

几块钱就能合成动态视频,可注册手机卡、支付账户

近日,陈先生来到浙江省温州市公安局瓯海分局仙岩派出所报案,称自己被“好友”骗了近五万元。经过警方核实,骗子用了AI换脸技术,利用陈先生好友阿诚社交平台上先前发布的视频,截取了面部视频画面并进行了“换脸”,从而对陈先生进行了诈骗。

2021年4月,安徽省合肥市警方在公安部“净网2021”专项行动中打掉一个犯罪团伙,该团伙利用人工智能技术伪造他人人脸动态视频,为黑灰产业链提供注册手机卡等技术支撑。

在警方抓捕现场,几名犯罪嫌疑人正用电脑将一张张静态照片制作为人脸动态视频。模拟制作出来的动态人物不仅能做点头、摇头等动作,还可完成眨眼、张嘴、皱眉等丰富表情,效果极为逼真。

在嫌疑人的电脑里,警方发现了十几个G的公民人脸数据,人脸照片和身份证照片分门别类存放在一个个文件夹里。“身份证正反面照片、手持身份证照片、自拍照等,被称为一套。”民警介绍,成套照片被称为“料”,出售照片的人被称为“料商”,这些“料”在网上已转手多次,而“料”的主人却毫不知情。

犯罪嫌疑人马某交代,由于制作简单,一个视频价格仅为2至10元,“客户”往往是成百上千购买,牟利空间巨大。

近年来,类似案件在浙江、江苏、河南等多地发生。浙江衢州中级人民法院的一份刑事裁定书披露:张某、余某等人运用技术手段骗过支付宝人脸识别认证,并使用公民个人信息注册支付宝账户,非法获利数万元。

这些案件的作案流程颇为雷同:不法分子非法获取他人照片或有偿收购他人声音等“物料”,仅需少量音视频样本数据,便可合成媲美真人的伪造音视频,用来实施精准诈骗,侵害他人人身和财产安全,或销售、恶意传播技术换脸不雅视频等,造成肖像权人名誉受损。

网络传播环境日趋复杂,反深伪检测难度越来越大

据合肥市公安局包河分局网安大队民警王祥瑞介绍,前述案件中8名犯罪嫌疑人多为社会闲散人员,有的连高中都没有读完。他们按照网购教程下载软件,花几个月便“自学成才”。

记者在網上联系到一位售卖相关教程的卖家。卖家介绍,全套软件及教程售价有400元、800元两档,800元的为高阶版本,“过人脸成功率超高”。记者在演示视频中看到,照片上传至软件后,标注出五官位置,调整脚本参数,一张脸便动了起来。“五官参数随教程送上,照抄即可。”据介绍,这些伪造视频不仅通过率高,人工审核都难辨真假。

“目前公众对照片等静态信息易被篡改已有所警惕,但对视频、声音等动态信息内容仍持有较高信任度。”

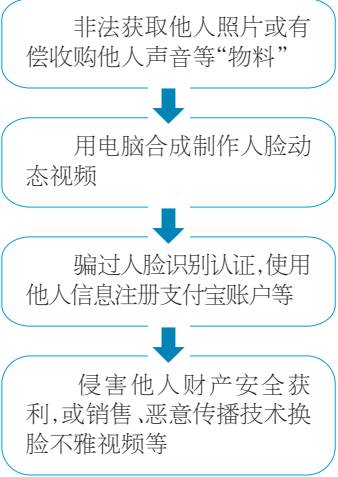
一段视频、一段语音未必是真人拍摄或者录制。在你不知道的手机App后台、支付界面、门禁闸机,或许有人正在盗刷你的脸……近年来,多地发生“变脸”诈骗案。

记者调查发现,随着深度合成技术迅猛发展,落地场景激增,一些不法分子趁机牟利。音频、视频等合成技术滥用,对人脸、声纹、指纹等个人敏感信息保护形成挑战。

一段段逼真的视频、语音竟是合成伪造的……

“变脸”诈骗案件频现 谁来为我护住“颜面”

不法分子一般作案流程



相关案例

变脸软件成帮凶,团伙“复活”涉诈微信获利百万

在“净网2021”专项行动中,江苏省南通市公安局网安支队会同如皋市公安局网安大队,成功破获一起新型网络犯罪案件,5名犯罪嫌疑人落网。

据如皋市公安局网络安全保卫大队办案民警介绍,他们接到公安部下发的一条案件线索,一名安徽籍涉案人员李某旗出现在如皋地区。“我们通过对嫌疑人的研判,发现嫌疑人在用一个前期被腾讯停用的微信账号。注册这些微信账号的都是一些偏远地区的人,他们注册了这些微信账号之后,都卖给了别人赚取一些蝇头小利,至于其他人拿这些微信账号来做什么,他们也不清楚。”

民警通过技术手段侦查到,被重启的微信均被境外诈骗分子所使用。而解除限制登录的关键是要进行人脸核验。可注册人分散在各地,召集到境外人脸核验不太现实。

男子谎称帮客户贷款,“刷脸”盗窃、诈骗被判刑

为了更加方便快捷,很多人在手机中设置了“刷脸”支付,只要掏出手机对准脸部进行人脸识别,就能轻松支付成功。虽然缩减了验证、支付的时间,可使用“刷脸”方式真的没有风险吗?安徽省马鞍山市雨山区人民法院审结一宗利用“刷脸”实施盗窃的案件,给公众以警示。

2020年5月19日中午,90后某保险公司业务员祝某在一家超市店内,以在手机上帮客户李某某贷款为名,让李某某“刷脸”进入其支付宝花呗,从李某某支付宝花呗贷款人民币10000元,后通过扫二维码的方式转进自己的支付宝账户。6月7日,祝某主动将人民币10000元归还给李某某。

当日,祝某还在李某某手机



图片来源新华社

“我们经过分析,怀疑背后存在一个为诈骗分子重新启用被限制登录的微信号的黑色产业链。”民警说。

专案组把突破重点锁定嫌疑人李某旗,并判断李某旗可能使用了某种生物特征的“变脸”技术,规避登录限制。

人脸核验的关键是微信注册人的身份隐私信息,嫌疑人李某旗是如何收集到这些信息的呢?

“不可能从微信使用人处获取照片,应该是通过非法的方式收购或者是获取了这个微信使用者本人的照片。”专案组经过甄别分析,发现从上游非法提供公民个人信息,到下游境外诈骗分子,都和嫌疑人李某旗有着千丝万缕的关系。由此一条黑灰色产业链浮出了水面。

民警通过对李某旗的微信聊天和银行转账分析发现,有4个银行卡账户有规律地向他的银行卡转账,而且金额比较固定。

根据银行账户信息,专案组又锁定了王某等另外4名犯罪嫌疑人,加上李某旗,显然是一个有组织有分工的犯罪团伙。

专案组派出抓捕小组,分赴安徽和浙江收网,抓获李某旗、王某等5名犯罪嫌疑人,成功打掉这个涉嫌获取公民个人信息,伪造人脸识别认证的犯罪团伙。在抓捕现场,民警发现了嫌疑人作案的20多部手机。

据犯罪嫌疑人李某旗交代,有一个QQ群时常发布要求重启被停用微信的小广告。他们看到后就会接单,然后分工。有的专门负责购买微信注册人的身份证号码以及头像照片,有的则用多个AI视频剪辑软件,把买来的照片制作成眨眼、张嘴、摇头的三色人脸动态短视频,解除限制登录,帮助诈骗团伙实施犯罪。

经审查,这个犯罪团伙重启的微信达一万多个,非法获利一百多万元。

别构成盗窃罪、诈骗罪。公诉机关指控的罪名成立。被告人祝某犯有数罪,应当数罪并罚。结合被告人犯罪的事实、性质、情节、对社会的危害程度,法院依法作出判决,被告人祝某犯盗窃罪判处拘役四个月,并处罚金人民币四千元;犯诈骗罪判处拘役三个月,并处罚金人民币一千元。决定执行拘役六个月,并处罚金人民币五千元。

网络支付平台正改变着社会公众的生活及消费方式,在享受网络支付带来便利的同时,广大市民也要提高警惕,保障个人通讯设备、账户信息及支付行为的私密安全。为防止电子账户、银行卡等被盗刷,切勿随意外借个人手机等通讯设备。

清华大学人工智能研究院基础理论研究中心主任朱军说,深度合成技术飞速演进,让“眼见不再为实”,破解身份核验的难度会越来越低,耗时将越来越短。

专家担心,尽管针对深度合成技术的识别技术不断迭代、检测手段持续增强,但依然没能跑赢“伪造”技术升级的速度。浙江大学网络空间安全学院院长任奎说,随着合成技术应用门槛的进一步降低,合成内容已模糊真实与伪造的边界。

北京智源人工智能研究院安全创新中心执行主任田天认为,新型伪造方法层出不穷,网络传播环境日趋复杂,检测算法存在漏洞缺陷等,反深伪检测难度越来越大。

法律规定相对滞后,也给不法分子留下可乘之机。中伦律师事务所合伙人陈际红说,目前法律规定,禁止利用信息技术手段伪造等方式侵害他人的肖像权,但技术如何使用算合理使用,哪些情形下应禁止使用等,没有具体规定;收集或收购个人声纹、照片,使用人脸、指纹、DNA、虹膜等个人生物信息等行为,在哪些范围内构成犯罪,将面临怎样的惩罚,需要司法裁判进一步给出明确指引。

律师建议规范合法使用边界,提高技术滥用违法成本

保护人脸、指纹、声纹等敏感信息,不再担忧信息“裸奔”损害个人隐私、财产、名誉等,是公众的共同期待。

我国首个国家层面的科技伦理治理指导性文件《关于加强科技伦理治理的意见》近日印发,凸显技术伦理治理的重要性紧迫性。在今年的最高法工作报告中,包括人脸安全在内的个人信息安全等多次被提及。

中伦律师事务所合伙人陈际红表示,打击“变脸”诈骗犯罪,应从技术的合法使用边界、技术的安全评估程序、滥用技术的法律规制等方面予以规范,提高技术滥用的违法成本。

中国工程院院士、信息技术专家邬贺铨提出,针对深度合成技术滥用现象,应以技术规制技术,利用技术创新、技术对抗等方式,提升和迭代检测技术的能力。

技术规制之外,针对技术滥用暴露的风险治理应当体系化、完善化。“要构建数据集质量规范,根据应用场景对相关技术进行风险分级分类管理,明确设计开发单位、运维单位、数据提供方的责任。”国家工业信息安全发展研究中心副总工程师邱惠君说。

专家提醒,针对花样翻新的“变脸”诈骗,公众要提高防范意识,不轻易提供人脸、指纹等个人生物信息给他人,不过度公开或分享动图、视频等;网络转账前要通过电话、视频等多种沟通渠道核验对方身份。一旦发现风险,及时报警求助。

本版稿件综合新华社、央视财经、南通新闻等



编辑:彭传刚 美编:马秀霞 组版:刘燕