

编者按

很多市民都有过这样的遭遇:只要一买房子,就会接到无数装修公司的电话;只要一买车,就会接到无数保险公司的电话;只要小孩参加了一个培训班,就会接到无数培训班的电话……这些电话给市民正常工作和生活带来极大困扰。其实,这是公民个人信息被非法倒卖的结果。部分犯罪团伙专门购买公民个人信息非法倒卖,赚取非法利润。本周是网络安全周,即日起,本报将刊发连续报道,以案说法,保障公民的合法权益不受侵害。

■记者 谭祥军 特约记者 董萱



倒卖公民信息非法获利30余万

网安民警教你如何不再让自己的信息裸奔

别大意,我们身边的买卖信息案时有发生

团伙作案,非法倒卖公民信息数十万条获利30余万元

今年2月26日,潜逃一年多的四川省开江县22岁男子刘某,主动到十堰市公安局茅箭区分局投案自首。至此,公安部督办的“5·25”特大侵犯公民个人信息案所有涉案人员全部到案。

2017年5月25日,茅箭警方摸排发现一条涉嫌买卖公民个人信息的案件线索。警方经进一步深挖摸排扩线,远赴北京、广东两省开展工作,至当年7月16日,共抓获高某、臧某等26名涉案犯罪嫌疑人。

经调查,2017年2月到5月间,臧某等人受高某委托,非法查询了多名公民的个人户籍信息、快递收货地址、车辆档案、住宿记录、民航火车乘坐记录、手机号码通话记录等信息进行倒卖,非法牟利。当年6月底,在北京、广东两地警方协作下,臧某落网,当场查获作案手机3部、笔记本电脑1部、涉案银行卡数张以及倒卖的公民个人信息数百条。

随后,我市警方经进一步侦查梳理,又先后辗转福建、江苏和四川等地,将涉案的福建永定人谢某城、江苏

公职人员唐某等犯罪嫌疑人相继抓获,该案中所有涉案人员非法获取公民信息数十万条,非法牟利30余万元。

2018年5月,该案被依法提起公诉,谢某城、唐某等26名涉案人员分别被判处1年至3年6个月不等的有期徒刑。今年2月,慑于十堰警方高压严打宣传攻势,刘某主动投案自首。

类似案件,近年来我市警方破获多起。

培训学校校长倒卖学生信息2万余条

2016年6月,十堰网警接到多位网民举报:一教育培训学校多次打电话要求学生报名参加教育培训,怀疑自己和孩子的信息被人倒卖。

经侦查,市公安局网安支队先后在武汉和十堰抓获犯罪嫌疑人马某、简某、项某。

原来,2014年至2016年6月,在武汉开办教育培训学校的马某,通过非法渠道获得湖北省各大中小学的学生信息数万条,后通过网络联系,将十堰籍学生信息25311条,分别出售给十堰两家教育培训学校的法定代表人

简某、项某,非法获利数千元。

简某、项某为了拓展业务,通过与其他培训机构负责人相互置换等方式,非法获取十堰市学生信息总计26万余条,采取电话招生(即主动给学生家长打电话)的方式联系培训事宜。

物业经理盗取业主信息卖给装修公司

前年6月,根据网民举报,市公安局网安支队联合朝阳路派出所,对城区多家装饰装修公司进行了调查,先后将44岁的陈某(某装饰公司法人),23岁的女子赵某,28岁的男子江某和26岁的李某(某物业公司职员)抓获。

经查,任城区一新楼盘物业公司经理的李某,为获取非法利益,将所在公司的业主信息以5000元的价格,卖给某装饰公司的陈某。陈某将其非法获取的十堰3个新楼盘2000个业主的信息提供给赵某,赵某将上述信息以200至700元不等的价格,分别出售给陈某、江某等10余个与住房装修相关的公司,非法获利万余元。

据警方统计,李某、陈某非法获取十堰城区60个小区的业主信息3万余条。

多措并举,有效防范个人信息泄露

公民信息泄露是网络诈骗等违法犯罪猖獗的重要根源,近3年,我市警方成功侦办部督“5·25”、“8·27”等侵犯公民个人信息案件27起,抓获各类犯罪嫌疑人166名,其中涉及企事业单位等7个行业,“内鬼”13人。

当然,保护公民个人信息不仅需要公民个人有安全意识,更需要掌握公民个人信息的相关部门的行业自律。

警方提醒广大市民:购物办卡需谨慎。最好不留联系方式和个人信息。

网络信息隐藏好。网上申请某些账号时要注意里面的保密协议和所谓的个人信息显示,不要公开自己的手机号和住址。

网站活动少参加。参加网络“调查问卷”、购物抽奖活动,不要贸然填写个人信息。

简历管理要妥善。一般情况下,简历中不要过于详细填写本人具体信息,尤其是家庭住址、身份证号等。

快递信息要消除。收到快递我们一定要撕掉快递单号,避免别人冒用用户名骚扰和行骗。

实名车票要撕毁。如今的火车票票面都有完整姓名,还有二维码和身份证大部分的号。所以,车票用完一定要撕毁。

微信群聊不露财。

网上聊天六不提。在网络上交朋友和谈心时,身份证号、真实姓名、家庭住址、单位地址、银行卡号、支付宝用户名,坚决不能提。

只要大家做好防范,多给自己提个醒,犯罪分子就没有可乘之机。

十种情况可能泄露个人信息

市公安局网安支队相关负责人结合十堰发生的相关案例,发现十种情况可能泄露个人信息。

市民随意丢弃的快递包裹(单)、银行回执单、火车票、登机牌等,上面的个人信息可能被不法分子收集整理出售。

部分黑客通过破解教育、卫计、银行、社保、医疗等关系国计民生的行政企事业单位的数据库,窃取公民个人信息,然后非法倒卖给利益集团或诈骗团伙。

市民登录APP、社交软件时留下的个人信息,很容易被非法收集。

部分企业在经营过程中将问卷调查、优惠活动等形式收集的公民信息互相置换或赠送,造成公民信息大量传播。

网购交易中,买家只要下单,不论付款与否,卖家都能看到买家的手机号、地址、邮箱等个人信息及所有消费记录。

公共场所的免费WiFi已成不法分子非法获取用户密码账号等个人信息的重灾区。

一些网友在网上找工作投简历时,身份证、住址、联系方式等通常会以极低的价格被转手卖给任何以合法

名义注册的公司。

应聘工作或办理各种业务时,都要交一些含有个人信息的资料和复印件,一些复印店会将客户的资料悄悄留底,然后转手卖掉。

在QQ资料、空间里和微信资料、朋友圈等发照片或写日志时,在朋友的相关评论或者转发中常常出现姓名、单位和职务等与自己相关联的信息,一些不法分子可以从中获取你和网友的信息。

掌握个人信息资源的单位或企业的内部人员为牟利,非法出售公民个人信息。

