

陌生快递“送礼上门”为哪般?

前不久,演员孙艺洲在微博发文称收到一张蟹卡的快递,最后发现疑似诈骗。上海市公安局随后发布微博称,这是一种新型骗局:不法分子大范围投递大闸蟹兑换卡、湿巾等,以领奖为由,引导受害人扫码进群后实施刷单诈骗。

记者调查发现,现实中有不少人收到过这样的陌生快递,里面有杯子、手机支架、风扇、充电宝、刮刮乐……这些商品有一个共同点,就是都会附带一个二维码。在社交平台上,有多位用户发帖称收到大闸蟹兑换券,蟹卡包装精致,上面写着“阳澄湖大闸蟹”“VIP蟹礼卡”“2388型”等字样,暗示礼品价值不菲。

受访的业内人士指出,这些快递物品的成本很低,却具有很强的吸引力和迷惑性。部分群众收到快递后看到二维码,习惯“扫一扫”一探究竟,但扫码后大多数是“入群再领礼品”“引导下载App”“做任务”之类的刷单操作,最终被诱导进入诈骗圈套。消费者应提高警惕避免上当受骗。

陌生快递暗藏风险

今年国庆假期,山东济宁市民张女士收到一份陌生快递,里面有一封以天猫名义写的致谢信和一张金秋蟹礼提货单。

致谢信上写着:为让更多顾客朋友享受到实打实的优惠和回馈,现全网随机抽取100000名在平台有5年以上购物记录的活跃用户赠送2388型(价值约500元)鲜活螃蟹提货卡。提货卡背面提示需要用微信或浏览器扫描二维码联系客服进行提货。

张女士扫码后进入一个类似客服聊天的界面。一名自称是商家联盟平台的客服称,她“有幸”被选中,获得18元红包和大闸蟹一份。随后,客服又给她推送了一个二维码和一组数字,让她扫描后进入商家活动群。进群后,群主开始发任务红包,要求群里每个人完成相应的截图任务,便可收到数额不等的红包。

几轮下来,该群突然被停用。但很快张女士又收到了群主的好友申请,通过后才对方要求她下载商家App,有新人奖励38.88元和大闸蟹礼品,并附上下载链接。张女士点击链接显示是另一款软件,注册完成后她又被拉入一个有近千名成员的群内,群主称可订阅相关商家店铺获得返利,后期升级后可按数据福利单做任务。

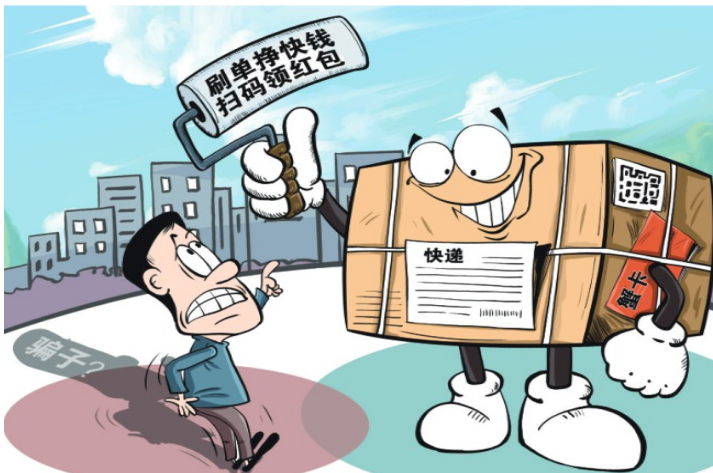
和张女士收到的蟹卡不同,广东湛江的陈女士收到的快递是一个水杯,里面还有一封自称来自“淘宝联盟”的感谢信,以及商家周年回馈赠送的“刮刮乐”。

刮开后,陈女士发现中了一个10元的红包和一份四季水果,兑奖方式为扫描“刮刮乐”右上角的二维码。陈女士扫码后,又跳出一个新的二维码。因害怕受骗,她没有进行下一步操作。

四川成都市民罗女士在莫名其妙收到一个手机支架后,选择扫一扫二级页面的二维码。很快,页面跳转至一个聊天界面。客服让罗女士提供手机号码、“刮刮乐”照片、快递单号进行验证,通过后便让她免费挑选一件赠品,可选项包括大米、牛奶、洗衣液、食用油等,随后又发来一个二维码要求其加群。

进群后,罗女士发现,群主会不定期发任务,群成员完成任务即可领红包。任务多为安装App、关注店铺,每个任务会发4.8元或5.8元红包。她根据指示下载App并完成注册后,又被拉进两个新群组,群主介绍称:“能来到这个群的都是忠粉,忠粉有福利,可以升级会员,会员返的钱更多。完成一次捐赠任务即可升级,捐30元返60元。”

“具体任务是在某支付平台公益



栏目内,选择一个项目捐款30元,再上传捐款证书截图。随后添加‘数据分析师’,对方会指导我们在下载的App内完成一次购买,便能得到60元红包。”罗女士回忆说,还有更高金额的返现,如捐150元返200元、捐350元返500元,但前提是要住一个银行账户内转账。

记者近日随机采访北京、湖南、广东等地数十位群众发现,不少人都收到过类似的陌生快递,有的是手机支架,有的是充电宝,有的是网店促销宣传单或者刮奖卡,但无一例外这些物品上面都印着一个二维码。有人及时止步,也有人损失了不少钱财。

刷单返利套路多多

这些陌生快递背后的真相是什么?

湖南长沙一位民警告诉记者,目前一些不法分子改头换面,不再以短视频、抢红包等途径发布点赞、刷单等虚假兼职信息,而是大范围投递大闸蟹兑换卡、湿巾、水果、手机支架、洗衣液、水杯等,以收快递扫二维码领奖为引流方式,引导受害人扫码进群后实施刷单。

“这些人的套路是让你看到实实在在的甜头,逐步放下戒备,最后对他们绝对信任。这时候,他们就会引诱你下载软件,完成刷单任务。当你不断加大投入后,你会发现自己的本金和佣金都无法提出。此时,诈骗分子又会以‘系统卡顿’‘任务超时’‘操作失误’等理由,要求你继续充值垫付。实际上,这些都是他们的话术,你根本没有办法提取自己的本金和佣金了。”该民警说。

他指出,这些陌生快递之所以能够精准发货到人,是因为不法分子从源头上掌握了大量的公民个人信息,“通过互联网黑灰产业链获得潜在受害人的信息,包括姓名、地址等,这些信息可能在各种网购环节中泄露”。

为什么快递送小礼物容易让人上当受骗?该民警分析道,将具有实用性的日常生活用品作为“小礼物”,能让目标群体尝到甜头。印在物品上的二维码就容易让人丧失警惕性并产生好奇心,进而扫码操作。

北京市中闻律师事务所律师杜秀军提出,不法分子通过送小礼品或红包套取用户个人信息,然后利用个人信息进行诈骗等违法活动,根据后续行为可能构成诈骗罪、集资诈骗罪、非法吸收公众存款罪等。而就套取用户个人信息出售或提供他人行为本身来说,情节严重的,可能构成侵犯公民个人信息罪。

“若平台方泄露个人信息,根据情节可能需承担民事责任、行政责任,严重的可能构成刑事犯罪。不仅被泄露信息的个人可以依据民法典相关规定追究其民事责任,有关主管部门还可以根据网络安全法相关规定责令违法平台立即改正,根据情节单处或者并处警告、没收违法所得、

处违法所得一倍以上十倍以下罚款,没有违法所得的,可处一百万元以下罚款,对直接负责的主管人员和其他直接责任人员可处一万元以上十万元以下罚款;情节严重的,可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照;构成犯罪的,可追究其刑事责任。”杜秀军说。

合力打击快递诈骗

公开数据显示,目前,刷单返利、虚假网络投资理财、虚假网络贷款、冒充电商物流客服、冒充公检法、冒充领导熟人、婚恋交友10种诈骗类型已经成为最常见的高发案件,占发案的80%左右;其中刷单返利类诈骗发案率最高,占发案的1/3左右。

多地警方提醒,网络刷单返利类诈骗已逐步演化成变种最多、变化最快的一种主要诈骗类型,成为虚假投资理财、贷款等其他复合型诈骗以及网络赌博、网络色情等其他违法犯罪的主要引流方式,被骗百万元以上的重大案件时有发生。受骗人群多为学生、老年人、低收入群体及无业人员。

受访的业内人士提出,在此背景下,凝聚多方合力打击陌生快递诈骗刻不容缓。快递公司要从严把关,实行快递实名收寄制度,从源头上阻止陌生快递诈骗行为。市场监管、公安机关等部门应对此类诈骗行为采取“零容忍”态度,发现一起查处一起,通过高额罚单、追究法律责任等方式,让不法分子付出代价。

“梳理陌生快递诈骗的套路,不难发现两个特点:一是操作手段大批量、广撒网,二是很多依托于网络平台和社群运营。”杜秀军说,因此当务之急是斩断泄露、贩卖用户个人信息的灰色产业链,公安机关可以考虑和快递公司合作,针对此类快递内容物轻薄、大批量寄出等特点,及时发现可疑行踪,对诈骗窝点进行查封处理。

他认为,根据我国现行的邮政法和《快递暂行条例》,快递企业应当依法建立并执行邮件收寄验视制度。发现邮件内夹带禁止寄递或者限制寄递的物品的,应当按照国家有关规定处理。对于快递包裹内有不明二维码等疑似诈骗的情况,可以及时报公安机关处理。

“平台要落实好监管责任,通过技术甄别、畅通举报渠道、做好风险提示等手段,及时发现并屏蔽可疑诈骗网站、规范社群运营,尽量为用户创造安全可靠的使用场景。”杜秀军建议。

他同时提醒,收件人也要加强防范,不轻易签收陌生快递,如遇可疑情况应拒绝签收;切勿扫描陌生快递内的二维码,也不要点开陌生链接填写银行卡、身份证、手机号等个人信息;及时销毁快递单上的个人信息,做好个人信息保护。

本报综合消息

警惕“百万保障”

续保退保新骗局

近期,有一些不法分子利用部分微信用户不了解微信支付“百万保障”的弱点,以微信支付“百万保障”已到期,需要缴费续保,或关闭扣费等为由实施诈骗。10月以来,已有多地公安局发布紧急预警,提示市民警惕“百万保障”退费新骗局。

微信支付“百万保障”完全免费 不需要续保

微信支付“百万保障”由财付通与中国人保财险PICC联合承保,用于保障用户的资金安全。此项保障完全免费,默认开通,只要用户在使用微信支付期间,发生微信支付账户被他人盗用而导致资金损失的情况,均可申请赔付,每年申请赔付金额最高100万元。

除了微信以外,支付宝同样为用户提供“百万保障”,当用户注册使用微信支付、支付宝时,将自动免费开启“百万保障”,此保障为APP自带安全设置,完全免费,不会“到期”或者“过期”,不会要求“缴费续保”,更不会影响征信。

腾讯微保对记者表示,只要用户还在使用微信支付,就能够享受微信支付“百万保障”,保障不会“到期”或者“过期”,不会要求“缴费续保”,更不会影响征信。用户可以在微信-我-服务-钱包-消费者保护-安全保障中,查看自己的微信支付“百万保障”。

在近期的多起受骗案件中,受害人接到骗子的电话称,用户已成功续保,每月将支付高额保费,一旦用户“上套”,要求退保,骗子便会一步步诱导用户进入转账骗局;此外还有谎称功能已到期,需要取消或续保,否则会影响征信,以此诱导用户转账等多种套路。

“百万保障”扣费骗局是如何行骗的?

案例一:

近日,受害人报警称,其接到一通陌生电话,对方自称是某微保客服,称自己的微信支付“百万保障”已到期,需要每月支付800元续保,如果不按期缴费会影响个人征信,随后诱导受害人转账。

案例二:

受害人报警称,其被他人网上以百万保障退保为由诈骗21万余元。此类诈骗话术一般是称受害人无意中投保了“百万保障”需要每月支付高额保险费,如用户要求退保,骗子就会一步步诱导用户安装远程操作软件等,骗取用户银行卡密码,最终转走受害人银行卡余额。

虽然看似诈骗话术形式多样,实则万变不离其宗,通常分为四步实施诈骗。

第一步,诈骗分子通常会谎称自己是微信、银行、保险、商家等人员,声称购买商品是点击了“百万保障”需要取消,或者微信支付“百万保障”现已到期,需要续保,又或者谎称对方的快递丢失,给予理赔,引导其点开微信百万保障页面。

第二步,指导用户查看自己微信、支付宝内的“百万保障”,以用户查到的页面为依据,这时对方会谎称受害人已经购买微信百万保障,每月要扣费数千元,引发受害人恐慌。

第三步,不法分子告诉受害人,可以将微信绑定的银行卡中的存款转出,避免微信扣款,同时引导受害人下载“共享屏幕”软件。

第四步,利用受害人下载的“共享屏幕”软件,窃取受害人银行卡号、短信验证码等信息,将受害人卡中资金转走。

近期,此类诈骗案件频发,已有北京、福建、安徽、青海、河北等多地警方接到此类诈骗案件报警,多地公安机关发布紧急提醒,警惕“百万保障”续保、退保新骗局。

微信平台方近期也同样关注到了多起“百万保障”退费骗局,腾讯微保对记者表示,微信支付、微保近期已经在多权威渠道公示警惕冒充电信诈骗短信。微保侧已在微保官网、微博、微信公众号等官方渠道都设立了弹窗提醒。如果用户在微保平台购买了保险产品,官方会通过公众号消息、微信服务通知、短信、电话等方式通知用户续保续费事宜,并且只会引导用户回到微保小程序操作续保,不会引导用户回拨电话、打开来路不明的网站网页。涉及续保、续费等事宜,请通过“腾讯微保”官方小程序进行处理,或拨打微保服务咨询热线400-909-6666,微保服务监督热线400-961-0315进行咨询。

广大消费者如接到有关微信支付“百万保障”需要续费、退保之类内容的电话,需一律保持警惕,只要提到关闭微信、支付宝“百万保障”设置的就是诈骗!微信支付“百万保障”完全免费,不存在“到期续保”,不要相信任何“百万保障”缴费续保、影响征信的骗局。

接到陌生电话或遇到类似情况时,要保持清醒的头脑,注意辨别真假,一旦进入上述诈骗流程,切忌被骗子牵着鼻子走,尤其涉及账号密码、转账操作的时候,务必提高警惕。切勿轻信来路不明的短信,切勿向陌生人转账汇款。如有疑问,可拨打反诈专线96110辨别真假。一旦发现被骗,保留证据第一时间向公安机关报案。

本报综合消息