你的个人信息是这样泄露的

内鬼泄露、非法采集……犯罪分子6大手法获取个人信息，公安机关近三年侦破侵犯公民个人信息案创新高，查获3亿余个网络黑号

N南方都市报 华商报

10日，公安部召开新闻发布会，通报公安机关打击整治侵犯公民个人信息违法犯罪行为举措成效。

公安部网络安全保卫局政委孙劲峰介绍，2021年和2022年，公安机关侦办侵犯公民个人信息类案件数同比均快速上升，此类案件涉及政府、医疗、教育、房地产、物流、电商等多个行业，以公民个人信息为核心，滋生电信诈骗、骚扰电话、抢号抢票、网络水军、人肉搜索、“呼死你”、“薅羊毛”等一系列黑灰产业。

手法拆解 中间商低买高卖赚差价

当前，侵犯公民个人信息花样繁多，犯罪分子究竟如何非法获取个人信息？公安部网络安全保卫局警务技术二级总监黄小苏表示，犯罪分子获取个人信息数据主要有“骗取信息、盗窃信息、内鬼泄露、非法采集、倒卖信息、变造信息”等6种手法。

孙劲峰表示，这些非法获取的公民个人信息，会流转到信息买卖中间商手中，通过低买高卖赚取差价，而购买公民个人信息的最终目的一方面为网络水军、网络洗钱等犯罪活动提供银行卡、虚拟身份等物料支撑，另一方面为电信网络诈骗、敲诈勒索等提供精准的靶心。据了解，目前公安机关全面摸清黑灰产业链各环节特点，开展上溯源头、下追买家的全链条打击，并同步跟进“一案双查”，对互联网企业平台严管严查，压实企业责任，坚决遏制侵犯公民个人信息违法犯罪蔓延趋势。

他也提醒，社会公众要提高个人信息保护意识，有关企业要提高责任意识，落实安全保护措施，规范信息采集和使用范围。

“净网”行动 近3年破案3.6万起

据介绍，2016年以来，公安部每年组织“净网”专项行动，依法打击侵犯公民个人信息违法犯罪活动，尤其近3年来破获案件数量和抓获人数连续创新高，自2020年以来已累计侦破案件3.6万起，抓获犯罪嫌疑人6.4万名，查获手机黑卡3000余万张、网络黑号3亿余个。

公安机关打击黑客犯罪，侦破一批利用木马病毒、钓鱼网站、渗透工具、网络爬虫等黑客手段窃取公民个人信息案件；重拳打击行业“内鬼”，2020年以来抓获电信运营商、医院、保险公司、房地产、物业、快递公司等行业“内鬼”2300余名；锚定买卖公民个人信息的重点网络平台，抓获一批数据中间商和物料供应商；紧盯ChatGPT、云计算、区块链、“AI换脸”等新技术、新应用、新业态，侦破一批利用人工智能技术侵犯公民个人信息的新型案件，同时循线深挖下游犯罪线索，连带破获大量电信诈骗、套路贷、网络盗窃、网络洗钱等违法犯罪案件。

AI换脸 开展技术测评升级安全措施

近年来随着人脸识别技术越来越普及，手机刷脸认证成为生活的常态。今年以来，不法分子利用AI换脸等技术实施盗窃、诈骗等犯罪屡次被媒体曝光，也引发公众对于个人信息安全的担忧。

公安部网络安全保卫局副局长李彤表示，随着人脸识别技术的广泛应用和人工智能技术的进步，人脸识别验证类犯罪伴随而生。犯罪分子用于实施“AI换脸”的物料主要为照片，特别是身份证照片，同时结合人员姓名、身份证号来突破人脸识别验证系统。为防范和打击此类新型犯罪，公安机关联合国家重点实验室等单位，开展人脸识别与活体检测技术安全测评，覆盖境内用户量大、问题隐患突出的即时通信、网络直播、网络社交、电商平台、金融支付等重点APP，及时发现人脸识别验证系统存在的风险隐患，通报运营主体升级安全保护措施和人脸识别算法。

此外，公安机关开展“净网”专项行动对此组织专项会战，严打泄露身份证照片等图像信息的犯罪源头，已侦破获“AI换脸”案件79起，抓获犯罪嫌疑人515名。

犯罪分子如何获取个人信息？

骗取信息

利用“地推”、假冒身份等手法骗取公民个人信息，如乡村地区流行的扫码送礼物、协助激活电子医保卡，以及冒充电商客服、冒充公安民警骗取个人信息等。

盗窃信息

线上和线下盗取公民个人信息，如利用木马病毒、钓鱼网站、渗透工具、网络爬虫等黑客技术盗取公民个人信息。或者通过非法入室等方式线下盗取公民个人信息。

内鬼泄露

利用职务便利非法泄露公民个人信息，如运营商、快递、汽车4S店、地产等企事业单位内部工作人员泄露公民个人信息。

非法采集

非法采集公民个人信息，如APP、机顶盒、手机、智能手表等供应链厂商利用其产品非法采集公民个人信息。

倒卖信息

收买或交换公民个人信息，如利用兼职形式从社会闲散人员处收买身份证、银行卡、人脸识别等信息，或者金融、教育、房产等行业从业者违规交换内部数据。

变造信息

加工变造公民个人信息，如将身份信息、购物信息等不同数据源进行碰撞，添加新标签后形成新的数据源，或者利用AI技术使用照片生成动态人脸识别信息等。

案例

龙岩一地产公司员工倒卖业主个人信息

当日，公安部发布了打击侵犯公民个人信息犯罪十大典型案例，其中龙岩某房地产公司员工倒卖业主个人信息案入选。

今年2月，福建龙岩公安机关接到大量群众举报，称购买新房后收到大量装修建材类营销骚扰电话。经查，龙岩某房地产公司员工利用职务便利，非法获取并向郭某等人出售大量业主信息，郭某再将上述信息分别转卖至建材家居、装修设计等公司，相关公司雇佣人员或违规使用外呼系统拨打骚扰电话进行精准营销。此外，相关公司还将工作中掌握的公民个人信息相互交换、转卖。今年3月，龙岩公安机关开展集中收网，抓获犯罪嫌疑人14名（其中，房地产行业工作人员1名），涉案金额30余万元。

以“网红素材”为诱饵骗取用户个人信息

今年5月，浙江宁波公安机关在侦办一起网络诈骗案件时发现，诈骗分子掌握大量公民个人信息。

经查，李某等人成立某网络传媒有限公司，联系“网红”在某平台直播间带货页面以低价销售“网红教学素材”为诱饵，骗取用户购买商品并提供公民个人信息，进而将相关信息出售给下游诈骗团伙。诈骗团伙利用受害人急迫希望成为“网红”赚钱的心理，对受害人开展精准营销，出售虚假直播培训课程，并许诺为其直播间提升粉丝数量，骗取大量受害人培训费。

今年6月，宁波公安机关开展集中收网，抓获犯罪嫌疑人12名，并顺线打掉下游直播培训诈骗团伙，涉案金额560余万元。

快递公司系统植入木马获取大量快递信息

今年3月，上海闵行公安机关在侦办一起网络诈骗案时发现，犯罪嫌疑人准确掌握受害人的网购记录、物流信息等公民个人信息。经查，彭某等人在境外网站发现有人有偿求购物流信息，随即与该人联系获取木马程序，并应聘为快递公司员工，利用职务工作便利在快递公司业务计算机内植入木马程序，其上线人员通过木马程序获取大量快递信息，并利用上述信息进一步实施电信网络诈骗。

今年5月，上海公安机关开展集中收网，抓获采取相似手法窃取公民个人信息的犯罪嫌疑人8名。

偷盗电信运营商个人信息卖给另一运营商

2022年7月，陕西西安公安机关接到电信部门通报，称本地存在违规开展外呼服务的第三方电信公司。经现场检查发现，该公司存有大量宽带装机记录等公民个人信息，立即对信息来源开展调查。经查，西安某电信公司员工刘某军为牟取不法利益，指使严某开发批量获取电信运营商内部系统数据的程序，部署于电信运营商内网，并将程序使用权限出售至第三方电信公司，第三方电信公司工作人员张某宁使用该程序非法获取公民个人信息后，按照其客户要求通过拨打骚扰电话的方式进行精准营销。今年6月，西安公安机关对该案开展集中收网，抓获犯罪嫌疑人6名（其中，电信运营商工作人员1名）。

出售事故车主信息牟利

今年2月，佛山公安部门发现，当地一家汽车服务公司工作人员利用通信群组非法出售事故车主信息截图。经查，该汽车服务有限公司为拓展汽车维修中介业务，勾结保险公司、拖车公司以及路政部门工作人员，非法获取其工作过程中掌握的交通事故车主信息，并根据车辆品牌、事发地等联系特定汽车4S店、汽修厂，通过送保养、油卡等好处诱导事故车主前往指定地点维修，赚取信息“中介”费用。相关汽车修理机构通过故意夸大损失、以换代修等方式侵害相关保险公司及车主利益。

今年3月，佛山公安机关对该案开展集中收网，抓获犯罪嫌疑人47名，涉案金额300余万元。