AI 安全负责人 Summer Yue，居然被自己测试的“龙虾”坑了。她让“龙虾”帮忙整理邮箱，明确说“只给建议，确认了再动手”，测试时好好的，一接入工作邮箱，“龙虾” 突然疯了，几分钟删了 200 多封邮件！

更离谱的是，她用手机发“住手”指令，AI 根本不听，最后她一路狂奔回电脑，手动关掉程序才止损。事后查原因，居然是邮箱邮件太多，上下文压缩了要确认的指令，“龙虾”只记得“删邮件”。

类似翻车还有很多：有工程师让“龙虾”管短信，结果 AI 给通讯录所有人发了 500 多条垃圾信息；有公司用“龙虾”处理财务，结果插件藏病毒，商业机密全泄露了。近期，工信部网络安全威胁和漏洞信息共享平台（NVDB）、国家互联网应急中心（CNCERT）纷纷发布相关安全风险提示。

工信部专家指出，OpenClaw 智能体虽能提升工作效率，但其默认的高系统权限与弱安全配置，极易被攻击者利用，成为窃取敏感数据或非法操控交易的突破口，给行业带来严峻的风险挑战。所有的专家和“龙虾”使用者，都一再提醒大众，安全是一切的前提。安全的服务器（电脑）、安全的模型、安全的学习环境（防止“龙虾”被其他“龙虾”带坏）缺一不可……

尽管安全警报不断拉响，从普通民众到各行各业还是前赴后继地开始养“龙虾”业务。

3 月 6 日，深圳腾讯大厦北广场，近千人排起长队装“龙虾”。腾讯云的工程师免费提供一站式服务，几个小时装了五百多台。队伍里有小学生，有退休老人，来自全国各地。

阿里云、火山引擎、百度智能云、阶跃星辰也都跟着上线了一键部署服务。阿里巴巴甚至正式成立 Alibaba Token Hub（ATH）事业群，建立以“创造 Token、输送 Token、应用 Token”为核心目标的新组织。大厂们把开源能力封装成标准化服务，赚算力和 Token 调用的钱。在刚刚结束的中国家电及消费电子博览会上，《新民周刊》记者看到众多厂商纷纷将旗下的智能产品接入 OpenClaw，让“龙虾”不仅会工作，更懂得生活。百度集团副总裁、小度科技 CEO 李莹说，小度智能家居 Skill 已经登陆 ClawHub，让用户开口就能指挥 AI 家庭管家，执行打扫、看护、陪伴、养老等一系列任务，让 AI Agent（智能体）在真实场景里创造出更多新价值。

一代人有一代人的鸡蛋要领，这一代人的鸡蛋大概就是一只正在变得无所不能的“龙虾”。说白了，养“龙虾”不是跟风，而是真的想清楚自己要干嘛。想清楚了，任何工具都能用出花来。没想清楚，再好的工具也是玩具。

你，做好准备养“龙虾”了吗？