2024年8月5日 星期一 策划:李婷 责编:哈欣 美编:孟宪东 TIANJINDAILY | 天津日报

有人会认为,我没钱,不会被骗;也有人会觉得,我文化水平高,不可能被骗;还有人会觉得,电诈手段我都知道,骗不了我。

但事实真的是这样吗?

警惕!电诈披上新羊皮

■本报记者 韩雯

暑期本是放松身心的时刻,打打游戏、刷刷视频、网购心仪的玩具,没想到却被诈骗分子盯上。免费领取游戏皮肤,点击进去,却收到“警方”发来的提示——未成年人参与领取福袋是违法行为,你的信息已被警察锁定!恐惧、害怕,按指令一波操作后,父母银行卡里的钱不翼而飞。

公司的会计因误点了一个陌生链接,电脑被诈骗分子操控——删除老板的微信,然后将其加为会计的好友,改成老板的头像,命令会计转账,令人察觉不到的“调包计”让公司损失上百万元。

“刷视频就能赚钱”“听小说就能赚钱”“答题就能赚钱”“走路就能赚钱”……在部分社交平台上,有不少软件号称可以让用户赚钱。因为有大把时间,所以刷手机“做任务”赚钱就成了不少老年人的日常生活状态。突然有一天“客服”来电,需要缴纳服务费,为了不缴费,着急,鬼使神差被骗子带走了理智,钱袋子也被卷走……

当前,我市正在开展“全民反诈在行动”集中反诈宣传月活动,听听公安机关公布的真实案例,对于电信网络诈骗的迷惑性,您可能会有不一样的认识。

这些案例就发生在我们身边,为什么电信网络诈骗防范宣传了这么多年还会有人上当?如何真正有效地预防电信网络诈骗?高发的电信网络诈骗又有怎样的特点?带着这些问题,记者采访了我市常年与电诈分子博弈的反诈民警。

上半年我市电诈案件大数据

当前,电信网络诈骗犯罪形势依然严峻,数据最有说服力。

从我市反诈中心获悉,今年1月至6月,我市电信网络诈骗案件发案数占总刑事案件的24.35%。通过对被骗案件进行梳理与分析,目前,高发电信网络诈骗类型分别为——刷单返利类诈骗,立案、损失占全部案件的27.5%、28.9%;虚假购物、服务类诈骗,立案、损失占全部案件的13.2%、7%;冒充领导、熟人等特定身份类诈骗,立案、损失占全部案件的7%、7%;虚假投资理财类诈骗,立案、损失占全部案件的6.5%、16.8%。

受侵害群体与文化水平、社会经历关系不大,诈骗方式对应的是各种各样的人群。

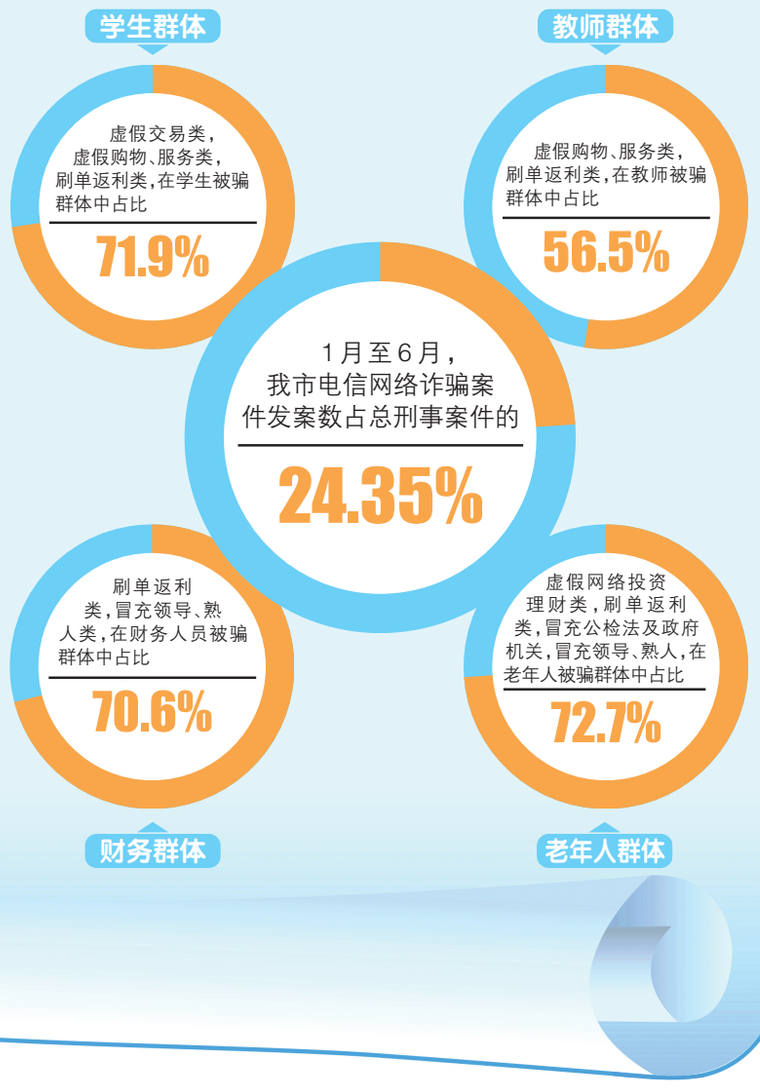
学生群体方面,被骗手段主要集中在网络游戏产品虚假交易类,虚假购物、服务类,刷单返利类,这三类手段在学生被骗群体中占比71.9%。

教师群体方面,被骗手段主要集中在虚假购物、服务类,刷单返利类,这两类手段在教师被骗群体中占比56.5%。

财务群体方面,被骗手段主要集中在刷单返利类,冒充领导、熟人类,这两类手段在财务人员被骗群体中占比70.6%。

60岁及以上老年人方面,被骗手段主要集中在虚假网络投资理财类,刷单返利类,冒充公检法及政府机关,冒充领导、熟人,这四类手段在60岁及以上老年人被骗群体中占比72.7%。

针对高发的电信网络诈骗类型,我市反诈民警以案为例,解析诈骗特点、手段、方法,层层揭开诈骗套路的面纱,希望提高群众的防范意识。



刷单诈骗——变种最多变化最快 成目前“诈骗之王”

案例

不费吹灰之力,动动手就能有钱进账,真有这样的好事吗?

万某在用手机看小说时,被一则广告吸引,随后按照广告的提示进入一个聊天群,里面有人声称通过下载某款软件赚了钱。对于不费吹灰之力,动动手就能有钱进账的好事,万某动了心。

万某点击了群内链接,进入了一个类似博彩的界面。初尝甜头后,他被诱导参与更多任务以获取更高返利。然而,当他试图提现时,却被告知系统升级资金无法取出,需再次充值才能修复。万某多次转账后仍无法提现,虽然最终意识到被骗,但已经损失了5万余元。

刷单返利类诈骗的特点是需要安装涉诈App、建群管理、按需设局,引流形式多样。例如,将刷单与找工作、网络赌博、同城交友、点赞打榜等相结合,刷单诈骗已逐步演变为变种最多、变化最快的诈骗类型,成为目前的“诈骗之王”。

手段特征

第一步引流阶段。通过网页、短信、社交软件、短视频平台等渠道发布信息,吸引受害者上钩。

第二步小额返利。受害者充值以后,诈骗分子会让受害人提现小额利润,以骗取受害人信任。

第三步完成骗局。诈骗分子以“任务未完成”“卡单”“操作异常账户被冻结”等各种借口,拒不支付本金和佣金,甚至诱导受害人加大投入,进而骗取更多资金。一旦受害人识破骗局,诈骗分子就会切断一切联系。

警方提醒:返的佣金是“饵”

凡是小利引诱、一单多任务、索要账户解冻费或者充值才能退本金的都是刷单诈骗,凡是以返还佣金为诱饵、逐渐增加刷单额度的兼职工作都是诈骗。

刷单违反《反不正当竞争法》,兼职刷单是骗子包装成兼职工作的骗局,不要被“足不出户、几百进账”“动动手指、日进千金”等迷惑性语言所蒙蔽,兼职刷单是骗子给你的一项永远无法完成的任务,刷单套路深,务必要当心。刷单诈骗返的佣金是“饵”,一定要擦亮眼睛、切勿上“钩”。

虚假购物、服务类诈骗——代购、0元购 诱你上钩陷阱多

案例

向“卖家”转账,为什么却说钱没收到?

大四学生李某想买两张演唱会门票,通过某款App联系上一个“卖家”。面对迫切需要演唱会门票的买家,“卖家”加价200元同意转让。

谈成价格后,李某向“卖家”指定银行账户转账2096元。本以为付了款就等着拿票了,“卖家”却告诉李某,因其操作错误,需要重新转账,并承诺之前的付款会退回。李某也没多想,就按照“卖家”的指令,再次向指定账户转账2096元,还是无法收款,“卖家”让李某扫码进入指定QQ群与“财务人员”联系,沟通付款事宜。

李某扫码入群后,在“财务人员”的要求下,下载了一款屏幕共享App,登录后,按照“财务人员”要求开启屏幕共享,并通过手机银行向“财务人员”转账2096元。转账没多久,李某收到银行卡扣款15000余元的短信,这时才发现自己被骗了。

手段特征

0元购物、消除个人不良征信,当心掉进骗子的陷阱!

案例中的诈骗方式属于虚假购物类诈骗。诈骗分子通过社交软件、网页、短信、电话等渠道发布商品广告信息,通常以盲盒购买、海外代购、低价转让、0元购物等方式为诱饵,诱导被害人与其联系,待被害人购物付款后,要么玩起了失联,被害人未收到约定的商品、货物;要么以加缴关税,缴纳定金、交易税、手续费等为由,诱骗被害人继续转账汇款。

除了虚构物品实施诈骗外,还有虚构服务骗取钱财。诈骗分子通过推广发布信息,谎称可以提供正常的生活型服务、技能型服务,例如,代为生活缴费、音乐制作、网站制作、论文发布等,以及谎称可以提供非法的各种虚假服务,例如,消除个人不良征信、证件办理、提供定位、处理交通违章等,待被害人上钩后,以缴纳定金、保证金为由,诱骗被害人转账汇款。

警方提醒:认准正规平台

网络购物需谨慎,高质低价商品私下交易要当心,防止财物与信息两空,注意甄别所使用的购物软件、交易平台是否正规、可信,对跳过平台私加QQ、微信的卖家一概终止交易,更不能随便点击对方发来的链接。

通过微商、微信群交易时,一定要详细了解商家真实信息,确定商品真实性,多方面综合评估,交易时最好有第三方做担保。

网络二手平台交易存在风险,在购买物品或者转卖闲置物品时,都应该选择有信誉保证的店铺或用户,财物交易也要在该平台上进行,采取正规的交易流程,选择有第三方担保的交易方式,一旦出现问题方便退换货,对于陌生人发来的购物链接要提高警惕性。

最后,在办理各类服务事项时,要到正规官方服务机构当面办理,确实需要通过平台办理的,一定要通过官方推送的正规平台,凡是让缴纳定金、交易税、手续费的都是骗子。

冒充身份类诈骗——假老板“设套” 真财务“中招”

案例

电脑竟“自己”动起来,假老板“设套”,真财务“中招”!

一天,某公司财务胡某的电脑里弹出一条信息,显示是“企业所得税缴纳标准最新版”的压缩文件,认为与公司交税有关,胡某没多想就点击了压缩文件,但无论点击多少次,压缩文件就是打不开,胡某就不再理会了。

当胡某离开工位,令人意想不到的事情发生了。电脑屏幕上的鼠标竟然“自己”动起来了,“电脑”点开公司内部文件及胡某的QQ聊天记录,删除胡某与老板的聊天记录,并“克隆”老板账号。后胡某被“老板”拉进一个QQ聊天群,“老板”在群聊内让胡某转账到指定账户。钱转完后,经与老板核实,胡某才发现被骗。

手段特征

此类骗局中,骗子会提前潜伏在财务人员的群里或者以邮件的方式发一些木马病毒的链接,财务人员一旦点击就会被骗子远程操控。在另一端,骗子会一直观察财务人员的用网习惯和转账方式,然后在获取领导真实姓名、职务、照片等相关信息后,将真领导删除,然后伪装成领导,在聊天群里,假装有订单或急需转账,并提供一些虚假的凭证、文件或相关订单信息,进一步迷惑财务人员,使其相信急需转账的真实性。

警方提醒:不要轻易添加陌生好友

不要轻易添加陌生QQ、微信的好友申请,特别是涉及公司老板、负责人名字的QQ、微信,一定要核实清楚。不要轻信QQ(群)、微信(群)中涉及转账汇款的信息,有公司老板、负责人通过网络社交工具要求转账汇款,一定要见面或者视频进行核实。同时提醒财务人员不要点击来历不明的邮件、网址链接、文件等,应定期查杀电脑病毒,加强防范能力,避免不法分子通过木马病毒盗窃电脑信息。

虚假投资理财类诈骗——瞄准中老年人 损失金额最大

案例

想钱生钱,找“投资理财专家”靠谱吗?

想理财却不懂方法的张先生希望借助网络寻找到技巧,于是,其通过某款软件搜索“投资理财”,看到一个投资理财专家的账号,便主动添加对方进行私信联系。

在说明意图后,“投资理财专家”让张先生下载一款聊天软件,在传授经验的过程中,“投资理财专家”让张先生点击一个链接,然后登录网页,教其如何投资赚钱。今年5月,在5天的时间里,张先生通过网页提示转账共计90万元,回报确实兑现了,却只有1万元。当其想再次提现时,“投资理财专家”不见了踪影,发现被骗后,张先生报警,共计损失89万元。

虚假投资理财类诈骗的个案损失金额最大,被害人通常为热衷于投资、炒股的群体,其中30岁至50岁的女性和刚退休的中老年人居多。这类诈骗的特点是以婚恋交友、炒股赚钱、提供彩票中奖内幕消息、教育机构退费、提供高额回报为名,诱导被害人进行投资理财。

手段特征

第一步:引流。骗子通过网络社交工具、短信、网页等多种渠道发布推广股票、外汇、期货、虚拟货币等投资理财的信息,或者通过在公众号、微博、短视频平台等投放广告,宣称有内部消息和投资门路从而网罗目标,寻找受害人群体并建立联系。

第二步:洗脑。在建立联系后,通过聊天交流投资经验、拉人进入“投资理财”群聊、听取“投资专家”“理财导师”直播授课等多种方式,以能够获取内幕消息、获得丰厚回报等谎言取得被害人初步信任。

第三步:诱导。在骗取信任后,逐步诱导被害人登录其提供的虚假网站、扫描二维码下载其分享的手机App,指导进行投资理财操作,引导被害人进行小额投资并获得低额返利,取得进一步信任后诱导加大投资。

第四步:收割。诱导加大资金投入,当被害人想要提现时,骗子会以“登录异常”“服务器异常”“银行账户冻结”等理由要求缴纳解冻费、保证金后才能完成提现,若不如数缴纳,投资理财账户内的资金就会全部损失。最后被害人会被对方拉黑,投资理财网站、App等也无法登录。

警方提醒:勿信只赚不赔的“买卖”

不要随便加入来历不明的QQ群、微信群,不要轻信陌生人发布的“发财”信息,不要相信投资小、回报快、收益高的字眼,切勿相信只赚不赔的“买卖”,不要被暂时的高利率迷惑双眼。在网络上进行投资理财时,务必要增强防范意识,一定要选择正规渠道进行投资,通过金融机构官方平台购买投资理财产品;不要向陌生账户转账汇款,一旦遭遇诈骗,保留好证据并立即报警。

(文中当事人均为化名)

警方说法

反诈宣传力度大,为何仍有人频频受骗?

为了筑牢反诈防线,近年来,公安等相关部门不断加大反诈骗宣传力度,通过各种渠道向公众普及防骗知识,提高民众的防骗意识。然而,令人困惑的是,尽管宣传力度不断加强,诈骗案件却仍然层出不穷。根据我市反诈民警介绍,诈骗案件仍然屡禁不止,原因可以归结为以下几点:

一是诈骗手段不断更新。就拿当前出现的最新诈骗手段来说,随着公安机关对涉网诈骗资金追查能力不断增强,追查时效不断提升,有效挤压了诈骗分子的洗钱空间,其转而向线下大量使用银行卡取现、购买黄金、线下消费等“短平快”的方式转移涉诈资金,且呈现多发、高发态势,近期我市就发生多起诈骗分子诱导被骗人购买黄金进行线下接收进而实施涉网诈骗案件。

今年4月,家住和平区的许某,接到自称是海口市公安局民警的电话,对方称有人用她的身份信息注册手机号发布违法信息,涉及经济犯罪,准备向其下达资金冻结令,后对方以优先调查资金监管为由,要求许某将银行卡内的钱换成90万元左右的黄金进行监管。

对于对方提出的要求,许某信以为真,于是到商场购买黄金,之后在家中将黄金交给了对方安排的接头人员,对方失联后,许某发现被骗报警。

二是在利益的驱使下,有人沦为电诈“工具人”。电诈“工具人”是一种比喻,是对帮助电信网络诈骗团伙实施违法犯罪行为相关人员的统称。

当前,电信网络诈骗犯罪整体形势严峻复杂。在电诈犯罪链条中,电诈分子需要将赃款分散转入多个层级的他人银行卡中,隐蔽赃款来源,逃避公安机关追查;境外电诈分子通常远程操控境内的手机、插卡设备拨打诈骗电话,冒充境内电话,具有极强的迷惑性;电诈分子还使用他人互联网账号,或冒用身份向亲友骗钱,或用来发布违规广告、推广引流信息,实名认证的支付账户还会被用来洗钱……

为完成上述违法犯罪行为,电诈分子大肆收购、获取“两卡”和个人信息,发展“跑分”洗钱、推广引流等网络黑灰产,利用多种手段利诱蒙骗群众沦为电信网络诈骗的“帮凶”,成为电诈“工具人”。根据法律规定,如果“工具人”具有犯罪的故意、过失,则构成帮信罪、诈骗罪共犯,将面临“牢狱之灾”。因此提醒广大群众提高防范意识和分辨能力,警惕诈骗新手法、不做电诈“工具人”。

三是贪念心理。无论人防还是技防,最难的还是心防,其实很多受害群众,都曾接受过反诈宣传,但在巨额利益诱惑下,往往沦陷。为了钱袋子不被觊觎,警方传授反诈秘籍,只需要做到“三不一多”:陌生来电不轻信、陌生链接不点击、个人信息不透露,转账汇款多核实,即使对方说得天花乱坠,也不会轻易被骗。