

大量购买实名制网络账号引流 涉嫌犯罪

□潍坊日报社全媒体记者 张益阁

安全大讲堂

在网络世界，大家虽都有自己的“虚拟马甲”，但网络并非法外之地，大家的一言一行仍然受道德与法律的约束。“网络水军”一词最初由简单的发帖“灌水”发展而来，并非简单的刷流量、控评论，还可能用于推广引流、舆情敲诈等。近日，寿光市公安局抓获了一名大量购买实名制网络账号用于推广引流，以此非法获利86万余元的嫌疑人。

真实案例

自公安部部署开展打击整治网络谣言和网络暴力专项行动以来，寿光市公安局积极响应，持续加大对网络谣言、“网络水军”等违法犯罪行为的打击整治力度，着力营造风清气正的网络空间。近日，寿光市公安局网安大队民警在工作中发现，自2023年4月份以来，寿光一网民在互联网上大量购买实名制网络账号用于推广引流，严重破坏了正常的网络生态环境。寿光市公安局立即组织警力分析研判、深度经营、实地摸排，最终将该嫌疑人抓获。经查，该嫌疑人借此已非法获利86万余元。目前，寿光市公安局已对该嫌疑人采取刑事强制措施。

民警提醒

寿光市公安局网安大队民警表示，广大网民应遵守法律底线，严格遵守网络法律法规。在网上“冲浪”时，不点击来历不明的网站，不随便在网上透露个人隐私和重要身份信息，谨防因信息泄露造成损失。在网上发表观点时，要对自己的言辞行为负责，不散布谣言、恶意侮辱诽谤他人、侵犯他人的隐私，做到言辞客观、理性、基于事实。在网上获取信息时，要注意甄别，查看信息来源是否权威，不轻易相信和传播未经证实的消息，避免误导他人，同时

□潍坊日报社全媒体记者 张益阁

去年以来，社会上出现一种新型的“手机口”诈骗，即架设GOIP、VOIP等网关设备，将境外的电话号码转化显示成国内通讯号码，使受害人接到的号码显示为本地号码，让人防不胜防。

真实案例

“你好，我是‘教育来学网’的工作人员，请问你是不是在网上购买过课程？现在可以申请退费。”此时的李某虽知道自己正在帮诈骗分子拨打诈骗电话，但想到自己囊中羞涩，仍心存侥幸：没事，就干这一次，不一定会被公安机关发现……然而正是这一次的“帮凶”行为，让公安机关获取了一条电诈引流线索，预警指令在第一时间发到了案发地派出所——寿光市公安局侯镇派出所。

接警后，侯镇派出所民警立即行动，经研判分析，查明涉案手机卡持卡人为辖区18岁的李某，于是立即将其传唤至派出所。面对民警讯问，李某起初矢口否认，见民警从自己手机上提取出犯罪证据后，沉默良久的李某才承认了自己利用“手机口”帮助诈骗分子拨打诈骗电话的违法行为。据李某供述，案发当日他利用一部手机与诈骗分子语音通话，开启扬声器，同时用另一部手机拨打受害人电话，以此达到诈骗分子与受害人直接通话的效果。

民警提醒

民警告诉记者，“手机口”诈骗有两种，一种是用两部手机，通过音频线、数据线连接或同时打开扬声器的方式实现语音中转，使得拨打出去的电话显示为本地号码。其中一部手机通过网络软件接通境外诈骗分子，另一部本地手机拨打国内受害人电话、发送短信，实现人机分离，帮助境外诈骗分子掩饰来电真实归属地。

另一种是架设GOIP、VOIP等网关设备，将境外的电话号码转化显示成国内通讯号码，使受害人接到的号码显示为本地号码。GOIP是利用手机卡接入电话网络，来电显示的就是手机号码；VOIP则是利用固定电话线路接入电话网络，来电显示的就是固话号码，实现将境外网络信号转化为本地固话信号的功能。远在海外的诈骗分子进行远程拨号，经过VOIP转换，来电显示就是国内或本地的固话号码，大大降低了被害人的心理防范。需注意的是，日前，青岛警方破获了一起“帮信”案件，嫌疑人冒充“某通信公司”工作人员，谎称上门免费安装能为网络提速的“黑盒子”，而该“黑盒子”就是可实现将境外网络信号转化为本地固话信号功能的VOIP。老年人由于信息获取渠道有限、防范意识相对较弱，容易成为该类诈骗的主要目标群体，因此要加强防范。

保护自己不受虚假信息的影。发现不良信息，要第一时间向有关部门举报，自觉抵制网络不良行为，共同营造健康有序、文明和谐的网络生态环境。

法律链接

《中华人民共和国治安管理处罚法》第二十五条规定，散布谣言，谎报险情、疫情、警情或者以其他方法故意扰乱公共秩序的，将被处五日以上十日以下拘留，可以并处五百元以下罚款；情节较轻的，处五日以下拘留或者五百元以下罚款。

《中华人民共和国网络安全法》(2016年)第十二条规定，任何个人和组织使用网络应当遵守宪法法律，遵守公共秩序，尊重社会公德，不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益等活动。

《中华人民共和国网络安全法》(2016年)第十四条规定，任何个人和组织有权对危害网络安全的行为向网信、电信、公安等部门举报。收到举报的部门应当及时依法作出处理。

《网络暴力信息治理规定(征求意见稿)》第十二条指出，网络信息服务提供者发现侮辱谩骂、造谣诽谤、侵犯隐私等网络暴力信息的，应当采取删除屏蔽、断开链接、限制传播等处置措施。

《网络暴力信息治理规定(征求意见稿)》第十七条指出，任何组织和个人不得借网络暴力事件实施蹭炒热度、推广引流、故意带偏节奏或者跨平台搬运拼接虚假信息等恶意营销炒作行为。网络信息服务提供者不得为传播网络暴力的账号、机构等提供流量、资金等支持。



□潍坊日报社全媒体记者 张益阁

众所周知，机动车号牌是车辆的“身份证”，故意污损机动车号牌是一种严重的道路交通违法行为。然而有的驾驶人为了躲避“电子警察”抓拍，故意污损、遮挡号牌，殊不知，“聪明反被聪明误”。

真实案例

近日，青州市公安局交警大队接连查获两起故意污损、遮挡号牌的道路交通违法行为，问及原因，两司机均表示是为了躲避“电子警察”抓拍。民警遂依法对二人的违法行为分别予以罚款200元、驾驶证记9分的处罚。

民警提醒

青州市公安局交警大队民警表示，故意污损、遮挡号牌的“手段”大致有四种，即使用纸片、光盘、布条等物品遮住机动车号牌；加装防撞装置、备胎等遮挡机动车号牌；使用油漆、泥浆等物质覆盖机动车号牌；人为使机动车号牌变形、折断、油漆脱落，影响号牌上汉字、字母或者数字识认。

民警介绍，除故意污损、遮挡号牌外，未按规定安装号牌、变造机动车牌证、伪造机动车号牌、机动车上路行驶未悬挂号牌等均属于“涉牌涉证”的道路交通违法行为。其中，未按规定安装号牌包括，前后机动车号牌未安装或者未粘贴在机动车指定位置；倒置、翻转、反向安装机动车号牌；只悬挂一块机动车号牌；使用可拆卸号牌架、翻转号牌架。

变造机动车牌证包括，在机动车号牌上粘贴数字贴、符号贴或者使用胶粘、涂抹、拼接等方式改变号牌原有汉字、数字、字母；涂改行驶证、临时号牌记载的信息；更换行驶证上的机动车照片。

伪造机动车牌证包括，非法制作的虚假机动车牌证；通过非法手段从有机动车牌证制作、生产资质的单位取得的机动车牌证；以欺骗、贿赂等不正当手段取得的机动车牌证。

机动车上路行驶未悬挂号牌包括，驾驶机动车尚未取得机动车号牌(临时号牌)；已经申领号牌，但未悬挂或粘贴；使用公告作废的机动车号牌；使用过期的临时号牌；继续使用应回收的号牌。

警惕『手机口』诈骗 莫沦为电诈帮凶

故意污损、遮挡号牌违法 切勿耍『小聪明』