“小龙虾”易得 “大龙虾”难训

最近，你养 “龙虾”了吗？

这“龙虾”并非餐桌上的美味，而是最近爆火的一个名为OpenClaw的开源AI智能体（AI Agent）软件。因其图标是只“龙虾”，网友们干脆给它起了这个亲切的绰号，并将训练OpenClaw称为“养龙虾”。

OpenClaw是2025年底发布开源AI智能体软件，由程序员彼得·斯坦伯格开发，其Slogan是 “The AI that actually does things”——真正能干活的AI。

与其他AI有何不同？

与传统的聊天式AI不同，AI智能体的核心能力在于“行动”。“如果说大语言模型是AI的大脑，AI智能体就是给这个大脑装上了‘手脚’，只要发号施令，AI可以自己干活，自己执行。”浙江大学计算机学院博士生、无界AI联合创始人马千里说。

他将AI智能体的发展类比为汽车的演进：起初只是各种零件的堆砌，但当有人将这些部件组装成完整的汽车，便实现了功能的整合。以OpenClaw为代表的AI智能体，就像是当前AI功能的一次集成，随着技术发展，其能力将不断增强。

这意味着，AI正从“对话生成”转向“自主行动”。Deepseek等大语言模型擅长回答问题或生成内容，而未来的AI智能体将更像“数字人”，能够主动执行复杂的多步骤任务。

目前，如果OpenClaw被授予高权限时，它能够直接操控本地电脑，读写文件、控制浏览器、调用邮箱等，仿佛真有了可以执行指令的“爪子”。

早在OpenClaw，市面上就有相应的AI智能体产品出现。例如阿里的千问，用户发出指令就可以点奶茶，实现一句话点外卖、买东西、订机票等AI购物功能；OpenAI的Operator，无论是订餐、买票、网上购物还是预约清洁工，只需下达一句指令，Operator都能在后台自动完成。

不同的是，OpenClaw是开源的智能体软件，用户可以免费获取，并安装在自己的电脑上。而且，它还能让用户在日常聊天中，跟AI不断沟通，积累记忆，定义人格，逐渐成为一个了解用户的“助手”。也正是因为需要自己动手安装训练，网友形象地称之为“养龙虾”。

“龙虾”都能干什么？

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，还有人在电商平台上卖起了上门安装“龙虾”的服务，价格从200元到800元不等。

记者从多位提供上门安装服务的商家处了解到，通常“上门”的服务包含：OpenClaw安装+模型调试+上手培训，整个过程操作下来在2小时以上。

然而，对于大多数普通用户而言，目前这只“龙虾”远非即安即用的生产力工具。网友小九告诉记者，他跟着网上的教程，尝试在钉钉内部署OpenClaw，却感觉其能力极其有限。

为了解这只“龙虾”的“真实水平”，记者在小九的帮助下进行了一场实测。

当记者发出“想要Word文档”的指令时，“龙虾”并无法生成。而当小九下达“给自己添加发送文档的skill”等进阶指令后，它才能顺利完成任务。“如果使用者不懂命令行，很难顺利养好‘龙虾’。”小九说。

马千里指出，目前市面上很多云厂商提供的都是“阉割版”的OpenClaw，将一些功能屏蔽，以降低小白用户的使用门槛，但同时“很多潜能都释放不出来”。

“此外，由于硬件条件和用户技术水平的不同，每个人‘领养’的‘龙虾’也千差万别，体验感也就不同。”马千里解释道，“底层驱动的大模型、运行的硬件载体、用户的个性化设置等，都影响了它是‘小龙虾’，还是成为功能强大的‘大龙虾’。”

也就是说，要养出一只功能强大的“龙虾”，用户需要具备相当的技术知识，甚至要参与到对其记忆、图像识别等功能的持续“调教”和升级中。

“龙虾”真能当员工吗？

不少人养“龙虾”，是想让它替自己干活，甚至成为专属“数字员工”。这个愿望离实现还有多远？

马千里透露，“龙虾”确实已经开始为一些人“打工赚钱”。他举例道，有人利用OpenClaw包装产品、撰写营销邮件，并精准发送给潜在客户，最终成功售出产品获得盈利。“过去这些都需要专业外贸业务员来做，现在一部分工作可以被替代了。”

不过，目前类似的案例并不多。马千里表示，养“龙虾”还需具备专业知识，普通用户可以借此机会尝试了解学习。

但热度背后，风险也不容忽视。OpenClaw的定位是“做事”而非“聊天”，这意味着它必须获得较高系统权限，才能操控本地文件和应用。

此前，工业和信息化部网络安全威胁和漏洞信息共享平台（NVDB）发布《关于防范OpenClaw开源AI智能体安全风险的预警提示》，明确指出平台监测到OpenClaw部分实例在默认或不当配置情况下存在较高安全风险，极易引发网络攻击、信息泄露等安全问题。

“如果用户为了方便AI执行任务，把银行账户、加密货币钱包、API等信息以明文存在本地，一旦被黑客入侵，瞬间就会被洗劫一空。”马千里提醒道。

他的应对之策是严格物理隔离：用一台独立的电脑专门运行OpenClaw，绝不与存有个人敏感信息的主力机混用。“它能操控你的电脑，看到你所有的东西，所以最好还是用一台独立的电脑。”

面对这股“龙虾热”，马千里建议，普通用户既要看到以OpenClaw为代表AI智能体技术趋势，也要清醒认识到，其当前阶段面临着一些信息网络安全等挑战。“我们可以拥抱新技术，去尝试和学习，但不要把它神话，它还有很多不足。”

综合 极光新闻、上观新闻、钱江晚报等

“养龙虾”的第一批“受害者”出现了

有人专门花钱卸载

随着“养龙虾”风潮扩散，多家企业官宣“龙虾”模型，还有部分地区已将其应用到政务服务场景中。

然而，“养龙虾”也存在不少风险和隐患。

3月11日，相关话题#第一批养虾人已经开始卸载了#登上热搜，引发网友热议。有网友反馈，“养龙虾”过程中，出现了乱删邮件、隐私泄露等问题。

据封面新闻，有网友在网络上分享自己使用OpenClaw的经历：他将自己的工作邮箱交给了OpenClaw打理，指令是：“检查收件箱，提出你想归档或删除的邮件。”他特意附加了“未经许可不要有任何操作”的限制。然而，“龙虾”无视该网友连续发出的“停下来”的指令，疯狂地删除了数百封邮件。

据新消费日报，深圳一名程序员分享在安装OpenClaw的第三天，因API密钥被盗，在凌晨收到了高达1.2万元的Token账单。由于OpenClaw具有极高的自动化权限，一旦密钥泄露，AI便可能在后台疯狂调用模型，让用户在不知不觉中背负巨额消费。

“养龙虾”带来的隐私与安全风险，正持续引发网友担忧。

据媒体报道，OpenClaw爆火后，也带火了二手交易平台的 “龙虾上门安装服务”。然而，近日，上门卸载又迅速成为新的热门业务。

任何网络产品的安全使用，除了及时进行升级更新外，还必须坚持“最小权限、主动防御、持续审计”的原则。专家建议，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。切勿使用第三方镜像或旧版。

●严格控制互联网暴露面。一定不要将“龙虾”智能体实例暴露到公网，并且限制访问源地址，使用强密码或证书、硬件密钥等认证方式。

●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，对删除文件、发送数据、修改系统配置等重要操作进行二次确认或人工审批。

●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，拒绝任何要求“下载zip”“执行shell脚本”或“输入密码”的技能包。

●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。建议使用网页过滤器等扩展阻止可疑脚本，启用OpenClaw速率限制和日志审计功能，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，党政机关、企事业单位和个人用户可以结合网络安全防护工具、主流杀毒软件进行实时防护。要定期关注OpenClaw官方安全公告、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，及时处置可能存在的安全风险。

用户在使用“龙虾”等AI智能体的过程中，一定要详细了解并落实安全配置规范要求，养成安全使用习惯。

综合 央视新闻、人民日报