投资“二维收款码”?原来是非法集资

警方:对“快速致富”的项目务必提高警惕

随着“扫码支付”的普及,不少商家都会在第三方支付平台中注册“二维收款码”以便于收付款。但有不法分子却以此编造高返利的投资项目,骗取投资者的血汗钱。近日,广州海珠警方在“八大专项行动”“飓风2021”专项行动中,侦破一宗以投资认购伪造的实体商家“二维收款码”获取高额分红为名,非法吸收公众存款750万元的案件,抓获张某(男,47岁)、李某(男,40岁)等犯罪嫌疑人14名。

鼓吹比开商铺更“靠谱”,“躺赚”分红收益

6月的一天,市民常先生到海珠区公安分局经济犯罪侦查大队报案,称被“团X公司”以投资认购第三方支付平台实体商家“二维收款码”的方式,骗取了50多万元。

经了解,2019年7月,常先生在朋友的介绍下,参加了一场由“团X公司”组织的招商推荐会,从中得知该公司旗下的第三方支付平台——“熊X平台”,正在推广一个引流投资项目。投资者可以通过认购该平台里的各实体商家“二维收款码”的形式参与投资,每月能获取该商家“二维收款码”当月收款额的0.05%和广告推销的10%作为分红收益。

推荐会中,该公司负责人张某介绍:“投资该项目比直接经营一家商铺更‘靠谱’,所有风险均由商家和平台承担。投资者无需支付店租水电,不用担心盈亏风险,就能‘躺赚’分红收益。”张某还承诺,每个均价200元的“二维码”每月最高可获收益能达50元。

于是,常先生在2019年10月至2020年1月期间,以平均每个“二维收款码”200元的价格,先后认购了2800个商家的“二维收款码”,共投资了57万元。

起初,常先生每月都能如期收到稳定的收益,并能在该平台查询到相关实体商家的详细运营情况。但从2020年2月开始,该公司以疫情、经济不景气等为由,多次暂缓或暂停发放分红收益,该平台也开始暂停更新相关商家的运营数据。2020年9月,常先生突然发现该平台已无法登录,投资进去的本金也已经无法提现,相关负责人相继失联,实地上门查看才发现,该公司的办公室早已人去楼空。

精准核查锁定证据,跨省抓获幕后头目

接到报案后,海珠警方立即成立专案组展开侦查。办案民警一方面积极联系相关投资受损人到公安机关报案,深入了解涉案公司的人员构成和作案手段,一方面加快核查涉案公司的背景信息和资金流水,固定相关犯罪证据。

经过近一个月的缜密侦查,专案组查明,2019年9月至2020年10月期间,该公司负责人张某伙同李某等人,在未经国家行政主管部门批准的情况下,在该平台伪造实体商家“二维收款码”,并以投资认购这些商家“二维收款码”获取高额分红为名,非法向社会公众募集资金,共计向200多名投资者出售“二维码”4万多个,涉案金额达750万元。

7月21日,专案组兵分多路展开抓捕行动,分别在重庆抓获该公司销售经理李某,在广州多地抓获、劝投销售团队成员12人。9月28日,办案民警在重庆将潜逃外地的幕后头目张某抓获归案。

经审讯,犯罪嫌疑人张某等人对其作案行为供认不讳。

操纵后台伪造“二维码”,利用投资款偿还债务

民警经审讯掌握到,张某于2017年与多名股东合资成立“团X公司”,开发经营了一款第三方支付平台“熊X平台”。该平台原本是专门为商家提供二维码收款服务,收益来源主要是消费者扫码支付产生的手续费和为商家刊登广告的费用。

2017年至2019年期间,该公司由于主推的该平台发展不尽人意,平台商家、用户数量以及各项收益均远未达到预期,导致公司债务高筑、资金链断裂,股东相继撤资。

为偿还公司债务,张某找到昔日认识的“销售专家”李某出手帮忙。李某提出了一个“大胆”的想法,就是由李某及其销售团队负责将该平台重新包装成一个“高质量”的第三方支付平台,以高额分红为名,通过网络推广、现场授课、亲友介绍以及举办大型招商推荐会等方式,将商家“二维收款码”的收益分拆卖给社会投资者。

在明知平台实际商家寥寥无几的情况下,张某仍然选择和李某合作,对外谎称该平台关联绑定着全国各地数十万商家,对内大量伪造商家“二维收款码”和操控实时收益数据,利用新进资金支付对投资者承诺的高额分红,以及偿还公司债务。随着“雪球”越滚越大,该公司最终因入不敷出而倒闭,该平台也被关停。

目前,警方已依法对犯罪嫌疑人张某刑事拘留,对李某等13名犯罪嫌疑人执行逮捕。案件仍在进一步侦办中。

警方提醒:

市民群众应理性投资,面对以“高额回报”“快速致富”等为噱头的投资项目务必要提高警惕,谨防落入非法吸存、非法集资诈骗陷阱。如发现从事此类违法犯罪活动的单位或人员,或者发现自己、亲友被骗参与其中的,应及时向公安机关举报。 **(信息时报)**

手机突然变静音?要当心了!

如果你遇到这种情况,千万警惕 陌生链接不要点

手机还在 钱被转走了

案例一: 辽宁省沈阳市的智先生收到朋友发来的信息,便顺手点击了短信上的网页,点开之后,并没有什么内容,但收到两条信息,一个是“激活成功”;一个是“软件安装完毕”。见手机也没有什么异常,智先生也没在意。没想到第二天早上智先生醒来后,翻看手机有10余个未接来电,随后看到有60余条短信提醒。原来手机变成了静音模式,自己的两张银行卡被盗刷1万余元。

案例二: 广东省广州市的吴先生收到了一条陌生号码发来的短信。短信上写着自己的名字,吴先生以为是某个没存号码的朋友发来的,就点击了短信中的链接。

由于手机并未出现什么异常,吴先生便没太在意。可一个星期之后,银行突然发来一条消费短信,原本存有5万多元钱的一张银行卡,余额竟然只剩下300多元钱了。 吴先生把手机拿到客服那里检查,被告知他的手机中了木马病毒,在一个星期内丧失了接收短信的功能,一个星期后木马病毒失效,短信功能才会恢复。

揭秘:骗局流程分五步

验证码是金融机构在用户进行诸如修改密码、转账等操作时向用户预留手机号码中发送的一次性密码,没有验证码无法进行操作,而要想获取验证码,犯罪分子最常用的手段就是向目标手机发送木马病毒。骗局流程如下:

1.植入木马。骗子群发打折优惠、假扮熟人等短信、链接网址植入木马病毒。

2.运行病毒。受害人点击后,木马就在手机运行。

3.监控手机。骗子随时掌握受害人在手机操作过的银行卡信息。

4.盗取信息。骗子盗取银行卡号,开通快捷支付,截获验证码。

5.刷走钱财。骗子操纵开通手机理财服务,把钱从银行卡转走。

提醒:陌生链接不要点

骗子一般在手机短信木马病毒链接前加上一句话,诱导你点开网址链接,诸如“聚餐照片”“老同学照片”等等,都是以“熟人”为切入点,还有就是以各种折扣优惠信息为诱饵,让接收方在不知不觉中随手点开病毒链接,植入了木马病毒。

而这种恶意程序,会优先运行,能盗取手机上一切跟账号、密码有关的资料,因此,只要是接收到类似短信,切记不点、不点,要马上删除。

如果不小心点了,要紧急挂失手机上的支付宝、股票等涉及财产的账户,确保账户安全后,再将手机拿到维修点重新安装系统。 **(河北省处非办)**

本报地址:石家庄市中山东路313号 邮编:050011 广告部:88629345 发行部:88629333 88629334(外埠) 广告经营许可证:1301034C00004号 石家庄日报印刷厂印刷 发行方式:自办、邮发