舟山晚报
2023年7月5日 星期三 责任编辑 陈海维 版式设计 丁页

“AI换脸”诈骗现涉政苗头

作案从广撒网向精准施骗转变

近日，北方某地警方发布了一起利用“AI换脸”对当事人实施诈骗的案件。诈骗分子运用人工智能技术，通过微信视频通话与受害人进行了十多分钟交流，受害人转账数百万元。

引人关注的是，该案不仅是一起新型网络诈骗，更是一起涉政诈骗案件。

不法分子模拟伪造的，是受害人认识的一名领导干部。在微信视频聊天中，“换脸”后的骗子提出，其朋友有一笔工程保证金需要借用受害人公司的对公账户走账。在视频画面中，骗子“换脸”后面部表情自然，声音逼真，受害人便放松了警惕，转账后打电话确认，才知道被骗。

“AI换脸”“AI拟声”、虚拟场景构建……随着设备性能提升和技术软件优化，利用“AI换脸”技术实施诈骗，已成为一种新型网络诈骗。近期，各地曝出多起人工智能“辅助”诈骗案件。一些不法分子利用人工智能“深度伪造”冒充领导干部行骗，值得引起高度警惕。

由于工作原因，一些领导干部的面部、声音等生物特征信息更易被获取，被人工智能学习利用后造成的潜在危害性也更大。接受《瞭望》新闻周刊采访的业内人士表示，社会各界都应提高识骗防骗意识，有关部门应依法加大对人工智能“辅助”诈骗案件的执法力度，严肃追究相关人员法律责任。

眼见不一定为实

近日，华北某地一名地方干部正为一件事犯愁。有人冒用他的名义，与他的亲朋好友大范围添加微信好友。

“和我的亲戚朋友加完好友后，骗子还给他们打了视频电话。通话时间只有几秒钟，朋友们感觉声音、画面都有点儿像。”这名干部说，直到许多朋友打电话询问具体情况，他才知道此事。

“估计下一步就要开始骗钱了。所以，最近几天我连续发了好几条朋友圈提醒大家。”这名干部说。

受访业内人士表示，只要有足够的图像、音频素材，不法分子就可以通过人工智能“换脸”软件、合成声音软件伪造虚拟形象，实施诈骗。“只需提取最少10个字、最多32个字，就可以合成其声音。”国网信息通信产业集团安全科研专家赵明明告诉记者。

一些领导干部由于工作原因出镜率相对较高，这为骗子提供了丰富的面部识别素材；在电视、广播新闻中也可以找到一些领导干部的大段同期声，这令“伪造成本”更低。

在一些案件中，不法分子通过“AI换脸”合成视频等方式，伪造与领导干部见面、合影等实施诈骗，增加了涉政类诈骗的欺骗性和危害性。

AI诈骗四大趋势

中国信息通信研究院相关负责人表示，当前，人工智能“辅助”诈骗存在四大趋势。随着人工智能技术的普及应用，不法分子实施诈骗的精准性、迷惑性、隐蔽性增强，公安、检察等政法机关办案将面临侦查破案难、电子证据调取难、认定处理难等现实困难。

——技术成本由高向低转变。腾讯安全玄武实验室负责人于旸告诉记者，随着技术发展，人工智能“深度伪造”“深度合成”已成为一种可以低成本实现的技术。

——技术应用由单一向多元转变。腾讯互联网安全专家杨建表示，实施人工智能“辅助”诈骗一般要满足多个要素，包括非法获取信息、构建熟人账号、“换脸换声”、破解手机摄像头权限等，涉及多项技术手段。

——伪造身份从模糊向具体转变。传统电信诈骗往往只能以“某派出所工作人员”“某网站客服”等模糊虚指人设实施。但在人工智能“辅助”诈骗中，骗子可以以具体的人物形象出现。

——作案模式从“广撒网”向精准施骗转变。社交媒体平台往往设有视频验证环节，这在客观上增加了冒充熟人、领导干部等诈骗的“可信度”。受访专家分析，随着技术发展，精准盗号、分析关系网等有指向性的网络诈骗案件占比可能有所上升。

多层面约束规范

奇安信安全专家裴智勇表示，目前，专业级别的人工智能“深度伪造”仍需通过较强的硬件在实验室环境实现。这意味着，近期“AI换脸”诈骗形成系统性风险的可能性不大，但仍需未雨绸缪、预防打击。

在源头端，需要进一步加强公民个人信息保护。杨建等专家建议，加强公民信息尤其是生物特征等隐私信息的技术、司法保护力度。针对冒充领导干部等涉政诈骗风险，可通过规范领导干部个人社交账号管理，普及提升账号安全意识等方式进行规避。

在技术层面，数字水印鉴伪等技术有待进一步普及利用。赵明明表示，数字水印能将特定的信息嵌入音频、图片或是视频等数字信号中，进行版权保护，以防止未经授权的复制和拷贝。他建议，加强打入数字水印、开发真伪鉴别等技术治理手段，使其为数字内容生产商以及用户端等提供广泛服务，以科技手段制约不法分子利用人工智能技术实施犯罪。

瑞莱智慧高级产品经理张旭东建议，对涉及政务、安防、金融、消费等重要应用的人脸识别技术漏洞进行完善和升级，防范不法分子通过后台劫持手机摄像头权限。

从法律制度方面看，反电信网络诈骗法、刑法等法律为打击治理各类网络诈骗活动提供了法律支撑。赵明明建议，进一步完善人工智能等领域相关法律，通过案例等指引，建立人工智能侵权纠纷法律框架、诉讼程序和赔偿标准等。

此外，还需通过完善相关制度进一步落实平台责任。新华三集团安全专家曹亮表示，对核心领域使用人脸识别技术的产品，监管部门应建立分级别、多层次的国家安全标准及行业安全标准；压实平台、企业主体责任，督促相关应用开发企业履行源头审查责任；建立健全用户注册、算法机制机理审核、数据安全个人信息保护、反电信网络诈骗、应急处置等管理制度。

据《瞭望》新闻周刊公众号“瞭望”