AI诈骗常用手法

第一种 声音合成

骗子通过骚扰电话录音等来提取某人声音,获取素材后进行声音合成,从而可以用伪造的声音骗过对方。

第二种 AI换脸

人脸效果更易取得对方信任,骗子用AI技术换脸,可以伪装成任何人,再通过视频方式进行信息确认。

骗子首先分析公众发布在网上的各类信息,根据所要实施的骗术,通过AI技术筛选目标人群。在视频通话中利用AI换脸,骗取信任。

第三种 转发微信语音

骗子在盗取微信号后,便向其好友"借钱",为取得对方的信任,他们会转发之前的语音,进而骗取钱款。

尽管微信没有语音转发功能,但他们通过提取语音文件或安装非官方版本(插件),实现语音转发。

第四种 AI程序筛选受害人

骗子利用AI来分析公众发布在网上的各类信息,根据所要实施的骗术对人群进行筛选,在短时间内便可生产出定制化的诈骗脚本,从而实施精准诈骗。

点开直播间乍一看,卖货的竟是当红女星。再定睛一看,"明星"其实是使用人工智能(AI)实时换脸技术的普通主播。他们冒充明星艺人,只为增加卖点,助力卖货……

近期,"AI换脸"的应用范围越来越广,但存在滥用之嫌,甚至有人利用AI换脸实施犯罪,例如伪造不雅视频、换脸诈骗等。前不久,就有一男子因AI"偷脸",10分钟被骗430万元。

如此以假乱真,让人防不胜防。"AI换脸"的法律边界在哪?普通人又该如何防范?

诈骗 \ 公司老板遭遇AI换脸诈骗 10分钟被骗取430万元

近日,内蒙古包头警方发布一起利用AI实施电信诈骗的典型案例。来自福建的郭先生是一家科技公司的法人代表。今年4月,他的好友突然通过微信视频联系他,称自己的朋友在外地竞标,需要430万元保证金,想借用郭先生公司的账户走账。基于对好友的信任,加上已经视频聊天"核实"了身份,郭先生在10分钟内,先后分两笔把430万元转到了对方的银行账户上。

事后,郭先生拨打好友电话才得知被骗,原来骗子通过AI换脸和拟声技术,佯装好友对其实施诈骗。"当时是给我打了视频的,我在视频中也确认了面孔和声音,所以才放松了戒备。"郭先生事后说。

魔幻一幕令人吃惊,但这并非AI换脸第一次作恶了。2022年2月,有位陈先生到浙江温州市公安局瓯海分局仙岩派出所报案称,自己被"好友"诈骗了近5万元。经警方核实,诈骗分子利用陈先生好友"阿诚"在社交平台发布的视频,截取其面部视频画面后再利用"AI换脸"技术合成,制造陈先生与"好友"视频聊天的假象骗取其信任,从而实施诈骗。

2021年拱宸桥派出所接到报警,受害人小陈称他在与女网友视频聊天后被对方敲诈勒索。经警方调查,对方利用AI换脸技术,将小陈视频中的面部合成到不雅视频中,借此对其实施勒索。

2020年,上海某公司高管因对方使用AI换脸与人工生成的语音技术制作公司领导的面孔,并要该高管转账,致使该高管被诈骗150万元。

直播 \ 换脸后的"杨幂""刘亦菲"都在直播间里带货

"看了好几个直播间,我都惊呆了,全都把脸换成明星带货了,那还要我们这些普通的主播干什么?"日前,一位网友在社交平台发文吐槽,她在逛某短视频软件的时候刷进了某品牌的直播间,直播间中的女主播正在热情推销商品,但这位女主播看起来似乎有点眼熟,直播弹幕中也有网友表达了相同的困惑。

在这位博主的帖子下,这类"明星脸"眼熟的巧合似乎未免有些太多了,网友"小虫"表示,这个品牌的直播间自己前几天也曾刷到,"那个是AI,我前几天刷到的,是另一个人。"网友"可乐"则回复说"刚刚看了下,还有一个号,好像是杨颖。"除了在这个牌子的直播间,也有网友刷到了其他"明星脸"的主播,"昨天我刷到殷桃,好吓人啊。""我还看过一个一直用杨幂的脸的。""上次还刷到了刘亦菲呢。"

随着AI技术的不断进步,AI实时换脸已逐渐成熟。近年来,AI实时换脸已从最初的娱乐"整活",向直播等多个应用场景发展。通过智能后台的AI换脸技术,主播可以实现形象的实时替换。

有视频换脸研究者表示,实时换脸不存在延迟,也不会有Bug,而直播画面传输的延迟则取决于使用者的网络配置和进行直播的平台。

记者以使用者的身份咨询了一家提供"换脸软件"的网站。该网站客服表示,使用AI换脸需要进行模型训练。"合成效果好不好,关键看模型和素材。"

据提供"换脸软件"的网站介绍,使用者自己从零开始训练模型,如果24小时挂机不停地训练模型,需要经过半个月到一个月的时间,才能达到可以合成视频的效果。

而比起自己花费大量时间训练模型,更多人选择购买现成的模型。"素材充足的话,你只要花费半个小时到几个小时的时间就可以直接合成视频。模型可以替换任意素材使用,不分张三李四。"

该网站客服称,他们提供的全套模型购买价格为3.5万元,AI实时换脸可适用于各大直播平台。

行业 \ 必须尽快立规 明确信息保护红线

为规范人工智能发展,去年12月,《互联网信息服务深度合成管理规定》正式发布,明确了合成数据和技术管理规范。其中提到:深度合成服务提供者对使用其服务生成或编辑的信息内容,应当添加不影响使用的标识。提供智能对话、合成人声、人脸生成、沉浸式拟真场景等生成或者显著改变信息内容功能的服务的,应当进行显著标识,避免公众混淆或者误认。

简单来说,这些技术服务公司,不能随便使用普通人的人脸来换脸,必须经过本人同意,换脸不是想换就能随便换,也不是骗子给钱就能随便换。

近期,也有平台和企业发布了"关于人工智能生成内容的平台规范暨行业倡议",明确禁止利用生成式人工智能技术创作、发布侵权内容,包括但不限于肖像权、知识产权等,一经发现,平台将严格处罚。

当然,人工智能开发还是一个高速成长的领域,规则的健全完善还需要时间。但不管怎么说,此次案件都提醒我们,技术被滥用的风险,对普通人造成的安全隐患和威胁,绝对不容低估。

对大众来说,在人工智能时代,我们得更加警惕,不要随意泄露个人信息,需要转账时应更加谨慎地核实。而对行业而言,必须尽快立规,明确信息保护红线,加强对技术服务商行为的规范引导等等。

律师说法 \

律师:
或侵犯肖像权、名誉权

北京盈科(合肥)律师事务所王海波律师称,"'AI换脸'属于深度合成技术,随意使用可能有肖像权和名誉权侵权的风险。"

王海波称,按照民法典规定,无论个人还是平台、软件开发商,未经肖像权人同意,通过技术手段提取肖像,并擅自使用或上传至换脸App中供用户选择使用的行为都涉嫌侵害了他人肖像权,如果有人将他人的脸换到不雅视频中,或者利用换脸软件对他人进行恶意丑化,就有可能侵犯他人的名誉权。

北京岳成律师事务所高级合伙人岳岫山律师表示,这样的换脸直播用于公开传播,可能涉嫌侵犯相关明星艺人的肖像权,如果涉及直播带货等商业行为,会成为加重情节。

在知名艺人工作室从事宣传工作的袁女士表示,"我经常刷一些平台都会看到。还是有一定的欺骗性的,如果不仔细辨认的话,就会认为是明星艺人本人,这一点我觉得还挺可怕的,万一卖的东西拿回去了以后货不对板,或者有一些更严重的问题,消费者就会觉得'这个东西我是看着谁谁谁的脸去买的',或者说'我是进了谁的直播间去买的'。"

袁女士认为,针对相关行为搜集证据和维权的成本比较高。而只要冒用了明星艺人的面部特征,不管是否提及姓名,侵权影响都类似。"说实话是没有差别的,因为他本质上还是用这个明星的脸去做文章。如果我负责的明星艺人摊上了这个事儿,其实维权成本特别大,并且效果可能没那么好。我们也不可能每天都去发律师函,发也发不过来,甚至有的时候可能要找到侵权人都很费劲。"

综合央视新闻微信公众号、央广之声、每日经济新闻消息