

刷单诈骗高居发案之首,冒充熟人诈骗出现新伎俩,市反诈中心提醒—— 小心! 骗子正潜伏在你的电脑

昨天,市反诈中心通报我市打击治理电信网络诈骗犯罪工作最新情况。通过对今年6月发案数据统计分析,当前在南通,刷单返利类、虚假购物服务类、虚假网络投资理财类、冒充领导熟人类诈骗是群众最易中招的诈骗类型,超过全市电诈发案总量的六成。

“我从来没有加过骗子的微信,他是怎么成为我的微信好友,冒充领导让我转账的?”在一起财会人员遭遇的电诈案件中,我市警方还发现了骗子远程操控电脑的作案新手段。

占比超1/3,刷单诈骗高居发案之首

市民程先生(化姓)怎么也没有想到,夜晚在家刷视频的放松时刻,5万余元积蓄被骗。6月23日深夜,程先生在手机QQ小世界刷视频时,不小心触碰一条广告,被推荐安装了一个陌生聊天软件。之后,软件里有人将他加为好友,拉他一起刷单赚钱。“‘老师’指导操作,在平台里指定了一个主播商品让我点赞、刷玫瑰、评论,完成后给我返钱。”抱着试试看的心态,程先生花费37元完成首笔刷单,很快获得45元返利。他紧接着做了第二单,支付300元,对方返还了360元。第三单,程先生转出1800元,对方却说操作错误,想要返现需要再做一单,金额是1800元的4倍,加上手续费,总共9600元。“看到群里其他人都重新做了,而且都有返现,我就相信了。”24日凌晨,程先生转出9600元做了第四单,不料对方仍说他操作失误。“群里都在抱怨,我也觉得好像被骗了,但群里的托儿还在诱导我。抱着侥幸心理,我做了第五单。”这一次,程先生转出4.58万元,对方以程先生没有在电子回单上附言为由,再次认定程先生操作失误,告诉他想要返现得走“绿色通道”,再转4.58万元。此时,程先生如梦初醒,知道遇上了电诈陷阱。因为向诈骗账号转了钱,24日一早,程先生便接到我市公安民警打来的反诈预警劝阻电话,他随后

前往派出所报了案。

“这是一起典型的刷单返利诈骗,此类诈骗已经成为我市发案最高的诈骗类型。”市公安局刑警支队一大队副大队长宋律钊说,骗子首先在短信、网站、社交软件、短视频等平台广发广告,以“低门槛高收益”“先垫付再返利”“刷单时间地点自由”等吸引宝妈、学生、无业人员、兼职人员等,之后以小额返利“引君入瓮”,前一两次小额刷单,迅速返现并兑现少量佣金来赢取受害人信任,待受害人放松警惕后投入大额资金,对方会以操作失误、系统故障、订单超时等各种理由让受害人重复转账,越陷越深,达到诈骗目的。

市反诈中心统计显示,上月,刷单返利类诈骗占据我市电诈案件总量的37.87%,较去年同期占比上升11.97%,发案远高于其他各类诈骗,是名副其实的“诈骗之王”。

“刷单返利诈骗与网络兼职诈骗、网络招嫖诈骗、退款诈骗、冒充客服诈骗以及网络赌博等相融合,形成复合型诈骗,迷惑性更强。”宋律钊说,比如,骗子先以招嫖短信引诱受害人上钩,之后声称完成刷单任务就能免费“约炮”,最终将受害人引入刷单骗局。“刷单本身就是违法行为,任何要求垫资的网络刷单都是诈骗,不要轻易扫描来历不明的二维码或点击来历不明的网站链接,贪小便宜容易吃大亏。”

冒充熟人诈骗升级,种植木马偷天换日

梳理6月我市电诈案情,尤其值得关注的是,冒充领导熟人类诈骗出现了新手法。

小范(化名)是我市一家公司的出纳会计。6月29日中午,他接到老板发来的微信,言语急促地询问公司账户资金情况,要求她向指定账户转账85万元。当小范完成转账,去找老板签字时,发现老板根本没有要求转账,方知上当受骗。“骗子的头像、昵称和老板的一模一样,我从来没有加过他的微信,他是怎么成为我的微信好友的?”小范充满疑惑,自己的微信设置了添加好友时需要验证,但骗子进入好友列表时,她根本没有收到提示。

“骗子很可能事先通过木马病毒远程控制了小范的办公电脑,偷偷在她微信里添加了好友。”宋律钊说,冒充领导熟人类诈骗近期套路升级。骗子首先通过投资理财、财务交流、内部办公的微信、QQ群或电子邮件,传播名为“2023企业所得税缴纳标准最新版”“电子发票”等压缩文件,该文件打开后内容为空

白,实际是木马病毒。一旦财务人员点击下载并解压,电脑即被植入木马病毒。骗子可通过病毒获取电脑后台权限,实现截屏、录屏、监控等操作,观察公司财务转账及内部交流情况。待时机成熟,骗子就会制造卡机、黑屏,并远程控制受害人电脑端微信、QQ或钉钉,删除老板真实聊天账号,添加“克隆”账号(使用相同头像及昵称),进而“指挥”公司财务进行转账。侦查中发现,骗子还会利用已经控制的财务人员聊天账号,将木马病毒传播至其他财务交流、公司内部群聊,循环往复,感染更多电脑。

“来历不明的链接、邮件及文件切勿轻易点击或打开。”宋律钊提醒广大财务人员,如果曾经点击过诸如“2023企业所得税缴纳标准最新版”“电子发票”等文件,打开后是空白的,务必立即检查电脑是否中毒,以防被骗子潜伏、远程控制。日常工作中要严格落实财务审批制度,对于借款和资金汇款要求,务必向责任领导当面求证或拨打手机电话核实(非微信电话),确认真实性后再进行操作。



CFP供图

扫码免费领礼品?“地推引流”小心有诈

市反诈中心数据显示,6月,除了高居诈骗榜首的刷单返利诈骗外,其余发案较高的诈骗类型依次是虚假购物服务类、虚假网络投资理财类、冒充领导熟人类、冒充电商物流购物类,占比分别为10.09%、9.61%、7.14%、5.90%。其中,虚假购物服务类、冒充领导熟人类诈骗同比去年占比均有小幅上升。

今年5月初,女子小雯(化名)在小红书上看到一个论文代投机构,主动联系对方,添加了微信,谈妥支付1万元,由对方负责论文润色、定稿、投稿并保证出刊。之后,对方告知论文已送至杂志社,主编认为适合发表,还通过邮件发来杂志社的接收函,小雯陆续转去1万元费用。6月3日,当她索要论文润色后的版本时,对方竟要求她再支付2万元的版权押金。小雯觉得这笔费用十分蹊跷,不愿支付,最终提出不再发表论文,但对方拒绝退款。“后来,我在网上没有查询到这个杂志的刊号,发现很多人遇到了同样的骗局。”小雯意识到上当受骗,随即报警。

无独有偶。6月初,小超(化名)在闲鱼上看中了一辆二手摩托车。卖家标记只能微信联系,小超于是添加了对方的微信,支付定金。之后,对方发来摩托车的装车视频,小超支付了部分货款,还添加了货车司机的QQ。得知摩托车运抵南通后,他又按要求支付了尾款,前前后后付款4.3万元,最终发现是一场骗局。

“只收款、不发货的虚假购物服务类诈骗,长期占据我市诈骗案件‘前三’。”宋律钊说,此类诈骗瞄准喜爱网购、淘货的人群,先在微信群、朋友圈等网络社交平台或正规网上商店等渠道发布商品广告信息,以优惠

打折、海外代购、低价转让、0元购物等方式为诱饵,诱导被害人脱离平台进行交易,待被害人为购物付款后,就会以各类理由延迟、拒绝发货,或者直接失联,被害人到最后也不会收到约定的商品、货物。“低价高质商品私下交易要当心,跳过平台私加QQ、微信风险大。”

相比虚假购物服务类诈骗,虚假网络投资理财类虽然发案数量略少,但案损更大。前不久,我市退休居民花女士(化姓)被骗子拉入炒股QQ群,下载了一款炒股软件,不到一个月时间,陆续投资27.9万余元,结果发现上当受骗。

“受害人一旦落入虚假投资理财陷阱,往往损失惨重,一代人甚至几代人辛苦创造积累的财富流入骗子的腰包。”宋律钊说,此类案件中,犯罪分子以“低投资、高回报、低风险”为诱饵,拉受害人进入各种各样的投资群聊,用直播教程对受害人洗脑,并让受害人直观感受到群里其他人每天都在赚钱,诱骗受害人充值投资,并以各种理由诱导受害人不断注入大量资金,最终平台关闭。“投资应选用正规官方平台,切勿通过不明链接、二维码下载登录所谓的投资网站和平台。明显高于市场投资回报的应当作诈骗看待。”

当前,诈骗套路千变万化,很多骗局首先会有“引流”的过程。宋律钊特别提醒广大市民,遇到在街头、市场出现的扫码就能免费领礼品等活动,要保持足够警惕,以防个人信息被收集贩卖给诈骗分子或是被不法分子拉入线上聊天群,伺机抛出刷单返利、高回报投资理财等诈骗诱饵,“切记不要轻易添加陌生人为好友,不要轻信陌生人的言论”。

本报记者张亮 沈雪梅