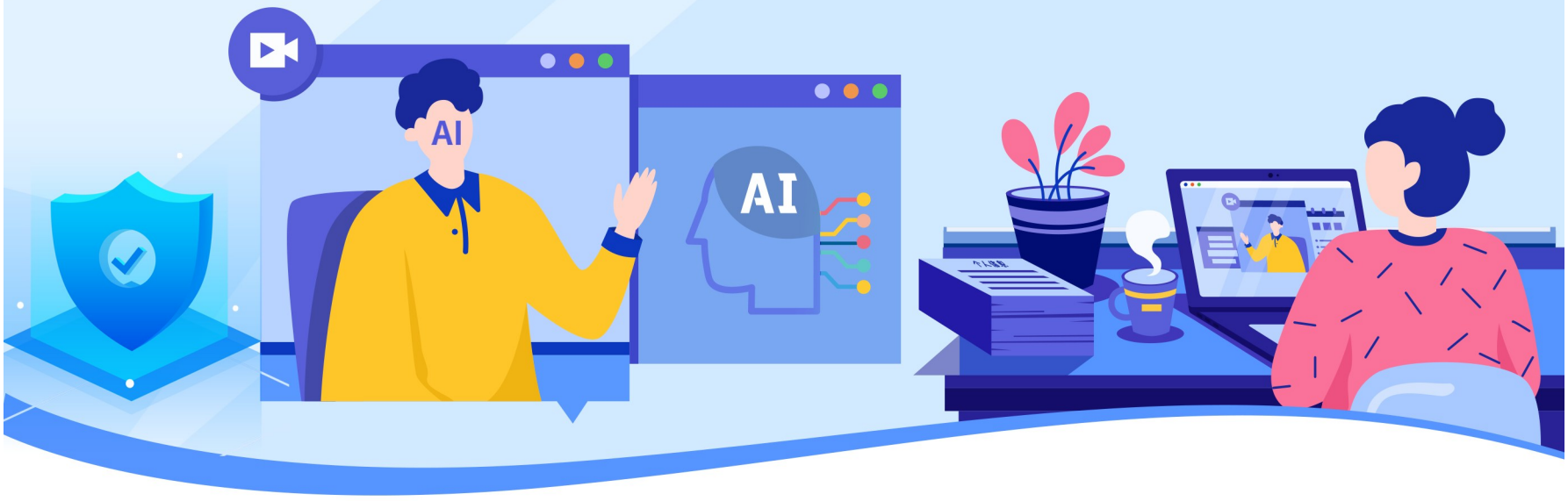
技术狂奔时代 我们如何守住“脸面安全”？

低至20元就能AI换脸 警惕骗子靠AI“开挂”



近四成的AI诈骗瞄准老人。“姐姐我今年67，上市公司老总，这辈子啥都齐了，就缺个你。”“大妹子，要是我把微信给你，你会添加我吗？不图别的，就想跟你说说心里话。”

在主流短视频平台上，有无数个这样喊着姐姐、说着情话的“AI霸总”。这些霸总大都穿着西装，有的戴着大金链，对着镜头深情款款，配以抒情音乐。如果仔细看，有的霸总“撞脸”明星，而画面底部有一行不起眼的小字：作品含AI生成。

关于“假靳东”的骗局已经曝光数年，但类似的套路仍在“收割”老年群体。瑞莱科技联合创始人萧子豪表示，近一年来利用AI进行诈骗、造谣等违法犯罪行为屡禁不止、愈演愈烈，呈显著上升趋势。犯罪行为变得更具迷惑性，也更加隐蔽。这与近年来生成式AI技术能力突飞猛进并持续开源开放有关，大量工具、产品问世，极大降低了不法分子的作恶门槛和成本。

记者调查发现，在电商平台200元可定制一条以名人声音“讲话”的视频，而制作AI换脸视频的价格在20~500元不等。AI伪造的账号和骗局泛滥成灾，被侵权的对象也从明星迅速蔓延至普通民众，让维权变得更加困难。

第一财经

AI换脸泛滥：从明星到普通人

近日，一位用户在社交平台反映自己的母亲被骗了，从他分享的用户私信图片来看，母亲账号与多个“AI霸总”账号私信互动，他们的话术如出一辙，“姐姐，终于等到你了”。其中一个账号的头像用的是演员靳东。

这不是孤例。此前有报道称，不少老人迷上“AI霸总”，甚至有八旬老太被骗2000元。这些账号的套路往往是针对老年女性用户量身定做霸总视频，提供情绪价值，进而实现带货或敛财。

公安部数据显示，2025年上半年全国电信网络诈骗涉案金额超百亿元，仅2025年第一季度，全国AI换脸、拟声诈骗案件数量环比激增45%，其中老年群体受骗占比达到38%。

在利用AI敛财的陷阱里，老年人成为重点的“围猎”目标，而被AI侵权的主要群体，是像靳东、温峥嵘这样的明星。曾被视为“高科技”的AI技术，早已成为小团队甚至个人可轻松操作的工具，而明星这样有大量素材的公众人物，进行换脸生成的门槛不高。

在电商平台，记者发现，直接搜索“AI换脸”会被平台拦截无法显示结果，但若将关键词替换为“AI视频制作”，则有更多操作空间。

记者问了近10个可以制作AI视频的商家，能否制作明星换脸视频，部分商家会明确拒绝AI换脸，但也有不少商家表示可以进一步沟通细节，并引导记者至微信交流。

有商家粗略报价，制作换脸视频的价格在20元至200元不等。也有商家要求看完视频内容和需求进行报价，记者发送了一份2分钟的视频，询问能否换脸一位明星，在简单询问是否商用后，这位商家称500元即可制作，对于价格他解释称，由于政策限制，现在行业里真人换脸的难度较大。

在AI拟声方面，一位商家告诉记者，制作一条涉及名人讲话的视频，一口价是200元。除了定制服务，各类可自行操作的AI工具更是让换脸和拟声变得人人可及。国内外多款AI视频软件都能生成逼真的人物视频，无需专业的技术知识，普通人跟着教程就能上手。

而2025年底，演员温峥嵘更是被迫在个人账号开启多场“我是真的温峥嵘”直播，以对抗网络上层出不穷的“AI分身”。温峥嵘团队工作人员表示，发现该现象后团队便持续进行举报，一天时间内曾举报50个假冒账号，有的造假账号被平台下架处理，有的账号刚被下架很快又换了个形式重新出现，令人防不胜防。

该工作人员称，商家只需要截取一段影像，通过简易工具便能生成虚假内容，但取证动作却需要花费很大精力。且造假团队喜欢在凌晨三四点钟打时间差发布虚假视频。虽然团队已送达相关律师函，但目前调查的仅仅是一部分造假商家。

更令人忧虑的是，近一年，AI换脸的侵权对象正在从明星蔓延至普通人，更隐形，维权难度也更高了。

在小红书上，一位万粉博主@阿尔忒弥斯舟提到，“打开小红书刷到自己的照片结果发现脸不是自己，被吓了一跳，后面才反应过来是AI换脸。”他表示，后续举报成功，这条作品已经被小红书官方删除了，但“不敢想象这种AI换脸被用到非法的途径会是什么后果”。

评论区不少用户反馈“辨认不出来哪个是AI”。但仔细看能发现，AI换脸后的照片还是有一些痕迹，脖子和脸比例不对等等，但并不是所有用户都有分清AI的能力。

另外一名仅几千粉的博主完全没想到自己会被换脸，“以为只有网红才会被盗用，没想到我这点粉丝也会。”他已经发现四个人套用他的脸了。

由于并非明星，这些仿冒账号用于婚恋诈骗和“杀猪盘”则更难被察觉，即便被发现，也就“一删了事”，违法成本极低。

反AI骗局：没有终点的“猫鼠游戏”

靳东是AI换脸的典型受害者，他也回应了AI换脸乱象，称维权很难，不法分子利用AI换脸伪造其形象，在短视频平台针对中老年群体实施情感诈骗与非法集资，性质极其恶劣。靳东呼吁对AI换脸立法，出台更多细则。

面对愈演愈烈的AI造假乱象，法律惩戒与平台治理已开始“亮剑”，但从实际效果来看，仍存在违法成本低、取证难度大、维权流程繁等诸多短板。

在法律层面，AI换脸侵权已有明确的法律依据：未经授权使用AI技术生成自然人面部特征、声音用于营利，违反《民法典》相关规定，构成肖像权侵权；若内容丑化、贬损当事人，还会同时侵害名誉权，而情节严重者还将承担刑事责任。

北京互联网法院去年曾发布涉人工智能侵权典型案例，其中一个是用知名教授的公开演讲视频合成近似的声音进行图书“带货”，法院审理后认为，涉案视频构成侵犯肖像权和声音权，判被告道歉赔偿12万元。

在平台治理方面，各大社交平台也开展了专项治理。3月初，微信发布关于打击利用AI仿冒名人进行引流虚假宣传的公告，累计处置AI仿冒名人违规内容1.3万余条，封禁账号1200余个。抖音电商也发布公告称“AI仿冒肖像及声音侵权”成为重点治理领域，累计处置侵权仿冒达人账号1.1万个，处置仿冒李亚鹏等名人的侵权内容16.5万条，关闭136个相关违规达人电商权限并冻结佣金30天。

部分AI技术平台也开始采取限制措施，今年2月，豆包旗下视频生成模型Seedance2.0上线后，执行严格限制：禁止生成明星、公众人物、网红等真实人物肖像/视频/语音，防范AI换脸/伪造/商用侵权。

不过，北京市京都律师事务所合伙人常莎认为，现有的法律运行存在侵权成本过低、平台责任虚化、维权链条过长的困境。权利人需要经历取证、公证、诉讼等漫长流程，因此治理AI换脸乱象的关键在于对现有法律进行针对性修补。例如引入惩罚性赔偿机制，让侵权成本高于收益；同时将平台责任从“事后删除”前移至“事前审核”，对涉及知名公众人物的AI合成内容主动筛查。

萧子豪表示，AI技术衍生安全风险的治理问题是个非常复杂的社会问题，涉及很多方面。既要在法律法规层面事前规范引导、事后监管惩戒，也需要有技术手段令AI更加安全、可控。

在技术层面，萧子豪认为，对AI的鉴伪是一场“猫鼠游戏”，此消彼长，相互博弈。因此，对AI骗局的识别也要随着生成技术的进展不断研究、更新、迭代，没有终点。