

“AI诈骗潮”真的要来了？

新华社 毛鑫 王成 熊丰 高亢

通过AI换脸和拟声技术,10分钟骗430万元;AI虚拟人在聊天中筛选出受害者,人工接力实施诈骗……近期,多起宣称利用AI技术实施诈骗的案件引发关注。

记者近日与公安部门核实确认,“AI诈骗全国爆发”的消息不实,目前此类诈骗发案占比很低。但公安机关已注意到此犯罪新手法,将加大力度会同有关部门开展技术反制和宣传防范。

专家表示,随着AI技术加速迭代,由于使用边界不清晰,涉诈风险正在积聚,需要高度警惕。

“换脸”式诈骗引发焦虑

近日,内蒙古包头警方通报一起利用AI实施诈骗的案件,福州市某公司法定代表人郭先生10分钟内被骗430万元。据通报,骗子通过AI换脸和拟声技术,佯装熟人实施诈骗。

该案披露后,不少报道称需警惕“AI诈骗潮”到来,并曝光多起类似案件。如江苏常州的小刘被骗子冒充其同学发语音、打视频电话,小刘看到“真人”后信以为真,“借”了6000元给骗子。

那么,“AI诈骗潮”是否真的到了?

记者调查了解到,AI在技术上确实能做到换脸、拟音,但被用来进行“广撒网”式诈骗需要具备很多条件。

一位被列入公安部专家库的民警告诉记者,这类诈骗如果得手必须做到:收集到被换脸对象的个人身份信息、大量人脸图片、语音素材,通过AI生成以假乱真的音视频;窃取被换脸对象的微信号;充分掌握诈骗对象个人信息,熟悉其与被换脸对象的社会关系,综合作案成本很高。

他认为:“相关报道对一些案件的典型细节描述不够准确。AI涉诈案件仍属零星发案状态。”他说,成熟的类型化诈骗犯罪往往具有在全国多地集中爆发的特点,但当前没有成规模的AI诈骗类案件发生。

公安机关研判,近期网上“AI换脸换声诈骗在全国爆发”传言不实,全国此类案件发生不到10起,但该动向值得高度关注。网上一键换脸功能的App、小程序有技术滥用风险,需要加强技术防范反制等工作。

AI进入快速迭代期

“当前AI技术发展来到螺旋式上升的拐点,未来几年技术迭代将会按月计算。”香港科技大学(广州)协理副校长、人工智能学域主任熊辉说。

工信部信息显示,伴随AI技术快速发展,合成技术门槛持续降低,逐渐向低算力、小样本学习方向演进,利用手机终端即可完成,对算力和数据的要求下降明显。同时,随着AI大模型的技术加持,正逐步由面部合成向全身、3D合成发展,效果更加逼真。

国家开发投资集团特级专家、厦门美亚柏科AI研发中心总经理赵建强表示, AI技术正加速向网络诈骗、虚假信息、色情等领域渗透。如在一些网络平台上假冒明星、公众人物生成视频图像,吸引网民。此外, AI技术也可能被用来规模化地实施违法犯罪,如批量、自动维护网络账号,发送虚假信息,模拟人工在线聊天等。

值得关注的是,当前AI技术不再是实验室的半成品,引发热议的“换脸”“拟音”技术已有较成熟的开源软件,使用门槛低。



记者注意到,网络上不乏AI换脸教程。在国内某知名App上输入“换脸”,弹出的高频检索记录显示有“换脸软件”“换脸App免费”“换脸视频怎么做”“换脸算法”等。一条名为“史上最强AI换脸软件正式上线了!技术门槛大大降低”的链接,介绍了一款换脸软件,通过视频演示教程,手把手教授如何使用。

“老话说‘眼见为实’,但今后眼睛看到的也不一定是真实的。”北京市天元律师事务所合伙人杨虎城表示,未来涉及AI合成技术的诈骗、敲诈勒索等违法犯罪和肖像、名誉等民事侵权问题可能逐步显现。

工信部相关负责人表示,随着AI技术的不断发展,通过少量图片、音频信息合成特定视频,利用人工智能模型批量设计诈骗脚本等成为可能,客观上降低了电信网络诈骗的实施难度,AI类新型犯罪爆发可能性进一步提升。

尽快完善相关法规制度

中国移动信息安全中心品质管理处副处长周晶告诉记者,近年来,国际国内各界在积极探索深度合成技术的有效治理路径,研判AI技术给社会带来的风险和潜在威胁,正设法将AI技术发展纳入一定规则中,做到安全可控。

业内人士建议,要加强AI反制技术研究,“以AI制AI”。一些科技公司正加强对图像、声音伪造技术的反制研究,在公安、金融的视频认证场景已有应用。有一线民警建议,要加强AI安全技术应用研发,将AI技术应用于犯罪识别、预警、对抗中,实现以“白”AI对抗“黑”AI。

其次,加强源头治理和行业引导,及时更新、完善相关法律、标准、规则,为AI技术发展保驾护航。

“数据是AI犯罪的源头,保护好公民的个人隐私数据安全,就能在最大程度上降低AI违法犯罪的能力。”熊辉说。

中国互联网协会监管支撑部主任郝智超建议, AI技术发展还要有相关法律法规来划红线、踩刹车。需进一步加强对个人隐私数据泄露问题的关注,明确信息监管红线,对AI技术的研发、传播、使用做到有规可循,并根据技术发展实际情况,及时完善对技术服务商行为的规范引导。

此外,还要有针对性地加强反诈宣传。熊辉表示,未来AI可根据大数据创造出无比接近真实的“真实”。“要通过不断的教育改变大众观念,让人知道眼见不一定为实,有图不一定有真相,提升对网络信息的辨识力。”他说。

公安部有关负责人表示,当前,诈骗集团利用区块链、虚拟货币、远程操控、共享屏幕等新技术新业态,不断更新升级犯罪工具,与公安机关在通讯网络和转账洗钱等方面攻防对抗不断加剧升级。公安机关会同相关部门与诈骗分子斗智斗勇,不断研究调整打击防范措施,确保始终保持主动权。

论文代写 —— 一条龙, 中介干成 老字号

《半月谈》吕梦琦 陈志豪

毕业季临近,“枪手代写”毕业论文现象有所抬头,“论文包过”“开题答辩一条龙服务”此类宣传用语在一些网络平台上并不鲜见。论文代写,严重违反诚实信用原则,践踏公平学术环境,助长畸形商业模式,这一不良风气和相关非法产业链亟须加强整治。

购物平台能买论文

尽管早有规定,但参与学位论文买卖、代写这类现象仍难以杜绝。受访学生中,超过半数大学生表示知道能“买”毕业论文,一些大学生表示他们身边就有同学正在找枪手代写论文。

记者调查发现,找“枪手”代写毕业论文主要是通过线上进行。一些购物平台成为论文代写隐秘的主要渠道。记者在某购物软件上输入“论文代写”,跳出来的页面显示相关法律法规作为警示,但输入“论文”“论文辅导”等关键词,页面显示的多个商家图标中包含“毕业论文”文字。记者联系多个客服询问是否可以代写论文,客服均表示可以。

通过交流得知,论文代写中介是通过题目、字数、专业、重复率、学历以及是否需要毕业设计来定价,价格通常在1000到1万元不等,一周左右就可完成,赠送后续隆重、修改服务,“一条龙”周到服务至学生毕业。一些中介的朋友圈聊天框截图显示,近期咨询量和成交量都在急速增长。

市场日渐成熟危害大

多名代写中介直言不讳,机构已经开设多年,服务链条成熟,每年到毕业季都会有不少订单。记者调查发现,如何寻找“枪手”,在新老大学毕业生中口口相传,这让很多大学生心存依赖和侥幸,平时不好好学习。

一名购买过毕业论文代写服务的学生表示,自己上学时疏于学习,写论文难度较大,只能找代写中介。“网上价格也很‘合理’,比自己写论文省事多了。”

另外,毕业论文代写者门槛并不高。记者联系了北京、太原、郑州等地多家代写中介,介绍自己是某211大学在读硕士后,想当论文“枪手”,商家表示马上就有相关论文分派,并不要求出示相关证件。

由于“枪手”通常是同专业的硕士、博士研究生,他们代写出的本科论文水平大多高于本科学生,往往在最后评选时获得高分,这极易引起原创毕业论文的学生不满。山西某高校一名往届毕业生回忆,自己毕业时知道身边有同学在找枪手代写论文,但又怕惹麻烦,不敢向学校举报。

论文代写,削弱了高校毕业生的创新能力,严重破坏了高校学习风气和公平公正。太原理工大学环境工程学院副教授温月丽认为,论文代写等于把高校毕业生归纳总结、理论升华的能力培养方式消解掉了,这类学术造假的歪风必须坚决刹住。

提高论文代写的失信成本

遏制源头需求,增加论文代写违法成本。中国人民大学法学院教授刘俊海表示,要打击论文代写现象,一定要提高论文代写的失信成本,使论文代写的造假成本高于造假收益。

论文代写,如果涉案金额巨大,则可能构成非法经营罪,将追究经营者的刑事责任。专家建议,增加对论文代写中介的惩治力度,不断完善法律法规,强化追究刑事责任,避免过于依赖罚款、黑名单等方式弱化打击效果。

相关部门要加大对论文造假的审查力度。太原理工大学化工学院讲师王斌认为,为整治论文代写现象,高校一方面应该加大惩处力度,另一方面应该加强对论文原始数据的保存和监管,以便发表前核查。