雷军曾发视频回应遭AI配音恶搞

AI软件对图片“一键去衣”

专家教大家如何辨别AI换脸

拆解AI造假4大套路

仿冒名人 炮制新闻 换脸敲诈 一键去衣

近日，有人用AI技术假冒知名医生张文宏带货的消息冲上热搜。15日，微信平台发布消息称，针对“利用AI技术仿冒名人进行不当营销”的情况进行了打击，关闭账号209个。AI（人工智能）作为一种新技术，面世以来被应用到社会多个领域，但近年来也出现了不少利用AI进行违法犯罪的案例，包括仿冒名人、造谣、换脸诈骗、窃取隐私等等。

涉及AI的套路有哪些？Z在现实生活中，我们该如何防范？

1 仿冒名人
炮制视频和声音

近日，有网友发现账号名为“般画XXX”发布的一段视频中，知名医生“张文宏”正在售卖一种蛋白棒。然而，媒体调查发现，该视频中口型和声音像是张文宏。经过核实，该视频并非张文宏医生本人拍摄，而是他人利用AI技术合成的虚拟人。网友截图显示，该蛋白棒产品已售出了1266份。事后，张文宏告诉记者，这样的卖货账号不止一个，而且一直在变，他已多次向平台投诉。

被AI技术假冒的，张文宏不是首个“躺枪”者。今年国庆假期，短视频平台上出现了大量“雷军AI配音”的视频，这些恶搞视频在社交平台上的相关话题浏览量过亿。视频中，“小米CEO雷军”锐评了堵车、调休、游戏等热门话题，言辞犀利，还常爆粗口。在事后接受采访时，雷军表示：“希望大家都不要玩了，这个事情不太好。”

今年11月，胖东来创始人于东来被人用AI技术生成声音去卖药，事后胖东来发布声明进行了辟谣。

据报道，今年11月，江西一位老人到银行办理业务，声称要贷款200万元给男朋友“靳东”拍戏。经调查发现，老人手机里的“靳东”出自由AI合成的视频。今年10月，老牌港星黄百鸣也通过社交媒体郑重声明，有人盗用其过去影片，利用AI替换声音，代言一个不知名的药膏品牌。

15日，微信平台发布消息称：“近期有媒体报道，网络存在利用AI技术仿冒名人进行不当营销的现象。我们从速从严打击了一批利用AI仿冒知名人士进行不当营销、恶意博取流量的违规行为，并针对相关情况开展专项治理。截至目前，累计处置内容532条，关闭账号209个。下一步，我们将持续对“利用AI仿冒知名人士进行营销宣传”等违规行为增加打击力度。”

2 炮制新闻
软件几秒钟生成

当前，AI技术存在被滥用的情况，一些不法分子利用AI技术生成造谣内容并传播。

公安部网安局公布一起案例：2023年12月，一条“西安市鄠邑区地下涌出热水”的信息在网络上大量传播，出现如“地下出热水是因为发生了地震”“是因为地下热管道破裂”等谣言。经查，相关谣言是通过AI洗稿方式生成的。今年6月20日，上海警方也发布通报，两名品牌营销人员为蹭热度吸引流量，使用AI软件生成视频技术，编造“中山公园地铁站捅人”等不实信息，相关人员已被行政拘留。

类似情况还有“济南一高层住宅楼起火，多人跳楼逃生”“晨练大爷在济南英雄山附近发现坟中有活人”……这些离谱的“重磅消息”引起大量关注，经有关部门调查，均系AI生成的谣言。

清华大学新闻与传播学院新媒体研究中心今年4月发布的一份研究报告显示，近一年来，经济与企业类AI谣言量增速高达99.91%，其中餐饮外卖、快递配送等行业更是AI谣言重灾区。

记者用市面上流行的多款人工智能软件测试发现，只要给出关键词，就能在几秒钟内生成一篇“新闻报道”，只要加上时间地点，再配上图片和背景音乐，一篇以假乱真的“新闻报道”便制作完成。

中国人民大学新闻与社会发展中心研究员曾持说，AI根据热点事件总结规律、拼接情节，很快就能制作出符合人们“预期”的谣言，传播十分迅速。

账号名称	违规情况	处置措施
般***4	仿冒知名人士进行营销宣传	永久封禁
阿***834	仿冒知名人士进行营销宣传	永久封禁
菠***5829	仿冒知名人士进行营销宣传	永久封禁
大***8842	仿冒知名人士进行营销宣传	永久封禁

微信近期处理的部分违规账号 “微信珊瑚安全”公众号

3 换脸敲诈
有人被骗20万元

近年来，各地出现了不少利用AI技术直接参与犯罪的案例，犯罪分子利用AI进行换脸、换声，冒充他人进行诈骗，也有人利用AI窃取他人隐私。

宁夏固原市居民马某某接到表哥视频电话求助后，毫不犹豫给对方指定账户转了1.5万元。事后，他给亲戚发微信核实时才得知被骗。原来骗子通过AI换脸和拟声技术，佯装亲戚对其实施诈骗。

AI技术实现“一键去衣”和换脸的功能被不法分子利用，成为敲诈勒索的工具。去年夏季，山东威海居民王某收到“自己和一名女子的裸照”，对方说“我有你全部的影像资料，赶紧跟我联系”，最后要求付款68万元。在没有多加核实的情况下，王某向敲诈团伙转账20万元。今年1月，威海警方赶赴浙江将两名犯罪嫌疑人抓获归案，为王某挽回了损失。

今年4月，北京市海淀区法院还审理了一起特殊的“制作、贩卖淫秽物品”案。被告白某某利用AI软件，对被害人的图片“一键去衣”，几秒钟、几分钟就能批量生成相应的图片。经查，他通过某款通信软件向351个人贩卖相关图片，图片数量将近7000张。

今年9月，杭州警方公布了一起利用AI窃取居民隐私信息的案件。嫌疑人胡某某等四人，在境外网络承接定向出售国内头部平台用户数据业务，使用境外多模态专用大模型，通过文字对话，输出活体视频，突破平台人脸认证，强制登录他人账号，获取大量受害人私人数据和敏感信息并出售获利。据悉，这是全国首起利用AI技术侵犯公民个人信息的案件。

知名医生张文宏回应被AI仿冒带货 央视财经截图

4 克隆声音
网站当成生意做

利用AI技术进行犯罪，绝不是新技术的试错或无心之举，而是别有用心之人刻意利用新技术违法乱纪，意图获取非法利益。

在上述贩卖“去衣”照片案件中，被告白某某在境外社交媒体上接触到了这项“一键去衣”的技术，于是打算利用这项技术来赚钱，他在境外的社交媒体上发布了广告，内容就是“去衣”，1.5元一张。他的广告发布后，有不少人联系白某某，给他发送照片并购买这项“去衣”服务。

相关专家解释，“去衣”照片并不是真的去掉别人照片上的衣服，其实是针对已有的模型和已有的模组进行图片重绘。白某某不仅通过AI软件制作裸体图片贩卖牟利，同时出售AI“去衣软件”及使用教程牟利。短短几个月的时间，白某某制作了几千张去衣的图片，赚了近1万元。

另外，在多起AI造谣事件背后，造谣者的动机主要也是引流和借此牟利。今年6月中旬，一家MCN机构的实际控制人王某某利用AI软件生成虚假新闻并大肆传播，被警方行政拘留。据警方通报，王某某共经营5家MCN机构，运营账号842个，自今年1月以来，他通过AI软件生成虚假新闻，最高峰一天能生成4000至7000篇。另据西安警方介绍，他们查获了某款AI软件，“一天能生成19万篇文章”。今年2月，上海警方发现，在一家电商平台上出现了某艺人“命运多舛、含恨离世”等短视频，引发大量点赞和转发。经查，该视频内容系伪造。视频发布者交代，他通过假新闻给自己经营土特产的网店账号吸引流量，因自己不会视频剪辑，便利用AI技术生成虚假文本和视频。

在于东来、雷军等人曝出声音被克隆的消息后，有媒体记者搜索发现，网络平台上有不少AI克隆声音的教程视频。记者登上某网站发现，该网站已有大量训练好的声音模板，包括雷军、郭德纲、周杰伦、丁真等明星名人。其中，雷军的AI声音累计被使用的次数超过7万次，丁真AI声音模型使用次数超33万次，位于榜首。

生成AI声音十分简单。记者测试发现，对于已有模型的AI语音，只需输入想要生成的语音文本，3秒钟即可生成相应的音频。没有模型怎么办？根据该网站提示，只需上传最短10秒钟的语音素材，不到1分钟即可训练出新的声音模型，整个操作过程零技术门槛、零成本。也就是说，只要获取10秒钟的语音，任何人的声音都能被AI“偷走”，生成不实内容。除了某些软件和网站外，网络购物平台上也有人工代做的服务销售，称“仅需一句话，克隆任何声音，还原度99.99%”。

支招 四招预防个人信息泄露

陌生WiFi不要连：在公共场合连接免费WiFi时，极易碰到不法分子搭建的山寨WiFi。

钓鱼链接不要点：一些不法分子会假冒银行、学校等机构给用户发送短信或邮件，以“通知”“账户验证”等名义诱导用户点击其中的网址链接。

不明二维码不要扫：二维码应用场景十分广泛，而且制作简单、真伪难辨，常常被不法分子用于传播手机病毒和恶意软件。

个人信息不要晒：机票、证书、照片等内容中包含姓名、身份证号、手机号、关键位置等个人信息，如果随意晒在朋友圈等社交平台，可能会导致信息泄露。

综合央视新闻、光明日报、法治日报等