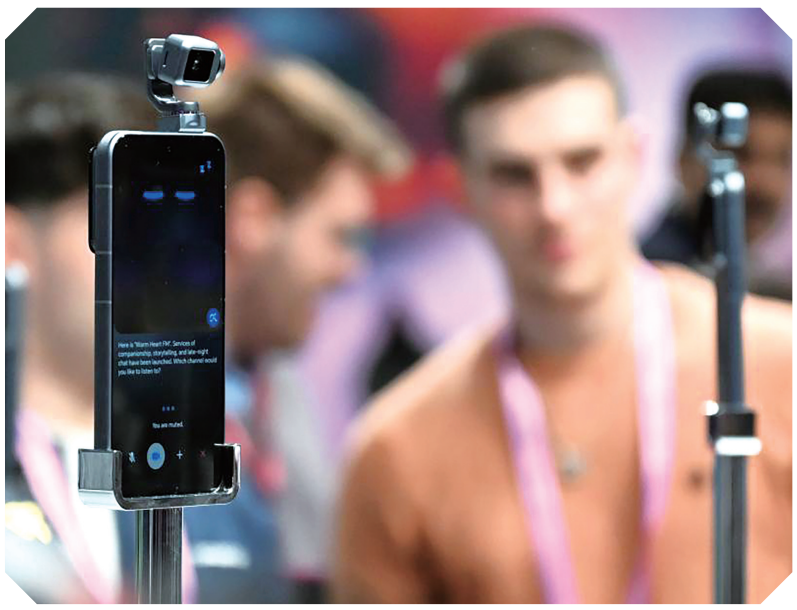
2026年3月12日 星期四 编辑 张海 版式 罗梅 校对 汪智博

# “养龙虾”，怎么就火了？

“你‘养龙虾’了吗？”

这句略显无厘头的有趣问话，说的可是最近科技圈的一件大事。

此“龙虾”并非餐桌上的美味，而是一款名为OpenClaw的开源AI智能体软件，因其图标酷似一只红色龙虾而得名。用户在设备中安装部署这款软件，被称为“养龙虾”。



人们在世界移动通信大会上参观荣耀机器人手机。

## “养龙虾”火爆出圈

“养龙虾”以超乎想象的速度火爆出圈，恰逢2026年全国两会首次将“打造智能经济新形态”写入政府工作报告，这不仅仅是时间上的巧合。

3月6日，深圳腾讯大厦门口排起长队。数百名开发者、AI爱好者聚集于此，在工程师协助下完成OpenClaw的云端部署。长长的队伍中，有老有少，大家的目光都投向了那只火热的“龙虾”。

“龙虾”的热度令人惊叹。在开源社区，这只红色小龙虾迅速蹿红，成为2026年以来的一颗耀眼新星。

相比于“对话版本”的人工智能体，“龙虾”是行动高手。它更像“数字人”，具有学习和动手能力，可直接帮人操作事务。正是因为需要自己动手安装训练，网友形象地把安装部署这款软件的过程，称为“养龙虾”。

在社交平台上，不少网友晒出自己“养龙虾”“用龙虾”的经历。从整理桌面到跨软件处理数据，效果令人惊叹。从“对话模型”到“动手操作”，AI正从“能说会道”进化为“动手干活”。

其实，“龙虾热”早有先声。

这几年，市场上出现了不少AI智能体产品。用户可以通过一键指令点外卖、买东西、订机票，不仅帮人做事情，还能与人沟通、提供建议，越来越多的AI“助手”，正在成为我们学习生活的好“帮手”。

2026年政府工作报告首次提出“打造智能经济新形态”，“促进新一代智能终端和智能体加快推广”“推动重点行业领域人工智能商业化规模化应用，培育智能原生新业态新模式”。

这说明国家的关注点，已从“AI+传统产业”的赋能模式，深化为对整体产业的布局、具体产品的落地。

## 潜在风险不容忽视

2025年8月，国务院发布《关于深入实施“人工智能+”行动的意见》，为新一代智能终端、智能体等应用普及率设定明确指标：到2027年，普及率超70%；到2030年，进一步增至90%以上。

业界对此热烈响应，国内云服务商和大模型厂商开始加速布局，相继推出相应的云服务，上线配套的配置面板，一场围绕“龙虾”的产业迅速展开。

如此“光速”跟上最前沿科技热点，再次展现“中国速度”在另一个维度上的“快”。

在强调发展智能经济的同时，政府工作报告重申了完善“人工智能治理”的重要性。

现阶段，养“龙虾”还须具备专业知识，普通用户可以尝试了解学习，但热度背后，潜在的风险也不容忽视。

“龙虾”的定位是“做事”而非“聊天”，这意味着它比过去的AI软件有更高的系统权限，因此也具有更高的安全风险，容易引发网络攻击、信息泄露等安全问题。

目前，智能体行业处在发展初期，对于新技术形态，要营造包容审慎的竞争环境和监管环境，监管部门要加强智能体相关规定的建立健全。

一方面，要完善相关法律法规，明确技术创新过程中的权利义务边界，为AI技术的研发、应用和推广提供清晰的法律指引。

另一方面，要加大执法力度，对侵犯知识产权、不正当竞争等违法行为依法惩处，维护公平有序的市场竞争环境。

从一只“龙虾”的火爆，到“智能经济”写入政府工作报告，中国的人工智能未来可期，注定有更多精彩故事即将上演！

**文图均据新华社**

# 使用『龙虾』智能体，如何确保安全？

近期，开源AI智能体“龙虾”（OpenClaw的别称）持续走热，并引发广泛讨论。其是否存在安全风险、怎样才能安全使用？对此，记者采访了中国信息通信研究院副院长魏亮。

魏亮说，作为本地运行的AI代理，“龙虾”智能体具有自主决策、调用系统资源等特点，加之信任边界模糊、技能包市场目前还缺乏严格审核，存在不少风险隐患。比如在调用大语言模型时可能误解用户指令内容，导致执行删除等有害操作；使用被植入恶意代码的技能包，可能导致数据泄露或系统受控等。

更新到最新版本，是否就没有安全风险了？在魏亮看来，更新到官方最新版本，确实能修复已知的安全漏洞，但并不意味着完全消除安全风险。“网络安全是动态的，黑客攻击手法也在不断迭代，不能把‘打补丁’和‘升版本’当成一劳永逸的安全保障。”

**使用“龙虾”智能体需要注意哪些？**

魏亮认为，必须坚持“最小权限、主动防御、持续审计”的原则。具体而言，建议从以下几方面来安全使用“龙虾”智能体。

**——使用官方最新版本。**在部署时，要优先从官方渠道下载最新稳定版，并开启自动更新提醒。在升级前备份数据，升级后重启服务并验证补丁是否生效。

**——严格控制互联网暴露面。**不要将“龙虾”智能体实例暴露到公网，确需互联网访问的，限制访问源地址，使用强密码或证书、硬件密钥等认证方式。同时，定期自查是否存在互联网暴露情况。

**——坚持最小权限原则。**在部署时，严禁使用管理员权限的账号，只授予完成任务必需的最小权限，建议在容器或虚拟机中隔离运行，以形成独立的权限区域。

**——谨慎使用技能市场。**ClawHub是专为“龙虾”智能体用户提供技能包的社区平台，其中的技能包存在恶意投毒风险，建议审慎下载，并在安装前审查技能包代码。

**——防范社会工程学攻击和浏览器劫持。**不要随意浏览来历不明的网站，避免点击陌生的网页链接。遇到可疑行为立即断开网关并重置密码。

**——建立长效防护机制。**启用详细日志审计功能，定期检查并修补漏洞。要定期关注工业和信息化部网络安全威胁和漏洞信息共享平台等漏洞库的风险预警。

**据新华社**