

□晚报记者 时晨

近期,一条“接到陌生来电先沉默三秒”的安全提示在短视频、朋友圈广泛传播,引发滨州市民热议。提示所说的套路,是不法分子拨通电话之后保持静默,引诱接听者下意识说出“喂,你好”“请问您哪位”等应答,短短数秒语音,就能被AI提取声纹样本,克隆出相似度极高的声音,进而冒充亲友身份实施电信诈骗。相关部门提醒广大市民,擦亮双眼,警惕生物信息被悄悄窃取。

接陌生来电 先沉默三秒? AI时代,守护好你的“生物钥匙”



陌生来电静默设圈套 AI声纹克隆悄然来袭

织密防护网络
多方发力守护“生物钥匙”

“我平时接电话,第一反应就是‘喂,哪位?’没想到这一句简单应答,就有可能被骗子采集声音。”家住滨城区的张女士,了解到AI声纹诈骗套路后,连连感慨防骗知识需要持续更新。她告诉记者,自己家中老人经常接到陌生推销、回访电话,老人习惯主动搭话,现在她已经叮嘱家人,接到不明来电,不要立刻出声。

市民杜先生是一名企业上班族,他向记者坦言,自己之前看过AI换脸诈骗新闻,知道照片和视频有合成风险,但从来没想

到一通陌生电话里藏着窃取声纹的陷阱。“以前总觉得诈骗离自己很远,骗子无非是骗银行卡密码,现在耳朵听到的声音、视频里看到的人脸,都有可能

是伪造的,真是眼见不一定为实,耳听不一定为真。”
相关人士表示,这种沉默来电是AI新型诈骗的前置手段。不法分子获取几秒语音样本后,借助AI语音合成工具,复刻当事人声线、语气,随后冒充本人,向其家人、朋友发起视频或者语音通话,编造车祸、突发疾病、资金周转等紧急理由,利

用亲情、友情制造紧张氛围,诱导对方快速转账,视频通话时神态、声音高度模仿普通人,突破传统反诈辨别方式,迷惑性极强。这类骗局对中老年群体危害更大,老年人对视频通话信任度高,紧急情况下很难分辨真伪。工作人员给出实操建议:接到陌生来电,先保持沉默三秒;如果对方长时间不说话,直接挂断。凡是亲友通过视频、语音紧急借钱,务必通过另外一个号码回拨核实,多方确认之后,再考虑资金往来。

生物识别技术给生活带来便捷,与此同时,治理AI滥用、保护生物信息,需要监管平台、企业、市民多方协同发力,构建全链条防护体系。

最高人民法院明确规定,非法获取、出售、提供人脸照片、视频等公民个人信息,情节严重的,构成侵犯公民个人信息罪,将依法追究刑事责任。相关部门持续开展专项整治行动,重点打击非法采集、买卖生物信息,严查AI换脸、声纹合成诈骗黑灰产业链,保持高压打击态势。

平台企业需要守住源头关口。相关行业人士表示,互联网平台、AI企业,要把合规审查嵌入数据采集、模型训练、产品上线整个流程,严格落实“非必要不采集、非授权不使用”。采集生物信息前,清晰告知用户采集目的、存储周期、数据用途,完善加密存储机制,防止数据泄露。

普通市民,作为生物信息的所有者,是最后一道也是最重要的防线。记者采访了社

区网格员李女士,她常年的小区开展反诈宣传。她提醒居民,树立“非必要不提供”的原则,谨慎授予APP人脸、麦克风等权限。社交平台不要随意发布清晰正面自拍、家庭语音视频;不要在不明网站、小程序上传人脸视频。线下遇到扫码礼品、免费检测,对方要求刷脸、录音,一定要问清采集主体、用途,拿不出合规说明,坚决拒绝。一旦发现非法采集生物信息、疑似AI诈骗线索,可以拨打96110、12339举报电话提交线索。

AI技术是一把双刃剑,便利生活的同时,新型风险随之而来。在滨州,反诈、网信、社区等各方持续开展常态化科普宣讲,走进乡村、社区、企业、校园,普及生物信息保护知识。

守护好我们独一无二的“生物钥匙”,既要依靠法律监管、平台自律,更离不开每一位市民提高警惕,绷紧生物信息安全这根弦,共同筑起抵御AI滥用诈骗的全民防线。

AI技术升级 生物信息安全面临多重风险

人脸、声纹、指纹、虹膜、步态,都属于敏感生物特征信息。和普通姓名、手机号不同,这类信息与生俱来,具有唯一性,一旦外泄,终身无法重置。随着AI图像、语音解析能力持续增强,不法分子窃取生物信息的方式也变得更加隐蔽,很多时候属于“无感窃取”,当事人察觉不到信息已经被采集。

不少市民在记者走访中提到,刷脸已经成为生活常态,手机解锁、登录APP、活动领礼品等,都要求刷脸认证。退休市民王大爷说,集市上偶尔有扫码送鸡蛋、纸巾的活动,拿出手机就

要人脸核验,当时只想着领小礼品,根本没想过对方为什么要采集人脸。

过度采集,悄悄抓取生物数据。相关人士解释,一些非法APP、不明营销活动,打着身份核验名义,超出业务必要范围采集人脸、声纹信息。AI还可以从短视频、社交平台公开照片、语音素材,批量提取生物特征,不需要当事人现场配合。按照法律要求,采集生物信息必须遵守“最小必要”原则,非必要不采集,不能强制刷脸。

深度伪造,催生新型违法犯罪。AI深度伪造技术,让虚假视

频、语音制作门槛大幅下降。不法分子拿到人脸照片、简短语音,就能生成动态视频、合成语音,用于冒充身份诈骗、网络造谣、伪造聊天记录。一旦被AI伪造影像造谣抹黑,当事人维权取证难度大,个人名誉会遭受严重损害。

信息整合,衍生更深层次安全隐患。AI还能够通过人脸影像、步态数据,推算年龄、体态、情绪特征等。生物信息泄露,风险早已不止财产损失,延伸到个人隐私、国家安全等多个层面。