天上不会掉馅饼 小心大闸蟹变“大诈蟹”

警方提醒:蟹卡兑换要求进群,实为刷单诈骗;陌生快递中的二维码千万不能扫!

品蟹季节来临,一种新型诈骗浮出水面。10月7日,知名演员孙艺洲在微博发文称,“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……”

无独有偶,近几天,在各大社交平台,不少网友都晒出了自己收到的蟹卡,各地警方也相继发出警示。10月8日,记者发现,部分蟹卡二维码已被屏蔽,但多家蟹卡店铺客服表示,想要单纯从蟹卡上辨别真伪,仍然很困难。

收到蟹卡一定要提高警惕。

以领取礼品为名 要求“进群”“下载App”

“前几天家里突然收到一张蟹卡,寄件人也不认识,当时就怀疑可能是诈骗。”10月8日,一位西安的网友告诉记者,他收到的包裹来自“浦东新区成功路6号”这个地址,寄件人为刘×姗,留下的手机号以171开头,尾号为6039。10月8日晚上7点左右,记者尝试拨打该号码,结果显示已停机。

除此以外,也有网友表示自己收到的包裹来自廊坊、东莞、杭州等地。从网友晒出来的图片来看,蟹卡的外观颜色略有不同,但大多为平台“回馈客户”所赠,且想要兑换,一般都需要先添加所谓的“在线客服”。

10月8日晚,记者尝试扫描某蟹卡上的二维码,结果微信自动发起了与“某燃煤集团有限公司客服”的对话。一进入客服页面,记者就收到一条信息:“金秋献礼,由于大闸蟹赠送活动已派送完毕,现活动豪礼为高档茶具或品牌化妆品一套,咨询领取请回复1。”

当记者向客服确认是否无法兑换大闸蟹时,客服解释说,由于中秋国庆假期已过,蟹卡活动已经结束,但可以选择茶具或化妆品作为替代方案。随后,客服要求记者提供手机号,表示核实后方可进行登记,礼品将在第二天下午5点由门店安排发货。不过当记者询问为何要核实手机号码后,客服便不再回复。

根据网友的反馈,扫描二维码添加“在线客服”后,各家“在线客服”的“套路”各不相同。有网友向“在线客服”提供手机号后,该客服表示在寄送大闸蟹前,有一份免费的水果和商家福利可以领;也有网友添加“在线客服”后,被多次要求扫码进群。

10月7日,平安北京在微博发文称,“扫码之后,大多数都是‘入群再领礼品’‘引导下载App’‘做任务’之类的操作。最终就是为了获取信息,骗走钱。”“天上不会掉螃蟹肉、月饼、粽子、烤鸭、香酥鸡、小龙虾、担担面等一切。”

此前,10月5日,上海闵行公安分局发布的紧急预警中就提到,2023年10月,崔某收到装有印着二维码的大闸蟹兑换卡的快递,其扫码后加入微信群聊,在群聊中根据客服的引导关注店铺、下载聊天App并进行刷单返利等任务,被骗2万元。

随着蟹卡诈骗事件的进一步发酵,记者发现,一些蟹卡附带的二维码关联账号已被微信屏蔽。也有网友表示,自己扫描蟹卡二维码后,接到了反诈中心的电话提醒。

客服:兑换过程需要付费就一定是诈骗

记者询问了淘宝上销量排名前5的蟹卡店铺客服。多家店铺的客服表示,一般蟹卡的兑换方式都相对简单,很少有需要通过客服来操作的。

记者梳理了几家店铺蟹卡兑换的方式。目前,蟹卡兑换一般有三种方式:电话、微信公众号和网站。通常而言,收到蟹卡后,用户可以自行选择相关的平台进行兑换。兑换的过程中,一般而言,首先需要消费者提供蟹卡号和密码进行验证,验证通过后,需要消费者留下手机号码、地址等收货信息。5家店铺客服都表示,整个操作过程可以自助完成,无需添加所谓的“在线客服”。不过,目前单从蟹卡本身还很难判断蟹卡的真伪。目前,消费者只能通过购买渠道是否正规,蟹卡上标注的公司是否靠谱来判断。对于收到来历不明蟹卡的消费者,大多数客服也仅是建议消费者通过正规途径购买,对不明包裹保持警惕,不要相信世界上有“免费的午餐”。

10月7日,上海市公安局官方微博发文称,近日,有不少市民都收到了大闸蟹兑换卡,扫码后却出现客服窗口发来进群邀请。注意这是新型骗局,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。

警方支招 蟹卡、兑奖券、礼品码…… 收到陌生快递,如何识别新型诈骗?

警方提示,陌生快递中的二维码千万不能扫!一些诈骗分子会大范围向市民寄发快递,内附小礼物和礼品兑换券等,吸引收货人扫描二维码,随后实施诈骗。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。不要被天上掉下来的“馅饼”砸晕,要提高反诈意识,警惕陌生快递类诈骗。

问:陌生快递诈骗的常见方式有哪些?

答: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。

实际上,这是一种以中奖或者兑换物品扫二维码为引流方式,打着兼职刷单的名义进行诈骗的手段。诈骗分子会大批量向居民寄出快递,里面往往是一些不值钱的小礼物或中奖通知、礼品兑换券等,这些东西上全都印有二维码,引诱收件人扫码添加客服、领取礼品。注意,这种二维码千万不能扫!

问:陌生快递中的二维码,扫了会怎么样?

答:如果不慎操作扫描了二维码,手机上可能会先出现客服窗口,拉你进一个群,诱导你下载App。这些客服、聊天群,甚至官方平台,看似制作地无比真实,但实际上都是诈骗分子找人扮演、自己运营和搭建的虚假平台。按照骗子的要求操作半天,不但拿不到所谓的“礼品”,还可能被卷入更深的骗局。

问:收到疑似诈骗的陌生包裹,应该如何处理?

答:收到陌生快递,我们应该先登录购物网站,查看物流信息,看是不是我们购买的快递。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。

相关链接

警惕退订“百万保障”新骗局

记者日前从安徽省合肥市公安局反电诈中心了解到,近期一种新型诈骗方式让不少人上当。骗子利用部分用户对支付宝、微信等软件上“百万保障”功能不了解,谎称“‘百万保障’功能到期,不取消会自动扣款”,以此套取用户支付信息或诱骗其转账。

10月8日傍晚,合肥市公安局反电诈中心接到市局110指挥调度中心推送的一起警情:当地高新区居民朱某遭遇网络诈骗。诈骗电话中,对方自称是保险客服,称其百万医疗保险即将到期,如果不及时取消,每月将被强制扣除2000元。起初朱某并不相信,然而在骗子引导下,受害者发现其微信页面里确实存在百万保险保单页面。随后,该“客服”以协助取消该保险为由,让朱某下载一款网络会议软件,在共享手机屏幕的情况下诱导朱某登录银行账户,套取其账户密码、验证码等信息,进而转出70余万元。万幸的是,反电诈中心联合110指挥调度中心、银行等部门,成功在涉案一级账户止付全部被骗资金。

据介绍,“百万保障”实际是微信和支付宝等软件为用户支付账户提供的一项免费的保险保障服务,即账户安全保险,当账户因被他人盗用导致资金损失时,每年累计赔付金额最高可到100万元。

“明明是免费保险,却被骗子谎称为扣费项目,不少受害者第一反应就是取消。”合肥市公安局反电诈中心民警朱云龙告诉记者,该诈骗套路中,骗子一般谎称自己是微信、支付宝、银行、保险等“官方客服”人员,声称受害人开通的“百万保障”保险服务即将到期,不取消会被强制扣款,甚至会影响征信。而后诱导受害人自行进入“百万保障”页面,骗取受害人信任。一旦上钩后,骗子会诱导受害人下载会议软件,设置屏幕共享,借机套取受害人银行卡号、短信验证码等支付信息,用以盗刷银行账户资金。一些骗子还声称需要将微信、支付宝等绑定的银行存款转出至“安全账户”,从而实施诈骗。

对此,警方提醒:凡是以不关闭“百万保障”业务会影响个人征信、按月扣费、影响理赔等为由要求转账,或者要求下载未知手机软件开启屏幕共享功能“协助指导操作”的,都是诈骗行为。接到所谓客服的电话,一定提高警惕不要轻信,有任何疑问可以向官方平台核实,或者咨询反诈专线。

综合新华社、央视新闻、澎湃新闻消息