“AI诈骗潮”真的要来了?

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。

CFP供图

“换脸”式诈骗引发焦虑:你会被亲友的脸骗到吗?

近日,内蒙古包头警方通报一起利用AI实施诈骗的案件,福州市某公司法人代表郭先生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”是否真的到来了?

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身份信息,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,涉诈犯罪风险正在积聚

“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。

“从现有案例看,这些技术已被不法分子利用。如假冒明星换脸直播、一键脱衣、造谣、制作色情视频等。虽然AI诈骗案件未成气候,但这一趋势值得关注,必须提早防范。”一位反诈民警说。

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,为AI技术发展立规画线

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中已有应用。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画红线、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,与公安机关在通信网络和转账洗钱等方面的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。

工信部表示,下一步,将强化监管执法,积极会同网信、公安等部门,督促企业健全完善深度合成信息管理及技术保障措施;鼓励技术攻关,凝聚产学研用各方力量,提升深度合成风险技术防范能力;加强行业自律,建立健全深度合成技术相关行业标准、行业准则和自律管理制度,督促指导深度合成服务提供者和技术支持者制定完善业务规范、依法开展业务和接受社会监督。

新华社记者**毛鑫**

新闻评论

警惕AI诈骗“防不胜防”

AI技术迅猛发展,带来无限商机的同时,层出不穷的骗局也随之而来。近日,#AI诈骗正在全国爆发#话题登上热搜,这些骗局巧妙地躲过层层人为设置的防线,迷惑性极强。

仿真人行骗竟让真正的人防不胜防。一方面是行骗过程真伪辨认难度系数更高,另一方面则是骗子的针对性也更强。

漫无目的地全面撒网早就“过时”,骗子们通过AI技术筛选受骗人群,别有用心地锁定特定对象。不同的骗术对应不同的人群,比如,一些金融诈骗,骗子会筛选那些搜集投资信息的人“优先”行骗。

人工智能诈骗席卷而来,提醒人们技术不仅解放人类生产力、便利日常生活,还带来了极高的风险。这些风险系数升高、防范难度加大,并在不同领域持续蔓延。

AI技术无边界地滥用,涉及非法盗取企业数据、私人财产,还会引发肖像权、知识产权等领域的纷争。眼下大火的“AI伴侣”,通过换脸来制作明星甚至普通人的不雅视频、AI歌手随意模仿翻唱一切,都把人工智能的风险指数一再调高。

作为个体,做好个人隐私保护、数据安全管理责无旁贷。无论是出于什么情景,对于任何可能造成风险的隐患,都要严格授权,三思而后行。在实操中发现问题,及时报警,用合法手段维护自身利益。

同时,对于越来越丰富的支付场景,所有使用人的面部、声音、指纹等生物信息,必须依法依规。企业对相关信息的处理使用,必须严格遵守规范,“越界”和“打擦边球”都要时时警惕,泄露、倒卖、滥用个人信息必须严惩,最大限度地遏止违规黑色产业链滋生。

在人工智能时代,当数字人无限接近于真人,极真实地模拟人的声画,让虚拟的一切融入我们的社交生活中,人类与数字人共存,如何保卫人的财产安全和合法权益成为一个严肃的话题。而只有真正的人的权益得到了很好的保护,科技才是真正被善用。

陶凤