他媒體等傳播工具，對公眾散布而犯之。

四、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犯之。

前項之未遂犯罰之。

十、參考資料

- 行政院 (2024) 新世代打擊詐欺策略行動綱領 2.0 版
<https://www.ey.gov.tw/Page/5A8A0CB5B41DA11E/c93637bd-ddc2-4447-8829-246a5ca0befc>
- 法務部 (2024) 法規名稱：中華民國刑法第 339-4 條。
<https://law.moj.gov.tw/LawClass/LawSingle.aspx?pcode=C0000001&flno=339-4>
- 內政部警政署刑事警察局 (2024) 。《112 年詐欺犯罪分析報告》。
<https://www.cib.npa.gov.tw/ch/index>
- 金融監督管理委員會 (2024 年 3 月) 。《防範生成式 AI 詐騙 提升金融防詐安全》。
- 中央社 (2023 年 5 月 22 日) 。〈AI 影片騙上千萬〉。
- 教育部 (2022) 。《資通安全與媒體素養白皮書》。
- Europol (2023) 。《Facing Reality? Law Enforcement and the Challenge of Deepfakes》。
- AlgorithmWatch (2023) 。《AI and Accountability in Platform Governance》。
- Media Literacy Council (2023) 。《Media Literacy Annual Report》。
- Digital Futures Commission (2022) 。《Platform Governance Report》。
- INTERPOL (2024) 。《Global Cybercrime and AI Fraud Trends》。



廣告



禁止性騷擾

No Sexual Harassment

禁止性騷擾及性侵害公開揭示

- 1 任何人不得對他人性騷擾或性侵害。
- 2 性騷擾他人者，依法得處新臺幣1萬元以上10萬元以下罰鍰；
利用權勢性騷擾他人者，依法得處新臺幣6萬元以上，60萬元以下罰鍰；
乘機襲胸摸臀或觸摸他人隱私部位，被害人可提出刑事告訴，
最高可處2年以下有期徒刑、拘役或併科新臺幣10萬元以下罰金。
性侵害他人者，依刑法規定最高可處死刑、無期徒刑或10年以上有期徒刑。
- 3 性騷擾或性侵害他人，除負有法律上之刑事與民事責任外，
本單位亦將依內部規定懲處。
- 4 遇到性侵害事件，請撥打110或113保護專線求助。
- 5 發現性騷擾或性侵害事件，需本單位立即協助處理者

請撥打本單位聯絡電話：**03-5593142 #3514**