

热搜

AI

内蒙古男子10分钟内被AI换脸诈骗430万元,安徽男子9秒被骗132万……

“AI换脸”诈骗防不胜防 要用“法”打败“魔法”

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……近日,中国互联网协会发文称,伴随着深度合成技术的开放开源,深度合成产品和服务逐渐增多,利用“AI换脸”“AI换声”等虚假音视频进行诈骗、诽谤的违法行为屡见不鲜。

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?

案例

2

合成不雅视频敲诈

在温州警方通报的一起案件中,温州的陈先生遭遇“AI换脸”敲诈,他收到一封“私家侦探”的敲诈信,同时附了他与一名女子的所谓的不雅视频,信件中对方要求陈先生收件后迅速与其联系,不要心存侥幸,并威胁将视频散播到互联网。因为知道这是一段合成视频,但不知如何处理,陈先生向警方求助。目前此案件正在调查中。

案例

1

AI“熟人”诈骗多人

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,伪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。幸运的是,接到报警后,福州、包头两地警银迅速启动止付机制,成功止付拦截336.84万元,但仍有93.16万元被转移,目前正在全力追缴中。

无独有偶,5月22日,安徽安庆的何先生接到熟人视频电话,让他帮忙转一笔账。但9秒之后,对方以“在开会”为由挂断了电话,还称“微信和电话不能说,加一下QQ”。“因为打了视频电话,又是熟人,我就没多想,就转账了”。发现被骗之后,何先生迅速报警。专案民警第一时间冻结相关账户,连夜赶赴北京市抓获3名涉诈嫌疑人,追回何先生被骗的132万元。

案例

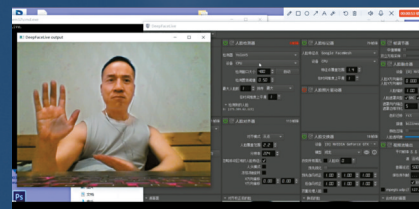
3

AI换脸冒充明星带货

除了伪装“熟人脸”实施诈骗,AI换脸还可能出现在直播带货中。最近,网上出现了一些“换脸直播”教程,教程发布者声称可以帮助用户轻松“变脸”,极大地助力引流卖货。

在一个展示换脸直播效果的视频中,使用者把名为“成龙”的模型载入相关软件后,摄像头前的人在直播画面中就有了与成龙相似的五官,但脸型和发型还保持原样。

记者发现,使用者歪头或变换表情时,五官动效切换得自然顺滑,只有手掌从脸前划过时,出现了比较明显的破绽。



发布者展示换脸为“成龙”的实时效果和软件界面(视频截图)。

警惕

务必保持防范意识

换脸术的滥用,已经对公共利益构成威胁。

对于个人而言,面对花样翻新的AI诈骗,必须保持防范意识。有人说,防骗最有效的一招就是不信,无论对方怎么“换”、怎么变、怎么翻着花样骗,就是“不听不信不转账”。

中国互联网协会表示,如果有人自称“家人”“朋友”“老师”“领导”,通过社交软件、短信、电子邮件等,以各种方式

和理由诱导你转账汇款,务必第一时间提高警惕。在AI时代,文字、声音、图像和视频都有可能是深度合成的。在转账汇款、资金往来这样的典型场景,要通过回拨对方手机号等额外通信方式核实确认,不要仅凭单一沟通渠道,未经核实就直接转账汇款,无论对方是谁。

如不慎被骗或遇可疑情形,请注意保护证据,并立即拨打96110报警。

整治

用“法”打败“魔法”

要整治AI换脸,我们应当用“法”去打败“魔法”,这个法是法规、法律的法。

此前,一款主打AI换脸的App很火,“只需一张照片,演遍天下好戏”。但很快,在监管部门约谈后,这款App下架,原因很简单,如此换脸侵犯了公民的肖像权。

去年12月,《互联网信息服务深度合成管理规定》发布,对人脸生成、替换、操

控,合成人声、仿声等都有明确约束。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。

说法

换脸或涉嫌侵权

北京岳成律师事务所高级合伙人岳岫山表示,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。

岳岫山解释,只要未经肖像权人同意,在直播中通过技术手段把自己的脸换成了明星的脸,就是对明星肖像的侵权。即便只是娱乐,不涉及盈利行为,也属于侵权。如果把明星肖像用于带货直播,属于商业行为,在赔偿数额上一定会给予考虑。如果主观恶性、过错程度比较大,且因此获利,赔偿数额可能会更高。

记者注意到,一些使用换脸技术的直播并不会直接提到相关明星艺人的名字,但也不主动声明或否认。岳岫山认为,该行为涉嫌欺诈或是虚假宣传,如果货品本身质量不好或者主播在带货过程中的言行导致公众对被换脸明星产生负面评价,明星可以主张名誉权的侵权责任。

思考

被打开的潘多拉魔盒

AI换脸术被滥用,也促使大家思考一个深层次问题。新技术不断面世,带给了人们便利,但可能被居心叵测之徒非法利用。人们固然不能因噎废食,但也不能忽略它的双刃剑效应。如果缺乏应有约束,AI换脸则可能打开潘多拉魔盒。因势利导,使其趋利避害,这是我们要全力做到的。

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。

显然,随着制度设计更精准,相关立法更健全,AI换脸空间将越来越逼仄。

(文图来源:据央视新闻、北京青年报、VCG等)