揭秘“AI换脸”诈骗黑色产业链

新华社 吴书光 邵鲁文 王凯

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。

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,查扣电脑和手机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,平日里沉迷网络。

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-删除-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。

标着3C认证却查无此证,廉价充电宝隐患重重

央视新闻客户端

充电宝已经成为人们日常出行习惯携带的电子产品。根据相关规定,未取得CCC认证证书或未标注认证标志的充电宝,一律不得出厂、销售。目前市面上在售的充电宝是否都符合要求?记者进行了调查。

记者调查7家商户,4家销售无CCC认证充电宝

北京一家充电宝商家告诉记者,目前很多充电宝多是前期积压的库存老款,尽管没有CCC认证,但由于价格低,销量也不错。

在记者随机调查的7家商户中,有4家在销售没有CCC认证标志的充电宝。目前,一些实体店仍在销售无CCC认证的充电宝,那电商平台上的情况又如何呢?

记者注意到,某平台一家舞莱3C数码店铺宣称所销售的充电宝能够带上飞机。

这款产品的详情页面标注了CCC认证编号,但记者核对后发现,这一编号对应的证书已被注销,被注销的证书为东莞市常辉电子科技有限公司所有,这家企业也正是商品页面所标称的产品制造商。为进一步核实情况,记者以普通消费者身份,在这家店铺花费12.9元购买了这款充电宝。

但收到货后,产品上标注的制造商却是东莞市得伴智行新能源有限公司,记者查询发现这家企业对应的CCC认证证书均已处于注销状态。也就是说,这款充电宝并没有有效的CCC认证证书。

在某平台跨浩电子优品直播间,主播拿出CCC认证证书在直播间展示。

在这个直播间里,主播展示了CCC认证证书编号,记者随即登录全国认证认可信息公共服务平台进行查询,结果发现这款商品的CCC认证证书已被暂停。

某商城“羽能数码专卖店”销售的这款充电宝,页面显示的CCC认证证书编号对应的制造商为深圳晟铭创科科技有限公司。然而记者购买了这款产品后发现,产品外壳标注的制造商变成了“深圳市电巨人科技有限公司”,记者通过查询发现,这家公司对应的CCC认证证书均处于失效状态。

也就是说,深圳市电巨人科技有限公司生产的充电宝CCC认证证书已经失效,在销售过程中这款充电宝使用的是深圳晟铭创科科技有限公司的CCC认证证书编号。

记者联系商家客服,询问CCC认证证书相关情况。客服回复,“目前产品数据正在优化,不满意可退款。”

无CCC认证充电宝电芯,没有标注产品信息

记者将多款没有有效CCC认证证书的充电宝,送到中国电子技术标准化研究院安全中心实验室进行检测,技术人员拆解发现,部分充电宝内部电芯没有按照要求印刷生产厂家的信息。

技术人员介绍,外壳阻燃性能是充电宝关键的安全性指标之一,试验中部分充电宝不但无法减缓燃烧,甚至可能成为“助燃物”。

技术人员介绍,取得CCC认证标志要经过一套极其严苛的审核流程。而不少劣质充电宝外壳易燃、电芯无标识,成本极低,安全性能完全不达标,只能冒用或者虚标CCC认证来迎合市场需求。

随后,记者在相应电商平台对本次购买的两款产品进行了投诉举报。截至发稿时,舞莱3C数码店铺的相关产品已下架,羽能数码专卖店的相关产品暂未下架。

专家介绍,CCC认证证书并非一经取得便永久有效。部分充电宝在证书被暂停、撤销或注销后,依然违规销售,是当前行业亟须整治的重点问题。

市场监管总局认证监管司消费品认证处处长张威表示,自认证证书注销、撤销之日起,或者在认证证书暂停期间,不符合认证要求的产品,不得继续出厂、销售、进口或者在其他经营活动中使用。如果有平台商家对证书已失效的充电宝继续标称CCC认证并公开销售,致使不符合认证要求的产品进入消费领域的,县级以上市场监管部门按照未经CCC认证的情形,对该违法行为依法予以查处。

监管部门表示,没有有效CCC认证的充电宝安全性无法保障,严重威胁消费者人身安全。

张威表示,对擅自出厂、销售以及在其他活动中使用未经CCC认证充电宝的行为,出重拳打击;严厉查处伪造、冒用、倒卖、转让CCC认证标志的行为。

市场监管总局(国家认监委)近日发布公告,调整完善移动电源等产品CCC认证实施要求。2027年4月1日起,应当按照新版CCC实施规则开展CCC认证活动。按照旧版CCC认证规则,已获证的移动电源及配套锂电池产品,须在过渡期结束前完成证书转换。同时,市场监管总局已与主要电商平台建立了CCC认证证书联网核查机制。

强制性产品认证,是守护大众安全、守住产品质量的底线,不应该沦为部分不良商贩用来装点门面、欺骗消费者的“幌子”。

监管部门、电商平台和消费者应该形成合力,才能让CCC认证违规的产品无处遁形,真正筑牢充电宝安全的防线。