花500元安装的“龙虾”，有人已经花199元卸载了

全网刷屏的“龙虾” 劝你不要盲目跟风

近日，“本地部署”“AI员工”“龙虾”等词频频刷屏。深圳腾讯大厦门口千人排队“领养”的场面令人震撼，社交平台上相关话题热得发烫，500元一次的上门部署服务供不应求。最近爆火的“龙虾”到底是什么？在如今AI浪潮下，我们要怎么做？

“龙虾”到底是个啥？

“龙虾”其实是一款叫OpenClaw的开源AI智能体，因为图标像龙虾，所以被网友称为“龙虾”，部署并调试使用它的过程，就被称为“养虾”。“龙虾”OpenClaw，说白了就是个“能干活的小帮手”。你可以把它想象成一个住在你电脑里的不知疲倦的员工，而不是只会聊天的“嘴炮”。

目前市面上比较流行的AI工具，比如豆包、ChatGPT，你问啥它都能说，但光说不做——你让它整理邮件，它只能告诉你步骤；你让它订机票，它只能给你建议，没法真的动手操作。但OpenClaw不一样，它有“手”有“脚”，能直接在你电脑上动手干活。更像养小龙虾一样，给它“喂”点积分、教它点规矩，它就会越来越听话。平时它能帮你整理乱糟糟的文件、自动回复邮件、查天气、订外卖，甚至做表格、写报告，把几小时的活缩到十几分钟。

另外，OpenClaw分两种：一种是“本地版”，就像把小龙虾养在自己家厨房，所有数据都在自己电脑里，安全放心，但得自己折腾电脑、装软件；另一种是腾讯、阿里等大厂推出的“云端版”，就像大厂开了个“小龙虾托管站”，帮你把小龙虾养好，你不用操心，点一下就能用，电脑关机也能让它24小时干活，就是数据存在大厂的服务器上，适合做不私密的活儿。比如你想让“龙虾”半夜帮你抢火车票，本地版得开着电脑一整夜；云端版不用开自己电脑，大厂的服务器会帮你盯着，抢到了还会给你发消息。有人问，用它是不是要花钱？OpenClaw运行主要花的是积分，而积分的获取方式有很多种，新用户注册、反馈问题、用免费模型，都能领免费积分，能够普通用户日常用。但如果想让它干重活、变聪明，就需要花钱买积分。比如，花钱的高级模型（比如GPT-5、Claude）能帮你做报表、写论文，这种“聪明脑子”才需要花钱。

刚装上“龙虾”就接到反诈中心电话“养虾”6小时花掉上千元“龙虾”会这么火，令人始料未及。毕竟，有专业人士表示，目前它存在“三高”问题：边际成本高、安全风险高、安装门槛高。虽然是免费开源软件，但别说用了，光是部署到本地的流程，一连串的专业术语，足以把非专业人士绕晕，难怪“付费安装”有市场。

热闹归热闹，但跟风有风险，“养虾”需谨慎。

Meta超级智能实验室AI对齐与安全总监Summer Yue，近日遭遇OpenClaw失控事件，个人邮箱中200多封邮件被删除；

有人称，在网店购买了OpenClaw远程安装服务，刚装上5分钟后，就接到反诈中心电话，吓出了一身冷汗；

就连想做本地版“龙虾”的周鸿祎都表示，AI幻觉可能导致一系列数据安全问题，可能会将用户C盘文件全删了。

跳过“风险”不谈，“龙虾”也并非部分营销号渲染的“免费AI打工人”。

让“龙虾”做任务，无论是邮件撰写、网页浏览还是代码生成，都要消耗大量的token，都是要钱的。有媒体报道称，月薪2万元的用户感叹“养不起龙虾”，也有人晒出了6小时花掉1172元的“天价账单”。

花钱卸载“龙虾”199元起

OpenClaw潜在的安全风险及使用过程中可能产生的高额费用问题引发争议，不少安装“龙虾”的人都称，打算卸载OpenClaw，网上也出现不少OpenClaw卸载教程。

3月10日，某交易平台上已出现代卸载OpenClaw的服务。一名IP地址显示在上海的商家报价，上门卸载OpenClaw收费299元（仅限在上海），远程卸载OpenClaw收费199元，并称“安全彻底，无残留”。

工信部专家：审慎使用“龙虾”等智能体

面对“龙虾”走红，近期，国家互联网应急中心发布关于OpenClaw安全应用的风险提示：

近期，OpenClaw（“小龙虾”，曾用名Clawdbot、Moltbot）应用下载与使用情况火爆，国内主流云平台均提供了一键部署服务。此款智能体软件依据自然语言指令直接操控计算机完成相关操作。为实现“自主执行任务”的能力，该应用被授予了较高的系统权限，包括访问本地文件系统、读取环境变量、调用外部服务应用程序编程接口（API）以及安装扩展功能等。然而，由于其默认的安全配置极为脆弱，攻击者一旦发现突破口，便能轻易获取系统的完全控制权。

前期，由于OpenClaw智能体的不当安装和使用，已经出现了一些严重的安全风险：

1.“提示词注入”风险。网络攻击者通过在网页中构造隐藏的恶意指令，诱导OpenClaw读取该网页，就可能导致其被诱导将用户系统密钥泄露。

2.“误操作”风险。由于错误地理解用户操作指令和意图，OpenClaw可能会将电子邮件、核心生产数据等重要信息彻底删除。

3.功能插件（skills）投毒风险。多个适用于OpenClaw的功能插件已被确认为恶意插件或存在潜在的安全风险，安装后可执行窃取密钥、部署木马后门软件等恶意操作，使得设备沦为“肉鸡”。

4.安全漏洞风险。目前为止，OpenClaw已经公开曝出多个高中危漏洞，一旦这些漏洞被网络攻击者恶意利用，则可能导致系统被控、隐私信息和敏感数据泄露的严重后果。对于个人用户，可导致隐私数据（像照片、文档、聊天记录）、支付账户、API密钥等敏感信息遭窃取。对于金融、能源等关键行业，可导致核心业务数据、商业机密和代码仓库泄露，甚至会使整个业务系统陷入瘫痪，造成难以估量的损失。

建议相关单位和个人用户在部署和应用OpenClaw时，采取以下安全措施：

1.强化网络控制，不将OpenClaw默认管理端口直接暴露在公网上，通过身份认证、访问控制等安全控制措施对访问服务进行安全管理。对运行环境进行严格隔离，使用容器等技术限制OpenClaw权限过高问题；

2.加强凭证管理，避免在环境变量中明文存储密钥；建立完整的操作日志审计机制；

3.严格管理插件来源，禁用自动更新功能，仅从可信渠道安装经过签名验证的扩展程序。

4.持续关注补丁和安全更新，及时进行版本更新和安装安全补丁。

目前，“龙虾”智能体通过更新到官方最新版本，确实能修复已知安全漏洞，但并不意味着完全消除安全风险。因为将实例暴露于互联网、使用管理员权限、明文存储密钥等配置问题，即使升级到最新版本，如果不采取针对性的防范措施，依然存在被攻击风险。

专家呼吁，党政机关、企事业单位和个人用户要审慎使用“龙虾”等智能体。在发现“龙虾”等智能体的安全漏洞，或者针对“龙虾”等智能体的安全威胁和攻击事件时，可以第一时间向工业和信息化部网络安全威胁和漏洞信息共享平台报送，平台将按照《网络产品安全漏洞管理规定》要求，及时组织处置。

好“虾”不怕晚，等等也无妨

从目前的用户反馈来看，使用“龙虾”体验较好的，大多是程序员、AI从业者、企业管理者或数据、市场分析相关工作者。总结来说，就是日常需要做大量跨软件、跨平台，收集分析信息，高度重复的数字化“搬砖”工作的人。

而大多数普通人，连安装流程都整不明白，花钱准备硬件，装完“龙虾”，赶完时髦，在网上感叹几句，很快就会放在电脑里“落灰”，属实白花钱还浪费时间。

其实，很多人急匆匆地想要“养虾”，说白了就是被AI焦虑给一把“钳”住了。总觉得科技发展如此迅猛，自己要是不跟上，分分钟就被淘汰了。于是，还没来得及学会用“龙虾”创收，就已经为了“养虾”掏钱了。

其实，人在焦虑的时候，很容易做出错误的决定，不管是多么先进的AI工具，其意义就是让人更轻松，更自由，更强大，如果说还没享受到“龙虾”的红利，就已经因为它急得连觉都睡不着，那不是本末倒置，得不偿失吗？

潮流越汹涌，普通人越要保持定力，清醒判断，“养虾”之前，不妨先问问自己：会安装吗？懂调试吗？用得上吗？三思而后行，才能避免成为“韭菜”和“冤种”。

中国工程院院士王坚也说了，OpenClaw会很快便宜下来并普及，所以，好“虾”不怕晚，等等也无妨。

据央视网