

视频确认了 钱还是被骗了

近期多起宣称利用AI技术实施诈骗的案件引发关注
但“AI诈骗全国爆发”的消息不实

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: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,伪装熟人实施诈骗。

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。

“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技术发展立规划线

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违法犯罪的力量。”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别力。”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。

小贴士

AI诈骗常用手法

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。

AI换脸

因为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。

转发微信语音

在盗取微信号后,骗子便向其好友“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),可实现语音转发。

AI筛选受骗人群

骗子不是漫无目的地全面撒网,而是根据所要实施的骗术,通过AI技术筛选受骗人群,别有用心地锁定特定对象。例如,当进行金融诈骗时,经常搜集投资信息的小伙伴就会成为他们潜在的目标。

如何防范

多重验证,确认身份

●在涉及到转账交易等行为时,小伙伴们要格外留意,可以通过电话、视频等方式确认对方是否是本人。

●在无法确认对方身份时,可以将到账时间设定为“2小时到账”或者“24小时到账”,以预留处理时间。尽量通过电话询问具体信息,确认对方是否为本人。

●即便对方运用AI技术行骗,也可以通过提问的方式进一步确认身份。建议大家最好向对方的银行账户转账,避免通过微信等社交软件转账。一方面有利于核实对方身份,另一方面也有助于跟进转账信息。

保护信息,避免诱惑

●加强个人信息保护意识,小伙伴们要谨防各种信息泄露,不管是在互联网上还是社交软件上,尽量避免过多地暴露自己的信息。

●对于不明平台发来的广告、中奖、交友等链接提高警惕,不随意填写个人信息,以免被骗子“精准围猎”。

相互提示,共同预防

●这些高科技手段的诈骗方式,迷惑了很多小伙伴。警察也提示各位要多多提醒、告诫身边的亲人、朋友提高安全意识和应对高科技诈骗的能力,共同预防受骗。

●做好家中老人的宣传防范工作。提醒老年人在接到陌生电话、短信时,要放下电话,再次拨打家人电话确认,不要贸然转账。

拒绝诱惑,提高警惕

●小伙伴们要学会拒绝诱惑,提高警惕。避免占便宜心理,警惕陌生人无端“献殷勤”。

●如果事先不知道骗子的这些伎俩,被骗的可能性非常大。还是那句话:你目前还没被骗,并不是因为你多聪明,也不是因为你没钱,而是适合你的“剧本”还在路上。

(综合新华社、工信部反诈专班)



扫码看更多防骗知识

