关于防范 OpenClaw 开源 AI 智能体安全风险的提醒

全校师生：

近期，开源 AI 智能体 OpenClaw（俗称“龙虾”）备受关注，但该工具目前存在多项安全隐患，使用不当会对校园网络安全、设备安全与个人信息安全造成严重风险。此前，工业和信息化部、国家互联网应急中心等部门已先后发布安全风险提示。为切实保障全校师生的个人信息安全、校园网络安全及数据资产安全，现就防范相关风险事项通知如下：

一、OpenClaw 核心风险警示

1.隐私泄露风险高：该工具需获取电脑高权限运行，聊天记录、账号密码、文件数据等敏感信息以明文存储本地，配置不当或被入侵即可能被窃取。

2.自主执行易失控：该工具存在意图误解、指令执行偏差等问题，曾出现无视限制、批量删邮件、误删重要文件等失控情况，安全审计通过率低。

3.权限管理有漏洞：该工具信任边界模糊，缺乏有效权限控制和审计机制，易被诱导或恶意接管，执行越权操作，导致系统被远程控制。

4.技术门槛与使用风险不匹配：该工具本质是属面向开发者的底层框架，需专业知识配置；普通用户非官方 “代装” 易因配置不当放大风险，还可能遭遇 “智商税”。

二、严格使用规范与管理要求

1.非必要不部署使用：全校师生应结合自身实际需求理性看待该工具，切勿因跟风心理盲目安装、部署 OpenClaw，尤其禁止在学校电脑、服务器、智能终端等各类生产环境与教学办公设备上安装。

2.严禁在工作场景使用：全体师生严禁在处理教学科研数据、行

政办公信息、学生信息等工作场景中使用该工具，杜绝校园工作数据泄露、系统受攻击等问题。

3.规范操作杜绝风险：如有技术研究部署需求，须通过官方正规渠道获取源码与教程，在容器或沙箱环境中运行，关闭不必要公网访问，完善身份认证、数据加密、安全审计等防护措施，妥善管理 API 密钥、账户凭证等信息，并持续关注官方安全公告与加固建议。

网络安全无小事。请全体师生高度重视，严格遵守通知要求，切实提升风险防范意识，坚持“不传密、不私装、不越权”，共同筑牢校园网络安全防线。联系电话：81050783。

图文信息中心

2026 年 3 月 13 日