

揭秘“AI换脸”诈骗黑色产业链

如今,“刷脸”已是生活日常。出入小区、超市买菜、手机登录……一个简单的动作,就能完成身份验证。然而,一张无法更改的“脸”,一旦被不法分子盗用,后果不堪设想。

近期,山东青岛胶州市警方破获一起案件,不法分子利用AI技术合成动态人脸视频,进行虚假实名认证,实施诈骗等犯罪行为。

新华社记者
吴书光 邵鲁文 王凯



数万条人脸信息现身“网络黑市”

记者从胶州市警方获悉,胶州市公安局网络安全保卫大队侦破了一起利用“AI换脸”技术突破实名认证的重大侵犯公民个人信息案件。

据办案民警介绍,犯罪嫌疑人在境外聊天工具上以每条5元到10元的价格购买大量公民个人信息。这些信息包含姓名、身份证号以及证件照等。

随后,他们借助境外AI工具,将非法获取的公民照片放大、变清晰,并合成“眨眼”“摇头”等动作,生成虚假动态人脸视频,进而用其注册实名账号。胶州市公安局网络安全保卫大队三中队中队长刘正大介绍,注册好的账号很多被犯罪嫌疑人以30元到50元不等的价格售卖。

截至案发,胶州公安围绕资金流、信息流对整个犯罪链条进行追溯,奔赴4省开展抓捕行动,共抓获犯罪嫌疑人14名,查封电脑和手机80余部、云服务器60台,缴获AI合成动态人脸视频5万余个。该团伙已贩卖

账号8万余个,非法获利60余万元。目前案件已移交检察院审查起诉。

办案民警介绍,抓获的犯罪嫌疑人年龄大多20来岁,最小的刚满18岁;他们大多没有工作,平日沉迷网络。

青岛市律师协会副监事长、山东德衡律师事务所律师姜保良表示,当前一些受教育程度较低的年轻人,辨别是非能力差,在境外网络接触了不良信息或受旁人蛊惑,很容易走上违法犯罪道路。随着AI工具越来越便利,使用AI从事违法犯罪行为的门槛变低,犯罪“成本”也大幅下降。

非法信息从哪来? 账号用于何处?

记者采访了解到,这起案件背后的利益链条和“运作模式”,既清晰又隐蔽。

办案民警告诉记者,在一些境外不法平台上,众多包含姓名、身份证号以及照片的公民个人信息被售卖。这些信息的来源,有的是境外网络黑客侵入了某些防护能力较弱的机构,有的是一些单位的“内鬼”私自卖出

公民个人信息;这些数据在境外平台经过层层倒卖,出现在一些不法平台上。

记者了解到,犯罪嫌疑人利用搭建的云服务器上的云手机工具,在一些主流社交、短视频平台上注册账号。注册时,他们通过一款名为“虚拟相机”的AI软件,在平台要求人脸认证的环节,不调用手机摄像头,而是直接使用事先制作好的合成视频来通过验证,以此批量注册大量实名账号。

据办案民警介绍,犯罪嫌疑人售卖这些账号,下游买家用来发布境外赌博、色情网站信息。他们之所以使用这类通过人脸识别注册的账号,是因为实名认证账号的信息发布权限比非实名账号更高,便于向非法网站引流。

从购买个人信息到制作视频,再到后续交易,整个过程使用的网络软件服务器均在境外,交易多使用虚拟货币,在一定程度上给网安部门带来了较大的侦办难度。

受访专家认为,随着AI工具迭代升级,一些图像生成模型合成人脸活动视频的能力很强,足以“以假乱真”。人脸信息在账号

注册、交易支付等方面使用广泛,一些不法分子盯上了这一领域。

奇安信集团网络安全专家刘夕铭说,当前普遍使用的人脸识别技术,主要是对脸部特征数据进行采集,比如眉眼间距、颧骨轮廓等,形成一个人脸特征的数据包,再上传到服务器进行比对。但有一些不正规的公司或者别有用心的公司,为了利益,在人脸验证环节,采集的不是人脸特征数据,而是完整的照片和背景。

“这些数据一旦被用于非法用途,比如‘AI换脸’诈骗,或是注册一些非法账号、伪造不雅照片进行敲诈勒索,不仅是对个人隐私的泄露,更会对用户的日常生活造成影响。”刘夕铭说。

守护每个人的“脸面”

多名专家认为,面对AI时代侵害公民信息的行为,应构建全链条、多层次、系统化的防护体系,全社会共同参与,充分保障公民个人信息。

基层公安民警介绍,公安机关一直在持续深化全链条打击,强化预警防控,对网络黑灰产、AI技术滥用、非法买卖账号、侵犯公民个人信息等犯罪保持高

压严打态势;同时,加强对重点平台、重点领域、重点人群的风险排查,推动从被动破案向主动预防转变,最大限度预防和减少案件发生。

提升侦办、打击的技术力量也是杜绝公民个人信息泄露案件的重要着力点。山东大学法学院教授胡常龙建议,公安机关应持续提升网络犯罪侦查技术水平,加强电子数据取证实验室建设,配备先进的AI伪造内容检测工具。要深化警企合作,公安部门与互联网企业、网络安全研究机构应建立长期性、常态化协作机制,针对平台漏洞和新型攻击手段及时提醒并共同防御,共同研发反制AI合成视频的检测算法。

受访专家还建议,加强平台监管,普及青少年网络社会教育。姜保良等法律工作者建议,压实网络平台主体责任,完善举报取证流程。平台应提升用户发言门槛,优化算法技术,减少极端内容推荐,不断升级异常内容的识别技术,设立“举报一删除一溯源追责”闭环流程。

此外,专家建议,进一步普及、完善道德法治教育,将人工智能时代下网络素养相关内容纳入中小学课程,引导广大青少年树立良好的网络价值观。

40层住宅每层两梯五户,一部电梯更换延期苦了业主 快两个月了,业主回家等电梯一等数十分钟

紫牛热点

近日,合肥一名业主在社交平台上发帖吐槽称,自己所住楼栋正在更换电梯,可迟迟未能到位,目前只有一部能使用,导致近两个月的时间里每天下班回家坐电梯都要“排长龙”,数十分钟等待是“家常便饭”。6月22日,扬子晚报/紫牛新闻记者从小区物业处得知,更换的电梯这几天就能安装到位。“因为这

段时间中、高考,所以延误了时间。”物业人员解释说。

这位业主多次记录了回家乘坐电梯的“心路历程”,从发帖时间看,多数集中在傍晚6点多。“无一例外,每天都是40分钟。”该业主吐槽的同时还配了图片(见右图),可以看见沿着走廊排着长长的队伍。6月21日,该业主再次记录了等电梯的过程,并标注称,“排队回家的第54天”。该业主表示,发帖只是单纯的希望能有幸被相关部门看到,解决日常出行的难题。

很多网友表示诧异,下班回家要排队等电梯?等个电梯还要这么长时间?对此,业主回帖解释说,自己这一栋是40层,一层两梯五户,但是有一部电梯老是出故障,动用了维修基金重新换了一部。“4月30日开始换的,说好的6月15日交付,现在延期了,物业相关部门也没给确切交付时间!”

“电梯在换新的,只有一部能用,总高40层,我们骑手都怕接这栋楼的订单,低层能爬就爬,高层不值得去爬了,一单就几块钱配送费!”一位外卖小哥

留言说。

据了解,被吐槽的这栋住宅楼位于合肥市蜀山区某小区的西区。6月22日下午,记者拨通了小区物业电话。“电梯不是坏了,是我们经过检测发现达到了更换标准,所以申请了物业维修基金进行更换。”物业公司工作人员介绍,因为中、高考期间禁止施工,所以延误了。“预计这几天就能安装到位,到时乘坐电梯就能和往常一样了。”

扬子晚报/紫牛新闻记者
郭一鹏

