

真假蟹卡背后：谁泄露了收货人地址？

“2388型，公蟹4.5两5只，母蟹3.3两5只。”当蟹卡邮递到家，这样的诱惑是否难挡？近日，蟹卡诈骗因演员孙艺洲发文成为焦点。记者搜索看到，不少人收到不明蟹卡。根据网友晒出的快递信息，寄送蟹卡的快递公司包括中国邮政、极兔、申通、韵达等。多名网友评论表示，收到了同样的蟹卡，并且寄件人和收件地址相同。

10月8日，记者就邮寄诈骗蟹卡等是否可以监控及相关预防问题，采访了部分快递公司，截至发稿，暂无收到回应。



吴女士提供的蟹卡照片。

体验

蟹卡扫码提货，客服发礼品先验手机号

吴女士告诉记者，自己收到了来自浙江金华义乌市的蟹卡快递，由于不认识寄件人，便拨打了对方电话，并未接通。

“收到蟹卡的时候很诧异，但没想这么多，就按照蟹卡提示扫码加客服了。”吴女士表示，当询问客服如何领大闸蟹时，对方却让她进群领取免费生活用品。出于警惕，吴女士并未操作并删除了对方微信账号。

根据蟹卡照片，这一“金秋蟹礼”卡与普通蟹卡并无差异，标注有螃蟹数量，卡片背面标榜“全国通用，产地直发”。卡片上不仅有提货卡号密码，还在显眼位置印有二维码，并标注“微信扫描二维码，激活/提货/客服/物流查询”。

记者注意到，这些卡片上大多宣称24小时在线扫描提货或者配送，并未标注电话联系方式。

10月7日，记者根据网友提供的蟹卡二维码扫码后发现，该网页因包含恶意欺诈内容被多人投诉，已被停止访问。

10月8日，记者再次扫描其

他蟹卡二维码后，页面跳转至一个企业微信聊天界面。页面显示，对方为成都燃煤集团有限公司客服，但所属公司却为福萨信息科技有限公司。该客服称，由于中秋国庆假期已过，蟹卡活动派送完毕，可以挑选茶具或化妆品一套，由线下门店统一发货，并称领取礼品需要提供手机号。客服发送的化妆品礼盒海报显示，标价均在1000元以上。不过，当记者提供手机号后，该客服表示查询不到这一号码，再次核实记者没有其他电话号码后，便将记者微信账号删除。

天眼查App显示，福萨信息科技有限公司位于云南昆明，成立日期为2023年9月19日，注册资本为10万元，其法定代表人凡鑫共在42家公司任职，这些公司均位于昆明。

记者在天眼查App搜索发现，并不存在名为“成都燃煤集团有限公司”的企业，福萨信息科技有限公司及凡鑫也不与该公司存在关联。

揭秘

暗藏刷单：返利为诱饵，群聊设套骗转账

10月7日，上海市公安局分享了蟹卡诈骗案例，称市民周女士收到不明大闸蟹兑换卡快递。周女士扫码后出现客服窗口，客服发来一个二维码，让她扫码进聊天群。若周女士没有识破骗局，对方便会要求其下载App开始刷单任务，前期以小额返利获取受害人信任，后期要求受害人大额充值后不予返还本金和返利，最终完成诈骗。

记者采访此次收到诈骗蟹卡的网友，值得一提的是，不同蟹卡上，客服虽然不同，但套路大致相同。

上海市公安局在进行套路分析时表示，以往不法分子直接通过短视频、添加社交账号、抢红包等途径发布点赞、刷单等虚假兼职信息，打着“高薪、轻松”的旗号吸引目标群体后实施诈骗。新骗局中，不法分子大范围投递大闸蟹兑换卡、湿巾、手机支架等，以领奖为由，引导受害人扫码进群后实施刷单诈骗。

实际上，“刷单”诈骗并不新鲜，记者一度进入所谓的“聊天群”，并摸清诈骗套路。

记者被一名“拉手”拉进疑似黑灰产分子控制的某微信群中，群主介绍称此群为“××合作商家福利群”，会在群里给大家发红包，并表示“为集团提高销量，麻烦亲们

做一些小工作领取红包奖励”。

在群主的要求下，记者与一些群成员下载了一个名为“企业密信”的App，并在其中添加了一名“接待员”，按照要求完成任务，记者收到了共计20元“返现佣金”红包。

此后，群主表示从“任务三”开始就是帮助平台兼职刷单。记者发现，刷单内容与网购平台没有任何关系，而是在一个名为“500国际”的博彩平台进行六合彩投注，记者将此前通过返利得到的20元都投入了该平台，成为了平台的充值数字，但若想要提现，就必须通过银行卡转账方式。到这一步，金额就提升到了数百元至数千元，为确保自己不上当受骗，记者并未继续。

记者接触了三家“刷单返利”兼职，第一家将记者引流到了上文中提到的“企业密信”，并在该App中进入了名为“500国际”的博彩页面平台；第二家将记者引流到了“is语音平台”，让一个“金牌讲解员”给记者讲解如何通过刷单赚钱；第三家则将记者引流到了“密聊”App，通过二次跳转让记者下载“小红书”App，声称可以通过“给小红书刷单”赚钱。该App并非小红书，而是诈骗分子制造的虚假网站。

陌生包裹送上门，黑灰产兜售快递数据1元/条



孙艺洲 3小时前

收到快递是一张蟹卡 以为是哪位朋友送的 扫了下觉得不对劲 又搜了搜 发现好像是诈骗！
天上不会掉馅饼 也不会掉螃蟹
大家要是莫名其妙收到蟹卡 或者其他任何没有源头的东西 千万谨慎！别扫码！谨防上当！
新型诈骗手段又多了.....



孙艺洲微博截图。

10月8日，记者联系到一名收到孙艺洲“同款蟹卡”的网友小诗。小诗告诉记者，她在收到蟹卡后不久就刷到了蟹卡诈骗事件的热搜，于是就将蟹卡销毁了。

根据小诗提供的快递单号和寄件人地址，该蟹卡的寄出地地址为广东汕头，但快递包裹上寄件人却来自广西梧州，而寄件人手机号的归属地则是上海。寄件人的三项信息可谓“互不关联”。

对此，记者咨询自己社区所属的反诈专班民警了解到，此类诈骗快递一般不会从线下寄出，而是从网上下单，快递上的信息一般都是假的。对于此类快递类型骗局，该民警坦言，其数量在所有诈骗案件类型中相对较少。

记者注意到，针对蟹卡骗局，“你们都是哪里发货来的？”成为话题。有网友称，自己收到的是韵达快递，且地址姓名电话全对，“不知道是快递公司偷偷卖了客户信息，还是哪个商家卖了信息。”

在这一话题下，已有400多条评论，网友回复中，蟹卡的邮寄地址涉及全国多地，包括江苏、安徽、浙江、江西、上海等。大多数人称名字和地址均与本人一致。

用户信息泄露已非个案，这是因为对用户个人信息的买卖已经形成了固定的黑灰产业链。

10月8日，记者在一黑灰产平台搜索发现，发布“专收当天网购实时快递”“寻求稳定中介源头合作”“大量收精品快递面单”等信息的买家不少。

记者咨询了一位买家，对方表示自己“当天手拍”的快递面单，可以以3.5元/张的价格收，不过只收包括保健品、家电、粮油等品类的单品。当记者询问购买这些快递信息用途，对方坦言“做坏事用”。

根据记者调查，黑灰产平台上此类数据商数量不少，他们承担了连接骗子与信息泄露方“中间商”的角色，而信息泄

露的渠道则多种多样，从电商平台到快递公司，均是信息泄露的环节。即便公司本身无泄露信息的主观意愿，但当遭遇“内鬼作案”或者黑客攻击，用户数据往往就会泄露，结局主要是低价转卖。

记者搜索发现，除了数据的购买方，也有不少明目张胆出售数据的黑灰产从业者，而出售的数据除了快递面单外，还包括精准到各行业的快递信息，如白酒类、情趣用品、翡翠等。

10月8日，一名数据商告诉记者，不限行业的快递数据出售价格是1元/条，1万条起卖。

实际上，“蟹卡”骗局只是快递诈骗的“变种”之一。

天津市反电信诈骗中心曾发文揭秘了多种和快递相关的“套路”，包括并未网购却收到了陌生快递，里面赠送了印有二维码的杯子、彩票、手机支架，或者是一张《退费公告》。这种“套路”之一是诈骗分子大批量盲发快递，并以刷单骗取钱财。

此外，记者还收到过快递“到付”，即收到快递后被要求到付数百元才能打开包裹，快递上记者的姓名、电话均正确，但快递寄件人记者却不认识。对此，警方提示，收到不明快递时，不要随意扫码，或是添加陌生人好友，重点提醒家中长辈和孩童，提高反诈意识，警惕陌生快递类型诈骗。（新京报）

一手网购快递数据，快递面单数据，京东商城抖音，圆通顺丰极兔申通等，下单联系：



记者在黑灰产平台上的截图。