

生成图像、合成语音、伪装客服、伪造场景……

以假乱真的 AI 诈骗,如何防范?

上传一张静态照片,即可生成动态视频;只需几秒语音,就能克隆声音……这不是科幻电影,而是发生在身边的真实事件,“AI换脸”正成为侵权违法的重灾区。

近期,为规范应用人脸识别技术处理人脸信息活动、保护个人信息权益,国家互联网信息办公室、公安部联合公布《人脸识别技术应用安全管理办法》,对应用人脸识别技术处理人脸信息的基本要求和处理规则、人脸识别技术应用安全规范、监督管理职责等作出了规定。办法将于2025年6月1日起施行。

人脸识别技术应用与人脸信息安全紧密相关。人脸识别具有唯一性、不可更改性、不可匿名性,一旦泄露,极易对个人的人身和财产安全造成危害,还可能威胁公共安全。



(网络图)

AI 诈骗形式多样

换脸、变声、对口型

贵州省黔东南苗族侗族自治州凯里市公安局反诈中心负责人吴西福介绍,一家科技公司的负责人郭先生有一天接到好友打来的视频电话,说自己正在外地投标,需要几百万元保证金,想用郭先生的公司账户走一下账。不久后,好友说已经把钱转到郭先生的账户并截图证明。郭先生觉得通过视频能看到好友本人,便没等收到转账成功的通知就给好友转了钱。后来,郭先生迟迟没收到转款,联系好友时才发现自己被骗。

宁夏回族自治区银川市某公司部门经理张先生接到“老板”视频电话,对方称因情况紧急,急需转账汇款。在视频中确认是“老板”后,张先生放下了戒心,十几分钟内将20万元转入指定账户。直到下午当面汇报工作时,张先生才发现上当受骗。

这些案件都是典型的AI诈骗。“你以为在和朋友亲人视频聊天,其实是骗子使用的‘AI换脸’技术,让别人的嘴能够‘对口型’。”宁夏回族自治区公安厅刑侦总队副队长、反诈中心负责人吴克刚介绍,如今,“AI换脸”技术不仅限于静态照片的活化,还能在即时视频通信中实时换脸。虽然需要采集大量不同角度的照片进行模型训练,

但一旦成功,便可以假乱真。过去,公民个人身份证号、手机号以及家人信息需要重点防范,现在,人脸、声音、指纹等同样要避免泄露。

新型AI诈骗主要有以下类型:语音合成诈骗,不法分子利用AI技术,合成受害人亲友或熟人的声音,让受害人误以为是亲友或熟人需要帮助,进而实施电话诈骗;图像生成诈骗,不法分子通过AI技术,生成虚假的照片或视频,制造出受害人亲友紧急且合理的情景,从而获取个人信息,骗取钱财;智能客服诈骗,不法分子利用AI技术,制作智能客服系统,通过语音或文字同受害人交流,诱骗受害人提供个人信息或进行转账操作;AI情感诈骗,不法分子运用AI训练面向网聊的大语言模型,通过伪造场景、声音与受害人建立情感关系,进而获取个人信息。

吴西福介绍,共享屏幕等新型诈骗也要注意。不法分子以“提升信用卡额度”“航班延误退费”“赠送礼品”等为借口,向个人发送短信或拨打电话,诱导受害人下载指定软件,并开启软件的“共享屏幕”功能,就可以“实时监控”受害人手机、电脑屏幕,同步获取个人银行账户、口令、验证码等重要信息,从而盗取银行卡资金。

相较于电信诈骗、网络诈骗,新型AI诈骗的受害者身份更广泛、多元,成功率更高,更难以追踪。

警方梳理后发现,新型AI诈骗有以下危害:造成经济损失,新型AI诈骗具有针对性强、高度逼真等特征,普通群众短时间内难以分辨,很容易上当受骗、遭受经济损失,甚至会给家庭带来沉重的经济负担;发生信息泄露,新型AI诈骗往往能获取受害人的个

AI 诈骗危害广泛

造成经济损失、心理创伤

人信息,包括身份证号、银行账户、人脸、指纹等,进而滥用这些信息从事非法活动,导致受害人信息泄露,身份被盗窃,引发潜在的法律风险;造成心理创伤,遭受新型AI诈骗,除了面临经济损失,受害人还可能产生焦虑、自责、抑郁等情绪,造成严重的心理创伤;危害社会治安,如果新型AI诈骗案件变多,容易让群众对社会产生不信任感,甚至造成恐慌情绪,有些受害者也因

无法承担损失,走上违法犯罪道路。

新型AI诈骗案件增加,侦破难度加大,对公安机关来说也是挑战。吴西福说,只有不断提升民警的专业素质和侦查能力,加强对新型电信网络诈骗犯罪的研究,才能创新侦查手段和方法,提高打击效能。要加强与其他地区公安机关的协作配合,建立健全跨区域警务合作机制,形成打击合力。

有效防范 AI 诈骗

保护个人信息、学习识别方法

新型AI诈骗花样频出,伪装性越来越强,该如何防范?

吴克刚给出了两条防骗建议:视频通话时,让对方做出指定动作,比如眨眼3次、摸摸鼻子,或者让对方用手指或其他遮挡物在脸前晃动,如画面出现延迟或者异常扭曲等不自然的微小变化,那对方很可能正在使用“AI换脸”技术。在与对方的沟通中,也可以问一些只有对方知道的问题,比如生日、电话号码、喜好等,来验证对方身份的真实性。

我们也应该提高安全防范意识,防止个人脸部信息被非法获取利用。贵州警方提示,不轻信他人,不贪图小便宜。妥善保管个人信息,把个人信息保护的第一道关。在非必要时,不向陌生人提供身份证号码、工作单位、家庭住址、职务等重要信息,不将身份证照片或号码保存

在手机中,尽可能避免将人脸、照片、声音、指纹等留存到网站和小程序上。在日常生活中,加强对人脸、声音、指纹等生物特征数据的安全防护,做好个人手机、电脑等终端设备的软硬件安全管理,不登录来路不明的网站,以免感染木马病毒。另外,对可能进行声音、图像甚至视频和定位等信息采集的应用,做好授权管理,不轻易给他人收集个人信息的机会,也能在一定程度上远离“AI换脸”诈骗。

此外,公安机关也要创新线上线下反诈宣传,打造全方位反诈宣传矩阵。一方面,利用线上平台,深入挖掘本地发生的电信网络诈骗典型案例,结合地区特色、民俗以及当下流行的网络文化,拍摄制作风格独特、通俗易懂的反诈宣传短视频。通过短视频的形式还原诈骗分子的话术、作案流程以及背后的犯罪逻辑,帮助

群众提高反诈意识。

推动反诈宣传进校园、进社区、进企业,将反诈宣传与群众喜爱的文化娱乐活动紧密结合,打造出一系列具有贴近性的反诈宣传场景。坚持精准施策,针对不同群体、行业和地区特点,开展有针对性的宣传,做到有的放矢,切实增强群众防骗意识和识别能力。

警方也警告不法分子:通过“AI换脸”进行视频合成、实施诈骗的行为,是利用新技术进行的诈骗,与传统诈骗行为没有本质区别。对于构成诈骗罪的,将依照我国刑法第二百六十六条的规定追究刑事责任;对于为利用“AI换脸”实施诈骗行为提供技术支持、帮助的,将根据反电信网络诈骗法的规定进行行政处罚,构成犯罪的,还要追究刑事责任。

(据《人民日报》)