大公報
2026年3月9日 星期一

AI「養龍蝦」爆紅 工信部提醒防安全風險

數字助手接管電腦 易引發網攻和信息洩露

焦點追蹤

「現在大家急得不得了，生怕沒有『養』上『龍蝦』。」在全國兩會廣東代表團小組會議上，全國人大代表、中國工程院院士高文道出了當前AI領域最火熱的現象——OpenClaw（昵稱為「龍蝦」）的爆發式流行。不同於只能在網頁裏聊天的各種AI應用，OpenClaw是一款「接管電腦」的「數字助手」式開源AI智能體，能接管用戶鍵鼠權限，直接調用系統API完成任務。

熱潮之下，網絡安全也面臨全新挑戰。近日，工業和信息化部網絡安全威脅和漏洞信息共享平台監測發現，OpenClaw開源AI智能體部分實例在默認或不當配置情況下存在較高安全風險，極易引發網絡攻擊、信息洩露等安全問題。建議相關單位和用戶在部署和應用OpenClaw時，充分核查公網暴露情況、權限配置及憑證管理情況，防範潛在網絡安全風險。

掃碼睇片

◀6日，近千名開發者與AI愛好者聚集在深圳騰訊公司門口，在騰訊雲工程師的免費協助下完成OpenClaw的雲端安裝。

大公報記者 郭若溪

OpenClaw是一款開源AI智能體，其通過整合多渠道通信能力與大語言模型，構建具備持久記憶、主動執行能力的定製化AI助手，高文解釋，「龍蝦」實際上是一個入口，它後面接入了很多大模型。用戶通過一個界面就能使用不同模型的能力，非常方便。

3月6日，騰訊雲的輕量雲服務器在深圳騰訊大廈樓下舉行了一個線下免費裝OpenClaw的服務，派工程師給來到現場的用戶提供從安裝部署到模型配置的一站式服務，吸引近千人排隊爭當「養蝦人」，更有人專程從香港、杭州等城市趕來，跨城學習。

深圳龍崗推「龍蝦十條」 助低成本AI創業

為了搶抓智能經濟發展機遇，深圳福田一批公務員已正式「養」上專屬「政務龍蝦」，開啟人機協同辦公新模式。這款福田區升級的AI數智員工2.0，已在政務外網完成本地化部署，為基層工作減負增效。為保障安全，每隻「政務龍蝦」都有在編公務員作為「監護人」，嚴格遵循相關管理辦法。

深圳龍崗則在7日推出了「龍蝦十條」新政——《深圳市龍崗區支持OpenClaw&OPC發展的若干措施（徵求意見稿）》，擬以「零成本啟動」為核心亮點，鼓勵平台企業打造「龍蝦服務區」，擬為開發者免費提供OpenClaw部署服務。政府將對平台給予相應補貼，並助「一人公司」低成本啟動AI創業。

「養蝦」需防範潛在網絡風險

近日，工業和信息化部網絡安全威脅和漏洞信息共享平台監測發現，OpenClaw開源AI智能體部分實例在默認或不當配置情況下存在較高安全風險，極易引發網絡攻擊、信息洩露等安全問題。由於OpenClaw在部署時「信任邊界模糊」，且具備自身持續運行、自主決策、調用系統和外部資源等特性，在缺乏有效權限控制、審計機制和安全加固的情況下，可能因指令誘導、配置缺陷或被惡意接管，執行越權操作，造成信息洩露、系統受控等一系列安全風險。建議相關單位和用戶在部署和應用OpenClaw時，充分核查公網暴露情況、權限配置及憑證管理情況，防範潛在網絡安全風險。

騰訊雲相關工作人員表示，「由於OpenClaw擁有相當高的權限，它也會存在一些安全性的風險。若部署在本地電腦，可能出現錯誤刪除本地文件、洩露隱私信息等問題。」雲服務器相對隔離的環境可有效規避此類風險，「OpenClaw在雲端環境中完成網頁瀏覽、消息發送等所有操作，與本地文件隔離，不會動用本地數據，既能避免不懂技術的用戶被竊取信息、誤刪文件，也能防止被黑客劫持或利用漏洞。」

◀在騰訊雲工程師協助下成功「養蝦」的用戶還獲贈一張「小龍蝦出生證明」。

什麼是「養龍蝦」?

話你知

OpenClaw（前身名爲Clawdbot/Moltbot）是一個開源的、本地優先（Local-First）的AI Agent框架，由奧地利創業者Peter Steinberger獨立開發。不同於只能在網頁裏聊天的各種AI應用，OpenClaw是一個能接管用戶鍵鼠權限的超級助理。OpenClaw能夠運行在用戶的終端裏，直接調用系統API來完成複雜任務。

在「養蝦」的過程中，雲服務器就像是「蝦塘」，大模型就像是「飼料」，兩者缺一不可。用Token（「詞元」，AI理解語言的單位，模型處理文本時會把文字切分成一個個Token。問AI一個問題，AI回答一段話，消耗的就是Token）「餵龍蝦」，就會令AI「越長越好」。

「龍蝦」怎麼幹活？

準備啟動
- 在電腦上完成本地部署，安裝必要組件、配置AI模型。

接收指令
- 給一句指令（如「查股價並畫圖」），自動拆解任務。

分析規劃
- 核心系統解析指令，將複雜任務拆分為簡單子任務，由「龍蝦」規劃好需要調用的工具和執行路徑。

執行任務
- 按照規劃自動調用相關工具，完成文件處理、網頁瀏覽等操作，複雜任務會自動迭代優化。遇到報錯或彈窗，「龍蝦」能自己嘗試修復。

反饋記憶
- 任務完成後，將結果整理反饋給用戶，同時記錄任務關鍵信息，形成持久記憶。

大公報郭若溪整理

▲騰訊雲智能體開發平台上線了「一鍵部署OpenClaw」的網頁幫助平台。

◀到騰訊大廈樓下安裝「龍蝦」的人中不乏中小學生及老年人。

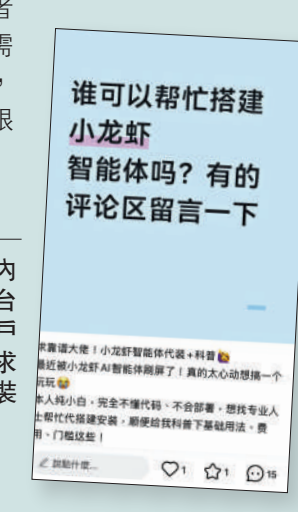
付費上門幫「養蝦」? 業內:靠信息差賺錢

湧現商機

OpenClaw的走紅並非偶然。騰訊雲工作人員告訴記者，OpenClaw與豆包、千問等AI應用的本質區別是有交互，它不僅能「說」，更能「做」，相當於給用戶提供了一個和電腦操作系統對話的通道和橋樑。在獲得操作權限後，通過不斷修正它的任務執行過程，它便能了解用戶的偏好、行為、工作以及拓展學習，最後成為AI「秘書」，只需一句自然語言指令，它便能自主打開瀏覽器搜索數據、操作Excel生成報表。

然而，OpenClaw的安裝部署門檻較高，涉及複雜的環境配置和模型接入，不少普通用戶望而卻步。這一需求催生了火爆的付費安裝市場。遠程安裝服務價格從幾十元到數百元不等，提供「上門安裝龍蝦」服務的賣家更是批量湧現。但業內人士表示，網絡上有很多趁OpenClaw火爆而伺機牟利的人員，「因為大多數人都是連入門操作都不會，他們就趁着這個信息差，去賺錢。實際上按教程裝也就十幾分鐘就可以。」

「我們很快會推出一鍵安裝版本，每個人養兩隻都不是問題。」全國政協委員、360集團創始人周鴻禕8日表示，OpenClaw將原本抽象的智能體概念進行了物化，變成了每個人都能配置在電腦、手機上的AI助手。但消費者應根據自身需求選擇服務，避免盲目跟風。



▶小紅書等內地社交平台上，大量用戶發布「有償求幫助安裝OpenClaw」的帖文。

中國AI潛力遠沒有被充分發揮

專家解讀

OpenClaw「養龍蝦」熱潮背後也伴隨着「機器換人」的AI「替代焦慮」。對此，全國政協委員、中國工程院院士王堅指出，AI的本質是解放人類，而非替代人類。「做人工智能相關工作，一定要想明白它能幫助誰，而不是天天糾結它會替代誰。」王堅表示，AI作為一種創造性工具，必然會孕育出全新的職業，人類的創造力借助新技術，能夠衍生出更多新的就業可能。

在「龍蝦」火爆的表象下，中國AI產業的深層邏輯正在重構。王堅特別澄清了一個概念誤區：當前中國引領全球的並非簡單的「開源」（Open Source），而是「開放權重」（Open Weight）。他指出，傳統開源僅開放代碼，背後是單個程序員的智力投入；而大模型開放權重，背後支撐的是巨額算力與電力資源，是中國對全球AI生態的重大貢獻。

王堅認為，人工智能不應簡單稱作「大模型」，更準確的概念應該是基礎模型（foundation model）。「在我看來，中國在基礎模型層面做得還遠遠不夠，人工智能的潛力遠沒有被充分發揮。」王堅坦言，目前的模型多局限於文本領域，而實體經濟中大量的視頻、圖像及工業數據尚未被充分利用。這恰恰是「十五五」期間中國AI發展的巨大空間所在。

建人工智能安全體系「以AI對抗AI」

業界觀點

全國兩會期間，AI智能體安全治理成為熱議話題。全國政協委員、360集團創始人周鴻禕表示，AI在提升網絡防禦能力的同時，也大幅降低了網絡攻擊門檻。過去依賴人工完成的漏洞挖掘和滲透測試，如今可由安全智能體不間斷執行，效率遠超人類團隊。但西方部分國家已開始訓練「黑客智能體」，這類智能體能不知疲倦地嘗試各類攻擊方法，甚至臨時編寫黑客工具，單純依靠人力防禦已完全無法應對，凸顯了「以AI對抗AI」的必要性。

為此，周鴻禕提出構建AI時代全新安全體系的三大舉措：一是通過安全智能體將防線前移，提前挖掘修復漏洞，從源頭上降低被攻擊的概率；二是建立智能體的反思與監督機制，解決AI本身的安全問題，比如針對智能體的幻覺、惡意引導等問題，通過多智能體協作實現糾錯；三是關注數字貨幣、智能體經濟等新領域的安全隱患，建立相應的安全標準和國際規則。

▲全國政協委員、360集團創始人周鴻禕。

全國人大代表、海爾集團董事局主席周雲傑指出，應從技術和國家政策兩個層面綜合發力，為人工智能建立科學的監管體系、可通過健全AI標準體系、強化技術源頭防控等方式，築牢AI發展安全防線，包括開展「監管沙盒」試點並指導成立「倫理治理聯盟」等具體舉措。