

多人被骗,有人因刷单被骗40万元……

快递包裹暗藏“二维码陷阱”

“扫一扫最高可领20元”“扫码送水杯”“扫码送话费”……双十一期间,快递成了不少消费者期盼的事情,然而不少快递包裹却暗藏诈骗“陷阱”。

今年10月底,网友“土豆”收到了一个快递包裹,里面放着两张抽奖卡片,她扫码后掉进刷单陷阱被骗40万元。相比老套的抽奖卡片,快递包裹面单上的新型“二维码广告”更有迷惑性,有人原本打算扫码“薅点羊毛”,却在不断跳转的链接里“越陷越深”。这些“广告二维码”到底是谁设置的?有没有监管?消费者被骗后又该怎么办?



扫码掉进刷单陷阱被骗40万元

“扫了个单子,40万元没了。”今年10月底,网友“土豆”收到了一个快递包裹,里面放着两张卡片,一张写着“双11狂欢购,良品铺子坚果大礼包”的字样,另一张则是所谓“良品铺子”的企业介绍和给用户的感谢信。

其中,“双11狂欢购”的卡片背面还印着“0元领三重双11好礼”的抽奖信息,旁边有一个二维码,奖品内容包括所谓“良品铺子”巨型零食大礼包×3袋(价值1388元)、所谓“蓝月亮”去渍养护薰衣草洗衣液(价值39.9元)以及领取现金红包20元。

在收到这个包裹后,“土豆”抱着试一试的心态,拿出手机扫描二维码,很快就被拉入一个“极光音乐推广”的群里,群主开始介绍做任务返利活动。

“做了2天赚了几百块。”尝到甜头后,“土豆”渐渐有些“上头”,随着任务越做越多,慢慢地开始出现“任务失误”的提示,要她继续投入更多的资金才能取出返利。

此时,“土豆”虽然有所警觉,但为了拿回自己的收益,她还是决定试一试,充过一次钱后,因为“任务失误”的收益又能拿到了,自此,“土豆”已经百分之百相信了这个活动。

接着就是再次出现“任务失误”,而“土豆”又加倍充钱,到了后期更是瞒着家人,贷款往里充钱,没多久就搭进去了40万元,其中大部分钱都是通过各个借贷平台借出来的。

“现在怎么都睡不着,感觉天塌了。”因为正在和男朋友筹办婚礼,这次受骗也让“土豆”感到打击沉重。

在将自己的遭遇发在社交平台上之后,不少网友都留言称自己也碰到了类似情况,都是前期返利能赚几十上百块,然后金额越来越大,直至最后被騙上万元。

甚至有部分网友明知这是一个骗局,仍抱着侥幸心理,想着“赚一点就收手”,殊不知骗子也会针对不同人群,在不同阶段“收网”。

“骗子可能会比你想象的收网收得早,我忙活了三天赚了600多元,骗子让我打款500元,我以为还在放长线就打了,结果人家收网了。”一位网友留言道。

另一位网友分析认为,这种手法与以往塞在信箱里的诈骗小广告类似,只不过投放渠道变成了快递包裹。

扫描二维码充话费后“打水漂”

除了快递包裹里的小卡片,不

少网友还发现,快递包裹的面单上也常常会出现一个类似广告的二

二维码。“无门槛优惠券,扫一扫最高可领20元”“扫码送水杯”“扫码送话费”……对小李而言,快递包裹上的广告早已司空见惯,在一次好奇心的驱使下,她扫了其中一个二维码,很快就转到一个话费充值的界面。

“这个小程序说我中了200元话费。”小李说,小程序的界面设置得跟她平时充话费几乎一样,显示充值99元就能获得200元,本以为自己幸运加身,在该页面充值了99元后,小李却始终等不来自己的200元话费到账。

尽管这个界面写着三大运营商联网充值,但是客服电话却仅仅是一个普通的座机号码,而小李多次拨打始终无人接听,至此,她才确认自己上当受骗。

实际上,不少人都遇到过类似的情况。

此前,小王在一个快递包装上看到“扫码送水杯”的活动二维码,当他扫码后,跳转到了一个“充值100元送200元话费”网页,他心想,正规快递包装上的二维码应该不会骗人,便支付了100元。

然而,等支付完成后小王才发现,200元话费确实能拿到,但是要分20个月发放,且消费者必须到该网站上主动领取,当月不领则当月话费权益作废。

“网站上的电话根本打不通,手机管家还把这个电话标记为疑似诈骗电话。”为了讨个说法,小王连续向市场监管、物流公司甚至向公安报警,但是始终没有找到一个解决办法。

快递面单上的二维码来自哪里?

记者调查发现,如今再次扫描小王和小李提供的二维码,页面已经不会跳转到“话费充值”上,而是“双11精选”“幸运赢免单”字样的优惠券领取网站,如果再点击购买商品,页面又会跳到第三方电商平台。

曾经被快递单二维码充话费骗过的小胡告诉记者,此前他充的话费一直没有到账,他就会时不时地扫码进入之前的网站查看,可是一段时间后,网站的内容一下变了,从充话费变成了普通的电商网站,可是新收到的快递面单上,还有几乎扫码进入“充话费”页面。

“也就是说,扫描二维码跳转的网站是可以更换的,一段时间就换一个。”小胡说。

那么,快递包裹面单上的二维码究竟是谁设置的?

记者走访多家快递驿站发现,

一位工作人员表示,快递面单上的二维码是他们打印出来的,但是面单上的内容都是设置好的,打印出来就是这样的。

一名快递驿站的工作人员告诉记者,正常情况下,快递面单上的收件人电话都是加密或者模糊处理的,快递员没法直接看到收件人的电话,只能拨打虚拟号码,而有的快递面单上,则将收件人的手机号码完完整整地写出来,通常这种快递单就有涉嫌诈骗的可能。

记者联系上快递驿站官方客服工作人员后,对方表示快递面单上的二维码与驿站无关,建议记者联系对应的物流公司。

对此,记者又采访到多位快递员,他们表示这些快递面单是商家自己贴的,或是与第三方公司合作的,他们只负责配送,不太清楚二维码的情况。

另一位快递员则透露,如果是个人寄件,是由快递员打印单子,这上面是没有广告的;但如果是网上购物,则是商家自己打印单子,这上面大部分都会有广告。

“二维码广告”可以定制投放?

针对快递员所说的情况,记者以消费者的身份去电商平台咨询了多家商户,为何快递单上有广告二维码?然而,所有客服的回复都表示与自己无关。

一位淘宝客服直言:“不是我们弄的,您扫了可能会有一些不安全的诈骗网站,我们不知道是谁弄的。”

然而,当记者以商户的身份对快递面单的“二维码广告”进行询问时,又得到了不一样的答案。

一位淘宝卖家工作人员告诉记者:“您如果需要定制广告‘二维码’,可以联系快递驿站处理面单的工作人员,有需要的话可以留个您的联系方式,我们转达。”

当记者给对方提供电话号码后,没过多久,一位自称“菜鸟驿站”的工作人员打来电话,对方表示,对于广告投放的素材,他们会有一个规范设置,有些行业广告不能投放,例如金融类、整形整容类以及拉人进群涉及诈骗的这类链接,是无法通过审核的。

“之前碰到过一个跳转很多次的链接,最后跳转到哪里去了也不知道,是一个聊天群,在里面就有人被‘杀猪’(诈骗)了。”该工作人员说道。

然而,当记者问到已经通过审核的广告链接,是否还能更改链接里的内容时,对方表示这个他们无法做到,但是商户要在自己的网站里更改内容,他们也无法阻止。

本报综合消息

汇总购物骗局 提醒市民留神陷阱

一年一度的“双11”再次点燃消费者热情,各大购物平台的“预售”模式也已经开启。然而,“双11”不仅仅是买家与卖家的盛会,也可能是网络诈骗人员的“狂欢”。天津反诈中心汇总近期购物骗局,提示市民开心购物的同时要警惕背后的陷阱。

冒充客服操作“退款”

市民小王接到一个自称某电商平台客服的电话,对方准确报出了小王近期购买的化妆品名称和订单号,并称商品被检测出质量问题,现在要进行全额退款赔偿。随后,客服让小王添加了一个QQ号,并在QQ上指导她进行退款操作。客服先是让小王打开支付宝,查看借呗额度,并让小王从借呗中借出一笔钱,转到指定的“安全账户”,声称这是为了验证小王的身份,退款完成后这笔钱会自动返还。小王按照客服的指示操作后,却发现自己不仅没有收到退款,还被骗走了从借呗中借出来的5万余元。

直播间买珠宝卖家消失

张先生在刷短视频时看到一场直播推销翡翠手镯,精致的款式和低廉的价格让他心动不已。他随即联系主播索要购买链接,并按照指引加入了客服的聊天窗口。客服发来的购物链接显示支付失败,对方便提出他可以直接通过银行卡转账完成购买。张先生未多想,通过手机银行向对方提供的账户转账6500元。付款后,他发现无论是直播间还是卖家账号都消失无踪,彻底失去联系。意识到被骗后,张先生迅速报了警。

低价售卖相机骗局

李先生在朋友圈刷到一则诱人的信息,宣传低价售卖相机。正好打算购入一台相机的李先生顺势点开广告,页面引导他添加了一个企业微信好友,李先生立刻与对方客服沟通。对方表现得十分专业,还给出了多种相机型号供选择。选定相机后,对方要求他将费用分两次转到指定银行账户。李先生按要求向指定账户转账1万余元。然而,当他再联系对方确认发货时,发现自己已被拉黑,他才意识到自己被骗了。

“团购”手机预付款打水漂

在网上发布开箱视频,展示自己刚刚购入的最新款手机,主播表示如果大家感兴趣可以考虑搞一次团购,价格十分诱人。张某赶忙添加了主播的微信号,又担心网上购物不靠谱,经过沟通达成一致,张某先预付一半的货款,等手机到手并验收后再支付余下的款项。张某支付预付款后,先是收到了一个显示在运输中的快递单号。转过天来,卖家联系张某称快递出现问题,原有的单号作废,需要换一个新的单号。然而,新快递单号始终没有收到。等了一段时间,张某发现自己被对方删除了微信好友,而网上的短视频账号也已注销。

没挡住扫码抽奖“诱惑”

市民马先生手机收到名为“双11狂欢购、××旗舰店坚果大礼包”的邀请卡信息。随后,其通过支付宝扫描邀请卡上的二维码进入群聊,并下载对方指定的App参与抽奖活动,只需要听完歌曲便可领取佣金,马先生按对方要求完成两单任务后,系统提示数据异常,称要以用现金方式修复系统,要求马先生邮寄2万元现金到某门店。马先生寄现金后发现被骗,共计损失2万余元。

刷单不停 等不来的“返利”

市民林女士收到一个内含“某电商”感谢信的陌生快递,附有“双11狂欢0元领三重豪礼”的宣传单,刮开涂层后显示“中奖”了。“客服”以想要免费领取礼品先要完成任务为由,诱导林女士下载某App刷单。她按照“客服”指示不断刷单,小赚一笔后,“客服”突然告知她某个操作步骤出现了问题,要想继续返利,需要支付25万元来修复出错的操作,得到林女士同意后,对方又以线上不能进行大额转账为由让她去银行取出现金,然后预约网约车让司机将打包好的现金包裹送到指定地点。没想到现金寄出后,林女士发现自己仍旧无法获取“返利”,“客服”又以“修复信誉”等理由要求她继续付钱。直到她资金不够,对方要求她去某平台贷款时,林女士才意识到被骗。

银行卡瞬间被转走近3万元

市民李先生在手机朋友圈点击了一个电商平台抢红包的链接,显示抢到了188元的“现金礼包”,按链接上的提示输入姓名、身份证号和银行卡号等信息后可进行提现。李先生按照要求操作后,银行卡随即就被转走了27500元。这是骗子瞄准“双11”各大电商企业发红包的做法,制作山寨网页,借此收集大量个人信息,进而实施诈骗。

帮好友“代付”被骗

杨先生收到好友“刘某某”的信息,请求帮忙代付购买一款包包,杨先生信以为真,按照“刘某某”提供的二维码扫码进入到亚马逊购物页面,根据对方要求,先付定金才能抢购包包,杨先生便按客服提供的转账方式向对方付款和转账,后经与朋友核实发现并无此事,杨先生这才意识到被骗,损失共计2万余元。

民警提示

这段时间诈骗案例分为冒充电商类物流客服诈骗、虚假购物类诈骗、刷单返利类诈骗,以及虚假红包等几类。

“双11”期间,各种抽奖活动较多,消费者收到这类信息后一定要仔细甄别,向官方客服联系求证。网购时一定要选择正规交易平台,不脱离官方平台进行交易,对避开正规购物平台,要求添加微信、QQ开展交易的卖家,一律停止交易。购买商品时不要贪小便宜,要对异常低价的商品提高警惕,凡是在购物前需要先行充值、垫付资金、交付手续费、保证金等均属诈骗。遇到“账户异常”“缴纳保证金”等情况务必谨慎,不要轻易汇款、转账。

同时,记住不点击陌生链接、不扫描陌生二维码、不随意加入陌生群聊,如果经常在网上购物,建议在手机上安装“国家反诈中心”App,为自己创造安全的防护网。

本报综合消息