

“双11”来了

当心这些骗局搭便车

南京警方教你避坑:多留个心眼,不要轻信陌生人

“双11”将至,各类新兴网购模式的出现,让消费者拥有了更多“清空”购物车的姿势。然而,一些不法分子的诈骗手段也随之变化“升级”。南京警方根据近期接报的多起案件,梳理了4类常见的骗局,请大家多加防范。

通讯员 宁公宣 现代快报+/ZAKER南京见习记者 陈子秋 记者 顾元森

骗局1

快件丢失双倍赔付? 当心!

●●● 案件回放

“很抱歉,由于我们的快递车在转运过程中后门未关好,导致您的快件丢失,我司将对您进行赔付,请按照相关提示操作……”11月1日,小于在网上买了一箱食品,两天后接到了自称快递公司员工打来的电话,对方能准确报出他的快递单尾号,小于没有怀疑,便添加对方为微信好友办理“赔付手续”。按照提示,小于扫描了对方发来的二维码,随即在弹出的界面依次输入身份证号、银行卡卡号、密码、手机号等信息,最后一步填写手机验证码时,小于犹豫再三,但还是填了。这时,界面显示验证码超时,小于意识到不对劲,暂停了操作,并向南京市公安局秦淮分局淮海路派出所求助。由于终止及时,小于避免了财产损失。

民警介绍,这是典型的快递赔付骗局。不法分子往往通过非法手段获取消费者信息,假称“快件丢失”或是“少寄了商品”,并主动要求赔付,买家如果信以为真,不法分子便趁机进行诱骗。有的向受害人发送钓鱼链接,窃取其个人账户信息,有些则以“手续费”等名义让受害人先行转账。

类似的还有伪装成客服进行诈骗。不法分子自称网店客服,以“产品质量问题”等为由,通知用户办理退款赔付手续,逐步引导其落入圈套。

●●● 警方提醒

接到自称快递或网店客服打来的电话,听到类似“双倍赔付”等字眼得留心,涉及填写个人账户信息或进行金钱交易时,需联系网店或快递官方确认核实;确要办理赔付等手续,尽量在官方程序或平台内操作,勿盲目添加陌生人微信私下交易,以免被坑。



骗局2

陌生平台安全交易? 当心!

●●● 案件回放

日前,市民江先生在某平台看直播时,看到一条弹幕显示高价收购某平台账号。想到自己有闲置账号,江先生便联系了弹幕发送者,一番沟通后,对方表示愿意花2000元购买。

对方给江先生发来一个链接,称是专门用于账号交易的平台,“走这个平台对双方资金和账户安全都有保障。”江先生注册该平台后,把自己的账号挂上去出售。没多久,平台显示江先生的账号已被买走,资金到账。

江先生满心欢喜准备提现,却发现钱无法取出。与平台“客服”联系后,“客服”表示,是江先生误操作导致资金被冻结,需要江先生转账2000元“解冻”。转账完毕,江先生却发现平台已无法登录。江先生回头质问“买家”,却又被推送了另一款交易平台,称“这次肯定没问题”。

一番操作后,江先生再次卡在提现这一步,他又听信“客服”,先后转账8000元“解冻费”。直到对方以“未在平台输入身份信息”为由,要求江先生再转账时,江先生恍然大悟,赶紧向南京市公安局江宁分局报案。

民警表示,这个所谓“安全有保障”的第三方交易平台,其实是不法分子设下的圈套。不法分子在直播间发布广告,诱导受害人到该平台进行交易,随后平台生成虚假的“账号被拍下”“资金入账”界面,让受害人信以为真。此时,不法分子扮演的“客服”利用受害人急于提现的心理,编造出“缴纳押金”“充值解冻”“提现要交手续费”等各种理由,让受害人支付相关费用,以骗取其钱财。

●●● 警方提醒

面对陌生网友与陌生平台,网民切记捂好钱包、不要轻信。在直播间或其他社交平台遇到陌生账号,要保持警惕,不要轻易透露自己的个人信息,更不要轻易进行金钱交易;线上交易一定要通过正规的交易平台,不可轻信他人提供的第三方交易网址、网站,并避免直接转账给对方。



骗局3

预售链接加倍优惠? 当心!

●●● 案件回放

“您好,点击本店预售链接支付定金,付尾款时可翻倍抵用……”11月1日,南京市公安局玄武分局板仓派出所接连受理两起案件,受害人称因点击了短信发来的预售链接,导致被骗。受害人王女士告诉民警,“最近很多商家都发了类似的预售短信,我没多想就点开了。”见有翻倍抵用的优惠,王女士支付了一笔定金,谁知,在购物平台根本找不到这笔订单。受害人张女士表示,点开短信里的链接后,自己的手机还自动向通讯录里的朋友发送了这条附带预售链接的短信,“好多朋友都说收到了我群发的这条短信,可是我没有发过,我手机是不是中毒了?”经调查,民警发现两人的手机均是智能手机,具备上网功能,接到的短信均含有链接内容,点击链接之后,手机就出现了中毒现象。

民警介绍,不法分子通过即时通讯软件或手机短信发送包含病毒的链接,以“预购”“限时购”“预先降价”等关键字冒充商家,一旦用户点开,便可能遭遇钓鱼网站或是木马攻击,进而被窃取私密信息,导致被骗。此外,也有不法分子会在预购活动上动歪心思,骗取消费者的定金。

●●● 警方提醒

无论预售还是直接购买都应在正规交易平台,不要随便点开短信里的链接,不要轻易在跳转页面支付;如果手机中毒并未被骗钱款,可以下载并安装杀毒软件,对恶意软件进行查杀。一旦发生中毒被骗钱款的情况,应立即报警。

骗局4

网络刷单轻松赚钱? 当心!

●●● 案件回放

10月11日上午,南京市公安局建邺分局兴隆派出所接到小颖报警,称自己因刷单被骗上百万元。经询问,9月,小颖在某社交平台上收到名为张某的留言,称正在招网络兼职。小颖心想,刚好能挣点零花钱,便询问是否有适合自己做的,很快得到张某肯定的回复。就这样,小颖在张某的引导下注册了某平台,开始了“刷单”任务。

张某告诉小颖,只要点击平台上发布的任务,等自动跳转到商品订单页面,选择支付,就算完成了一单,后期会连本带利返还。小颖尝试着做了几单金额小的,看到本金及佣金可正常返还、提现后,便信以为真,继续“刷单”。然而,随着金额越来越大,本金和佣金却迟迟不到账。小颖询问张某,对方以各种理由搪塞,并哄骗其继续做任务。国庆节过后,已经投入120多万元的小颖越想越不对劲,便报警求助。目前案件正在侦办中。

民警介绍,刷单返利类诈骗虽然并非新兴手段,但一直以来都是通讯网络诈骗案件中的高发类型。在这类骗局中,不法分子会冒充电商,以提高店铺销售量、信誉度、好评度为由,找人刷单刷信誉。起初,不法分子可能会在小金额范围内作出“连本带利返还”的动作,以骗取受害者信任。但随着受害者刷单金额越来越大,对方便会开始找理由拒绝返款。

●●● 警方提醒

网上找兼职,一定要警惕所谓“小投入、大回报”的广告,更不要轻信对方,先行垫付任何费用;类似的骗局还有“视频点赞返利”等形式,本质都是换汤不换药,只是换了新“马甲”的刷单陷阱,广大网民切勿因贪图小利,上当受骗。

●●● 警方提醒

网上找兼职,一定要警惕所谓“小投入、大回报”的广告,更不要轻信对方,先行垫付任何费用;类似的骗局还有“视频点赞返利”等形式,本质都是换汤不换药,只是换了新“马甲”的刷单陷阱,广大网民切勿因贪图小利,上当受骗。

●●● 警方提醒

网上找兼职,一定要警惕所谓“小投入、大回报”的广告,更不要轻信对方,先行垫付任何费用;类似的骗局还有“视频点赞返利”等形式,本质都是换汤不换药,只是换了新“马甲”的刷单陷阱,广大网民切勿因贪图小利,上当受骗。