OpenClaw爆红背后存高风险，工信部紧急发布安全预警

跟风“养龙虾”：“六要六不要”

全网掀起“养龙虾”热潮，与之相对的是，监管部门已多次发布安全提醒。3月11日晚，工业和信息化部网络安全威胁和漏洞信息共享平台发布关于防范OpenClaw（“龙虾”）开源智能体安全风险的“六要六不要”建议。工信部建议，使用官方最新版本，严格控制互联网暴露面，坚持最小权限原则，谨慎使用技能市场，防范社会工程学攻击和浏览器劫持，建立长效防护机制。

近期，开源AI智能体“龙虾”持续走热，引发广泛讨论。　新华社发

工信部晚间发布风险防范建议

3月11日晚，针对OpenClaw（“龙虾”）开源智能体，工信部明确四大典型应用场景安全风险：智能办公场景主要存在供应链攻击和企业内网渗透的突出风险，开发运维场景主要存在系统设备敏感信息泄露和被劫持控制的突出风险，个人助手场景主要存在个人信息被窃和敏感信息泄露的突出风险，金融交易场景主要存在引发错误交易甚至账户被接管的突出风险。

针对“龙虾”典型应用场景下的安全风险，工业和信息化部网络安全威胁和漏洞信息共享平台（NVDB）组织智能体提供商、漏洞收集平台运营单位、网络安全企业等，研究提出“六要六不要”建议。

其中，工信部建议，首先要使用官方最新版本。要从官方渠道下载最新稳定版本，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。不要使用第三方镜像版本或历史版本。

其次，要严格控制互联网暴露面。要定期自查是否存在互联网暴露情况，一旦发现立即下线整改。不要将“龙虾”智能体实例暴露到互联网，确需互联网访问的可以使用SSH等加密通道，并限制访问源地址，使用强密码或证书、硬件密钥等认证方式。

同时，要坚持最小权限原则。要根据业务需要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。优先考虑在容器或虚拟机中隔离运行，形成独立的权限区域。不要在部署时使用管理员权限账号。

此外，要谨慎使用技能市场。要审慎下载ClawHub“技能包”，并在安装前审查技能包代码。不要使用要求“下载ZIP”“执行shell脚本”或“输入密码”的技能包。

另外，要防范社会工程学攻击和浏览器劫持。要使用浏览器沙箱、网页过滤器等扩展阻止可疑脚本，启用日志审计功能，遇到可疑行为立即断开网关并重置密码。不要浏览来历不明的网站、点击陌生的网页链接、读取不可信文档。

最后，要建立长效防护机制。要定期检查并修补漏洞，及时关注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。对于党政机关、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，及时处置可能存在的安全风险。需要注意的是，不要禁用详细日志审计功能。

目前已确认四类核心风险

不仅工信部发文提示，日前国家互联网应急中心发布的《关于OpenClaw安全应用的风险提示》指出，近期，AI智能体应用OpenClaw（曾用名Clawdbot、Moltbot）因支持自然语言操控计算机而受到广泛关注，并获国内主流云平台一键部署支持。然而，由于该软件运行需要包括访问本地文件系统、调用外部API等较高系统权限，加之其默认安全配置薄弱，目前已被曝出存在严重安全隐患，攻击者利用这些缺陷可轻易获取系统完全控制权。

针对OpenClaw的不当部署与使用，目前已确认四类核心风险。首先是提示词注入风险，攻击者可通过网页暗藏恶意指令，诱导软件泄露用户系统密钥；其次为误操作风险，软件在错误解析用户意图时，可能直接彻底删除电子邮件及核心生产数据；第三是插件投毒风险，目前已发现多个适用于该应用的恶意扩展程序，安装后可执行窃取凭证或部署木马后门等操作，导致设备沦为“肉鸡”；最后是严重的安全漏洞风险，该应用已被公开披露多个高中危漏洞，直接威胁个人用户的支付账户、隐私文档等敏感信息，甚至可能导致金融、能源等关键行业发生代码仓库泄露或业务系统瘫痪。

鉴于潜在的严重损失，安全专家建议相关部署单位与个人采取严格的安全防护策略。在网络配置层面，必须避免将默认管理端口直接暴露于公网，同时利用容器技术隔离运行环境以限制其过高的权限。在凭证管理方面，严禁在环境变量中明文存储密钥，并需建立完整的操作日志审计机制。

此外，用户应严格审核插件来源，禁用自动更新功能，仅安装经签名验证的扩展程序，并持续关注官方通报及时部署安全补丁与版本更新。

综合新华社、北京商报等

提升消费品质　安利深耕大健康护航美好生活

消费是民生改善的重要内容，也是经济增长的持久动力。

“十五五”规划开局之年，“3·15国际消费者权益日”来临之际，中国消费者协会将2026年度主题确定为“提升消费品质”，倡导以优质供给、高效维权、优化环境，助力消费从“数量型”向“质量型”转变，满足人民群众日益增长的高品质生活需求。

作为大健康行业领军企业，安利不断加大对中国、这一全球最大战略市场的投入，升级产业链、创新链，以消费者需求为导向，持续推出科学完善的健康解决方案，精心打造线下美好生活能量场，优化售后服务体系、升级消费体验，用诚信与责任守护消费者权益，以实际行动践行企业担当，为消费品质提升注入持久动能。


安利上海体验馆社群活动。

深耕植物抗衰　以科技创新提升消费品质

去年4月，商务部、国家卫健委等12部门印发《促进健康消费专项行动方案》，政策红利加速释放，健康消费站上风口。

截至2025年末，我国60岁及以上人口已达3.23亿，占全国人口的23.0%，其中65岁及以上人口2.24亿，占比达15.9%。随着人口老龄化进程加深，提升健康预期寿命、科学抗衰已成为消费者刚需。

服务国家战略，立足市场需求，近年来，安利加大植物抗衰赛道的科研工作，聚焦人体的细胞、脑力、行动力等推出一系列抗衰产品，助力消费者拥有优质健康状态，享受高品质生活：

细胞类抗衰产品：改善细胞衰老、线粒体受损，核心原料为铁皮石斛、野樱莓、槐花、石榴、余甘子提取物；

行动力抗衰产品：提升骨密度，核心原料为淫羊藿、骨碎补、丹参提取物；

脑力抗衰产品：强健神经元细胞，核心原料为肉苁蓉、银杏叶提取物；

皮肤抗衰产品：内调外养改善肌肤，核心原料为狭叶松果菊、积雪草、迷迭香叶提取物；

此外，安利还连续推出改善“三高”问题的“代谢健康产品”、关注膳食均衡的“营养早餐产品”，以及“体重管理”“心血管健康”等产品，覆盖基础营养和功能性健康解决方案。

新品迭代、全面覆盖，引领并满足健康消费新需求，离不开硬核科技能力支撑。安利与中国航天、高校、科研机构、科技企业等深入合作，进行航天育种、植物新原料培育、有机种植和智慧农业探索，推动中草药种植标准化、现代化。

安利融合AI与算法技术开发的“神农系统”，整合超过7万条传统中药方剂数据、2万多种中草药植物原料数据、6万多种植物营养素成分数据，以及超过100万条靶向疾病关联数据，将传统中医药智慧与现代生物医学熔为一炉，提升产品开发效率。

焕新线下体验设施　打造美好生活能量场

提升消费品质，离不开优质的产品供给，更离不开多元贴心的消费体验。去年以来，安利持续升级全国100多家线下实体，以全新场景为消费者打造集体验、交流、服务于一体的多元空间，让健康生活理念可触可感。

以重装焕新的上海及广州旗舰体验馆为例，应健康消费、绿色消费、情绪消费、品质消费等消费新趋势，融入更多时尚设计、科技元素和互动体验，消费者可以参与健康检测、美食制作、健身活动、人际交流，享受艺术展或小型音乐会，一站式满足高品质健康生活消费需求。

安利遍布全国的体验馆/体验店，已成为传递美好生活理念的能量场，及安利“投资于人”企业理念的重要落地载体。依托线下体验馆与线上数字化工具，安利支持20多万营销人员运营数十万个大健康和美好生活社群，定期组织健康科普、营养讲座、社群互动等各类活动。营销人员化身健康服务者，帮助消费者培养均衡膳食、适度运动、积极社交的健康生活习惯，实现从“产品消费”到“生活方式改变”的升级，构建一个以“健康、美丽、品质生活”为核心的生态圈，带动千百万人享有健康和美好的生活。

优化全链条服务　坚守正品保障底线

优质产品与体验，是消费品质的基础；完善服务与正品保障，则是核心防线。安利始终将消费者权益放在首位，不断优化服务体系，落实质量和服务保障，让消费者买得放心、用得安心。

线上，“安利云购”平台持续迭代升级，打造便捷、高效、安全的线上购物渠道，实现产品一键下单、物流快速配送，让消费者足不出户就能轻松选购心仪产品，享受便捷的购物体验；线下，依托全国线下体验馆与专业营销人员，为消费者提供一对一咨询、产品体验、健康指导等个性化服务，精准满足不同消费者的健康需求。

在售后服务方面，安利在践行“7天无理由退货”基础上，推出30天无忧退货保障机制，即便部分已开封使用的产品，在使用未过半的情况下也可办理退货并获得等值补偿，真诚守护消费者权益。同时，为杜绝假冒伪劣产品侵害消费者利益，安利自2010年起发起“正品源于正道”专项行动，十余年间持续配合执法部门开展打假行动，捣毁制假窝点，用实际行动筑牢正品防线。

“3·15”不仅是消费者权益的守护者，更是企业践行责任、提升品质的风向标。安利正以“提升消费品质”为指引，锚定“健康中国”建设目标，深耕大健康赛道，以优质产品和服务守护消费信任，共筑美好生活。

编辑：彭传刚　美编：马秀霞　组版：刘淼