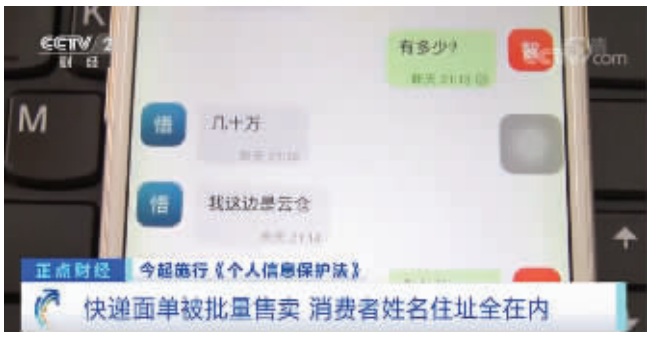
黑产曝光

你扔掉的快递面单被标价售卖

从11月1日起,《中华人民共和国个人信息保护法》正式施行。个人信息保护法明确:不得过度收集个人信息、滥用人脸识别技术、大数据杀熟等。对于提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者,个人信息保护法特别规定了其需要履行的义务,如建立健全个人信息保护合规制度体系,定期发布个人信息保护社会责任报告,接受社会监督等。



央视视频截图

快递面单被批量售卖 消费者姓名住址全在内

一年一度的"双十一"快到了,对于许多网购族来说,又到了迎接快递潮的时候。不过,随着快递量的增加,个人信息安全也可能面临泄露的风险。在快递包裹上,都会贴有一张"快递面单",主要用来记录发件人、收件人以及货物种类等相关信息,其中还包含收件人的姓名、电话、家庭住址等隐私信息。最近,记者调查就发现,目前这些快递面单在网上被明码标价批量售卖,情况十分猖獗。

记者试着在百度贴吧输入"快递""面单"等关键词之后,出现很多相关的分类群组,而为了逃避打击,不法分子都会使用一些暗语来代替,快递信息通常被称为"料""菜"等简称。

在"快递吧"一个网名os开头的人打出了"收菜,来中介对接"的广告,并留下一个联系方式;另外还有人打出"工作室对接,出历史,可测试"的广告。据记者了解,快递面单被收购者分为"实时"和"历史"两种,而实时面单也是最抢手的所谓货源。

网络安全专家万仁国表示,实时面单是新鲜出炉的,比如当天刚出来的,这种面单时效性强;这些面单一旦被卖了,并且被联系过、处理过之后,那么它就叫历史面单。

记者通过一款即时通讯软件联系了多位买家,其中一个叫"橘子"的人给记者报价,实时面单超过1000张每张价格3.5元,精品面单每张4元;而历史面单只收车载、童装童鞋、化妆品类的,每张1.5元。

记者又联系了一个卖家,这个叫"悟空"的人声称,自己手里有几十万历史快递面单,货源是一家物流"云仓"。为了证明自己的实力,他还给记者发了一份文档,里面按照化妆品、母婴、服装等进行分门别类,其中包括上百位消费者的姓名、所购商品、家庭住址和电话号码等隐私信息,甚至还有商品的价格。

快递信息泄露成为"网购理赔"类诈骗帮凶

据记者调查,诈骗分子在获取个人快递信息后,通常会冒充"电商客服"或"快递员",使用的诈骗手法包括"发送退货链接,骗取银行账号信息""快递遗失、商家理赔"等几类。其中"网购理赔类"是目前比较高发的诈骗类型。

9月23日,"UP主自述30分钟内被诈骗16万"的话题成为热搜。据受害者讲述,她当天接到了一个自称申通快递员的电话,对方表示因为快件丢失需要进行理赔。

在冒充快递员的骗子一步步诱导下,受害者30分钟内陆续被骗了16万元。记者了解到,一张快递单背后其实可以延伸出很多个人信息,一个人的姓名、电话号码,而通过电话号码还可以找到微信、支付宝等账号,另外还有家庭或工作地址、消费习惯、经济能力等信息。

不法者"卧底"快递公司 大量信息被售卖

快递面单上的个人信息是怎样被窃取和贩卖的呢?浙江宁波警方近日就侦破一个非法获取、倒卖快递面单信息的犯罪团伙,抓获犯罪嫌疑人9名,查获快递面单照片2万余张。

今年9月初,浙江省宁波市北仑区一家进口外贸公司报警称,公司陆续收到消费者的投诉电话,称大量个人信息泄露,已经有客户被诈骗。接到报警后,宁波警方立即展开侦查,通过实地走访,民警很快获取了一些线索。

据警方了解,这个犯罪团伙为了获取快递包含的个人信息进行非法牟利,竟然通过临时应聘的方式进入快递公司,然后,他们再利用整理快递包裹之机,偷拍快递面单照片,汇总整理后在网上倒卖。

据犯罪嫌疑人何某称,多的时候,最高有一次差不多每张照片8角,上家说他那边的成交金额是每张照片1.2元左右。犯罪嫌疑人李某称,一般下午五六点钟去拍,拍一个多小时,7角一张,当天大概能赢利三四百元。

在掌握大量线索后,宁波警方开展了抓捕行动,先后共抓获犯罪嫌疑人9名,查获快递面单照片2万余张。

据央视

水军揭秘

给明星刷赞、泼污水挣零花钱

晚上8点,一条影视宣传任务在微信群内发布。姜瑞(化名)很快就在群内敲下回复,随后她登录自己的微博账号,将群内早已准备好的文案和图片发送出去,"xx的演技真的好有感染力,情绪传达相当到位。"结尾附上作为宣传重点的话题词条。待群主审核完任务发送情况后,姜瑞便成功获得两元的收入。这就是姜瑞兼职工作的主要内容——当一名娱乐圈"水军"。

微博水军招募信息

"水军"交流群 (均为截图)

刷好评、写推广软文、泼污水……有的一个月能挣上千元。"新华视点"记者调查发现,游走在灰色地带的网络"水军"主要是一些兼职人员,他们在网上接单,兼职做"水军"挣零花钱。

几个月前,姜瑞经介绍加入一个兼职群。经过简单培训,她成了一名"水军"。姜瑞说,主要工作内容是在微博宣传明星动态、影视作品,由派单人发送任务,群内的兼职"水军"抢单,随后在微博内发送撰写好的宣传文案。"只要有社交账号就能挣这个钱。"

据业内人士介绍,网络"水军"既有机器账号,也有真人账号。机器账号俗称"僵尸号",主页通常都是批量的广告宣传,容易造成"一眼假"。而真人账号则因更为个性化的表达,在网络炒作中更受青睐。

广州某营销公司工作人员秦小燕(化名)告诉记者,一些"水军"公司披着公关公司的"马甲",实则是几个人的"小作坊",大量收集真人账号。由于雇佣专职"水军"成本高,他们瞄准了兼职群体。

"点个赞、发条评论就能有几毛到几元的收入。这种时间灵活、工作量不大的'兼职',对想赚点零花钱的年轻人很有吸引力。"暨南大学新闻与传播学院教授张潇潇说。

广州市民刘方方(化名)说,不少朋友都加入了兼职"水军"群。"起初是某个人在微博上看到招募。为了挣钱,我们几个人都跟着她进群当了'水军'。"

记者在QQ上输入"推广""数据维护"等关键词进行搜索,发现存在大量提供"水军"购买服务的QQ群,覆盖各种社交平台。

此外,据一名"水军"招募者透露,拉人头还可以提成。这种招募方式使兼职"水军"社群病毒式膨胀。

广州市白云区检察院第一检察部检察官肖雅菁介绍,购买"水军"服务的过程一般来说需要多层级流转,每一层级的获利都是赚取差价。做推广的多数兼职人员,位于这个灰色产业链的最底层。

张潇潇认为,"水军"在网络世界控制热搜、流量,炮制虚假舆论,轻则影响公众的判断、选择,重则损害他人权利、影响社会公平,危害严重。大家对此要有清醒认识,坚决拒绝以这种不正当方式获得报酬。

此外,法律界人士提醒,兼职"水军"还可能潜藏着法律风险。

肖雅菁表示,兼职"水军"如果发表不当言论,侵犯他人人身、财产权利,可能违反治安管理处罚法,情节严重的甚至可能触犯刑法,涉嫌的罪名包括网络型寻衅滋事罪、诽谤罪、故意传播虚假信息罪、非法利用信息网络罪等。如果作为组织者,组织、招揽其他人员散布虚假信息,同样可能涉嫌上述犯罪,且在共同犯罪中如果起到主要作用,则要被作为主犯处理。

多年来,"水军"如同网络空间的牛皮癣,长期存在却又难以根治。

秦小燕说,"水军"在一定程度上给平台带来了流量。为了热度,平台在监管方面有时"睁一只眼闭一只眼"。同时,兼职"水军"背后代表的是真人账号,相比机器账号而言,在监测层面具有一定难度,出现平台"不愿管""不好管"的局面。

张潇潇认为,加强行业监管是斩断"水军"产业链的关键。在技术层面上,平台应当加强对异常转发、评论等网络活动的识别与监管。肖雅菁建议,加大对互联网公司的行政监管,落实互联网用户实名制。

受访专家表示,当前"水军"产业已经形成了完整的灰色乃至黑色产业链,但由于各个链条之间的联系并不紧密,在信息网络上将任务化整为零进行发布,由网络兼职人员去"认领",这种跨地域性和分散性增加了打击难度。

肖雅菁表示,网民在网络中的身份虚拟性和主题的不确定性,也为"水军"提供了保护的外衣,导致发生网络"水军"案件时,监管部门确定行为主体具有一定的难度和不可控性。

"网络'水军'活动的开展都是依靠网络平台进行,因此其发布信息和资金交易留下的都是电子证据。收集电子证据需要有很强的专业知识和技能,目前侦查机关或者相关监管部门与网络企业的信息共享机制有待健全,很难保证及时、高效、规范进行电子取证,影响了对'水军'的查处。"肖雅菁说。

受访专家建议,进一步完善相关法律法规,提升相关部门对网络平台的监管能力,加大对"水军"的打击力度。对于涉嫌犯罪的网络"水军",必须深挖产业链,斩断利益链条。"同时,还要加大网络权益的民法保障力度,对网络侵权行为,要加大赔偿处罚力度。"肖雅菁说。

据新华社