

电信网络诈骗犯罪进入流水线操作时代 谨防个人信息 流入诈骗团伙之手

记者 王晓峰 通讯员 杨航 史杰柯 实习生 樊欣宜

每年6月，是电信网络诈骗的高发时段。不少参加完“6·18”网络购物节狂欢、正在等待包裹的市民，会收到“客服”的特殊“关爱”——你的快递在运输过程中丢失了，或者因疫情原因被销毁了，现在要给你补偿，补偿的金额往往是数倍于购物的金额……

看到这里，大多数人知道这是电信网络诈骗的一种——冒充客服诈骗。不过，大家也有一个疑问：“我在网上买了什么东西，骗子是怎么知道的？”这就涉及骗子筛选“猎物”的环节了。

在电信网络诈骗日益猖狂的今天，提高反诈意识，是守好钱袋子的重要一环。但反诈好比打仗，知己知彼才能百战百胜。今天，记者借宁波公安近期破获的几起重大案件，为大家分析一下骗子是如何锁定受害人的。



嫌疑人指认现场，这台打印快递面单的电脑曾经被他动了手脚。

冒充客服诈骗套路一致 诈骗手法极其精准

本版图片由
余姚公安提供

6月18日，余姚一男子跑到西門派出所报警。当天下午1时47分，他接到自称是快递公司工作人员的电话，对方告诉他，他妻子网购的物品丢了，一再道歉后，对方表示会赔偿他们的损失。

看对方态度不错，该男子爽快地接受了道歉，添加了对方的微信，并在对方“话术”的指导下扫码、安装相应APP。一顿操作下来，该男子银行卡里的3.3万元就转出去了，等收到扣费短信时，他才知道自己被骗了。

警方对6月份我市电信网络诈骗发案情况进行分析，发现这个月排在前三位的案件分别是刷单、冒充客服、投资诈骗、购物诈骗，这4类案件的数量占总发案量的70%以上，多的时候甚至接近80%。

第一周(6月4日至10日)：4类主要诈骗中，除投资诈骗较前一周略有下降外，其他3类都呈上升趋势。其中冒充客服诈骗发案数量占比达到16.7%，比上月同期上升31%。

第二周(6月11日至17日)，一直排在首位的刷单诈骗发案数量有所下降，但冒充客服诈骗仍呈

上升趋势，较前一周上升2.8个百分点。

第三周(6月18日至24日)，刷单诈骗继续下降，较前一周占比下降近10个百分点，冒充客服诈骗继续保持上升趋势。本周“异军突起”的是购物诈骗，较前一周上升3个百分点。

第四周(6月25日至7月1日)，随着“6·18”网络购物节的结束，刷单诈骗死灰复燃，较前一周上升12.4个百分点。

“分析数据可以发现，6月份的前三周，冒充客服诈骗一直在增加，而且冒充电商物流客服的案件占了绝大多数。受害人中，女性占比超过50%，且以25岁至35年龄段的女性为主。直到第四周，这类案件才开始减少。”反诈民警说，冒充电商物流客服诈骗的套路基本一致：陌生电话——“客服”上门——精准退赔——指导下载APP——“话术”洗脑——汇款。整个过程中，犯罪团伙的诈骗手法极其精准，显而易见，是受害人的个人信息泄露了，但骗子是如何获取受害人精确信息的，至今说法纷纭。

云仓进行了调查。

仓库内的公共视频显示，今年3月，曾有一名神秘男子在深夜时翻墙进入，还对其中一台专门打印快递面单的电脑动了手脚。后来警方了解到，这名神秘男子在电脑上安装了木马程序，专门用来盗取快递数据。

“这台打印快递面单的电脑一工作，数据就会被实时发送出去。窃取这些信息后，会有专人筛选并汇总整理，然后传输给上一级的‘料商’，层层转卖，最后流入诈骗团伙之手。”民警说。4月15日，警方将有重大作案嫌疑的马某抓获，并当场在其身上缴获带有同款木马程序的U盘。随后，警方又于4月28日赴广州和重庆，抓捕马某的上家鲍某和提供技术支持的高某。

证据链进一步完整后，警方逐渐梳理出一条隐藏其后的涉嫌盗取快递面单的黑灰产业链。

快递面单信息，被这些不法分子称为“料”。像马某这样负责去各

个快递始发云仓非法安装木马软件的，被称为“马仔”。“马仔”一般会通过临时应聘的方式，渗透进各地的快递始发云仓，或者利用一些快递始发云仓的防盗漏洞偷偷潜入，对电脑动手脚。在这一犯罪组织中，还有专门的技术人员为这些木马程序提供技术支持和保障。

另据犯罪嫌疑人交代，他们出售的快递面单信息会根据新鲜度和类别进行标价。价格最高的是单品类的实时面单，多为当天新鲜“出炉”、还未签收的。另外一种则是历史面单，一般不限时间，但价值会大打折扣。平均下来，一张快递面单，“马仔”会以1元至2元的价格卖出，然后上家会层层加价，最后以5.5元至7元的价格卖到境外“料商”手中……

警方查证，从去年11月起至被抓的半年内，这个犯罪组织已非法买卖快递面单信息500余万条。最终，这些个人信息会流入诈骗团伙之手。

别让钱包“流泪” 齐心协力守好个人信息

知道骗子是如何筛选“猎物”的秘密后，有助于我们有针对性地应对各类骗局。

对个人而言，首先要提升自己的防范意识，注意个人信息的保护。陌生的链接不要点，需详细填写个人信息的第三方APP请谨慎对待；不管是谁，让你提供银行卡、验证码等隐私信息的，不怀好意的居多；主动跳出来要赔你钱的，估计也是盯上你的钱包了……

另外，在网购时要特别注意个人信息的保护。市民张女士告诉记者：“快递邮寄实名制，对寄件人很严格，但对收件人的要求相对宽松。所以我在网购时填写的收货地址只写小区名称，没有具体到门牌号，收件人也用的是化名。”

最后，还有反诈民警贡献的“金点子”——下载并安装国家反诈中心APP。这个APP，其实就是一道针对电信网络诈骗的“防火墙”，其针对银行汇款账户的“风险查询功能”、针对骗子伪装的“身份核验功能”以及“来电预警功能”，都非常实用。

而对容易接触到大量个人隐私

的服务行业而言，个人信息保护这件事，更需要引起高度重视。因为我国已出台相关的政策及法律法规，对近年来这些“敏感”行业发展中出现的诸多新型问题做了详细规定，其中一大重点就是明确了泄露个人信息应承担的法律责任。

例如，去年11月正式施行的《个人信息保护法》，对过度收集个人信息、滥用人脸识别技术、大数据杀熟等违法行为作了进一步明确。尤其是类似于快递行业这种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。

因此，这些“敏感”行业除了平时要加强企业内部人员管理外，还应落实专人对专用电脑进行监管，设置密码并定期使用专业查杀软件进行木马查杀，或是在电脑上安装公共视频进行监控，以各种方式确保用户个人信息不被挪作他用。

犯罪组织半年非法买卖 快递面单信息500余万条

骗子到底是如何筛选“猎物”的？市公安局在近日举行的“净网2022”专项行动新闻发布会上公布了8起典型案例，其中一起揭开了骗子冒充电商物流客服进行精准诈骗的秘密。

经办这起案件的是余姚公安。据了解，这是我市公安部门破获的全国首例利用木马软件盗取快递

始发云仓快递面单信息案。截至目前，已抓获嫌疑人35名，涉案金额3000余万元。

案件还要从今年4月说起。当时，余姚发生多起冒充电商物流客服诈骗的案件，警方在对受害人回访时，发现了一个共同点——他们的快递都曾在某一快递始发云仓停留。随后，警方对这个快递始发

“广撒网”的背后 几起案件都指向“诈骗引流”

说完骗子精准筛选“猎物”的手段后，再来说说骗子另一种锁定“猎物”的方式——“广撒网”筛选。

就以刷单诈骗为例，很早以前是骗子直接上场，在网上发布各种“兼职”小广告。“广撒网”之后，只要有人上钩，就会以缴纳保证金的名义进行诈骗，这种“效率低下”且以单干为主的诈骗方式后来被抛弃了。如今的刷单诈骗分工明确且以团伙作案为主，前置工作均由黑灰产业链上的不法分子完成，这个过程就叫“诈骗引流”。

6月底，慈溪公安通报了一起为诈骗团伙“引流”的特大涉黑灰产业案件，目前查证的涉案金额有1200余万元。

这起特大案件，要从去年7月发生在慈溪的一起小诈骗案说起。受害人黎某在网上看到刷单招聘信息后，就留言应聘，后来她接到一个电话，“客服”来指导她如何进行刷单，最终被骗取1万余元。调查中，警方发现了一个在河北定州等地为电诈“引流”的团伙，顺藤摸瓜查下去，

先后抓获171名违法犯罪嫌疑人。

经过审讯，“诈骗引流”的全环节厘清了：这个犯罪团伙建立了一个QQ指挥群，群成员包含境外诈骗人员及国内重要成员；下设8个“引流吸粉”QQ群，每个群由10名至20名国内“引流”成员组成。

“引流”成员接收组长下发的“客户”（即受害人）名单后，使用特定的网络拨号软件与其取得联系，然后根据专门的“话术”模板与受害人交流。他们通常谎称自己为某短视频平台工作人员，并以介绍平台点赞等各种网络兼职为由，诱导“客户”添加上级提供的QQ或者微信公众号。等“猎物”主动送上门后，等候多时的骗子就会进场，诱骗“客户”下载APP进行刷单诈骗。该团伙成员每成功“引流”一人，就可获利40元。

2020年8月，慈溪公安通报了一起与“免费领榴莲”有关的案件：不法分子在朋友圈狂推“扫码领福利”的广告，诱导受害人加群并开展刷单诈骗。经过深入侦查，慈溪警方挖出一个横跨三省的微信“引流”、网站“吸金”的诈骗团伙，该团伙通过“免费领榴莲”吸引人员聚集，组群后将群转手倒卖给诈骗团伙。

今年5月12日，慈溪公安在广东惠州、深圳等地抓获周某等犯罪嫌疑人19名。据周某等人交代，自今年2月开始，他们接受境外上家指令，勾结境外色情直播平台的主播，通过“话术”来“吸粉”，为境外诈骗团伙“引流”。每成功拉一人下载APP，他们就能得到40元至45元的提成，多的时候一天能“引流”100多人。

“通过这几起案件，我们可以发现，‘诈骗引流’的随机性是比较大的，如果你抵挡不住那份诱惑，立马会被不法分子‘卖’给诈骗团伙。”反诈民警说。

图 示

警方对6月份我市电信网络诈骗发案情况进行分析，排在前三位的案件分别是

✓ 刷单 ✓ 冒充客服 ✓ 投资诈骗 ✓ 购物诈骗

这4类案件的数量占总发案量的70%以上。

冒充电商物流客服诈骗的套路基本一致

陌生电话 → “客服”上门 → 精准退赔

↓

汇款 ← “话术”洗脑 ← 指导下载APP

受害人中，女性占比超过50%，且以25岁至35年龄段的女性为主。

我市公安部门近日破获的全国首例利用木马软件盗取快递始发云仓快递面单信息案

↓

揭开了骗子冒充电商物流客服进行精准诈骗的秘密

截至目前

已抓获嫌疑人35名，涉案金额3000余万元。

从去年11月起至被抓的半年内，这个犯罪组织已非法买卖快递面单信息500余万条。

韩立萍 制图



抓捕现场，嫌疑人落网。

警方收缴的涉案物品，其中的U盘含有木马程序。