扫码关注河北法治报微信微博

燕赵都市报

河北日报报业集团主管主办 燕赵都市报编辑部出版 国内统一连续出版物号 CN 13-0069 邮发代号 17-92 新闻热线 0311-89920077

2026年
3月18日 星期三
农历丙午年正月三十
今日16版
总第[10144]期

“龙虾”安全养殖手册，请收好！

OpenClaw（昵称“龙虾”）是一款开源AI智能体工具，上线不久便迅速成长为2026年度现象级“开源奇迹”。不少用户从付费安装“龙虾”，到付费卸载“龙虾”，养“龙虾”正在成为一场智能体的狂欢。但火热的“龙虾”在创新改变生活的同时，也存在原生风险。在此特别提示，广大用户要理性辨别、规范使用，以积极的心态和慎重的执行拥抱人工智能时代，让“龙虾”成为遵规守纪、产能高效的“数字员工”。

了解养『龙虾』的风险隐患

——主机可能被接管。为实现“做事”能力，用户常赋予其最高系统权限，可能引发因AI误操作造成的数据损失。更严重的是，运行后可能被攻击者神不知鬼不觉获取设备管理权限，从而引发主机被远程操控，资源被非法占用等安全风险。

——数据可能被窃取。部分用户缺乏数据安全意识，个人敏感数据交由“龙虾”处理，一旦被攻破，可能造成个人隐私泄露，带来财产与安全风险。

——言论可能被篡改。“龙虾”智能体可在社交网络自主发声，一旦被攻击者接管，可能被用于生成和传播虚假信息、实施诈骗等不法活动。

——技术可能有漏洞。“龙虾”缺乏专业维护与漏洞修复机制，攻击者可能通过恶意插件投毒等方式，诱导智能体突破权限管控，主动窃取本地设备的核心敏感信息，其隐蔽性远超传统木马程序。

『养虾人』必看安全指南

——给自己的“龙虾”全面体检。检查控制界面是否暴露在公网、权限配置是否过高、存储的凭证是否已泄露、安装的插件来源是否可信等问题。对于严重安全风险，请立即采取隔离、下线等处置措施。

——为自己的“龙虾”做好防护。必须遵循最小权限原则，严格限制智能体的操作范围。对存储的敏感数据必须进行加密，建立完整的操作审计日志，尽量在隔离环境（如专用虚拟机、沙箱）中运行“龙虾”，限制其对核心资源的访问。

——让自己的“龙虾”老实好用。“龙虾”并非供人娱乐的数字宠物，而是能够自主执行任务、承担流程操作、持续学习成长的“数字员工”，养“虾”人应理性看待、规范使用，让其在合规、安全、可控的前提下成为提升治理效能，服务生产生活的数字化生产工具。

（据人民日报）

印刷：河北报业传媒集团印务有限公司 地址：石家庄市栾城区装备制造产业园区南车路23号 本版编辑 李胜男 美术编辑 秦浩淼