2026年6月16日 星期二 责编:祁振 美编:王宇 TIANJINDAILY 天津日报

诈骗从“随机碰运气”转向“精准定制”

警惕“生活场景化”骗局

■ 记者 韩雯 史莺

“哎呀,反诈中心怎么又给我打来了?”

“我,肯定不会被骗!”

“你——确——定?”

当前,全国正在开展以“不听不信不贪恋,构筑反诈‘心’防线”为主题的“全民反诈在行动”集中宣传月活动。与此同时,《2026年电信网络诈骗犯罪白皮书》正式发布。白皮书显示:就在过去一年,国家反诈中心平均每天下发超200万条预警指令,这其中的很多人,可能只差一步,就坠入深渊。

为何只差一步,便浑然不觉坠入骗局?因为当前的骗局太贴近生活了。

在对近年来电信网络诈骗案件进行系统梳理后,我市公安机关发现:骗局早已不是广撒网式的低级套路,而是悄悄渗透进日常生活的方方面面。点外卖、收快递、刷短视频、网上聊天,这些再平常不过的事,都可能成为骗子精心设计的“入口”。更值得警惕的是,诈骗正在从“随机碰运气”转向“精准定制”,针对不同人群、不同场景、不同心理状态,量身打造骗局。

一条快递短信,骗走18万元;一个投资群聊,套走25万元;一次屏幕共享,转走45万元……你以为骗局离自己很远,其实它就发生在我们身边。

骗术新特征
专挑熟悉的场景下手

市民张女士收到一条短信:“您的快递因地址不详无法配送,请及时联系客服。”她确实有快递在途中,没多想便拨通了电话。对方自称是短视频平台客服,称曾寄送过一份直播会员纸质合同,张女士并未购买会员,为避免扣费提出取消。对方引导她下载“短视频平台内部理赔App”并开启远程操控。其间,手机黑屏,待恢复正常后,张女士多张银行卡及数字钱包资金被掏空,损失18万元。

事后民警问张女士:“当时没觉得不对劲吗?”张女士愣了很久,回应道:“我以为就是在处理快递的事,怎么会想到是诈骗呢?”

张女士的遭遇并非个例。市公安局刑侦总队防治电诈支队梳理发现,当前,诈骗正呈现明显趋势——“生活场景化”。诈骗分子在接触受害人之前,会通过各种渠道了解其兴趣爱好、行为习惯乃至心理需求,再将骗局伪装成服务提醒、购物沟通、朋友介绍等日常信息,让接触从一开始就贴合受害人的日常生活场景。

与此同时,骗术在两个关键维度上持续升级:一是精准化,骗子不再盲目群发,而是通过多次试探,筛选出“最有可能上当”的目标;二是情感化,骗子不再冷冰冰,而是热情、耐心、体贴,甚至与受害人建立长期“友谊”或“恋爱关系”,使其从情感上难以拒绝。

六 种话术 骗子最爱这么说

这些升级特征,最终都落实到骗子与受害人一句句的沟通之中。他们反复使用一套成熟的话术套路,让人在不知不觉中上钩。以下是公安机关总结出的六种常见话术套路,他们有的是组合使用,层层递进,如果您在沟通中听到以下类似说法,请立刻提高警惕。

1. 先给甜头

小额返利、免费资料、几元红包,让人觉得“对方是好人”,为后续提出更高要求铺路。

2. 制造紧张

“名额有限”“仅限今日”“不操作就会扣费”,压缩思考时间,诱导冲动决策。

3. 拉近关系

热情沟通、找共同话题、嘘寒问暖,让您觉得对方是“自己人”,降低戒备。

4. 借用身份

借助境外虚拟改号来电,冒充客服、银行工作人员、执法人员、老师、领导等,利用人们对权威和熟悉角色的天然信任实施诈骗。

5. 营造氛围

制造“大家都在做”“邻居刚赚了钱”的从众心理,误导独立判断。

6. 步步为营

先让您做简单操作(扫码、填信息),再层层加码,逐步引导至转账、泄露密码等关键步骤。

为什么容易被骗 三类高发骗局深度解析

公安机关结合真实案例,梳理出当前最为典型的三类高发诈骗路径,并附上“骗术背后的心理陷阱”和“核心防范要点”,帮助群众从根本上理解自己为什么容易被骗。

消费交易类诈骗:“您购买的商品出了问题”

真实案例:市民王先生接到“某电商平台客服”电话,称其购买的商品存在质量问题,要给他三倍赔偿。对方准确说出了订单号、商品名称和收货地址。王先生信以为真,按对方引导操作后,银行卡内1.2万元被转走。

骗术背后的心理陷阱:这类骗局利用了人们对“真实购物信息”的信任。当对方能准确说出订单细节时,大脑会自动降低戒备。同时,“赔偿”“退款”激发了“不拿白不拿”的心理,让人忽略核实。

核心防范要点:凡是自称客服、快递员主动联系说“退款”“理赔”“取消会员”的,一律挂断。官方平台的所有售后操作,都应在原App或网站内完成。记住谁主动打来、谁让您离开官方平台,谁就是骗子。

获利诱导类诈骗:“这个机会您不能错过”

真实案例:李女士被拉入“投资交流群”,群里每天有人晒收益截图。她投500元拿回600元,随后加大投入至15万元,对方又以“账户冻结需解冻费”为由让她线下交付18万元现金,最终损失33万元。

骗术背后的心理陷阱:“先给甜头”是最经典的心理操控术。小额返利足以让大脑产生“这件事是真的”的错觉;“名额紧张”“限时活动”则利用损失厌恶心理,让人害怕错过收益。

核心防范要点:不存在稳赚不赔的投资,正规理财不会让您下载陌生App,更不会要求线下交付现金。记住任何让您“先尝甜头再投大钱”的事,都是在钓您。

权威压迫类诈骗:“我是警察,请您配合调查”

真实案例:一名初中生接到自称“北京民警”的微信好友申请,称其父母涉嫌犯罪,要求“配合调查否则抓人”。孩子被吓住,偷偷拿到家长手机下载指定软件。虽被家长及时发现,但次日家长多张银行卡仍被盗刷近6万元。

骗术背后的心理陷阱:“权威+恐惧”是最高效的操控组合。骗子用“警察”“法官”等身份和“涉嫌洗钱”“会被逮捕”等词制造恐慌,让受害人理性思考能力急剧下降。同时强调“案件保密,不能告诉任何人”,切断求助渠道。

核心防范要点:公检法机关不会通过电话或网络办案,更不会要求转账、提供密码、下载不明软件。凡是自称执法人员、要求“不要告诉家人”“把钱转到安全账户”的,一律是诈骗。挂断后拨打110或去派出所核实,只需一分钟就能戳穿骗局。

诈骗的“三步走”
看懂流程,就能及时刹车

“几乎所有诈骗都遵循三个关键环节。只要在任何一个环节停下来,骗局就无法继续。”市公安局刑侦总队防治电诈支队支队长芦健说。

第一步:首次接触——最容易被忽略的“平常时刻”

骗子通过短信、电话、社交媒体私信、短视频评论区等方式主动联系您。理由永远是日常话题:“快递问题”“优惠活动”“熟人介绍”“投资机会”“账户异常”。这一步的危险性在于,它太“正常”了,“正常”到您不会多想。

第二步:引流与平台迁移——制造“信息盲区”

骗子会要求您“加微信”“加QQ”“下载指定App”“点击链接”。一旦离开官方平台,就失去了交易保护和风险提示,在陌生的聊天环境里,您更容易被操控。

第三步:资金转移——拆解成“正常操作”

无论前面铺垫多少步骤,最终都会落到这一步,要您转账、提供验证码、交出银行卡密码、扫描二维码、线下交付现金。骗子会把这些操作包装成“解冻”“认证”“做流水”“交保证金”等听起来合理的名目。

芦健特别提醒:只要对方要求您“离开官方平台”或“不要告诉任何人”,请立刻停止操作,这是所有骗局的共同信号。挂断电话后,主动拨打官方客服电话或110核实。

警方提醒

只要对方在沟通中同时出现“制造紧张”和“引导您离开官方平台操作”这两个特征,基本可判定为诈骗。正确做法是挂断电话、删除信息、不点击任何链接。

防骗“三部曲” 日常做对 突发稳住 被骗止损

针对日常防护和被骗后的应急处置,芦健从三个层面给出了详细指导。

首先是个人信息防泄露的长效做法。芦健强调,要筑牢浏览与交往底线,不随意点击未知链接、陌生网址,绝不向陌生人泄露身份证号、家庭住址、手机号、银行卡信息及通讯录等核心隐私。纸质单据方面,快递面单、购物订单、车票、外卖小票等印有个人信息的票据,使用后要及时撕碎销毁,不能随意丢弃。手机权限要严格管理,及时关闭各类陌生App的通讯录、相册、定位、麦克风、摄像头等敏感授权,只给正规常用软件开放必要权限。网络社交要谨慎,不随意添加陌生好友,不加入来历不明的群聊,果断拒绝人脸核验、实名绑定等不合理要求。最后,要养成日常安全习惯,安装国家反诈中心App,定期清理垃圾软件,开启骚扰电话和垃圾短信拦截功能。

其次是突发异常时的紧急应对。芦健指出,如果手机突然黑屏、卡顿、不受控制,要立刻强制关机、拔出手机卡、断开网络,千万不要输入任何密码或验证码。开机后第一时间卸载陌生App,关闭所有悬浮窗和远程控制权限。如果被诱导开启了屏幕共享,要立即前往手机设置,关闭所有陌生软件的屏幕录制、远程协助、投屏等功能。一旦已经泄露了验证码、银行卡号或支付密码,要立刻冻结微信和支付宝支付,联系银行客服紧急挂失账户,关闭快捷支付和免密支付,并修改所有社交、支付、银行App的登录密码。

最后,如果不幸已经被骗,要按步骤紧急止损。芦健强调,第一步是立刻报警,拨打110或96110,清晰说明被骗经过、转账时间、金额及对方信息,并尽快前往就近派出所制作笔录。第二步是紧急止付,马上停止一切转账,联系银行、微信、支付宝官方客服,申请冻结个人账户、拦截未到账资金。第三步是固定完整证据,切勿删除任何记录,要保存好聊天记录、通话录音、短信截图、转账凭证、陌生App、对方账号等全部线索。第四步是全面修改账号密码,同时解绑陌生登录设备,关闭异常权限。第五步是严防二次诈骗,被骗后千万不要相信网上所谓“网警追回”“黑客回款”“付费解冻”等虚假服务,所有私下追款都是连环骗局。

记住这几点 骗局就走不下去

对个人而言

“绝大多数诈骗之所以得手,不是因为手段有多高明,而是受害人少做了一次核实。”市公安局刑侦总队防治电诈支队政委单威说,多核实一步,很多骗局就走不下去。

三个“凡是”要牢记:凡是陌生人让您下载App、点击链接的,一律不下载、不点击。凡是自称客服、公检法让您转账的,一律挂断后主动核实。凡是“先给甜头再要大钱”的,一律认定为骗局。

两个“习惯”要养成:网购售后只通过原平台操作,不理会短信、电话中的“客服”。遇到“紧急”“限时”“保密”等字眼,先冷静,问问家人或打96110。

对家庭而言

“未成年人在权威型诈骗中尤为脆弱,老年人则在冒充公检法、虚假保健品类诈骗中风险较高。家长和子女应主动承担‘家庭防骗教育’责任。”单威说。

单威给出建议,家长应该提前进行情境教育,告诉孩子,任何自称警察、老师、客服的人,要求操作手机、转账、提供验证码的,必须先告诉家长。子女要提醒老人,凡是陌生电话提到“钱”“账户”“安全”“保密”的,一律挂断。子女可帮老人设置手机拦截功能,并定期分享最新骗术案例。

对社区与学校而言

“高校及流动人口密集的社区,诈骗案件更易发生。建议定期开展防诈骗宣传和模拟演练,通过案例讲解、互动问答、情景模拟,让居民和学生在真实场景中学会识别风险、掌握应对策略。”单威说,高校不仅是知识学习的场所,也是风险意识养成的重要阶段,把防诈骗教育融入学生日常交流,有助于把“提醒”转化为习惯。

全民反诈在行动

“防范电信网络诈骗,不只是技术防控问题,更是日常习惯与风险意识的养成问题。主动了解套路、保持理性判断,就是守护自身与家人财产安全的第一道防线。”市公安局刑侦总队副总队长杨彬介绍,下一步,市公安局刑侦总队将与南开大学深化反诈合作,融合技术分析与传播学优势,推动反诈宣传更智能、更精准。持续开展“反诈进社区、进校园、进企业”活动,把风险信号转化为通俗易懂的提示,让群众在关键节点多一份冷静、多一重判断。

最后,警方再次提醒广大市民:无论骗术怎么变,核心目的只有一个——让您转账或交出密码。只要守住“不轻信、不转账、不泄露”这三条底线,骗子的剧本就演不下去。如遇可疑情况,请立即拨打110或96110咨询。