AI 行騙防不勝防 冷靜查核以免上當

自今年 4 月本澳首次出現 AI 騙案以來，司法警察局累計接獲兩宗相關案件。由於警方自 2023 年起持續宣傳 AI 詐騙手法，公眾已具備一定認知和警惕性，這兩宗案件均未造成財產損失。然而，隨著全球範圍內利用人工智能實施詐騙及其他犯罪的案件日益增多，本文將剖析 AI 騙案的常見手法，幫助公眾全面了解並及時識別騙局，避免蒙受損失。

人工智能（AI）是一種通過電腦系統模擬人類思維模式，經自我學習不斷優化，最終按用戶需求生成結果的技術。目前，AI 已廣泛應用於日常生活，為公眾帶來諸多便利。與此同時，犯罪團伙亦不斷利用 AI 技術實施或預備犯罪，使詐騙套路的迷惑性、複雜度顯著提升，得手率大幅提高，對公眾構成更大威脅。

AI 騙案的常見手法

在犯罪實施方面，最為常見的是利用 AI 深度偽造（Deepfake）技術“換臉換聲”製作影片或進行實時視頻通話以實施詐騙，司警局立案的兩宗案件即屬此類。騙徒從本澳知名人士公開受訪片段中擷取面容及聲音，利用深偽技術製作影片，假裝相關人士推介投資，又架設偽冒本澳報章的釣魚網站作配套，企圖誘使公眾進行虛假投資從而騙取巨額款項。

同理，騙徒可以利用深偽技術換裝成任何人，例如假冒親友視頻致電事主訛稱患急病、遇意外等緊迫理由以要求“救急”；又或者假冒上司致電下屬要求進行商業轉帳等。香港特區曾發生兩宗涉款逾億的 AI 騙案，均以假冒上司方式作案，其中一案的騙徒甚至同時分飾多角召集視頻會議，事主信以為真，按“上級”要求匯出兩億港元。由此可知，不只一般民眾，連跨國公司、中小企業皆有可能成為 AI 詐騙的目標。

AI 技術在犯罪全流程的應用

除了直接實施詐騙，AI 技術已滲透到犯罪的各個環節：在預備階段，AI 可自動化完成網絡信息收集分析、篩選潛在受害人及關鍵資料、生成騙局所需的語音和文字內容；在實施階段，AI 聊天機器人可模擬“客服”或“情人”與受害人日常聯繫，逐步建立信任；在技術支持方面，AI 能自動搜索系統漏洞發動網絡攻擊，或快速編寫釣魚網站。

AI 技術的應用使犯罪活動更具迷惑性、精準性和個性化，不僅降低了犯罪成本，還提高了非法收益。更值得警惕的是，AI 技術的迭代速度遠超防範工具的研發進度，預計未來 AI 驅動的非接觸式犯罪將成為主流趨勢之一。

政府應對措施與公眾防範建議

為防範 AI 犯罪，全球各地政府、警方及科技企業已積極採取行動，通過立法要求 AI 生成影像必須附加標識；開發具備 AI 檢測功能的手機軟件等。本澳司法警察局也在網絡安全系統中引入 AI 技術分析風險，反詐中心新設 AI 換臉換聲示範的互動宣傳設備，貫徹科技強警理念，強化預防和檢測 AI 犯罪的能力。

儘管技術防範不斷升級，但騙徒也會隨著技術發展更新作案手法，因此提高公眾的防騙意識仍是根本對策。有效防範 AI 詐騙需做到：**嚴格管理個人信息、多重核實身份、反覆查證事實、遇事保持冷靜應對。**具體建議如下：

1. 謹慎處理任何個人資料，切勿輕易在網上披露或向陌生人提供人臉、指紋、聲紋等生物辨識資料，妥善管理社交平台的閱覽權限，嚴密保管身分或銀行帳戶密碼等重要個人及財務資料，防範被盜用作不法行為。

2. 對網上視頻內容，尤其是“名人推薦”或“投資指導”時常保持警惕；進行視像通話或語音訊息聯絡時，如對對方身分存疑，須多注意對方動作異樣（如輪廓或肢體邊緣），或提問只有雙方知悉的問題，反覆核查。

3. 若對方要求索取金錢或進行大額交易，或以情況緊急為由要求轉帳匯款，切勿馬上遵從，應設法以慣常聯絡方式再三查證，並向對方當面求證。

4. 懷疑遇騙時，立即撥打司法警察局防詐騙查詢熱線 8800 7777 或報案熱線 993 求助。

“有聲有畫未必真，冷靜查核辨虛實”。雖然 AI 犯罪具有高度迷惑性且不斷演變，但只要公眾做好個人信息防護，保持警惕並認真核實，就能顯著降低上當風險。同時，公眾更應密切關注最新防騙資訊，做好個人防範，並主動向身邊人轉發資訊，共同構建社區防騙體系，保障個人與社會的財產安全。