南宁学院信息化处文件

网字〔2026〕6号

关于加强防范“龙虾”（OpenClaw）AI智能体安全风险的通知

全校师生：

近期，开源AI智能体工具OpenClaw（俗称“龙虾”）因其强大的自动化能力而得到广泛关注。根据国家工业和信息化部、国家互联网应急中心（CNCERT）等权威机构发布的风险预警，该工具在默认配置下存在显著安全隐患，极易引发网络攻击、数据泄露及系统被恶意控制等安全风险。

为切实筑牢校园网络安全防线，保障师生个人信息及教学科研数据安全，现就规范使用OpenClaw工具的有关事项提示如下：

一、认清核心风险，保持高度警惕

OpenClaw作为一种高权限AI智能体框架，其设计初衷是“自主执行任务”，但这也是安全威胁的主要来源，其默认设置安全级别较低，仅在设备内采用单次身份认证即获永

久授权，导致实例暴露在网络时，极易被黑客远程接管：

（一）权限过大且易失控。该工具需获取文件系统读写、命令执行等高系统权限。若遭恶意利用或出现“AI 幻觉”，可导致核心数据被窃、系统瘫痪甚至被远程提权。

（二）供应链投毒隐患。其官方技能市场（ClawHub）缺乏严格审核，目前已发现大量植入恶意代码的技能包，具备自动窃取用户凭证的安全隐患。

（三）高危漏洞频发。目前已公开披露多个超危及高危漏洞，攻击者可利用这些漏洞轻易获取系统完全控制权。

二、相关禁止事项

为杜绝安全隐患，请全校师生在使用相关工具时注意以下事项：

（一）禁止在生产环境部署

禁止在办公电脑、服务器等生产设备及存储有教学科研数据、行政办公信息的终端上安装、运行 OpenClaw。

（二）禁止接入校园网使用

禁止在接入校园网的计算机设备上安装 openclaw，防止风险渗透扩散，破坏校园安全稳定。

（三）禁止输入敏感信息

在使用过程中，请勿向该工具输入智慧校园账号密码、个人身份信息、科研涉密数据及各类 API 密钥。

三、科研测试环境需落实的安全加固事项

科研、测试用途，需落实“最小权限、主动防御、持续审计”原则，并参照以下指引进行安全加固：

（一）运行环境需隔离。在容器（Docker）、沙箱或虚拟机等隔离环境中运行，避免赋予 Root/Administrator 超级管理员权限。

（二）暴露面需收敛。禁止将软件实例及端口直接暴露在公网。确需访问的，需严格限制访问源 IP。

（三）插件与凭证需严控：禁用自动更新功能，仅从官方渠道下载经过签名验证的插件；请勿在相关配置文件中明文存储任何密钥或密码。

（四）开启人工复核。具体操作时，须开启日志审计功能，进行人工介入和二次确认。

信息化处

2026 年 4 月 3 日