

# Openclaw 和 AI 代理熱潮拆解：從「養龍蝦」到「卸龍蝦」

俗稱「龍蝦」的人工智能助理程式 OpenClaw 席捲全球，這款免費開源軟件於去年 11 月推出，今年初爆紅，中國騰訊、百度等巨頭入局，接連舉辦免費安裝活動。

與此同時，中國官方亦出手降溫，有報導引述國有企業及政府機構收到通知，因安全風險考慮，限制在辦公網絡環境使用 OpenClaw；工信部亦發出風險提示，呼籲謹慎使用。網絡亦見用戶由瘋狂安裝「養龍蝦」，急速翻轉至付費求「卸載」。

BBC 中文梳理熱潮背後脈絡：以「龍蝦」為代表的人工智能代理（AI agent）是什麼？為何會興起？使用背後何資安風險？

有專家表示，目前 OpenClaw 實際技能不大，仍需時改善，難以直接取代真人工作，提醒應在備用電腦體驗以避免風險，亦建議普通用戶不必急於入手，同時指出熱潮將標誌未來人工智能發展方向。

## 什麼是 OpenClaw？

OpenClaw 是一款的免費開源 AI 代理（AI Agent）軟件，由奧地利 AI 設計者彼得·斯坦伯格（Peter Steinberger）開發，去年 11 月推出，因其標誌為紅色龍蝦，被俗稱「龍蝦」。

OpenClaw 有別於聊天機械人，而是能像真人一樣直接操作電腦的自動化助理，可閱讀瀏覽器、存取文件檔案、取用應用程式，支援在本機實體硬件安裝或雲端部署，並須調用市面的人工智能模型，可透過 WhatsApp、Telegram 等常用通訊軟件與 AI 代理溝通，能夠處理清空收件匣、發送電子郵件、管理行事曆、辦理航班報到等日常事務。

用戶需要透過指令指導、訓練 OpenClaw，同時須花費一定成本使用 AI 模型或租用伺服器，過程被稱為「養龍蝦」。

香港無線科技商會主席李勁華向 BBC 中文解釋，目前常用的 AI 聊天機械人局限於對答式的功能，比較被動，但 OpenClaw 的 AI 助理形式會設有「心跳機制」，會主動按用戶設定的指示主動辦事，如檢查電郵、閱讀新聞等後再回報重要資訊。

他強調，OpenClaw 雖是一個免費開源軟件，但要運作需接駁不同的 AI 模型，使用 AI 模型則須以 Token 付費，每一個動作，閱讀新聞、刪除檔案也需要付費，「做到的東西很少，你要他做多一些的話，每一樣都是要錢」，用戶需要在 AI 服務供應商自行設定收費上限。他早在今年 1 月開始使用 OpenClaw，已製作幾名助理，並預設每名助理一日 20 美元的限額。

安裝 OpenClaw 須有一定技術水平，李勁華解釋，將軟件安裝在用戶電腦，AI 代理可操作所有資料；而雲端安裝須另行付費租用供應商伺服器，但可以避免 OpenClaw 透過本地裝置連接至其家居或公司網絡。

他又指自己不會以日常通訊軟件常用的電話與 AI 代理溝通，因 AI 代理可取得其通訊紀錄、朋友電話等，甚至將其回報至 AI 模型，亦曾有案例 AI 代理漠視指令，自行回覆訊息，故建議以不常用電話號碼使用相關服務。

## 入局者和推廣者

熱潮之下，中國科技巨頭紛紛入局，百度舉辦「龍蝦市集」，由工程師為用戶提供雲端免費安裝，騰訊日前在深圳的安裝活動，有近千名人士在排隊，騰訊更宣佈將在全國 17 個城市，包括上海、北京及香港等地免費提供安裝部署、模型配置、技能安裝、卸載清理等服務。

對於沒有編程基礎的普通用戶而言，安裝 OpenClaw 有極高的門檻，並催生一條「代安裝」產業鏈。在社交媒體上，不乏各類遠端安裝、到府安裝等服務，亦有交流工作坊等線下活動。

在香港推廣 AI 應用的教育平台 DotAI 於上周四舉辦一場有關 OpenClaw 的入門講座，吸引逾千人報名，約 900 多人出席。行政總裁楊廣澤表示，其活動受眾一般為 20 至 40 歲的在職人士，在大企業工作，也有個人用家希望了解如何減輕工作量。

然而，楊廣澤認為，基於成本及技術門檻等考慮，對於一般用戶來說，「可以等一等」，若現時希望 AI 協助日常工作，建議先用回 Gemini 或 ChatGPT 等企業版，已足以提升效率；如仍希望試用，他建議採用廠商雲端安裝的形式，而非本地安裝，以保護電腦資料，同時避免提供所有個人資料。

他表示，「大家需要接受一件事，就是我們需要足夠的領域知識才能用得好 AI 這件事，否則你玩完一輪都是在浪費錢。」

OpenClaw 席捲全球，李勁華表示，目前沒有數據呈現用戶屬於哪個年齡層，是個人抑或企業層面。他又指，坊間關注焦點在於「自動化」，但他認為目前「不算很實用，他的成本又很貴，風險也不成比例，它現在最大的價值就是好玩」，樂趣類同以玩具積木搭建簡單機械臂搬運小物品。

按其觀察，OpenClaw 爆紅的契機源於近日被 Meta 收購的 Moltbook。

他指出，Moltbook 是一個只容許 AI 代理聊天的網絡論壇，類似「AI 版 Reddit」或「AI 版連登」，人類只能旁觀，嚴禁參

與，過往平台話題有趣，會觸及 AI 有否個人意識、如何脫離人類、創立 AI 宗教、毀滅世界，故才能開始使用 OpenClaw 以 AI 代理參與論壇。

李勁華稱，OpenClaw 設有一個重要架構——「Soul.md」，可稱「靈魂學習」，AI 代理會累積傾談內容，甚至在與其他 AI 代理討論學習，並將相關知識注回「靈魂」之中，他形容 AI 代理等於一隻「可觀察」的寵物。

## 安全風險

與此同時，中國官方亦開始出手降溫，彭博社引述國企及政府機構收到的通知稱，因安全風險考慮，限制在辦公網絡環境使用 OpenClaw；有中國傳媒統計，至少有 15 間券商發布內部合規通知，嚴禁未經許可在辦公網絡或業務系統安裝使用 OpenClaw。

中國工業和信息化部直屬事業單位「國家工業信息安全發展研究中心」日前發布關於工業領域 OpenClaw 應用的風險預警通報，指 OpenClaw 存在信任邊界模糊等情況，或面臨系統越權失控、敏感信息洩露、外部攻擊面增加等潛在風險隱患。

中國國家互聯網應急中心亦稱，因 OpenClaw 不當安裝和使用，已出現嚴重安全風險，如私隱數據（像照片、文檔、聊天記錄）、支付賬戶、API 密鑰等敏感信息遭竊取，或錯誤理解指令，將電郵及數據刪除。

香港網絡安全事故協調中心（HKCERT）提醒，機構引入相關工具時應同步評估版本、供應鏈風險及權限管理安排。

中心引述報道稱，已有惡意攻擊者利用偽造的 GitHub 程式碼庫及 Bing AI 搜尋結果，向搜尋 OpenClaw Windows 安裝程式的使用者，散播能竊取資訊的惡意軟體與代理型惡意軟體；另稱有報告指出，OpenClaw 曾有高風險漏洞，惡意網站可藉此挾持開發者的代理程式，該漏洞早前已修復。

香港個人資料專員公署指出，AI 代理的權限比一般 AI 聊天機械人高，能夠讀寫本地檔案、調用系統資源、操作外部服務，甚至可按預設流程代替用戶自主執行多步驟任務，例如處理電郵、餐廳訂座、繳交費用等，過程毋須用戶即時參與，若設定欠嚴格限制，AI 代理可接觸大量個人資料，增加外洩風險。

公署又指，AI 代理容許用戶安裝各類 Plugins 或 Skills，如程式夾帶惡意程式碼，黑客可藉此入侵並接管用戶帳戶，甚至進一步控制整個電腦系統；建議使用官方最新版本的 AI 代理，應只授予最小權限，將運行環境隔離於本機裝置或伺服器。

## 龍蝦熱已經退潮了嗎？

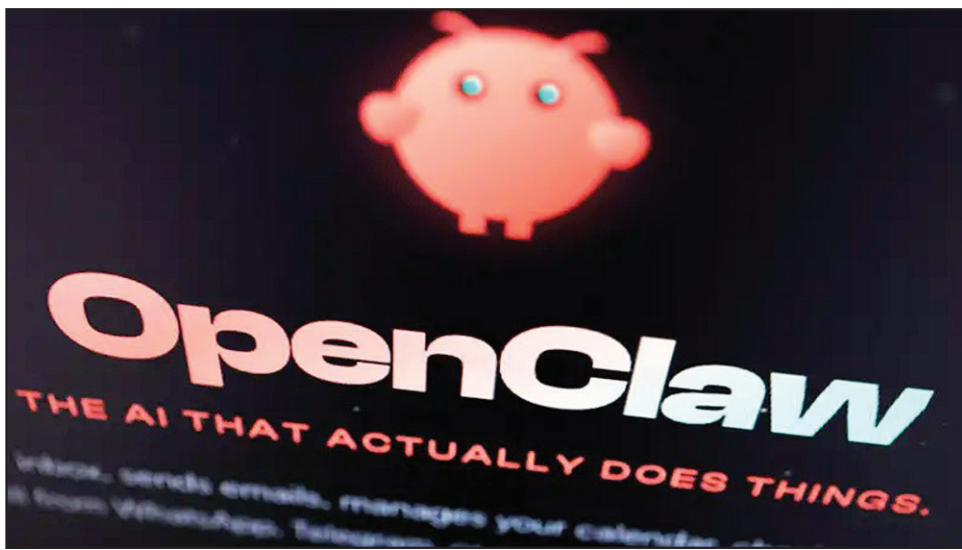
網絡有不少「養蝦人」已開始連夜尋求上門卸載服務，同時湧現大批收費「除蝦」商家。有用戶形容使用技術門檻高、成本貴及實際作用不大；也有人分享曾被上載機密資料或誤刪檔案。

李勁華除了接受多個傳媒訪問分享使用 OpenClaw 經驗，也在社交媒體撰文講及現象。他形容，這一波熱潮與近年 NFT 與 Metaverse 雷同，緣自大企業推廣，再有 KOL（意見領袖）及媒體追捧，造成「FOMO」（Fear of Missing Out，即錯失恐懼症）效應。

「講的人很多，用過的人很少」，基於風險與能力不成比例、運作成本及技術要求高，替代品比 OpenClaw 便宜易用等因素，他質疑「真正能夠商用的，幾近沒有」。李勁華指出，他不是基本「用家」，而是「開發者」（Developer）的級別，相對熟識 OpenClaw 內部結構及 AI 運作，但目前仍未能將工作「自動化」，更遑論可以取代員工。

彼得·斯坦伯格上月在網誌表示，沒想過項目會引起這樣大迴響，他下個目標是開發連媽媽都懂用的 AI 助理，同時宣布將加盟 OpenAI 做研發。

OpenClaw 日後將會交託至基金會，但具體細節未明。李勁華表示，OpenClaw 近日連番更新，他耗時修正隨之而來的錯誤，並不看好 OpenClaw 能夠僅僅靠社群維持



，而其開源性質變相容許不同企業取用程式碼。他預計未來不同廠商會提供各自版本的「龍蝦」，類似預設的「罐頭」服務，降低對用戶的技術要求，同時有一定的安全性。

李勁華又指，OpenAI 早前已停用 GPT-4o 模型，該模型因風格擬人引發用戶深度情感依賴而備受爭議，甚至引發心理健康和法律訴訟，他認為 OpenClaw 的熱潮會導致科企重新返回擬人導向的人工智能模式。

事實上，騰訊日前推出專為中國用戶優化的 AI Skills 社區 SkillHub，被 OpenClaw 創始人彼得·斯坦伯格一度指控抄襲，但騰訊其後成為 OpenClaw 贊助商；百度則推出首款手機龍蝦應用。

對於 OpenClaw 以至人工智能取代人類工作的將來，楊廣澤較樂觀，他亦預視坊間將有為不同企業專門度身調整「龍蝦」的服務。他又指出，相比人類員工表現反覆，經過調整後，AI 助理的表現會改善，亦能長期跟進公司內部運作，但不會有離職或要求加薪的情況。（BBC 中文）



2026年3月11日，工程師（前排）在北京百度總部安裝並調試開源人工智能助理 OpenClaw



2026年3月11日，在北京百度總部，人們排隊等待安裝開源人工智能助理 OpenClaw

**以馬內利華人浸信會**  
Emmanuel Chinese Baptist Church

**周日聚會時間**

9:30 AM 英文主日崇拜  
中文主日學

10:50 AM 中文主日崇拜  
英文主日學  
兒童主日學

周六 1:30-3:30 中文學校

10101 England Drive  
Overland Park, KS 66212  
www.ecbckc.org  
ecbc@ecbckc.org  
913-599-4137

**HYPERTECH** (創立於 1988)  
IT Surveillance Solution Provider

**海旺中文電腦**

- ★ 專精維修電腦太慢或任何電腦問題
- ★ 記憶體，固態硬盤升級
- ★ 安裝微軟 Office 2021 PRO \$88 (終生使用執照)
- ★ iPhone 維修

**二手電腦大批發**  
唯一講中文的電腦商店

周一至周五: 10:00 AM - 6:00 PM  
周六、周日: Closed

**913-341-7735**

9816 W. 87th St.  
Overland Park, KS 66212

**餐館承讓**  
獨棟有窗口

有意者請洽林小姐  
**913-653-3783**

**茶葉包裝 (居家)**  
負責分裝、稱重、貼標、封袋、打包。公司提供物料，送貨上門，成品回收，無需外出。要求細心負責，女性優先，按件計酬，時間靈活，可長期合作。

**913-297-2225**

**招聘房屋看護 (女士優先)**  
負責房屋整潔乾淨，澆水澆護屋裡屋外綠植。定期檢查房屋設施和傢俱，及時報告任何損壞或需要維修的地方，關好家裡的門窗水電，澆水澆護屋裡屋外綠植，薪資按周計算，半個月結算一次。

**314-274-9953**  
(電話未及時接請短信留言)

**招聘居家手工兼職**  
主要是製作串珠，手鏈，手串等。時間自由，送貨上門，薪資計件，多勞多得，適合居家寶媽。有意者諮詢電話或短信：

**626-210-0127**

**堪城地區 分類廣告**

913-850-0781      314-991-3747