

# “囤词元能暴富”藏间谍窃取数据陷阱

## 国安机关提醒:主动拥抱、善加运用,防范风险、确保安全

### 相关新闻

### “龙虾”(OpenClaw) 安全养殖手册

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”,“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。

#### 摸清“龙虾”的生产特点

“龙虾”智能体通过整合通信软件和大语言模型,依托高权限实现自主操作,成为其核心优势。从“给出方案”到“落地执行”,“龙虾”不像大模型智能体通过问答提供咨询建议,而是可以通过聊天程序远程执行用户指令,自主完成任务。从“固定功能”到“多种插件”,“龙虾”内置了大量技能插件,用户可直接下载使用,形成覆盖文件管理、邮件撰写、日历调度、网页浏览、定时任务等多场景的工具链。从“普通工具”到“自我进化”,“龙虾”可以长期记忆用户使用记录,持续理解用户行为偏好,“越用越懂用户”,所以大家称之为“养龙虾”。从“被动等待”到“主动服务”,“龙虾”可根据用户要求,主动感知外部情况,主动触发预警或执行动作,完成“夜间下达指令、晨间获取成果”的智能服务。

#### 了解养“龙虾”的风险隐患

主机可能被接管。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。

#### “养龙虾”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。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“龙虾”人应理性看待、规范使用。  
据国家安全部微信公众号

近期,国家数据局正式定名的AI领域核心术语——词元(Token)成为网络热词。据统计,截至今年3月,我国日均词元调用量已超过140万亿,较2024年初增长1000多倍。“词元”这个新词实际上早已融入我们生活的方方面面。面对新技术新应用,我们既要主动拥抱、善加运用,又要防范风险、确保安全。

据国家安全部



意象图片由AI生成

### 什么是词元(Token)?

简单来说,词元是AI大模型处理信息的最小单元,兼具可计量、可定价、可交易三大特征。它不仅是智能时代的价值锚点,更是连接技术供给与商业需求的“结算单位”。词元应用场景远超AI领域,与日常生活紧密相关。

身份凭证类。相当于数字世界的“临时身份证”,用于便捷登录各类平台、完成转账授权等,如微信登录第三方小程序、手机银行动态口令等,有明确有效期,兼顾便捷性与安全性。

AI场景类。即官方定名的“词元”核心应用,是使用如AI写作、修图、剪辑等AI服务的消耗性资源。

权益凭证类。可以理解成区块链场景下的“通证”,相当于数字化权益证明,如电子票、游戏皮肤、会员积分等,具有不易伪造、便于流转的特点。

### 词元热潮下的信息安全隐患

随着词元的爆火,一些不法分子开始打起了词元的主意,伺机布设各种陷阱。同时,词元本身在使用过程中也存在一定的安全风险,需要我们加以防范。

泄露劫持风险。不法分子可通过跨站脚本攻击(XSS)、公共Wi-Fi嗅探等方式,窃取、截获未加密的词元。一旦词元泄露,攻击者可直接盗用用户身份,获取隐私信息、登录账号、篡改数据,甚至实施诈骗、转账等操作,直接威胁个人财产安全。如果海量词元被汇总分析,则可能引发系统性风险,危害数据安全与国家安全。

伪造篡改风险。若词元缺乏加密或签名防护,不法分子可直接修改词元的权限字段,伪造管理员身份绕过系统验证,非法获取用户敏感隐私数据、实施越权操作。同时,不法分子还有可能制造“虚假词元”,诱导用户泄露身份证号、手机号等隐私信息。

诈骗陷阱风险。当前,各类“词元骗局”层出不穷:用低价AI词元套餐、词元投资等噱头,诱骗用户资金;冒充官方平台,以官方

升级、验证为由,骗取个人隐私信息。尤其是宣称“囤词元能暴富”“场外交易赚差价”等行为,不仅涉嫌非法金融活动,还可能被境外间谍情报机关用以开展数据窃取、资金渗透,危害国家经济安全与数据安全。

### 词元这么火,应该注意点啥?

面对词元热潮,我们既要理性看待其价值,又要注意信息安全、隐私安全,提高安全防范意识,做到了解词元、善用词元。

认清词元属性。词元可作为数字身份凭证,并非投资品,防范以“词元投资”“高收益回报”“词元理财”“词元挖矿”等为噱头的各类骗局,切勿盲目购买未经官方认证的小众、虚拟词元,不随意注册来路不明的词元服务,从源头上避免因贪利、跟风导致的个人隐私信息泄露和财产损失。

强化使用规范。使用词元相关服务时,优先选择正规平台与加密传输通道,不在公共网络、不安全环境下进行登录、转账、填写隐私信息等敏感操作;不点击陌生链接,不下载非官方App,不扫描可疑二维码,及时更新设备系统与安全防护;严格保管词元口令、授权码及绑定的手机号、身份证号等信息,开启双因素认证,不共用账号,不设置通用密码,发现账号异常立即采取改密、解绑、报备等止损措施。

遵守法律法规。面对词元等AI领域的新兴应用与概念,应保持理性认知,既不盲目追捧,也不跟风炒作,自觉遵守法律法规与监管要求,主动学习官方发布的词元安全知识,提高辨别能力;科学区分身份凭证类、AI场景词元与区块链通证、加密货币,不参与非法加密货币交易,如遭遇诈骗、信息泄露或发现非法活动,应及时向有关部门反映。

### 谨防深度伪造魔改陷阱

除了词元使用过程中存在安全风险,深度伪造魔改也有陷阱。国家安全机关也提醒用户,使用人工智能技术留个心眼。

生成式人工智能技术的突破性进展,正推动AI视频制作加速普及,在提升创作效

率、活化历史记忆等方面展现出巨大潜能,成为数字时代的内容生产利器。但技术若被恶意用于金融欺诈、政治渗透、谣言制造、间谍窃密等非法活动,将侵害公民合法权益,甚至扰乱社会秩序、危害国家安全。

伪造权威,动摇公信力。境外间谍情报机关、各种敌对势力可能利用深度伪造技术,捏造虚假言论、伪造公务人员不当视频、炮制虚假政策画面,以此制造社会恐慌、撕裂舆论、抹黑国家形象,冲击政治安全与制度安全。

精准诈骗,侵害公私财产。不法分子可能利用深度伪造克隆亲友、客服等声音面容,实施冒充转账、虚假投资、仿冒官方渠道诈骗等非法活动。更有甚者,企图通过伪造企业公告、专家言论,引发市场波动。

信息泄露,危害数据安全。不法分子可能利用深度伪造人脸、声纹等生物特征,突破身份认证、权限校验等核心数据防护机制,造成账号被盗、后台入侵、敏感数据批量泄露,甚至引发关键信息基础设施安全系统失控等重大安全事件,对数据安全造成危害。

《互联网信息服务深度合成管理规定》明确,任何组织和个人不得利用深度合成服务从事危害国家安全和利益、损害国家形象、侵害社会公共利益、扰乱经济和社会秩序、侵犯他人合法权益等活动。

国家安全机关提醒,技术本身并无善恶,关键在于如何使用。面对深伪技术,每一位公民都应自觉增强安全意识,提升辨别能力、遵守法律法规,以实际行动维护国家安全和网络清朗。

提高辨别能力。理性看待网络信息,不盲目轻信不合常理的音视频、图片内容,遇到可疑信息优先通过官方渠道核实真伪。

自觉遵守法律。合理合法使用各类AI生成、图像编辑、音视频处理工具,不参与、不支持制作、传播有害虚假信息。

维护网络文明。自觉抵制各类有害内容,不随意转发未经证实的信息,如发现AI视频平台或作品存在可能危害国家安全的问题线索,可通过电话、平台、微信公众号等方式向国家安全机关举报。

全民·爱·阅读

阅读收获正能量  
激发活力新思维

中宣部宣教局 中国文明网

分类广告 刊登热线:025-84783581、13675161757  
地址:洪武北路55号置地广场1806室

### 老年公寓

鼓楼区向阳养老院,有医疗、地铁口、环境好、价优。66776779  
养老院 1800、2000、2300、2500、2800、3000、3500元,晓街3-7号。  
电话:13770573022

### 遗失

遗失 张庆亚退役军人优待证,卡号:6216223000012865926,声明作废。  
遗失 尤俊退役军人优待证,身份证号:320105197903091411,声明作废。  
杨丹 遗失身份证,证号:230281200404283720,特此声明。

遗失 南京佰蝉传媒科技有限公司公章、法人章、财务章各一枚,声明作废,寻回后不再继续使用。  
项艺林 遗失南京林业大学学生证,证号:8241011283,声明作废。

### 公告

公告 途迹宿野文旅科技发展(江苏)有限公司经法院裁定破产,管理人为江苏斐多律师事务所,请公司的法定代表人、股东、董事、监事、财务人员配合接管。现公告公司的公章、法人章、财务章、财务优盾作废。请债权人自公告之日起45日内向管理人申报债权。