陌生快递不是“惊喜”而是圈套

警方提醒：快递类诈骗手法不断翻新，谨防二维码、链接等

最近，一种以大闸蟹兑换卡为切入点的诈骗手法——“天降螃蟹”刷单骗局成为热门话题。这个骗局利用了人们对于大闸蟹的喜爱和对于领奖活动的期待，以领奖为由引导受害人进群并实施刷单诈骗。近年来，随着互联网的普及和发展，各种新型诈骗手法层出不穷。从法律角度看，该如何斩断庞大的利益链条？如何防止不法分子制造骗局？消费者又该如何避免掉入圈套？专家表示，要从个人信息卖方等方面多管齐下，搭建严格的信息监控体系，强化个人信息的保护力度。

资料图片

案例一：打开包裹后发现是抽奖券 刮开后竟中大奖

蟹卡只是借助快递引导刷单、进行诈骗的一种方式。还有不少网友收到过附带抽奖或退费二维码的月饼、手机支架、课程学费单等诈骗快递。

10 月 6 日 15 时 45 分许，上海市金山区新农派出所接辖区居民许女士报警称，她收到不明快递，可能遭遇了诈骗。接报后，民警张超立即赶到现场。经查看，许女士收到的快递包裹上印有她的全名与电话号码，包裹里是一包湿巾和一封邀请函。打开邀请函，里面是一份某知名企业总裁邀请参加“抽奖活动”的邀请信和一份“商家周年回馈邀你一起撕豪礼”的抽奖券。邀请函上，显示其号码是“N0.88888888”。打开开奖区，该彩券中奖了 20 元红包及一台品牌空调，同城骑手会在 30 分钟内送达百元生活用品。

经了解，许女士近期并未在网上购物，通过查询快递信息，许女士发现这个快递从浙江发出，尝试与寄件人联系，却始终无法打通。

民警尝试扫描抽奖券的二维码，发现跳出的页面是一个钓鱼网站。民警随即研判这是一起诈骗，并对许女士的反诈意识表示肯定，并向她介绍了相关诈骗的惯用套路。

国庆期间，郭先生也收到了和许女士类似的快递。撕开卡片后发现自己中奖了，按要求扫码后，出现了一个客服聊天窗口，郭先生按客服指引下载了一个名为“因赛集团”的 APP，并按照客服要求开始刷单。一开始其成功收到了返利，可当他加大投入后想要再次提现时，却被客服告知由于任务未完成而需要继续充值。

正当郭先生筹措资金准备追加投资之际，廊下派出所民警上门对其开展反诈劝阻，明确告知郭先生这是一起典型的刷单返利类诈骗，他下载的软件也属于涉诈软件。

此类快递骗局，第一步，扫码加好友送“福利”，自称“客服人员”的 QQ、微信会主动来“添加好友”，通过私聊给受害人派发任务，开始会有小福利，刷单几百元返现几十元，任务完成即可领取红包让受害人先尝点甜头；第二步，放长线钓大鱼，受害人彻底放下戒备心后便被引诱下载软件、充值垫付，完成佣金更高的兼职任务，一步步走进刷单诈骗的陷阱。往往刷了几千元、几万元的大单后，被告知“系统卡顿”“任务超时”“操作失误”等理由，无法提现需要继续充值；第三步，卷款跑路，等受害人多次尝试均无法提现时才后知后觉自己被骗了，但为时已晚。

案例二：假借国家政策 退费需下载APP购买证券

扬州市江都区朱女士收到了一个陌生快递，拆开后是一张印有“中华人民共和国教育部”抬头及公章的文件，上面写道：“由于面临国家相关部门予以大力整顿，对嗨学网教育责令整改，针对本次事件给学员们带来困扰深表歉意，嗨学网教育因能力不足、经营不善，导致资金链断裂无法继续运营，今正式宣布清退所有学费。”

信以为真的朱女士就扫描快递中小卡片上的二维码，添加了“客服”QQ 进行办理。“客服”将她拉进一个 QQ 群，要求她下载“万和证券”APP 即可办理退费。

朱女士下载“万和热线”APP 后，“客服”让她自行选择退款方案购买证券。刚开始，朱女士选择了几个金额较低的，对方都返还了，直到朱女士选择了一个金额较大的 3000 元方案转账后，对方称其转账时候操作失误，需要转更多的钱进去修复数据才好拿回之前投进去的钱。朱女士便按对方要求先后转了七笔钱，直到接到 96110 的预警电话，才意识到被骗，于是赶紧到派出所报警。

对此，公安部门总结了这类快递诈骗的套路：不法分子在非法获取培训机构用户信息后，通过电话、短信或快递联系受害人并谎称办理退还学费，诱导受害人添加好友或加入 QQ 群。不法分子还会伪装成退费专员，贴出伪造的债权转让协议书、课程缴费记录等骗取受害人信任。在骗取受害人信任后，不法分子谎称退款必须要在指定 APP 内完成，引导点击陌生网址链接下载虚假 APP，从而获取银行卡、验证码等重要信息。受害人按照指引投入资金便能获得本金和返利，在微收益的驱动下，受害人会不断加大投入资金。此时，骗子不再返还，以操作完一次性返还、操作错误、账户冻结、交解冻金等理由不断诱导转账。

案例三：用话术引诱 冒充快递客服诱导打开“屏幕共享”

“快递丢失理赔”和“招聘兼职”是两种常见的诈骗类型，而据四川省乐山市反诈中心提醒，近期出现了一种“快递丢失理赔+招聘兼职”的结合升级版。

某日，在校高中生小秦在家中接到一通陌生电话，对方自称是某快递公司“客服”，因运送包裹时不慎将小秦的包裹遗失，公司将为其办理全额退款，为表“诚意”，对方提出添加小秦 QQ 好友，方便给他转账。由于前不久确实网购过物品，小秦没多想便添加了对方 QQ 号，他被对方的“专业话术”说服了，确信对方确实是“快递公司客服”。接着，小秦在对方“指导”下开启 QQ“分享屏幕”功能并打开支付宝，但因其未满 18 周岁，无法按“客服”所说完成后续操作。而小秦在察觉不对并报警后，对方看到获取支付信息无望又转而介绍起了 300 元一小时的高额工作……

民警推测，骗子本是想通过“屏幕共享”功能获取小秦的支付宝支付密码、银行卡账号、验证码等重要信息，进而将他支付宝中的钱款转走甚至可能使用其信息贷款。

此外，很多电信网络诈骗团伙会以高额回报为诱饵发展受害人及其朋友成为团伙成员，进行“传销式”诈骗。

警方：快递来历不明 市民应坚持“两验证”

警方总结，快递衍生出的诈骗有很多种类型，比如谎称快递被扣，冒充公检法实施的诈骗，或者虚假快递到付，要求支付高额费用等。最近，较为常见的是快递送礼骗局：市民莫名收到快递，打开后里面是水杯、手机支架或者大闸蟹兑换卡、刮奖卡等物品。这些物品上面无一例外都印着一个二维码，出于好奇心，很多人收到之后都会进行扫码操作，进而落入骗子的圈套。

警方提醒，收到陌生快递，应先登录购物网站，查看物流信息，看是不是自己购买的快递。或者询问亲人朋友，看是不是熟人送礼。

对于来路不明的到付快递，要坚持两验证：验证快递员身份，验证包裹内物品。有疑虑要通过官方途径进行核实，或到附近派出所询问。收到陌生包裹，切勿扫描里面的二维码，切勿填写银行账号等个人信息。不要被骗子耸人听闻的说辞吓到，也不要被天上掉下来的“馅饼”砸晕。一旦发现被骗，请立即拨打 110 报警电话。

快递类诈骗背后：

我的信息被谁卖了

梳理整个过程可以发现，最关键的环节在于，不法分子精准锁定收件人的姓名、电话、地址等信息，实现了蟹卡、会员卡寄送的精准抵达。

如何得到精准的个人信息？部分非法分子长期活跃于一些黑灰产平台，通过一些网络黑话兜售用户个人信息，快递面单被随意买卖，事实上，已形成了固定的黑灰产业链。

一般来说，收购快递面单个人信息，称之为“收面”“收料”等。10 月 16 日，记者在某黑灰产平台上搜索发现，发布“高价收面，急用”等信息的买家很多。

记者以急需面单数据为由咨询了一位卖家，对方表示，目前暂无实时面单（当日的面单数据），仅有历史面单，即可以提供半年以内的用户姓名、电话、地址等信息。在出售价格方面，多位卖家给出历史面单每张 1.5 元的价格，且面单数量不一，有的仅有 5000 条，有的可达到几十万的数量。也有卖家表示，面单价格有差异，实时面单价格会高于历史面单出售价格。

辽宁瀛沈律师事务所合伙人律师张迪表示，电信网络诈骗屡禁不止，个人信息买卖的泛滥是最重要的原因之一。张迪表示，应严厉打击个人信息买卖行为。建议建立严格的数据监控体系，对各企事业单位收集、处理、保管个人信息的行为进行严格规范。另外，也需要增强信息提供者的自我保护意识。

（来源：北京日报、长江日报、央视网等）