

这些活千万别交给AI干

当AI以前所未有的速度嵌入日常生活,我们乐于享受它带来的高效与便捷,却往往忽略了边界所在:蘑菇的毒性鉴别、户外线路的安全性评估关乎生命,用AI处理敏感信息容易造成泄密、个人隐私泄露。

技术工具再强大,也无法替代专业判断。



AI制图。图/湖北疾控

AI鉴菇

AI说“无毒”,男子吃完直接进ICU

近日,山上、草地里的野蘑菇又开始疯长,不少人还拍了视频上传社交媒体。有一些人让AI去鉴别野蘑菇是否有毒,但AI鉴菇真的靠谱吗?

前段时间,浙江诸暨一名男子就因为吃了经AI识别为“无毒”的蘑菇后被紧急送入ICU。

中招的男子姓王,出事前发现自家附近长出很多新鲜的野蘑菇,于是就采摘了一些。

为了安全,下锅之前,他还专门拍照让AI进行了识别,看到认证无毒后,中午就把蘑菇下锅煮了吃掉。

吃完的前几个小时还一切正常,可到了下午5点,王先生肚子开始不舒服,疯狂跑厕所,紧接着双上肢酸痛,全身像被抽空了力气。

随后,家属紧急将他送医。

五种蘑菇AI看错了两种

AI对蘑菇的识别能力究竟如何?都市快报记者找了5种野蘑菇,通过视频通话功能进行AI辅助辨认。

AI给出的判断依次为:黄白雅典娜小菇、白小鬼伞、硬柄小皮伞、大青褶伞以及大盖小皮伞。其中,部分品种明确标注含有毒性,另有部分提示与某些剧毒蘑菇相似,但均明确建议不可食用。

随后,经中国菌物学会科普工作委员会主任委员、浙江大学生命科学院食药菌研究所常务副所长林文飞鉴定,实际种类依次为黄白雅典娜小菇、硬柄小皮伞、大青褶伞、裸脚菇,其中两朵实为同一品种。

专家鉴定与AI识别结果相比,5种蘑菇存在两处差异,AI所说的白小鬼伞实为硬柄小皮伞,大盖小皮伞实为裸脚菇。

当更换不同的手机对同一种菌类进

行识别时,个别品种结果存在差别。以第2个品种为例,两台手机给出的结果分别为白小鬼伞和皱盖囊皮菇,均与专家鉴定的结果硬柄小皮伞不符。

AI识图看似便利,实则致命

我国已报道的有毒蘑菇多达600余种,所含毒素复杂,中毒症状因种类而异。根据临床表现,蘑菇中毒主要分为胃肠炎型、神经精神型、急性肝损害型、急性肾衰竭型、溶血型、横纹肌溶解型和光过敏性皮炎等七种类型。

其中,急性肝损害型死亡率最高,多由鹅膏属的剧毒种类引起。该类中毒潜伏期通常为6—12小时,部分可达20小时。患者初期出现恶心、呕吐、腹泻等胃肠道症状,随后进入1—2天的“假愈期”——症状看似缓解,实则毒素正“疯狂”攻击肝脏。假愈期过后,病情急转直下,出现黄疸、凝血功能障碍、肝衰竭,最终可致多器官衰竭死亡。

典型的剧毒蘑菇如致命鹅膏(俗称“白毒伞”),通体洁白朴素,却是我国蘑菇中毒的“头号杀手”,病死率高达40.37%。其特征为“头上戴帽、腰间系裙、脚上穿靴”,但普通人仅凭肉眼或照片,极易将其与无毒蘑菇混淆。

面对形态各异的蘑菇,许多人选择用手机拍照让AI鉴定。看似便捷,实则隐患巨大。野生蘑菇辨别难度极大,仅凭肉眼都无法保证100%识别正确,凭图片更无法100%排除有毒相似品种的可能。

AI识图本质上是基于海量图片的模式匹配算法,其结果易受拍摄角度、光线、背景、蘑菇生长阶段等因素干扰,识别准确率并不稳定。把生命交给概率模型,无异于用掷骰子赌博。

(都市快报、湖北疾控)

靠AI指引户外线路

男子和老婆吵架,让AI推荐散心线路被困

近日,浙江省杭州市临安区狼行公益应急救援队接到紧急求助:有人被困在海拔1300多米的浙西三尖(太子尖、百丈岭、童公尖)之一的大山上。

接到救援任务后,7名救援队员和两名民警、3名消防人员直奔现场。

这场持续了四五个小时的救援,竟然和AI有关。

被困者所在的童公尖海拔约1558米,地形复杂且大部分为未开发区域,山高林密、荆棘丛生,手机信号时断时续,夜间气温低,极易迷路或失温。

当晚9时40分,狼行公益应急救援队副大队长陈敏带队,赶到童公尖山脚下开始攀爬寻找被困者。

童公尖的山路非常陡峭,很难攀爬,救援人员经过一个半小时的徒步跋涉,在海拔约1300米的位置找到报警求救的小伙子。

小伙脚部和膝盖多处擦伤,体重至少有160斤。陈敏和队员轮换架着小伙,慢慢往下爬。走走停停赶到山核桃林地,这里有当地居民用来装运山核桃的小火车。小伙在队员们的帮助下,坐上小火车下了山。这场救援,一直持续到次日凌晨才结束。

当天,他和老婆因为琐事吵架,心情郁闷,就想外出闯闯,一时没有目标,于是向AI求助。

AI详细问了他的心理、性格、身高和体能后,郑重其事地给他推荐了一条户外线路:杭州临安浙西三尖的童公尖。

对AI的推荐,小伙深信不疑,从苏州直奔杭州临安。爬上童公尖无人开发区后,因为山高陡峭,他不慎摔倒受伤,结果被困在了海拔1300多米的的地方,山上一片黑暗,幸好还有手机信号,于是打电话报警。

“这种靠AI指引户外线路的游客,在这么多年的救援任务中,我们还是第一次碰到。”临安狼行公益应急救援队执行大队长沈晓斌分析,可能有不少驴友在网上分享过童公尖的徒步攻略,被AI捕捉整合了。“这种AI推荐的线路肯定不靠谱。他自己平常很少登山,也不户外运动,像童公尖这样海拔不断升高的户外路线,肯定是吃不消的。”

此外,沈晓斌指出,AI给小伙做推荐时,也没有提醒他在户外运动前要准备哪些装备。结果小伙子几乎什么装备都没带,只带了一把折叠小椅子,脚上只穿了一双板鞋。(国家应急科普宣传)



AI制图。

用AI工具处理敏感资料

用AI工具处理内部文件,敏感资料竟全部泄露

此前,国家安全部披露了一起典型案例:个别单位直接使用开源框架建立联网大模型,导致攻击者未经授权即可自由访问内部网络,从而引发数据泄露和安全风险。案例显示,某单位工作人员违规使用开源AI工具处理内部文件,因电脑系统默认开启公网访问且未设置密码,导致敏感资料被境外IP非法访问、下载。

这一案例,撕开了开源AI工具潜藏的泄密“暗门”,直观揭示了此类风险的严重性与危害性。

开源AI工具的数据安全隐患,主要源于其工作原理中的数据存储功能。“投喂”给AI的任何文件、图片、文字等数据,都会被模型存储下来,以此为基础完成分析处理。这一特性是AI高效工作的前提,却也在无形中为数据泄露埋下伏笔。

一旦数据被存进模型,就至少面临两种泄密风险:一方面,开源AI工具开发者拥有最高权限,可直接访问和查看所有存储数据,若开发者缺乏保密意识

或存在利益驱动,用户上传的敏感信息可能被非法利用或泄露;另一方面,开源属性让黑客有机可乘,他们可以利用此类工具本身的漏洞攻击入侵后台,批量窃取存储数据,无需接触用户终端即可实现远程窃密。

因此,对于机关单位或企业来说,若将工作秘密上传至开源AI工具,无异于将核心信息暴露在透明环境中;对于个人而言,身份证号、手机号、隐私照片等敏感信息的上传,也可能引发电信诈骗、信息倒卖等问题。尤其需要警惕的是,若涉及国家秘密的信息被“投喂”给此类工具,将直接威胁国家安全,造成不可挽回的损失。

在AI技术快速发展的今天,防范开源AI工具带来的安全风险至关重要,需要多方发力、层层设防。尤其要严守保密红线,坚决杜绝因AI使用不当造成的泄密事件。

对普通用户而言,需在使用过程中做到“数据不随意投喂”,避免向AI上传个人隐私信息。(保密观)