十大高发电信网络诈骗类型

山西云时代技术有限公司
法律合规部 党委办公室
二〇二五年七月

公安部公布十大高发电信网络诈骗类型

近年来，公安部聚焦电信网络诈骗犯罪，持续组织开展“云剑”“断卡”“断流”“拔钉”和打击缅北涉我电信网络诈骗犯罪等一系列打击行动，统筹推进打防管控建各项措施，打击治理工作取得明显成效，电信网络诈骗犯罪上升势头得到有效遏制。当前，诈骗分子一方面想方设法逃避公安机关的打击，另一方面不断翻新诈骗方式和手法，犯罪形势依然严峻复杂。

据统计，电信网络诈骗受害者的平均年龄为37岁，18岁至40岁的占比62.1%，41岁至65岁的占比33.1%，刷单返利、虚假网络投资理财、虚假购物服务、冒充电商物流客服、虚假征信等10种常见的电信网络诈骗类型发案占比近88.4%，其中刷单返利类诈骗是发案量最大和造成损失最多的诈骗类型，虚假网络投资理财类诈骗的个案损失

金额最大，虚假购物服务类诈骗发案量明显上升，已位居第三位。

刷单返利类诈骗

刷单返利类诈骗仍是变种最多、变化最快的一种诈骗类型，主要以招募兼职刷单、网络色情诱导刷单等复合型诈骗居多。诈骗分子在骗取受害人信

任后，以“充值越多、返利越多”诱骗受害人做任务，再以“连单”“卡单”等借口诱骗受害人不断转账。此类诈骗发案量和造成的损失数均居首位，受骗人群多为在校学生、低收入群体及无业人员。

典型案例一

2024 年 5 月，李某想找工作便在某招聘 APP 上填写了个人简历，7 月份有人添加李某微信为好友并向其介绍工作，李某添加对方为好友后，对方声称要先进行线上培训，李某按照对方发来的培训教程安装了一个名叫”x 诺“的 APP，第一天按照对方提示在该 APP 内通过观看培训视频获得了 130 元的报酬，第二天对方提出要完成数据垫资的任务，垫资完成后将按照比例返钱，第一次的垫资顺利返还并获利 150 元，第二次任务完成后，对方称需要完成三单任务才能返款，任务做完后又称李某提供的银行账号有误导致数据被封，需要加倍充值才能

解封安全数据，之后又诱导李某进行贷款充值，直到自己的银行卡被封停，平台无法提现，才发现自己被骗，共计损失 196285.38 元。

虚假网络投资理财类诈骗

诈骗分子主要通过网络平台、短信等渠道发布推广股票、外汇、期货、虚拟货币等投资理财信息，吸引目标人群加入群聊，通过聊天交流投资经验、

拉入内部“投资”群聊、听取“投资专家”“导师”直播课等多种方式获取受害人信任。在此基础上，诈骗分子打着有内幕消息、掌握漏洞、回报丰厚的幌子，诱导受害人在特定虚假网站、App 小额投资获利，随后诱导其不断加大投入。当受害人投入大量资金后，诈骗分子往往编造各种理由拒绝提现，而是让其继续追加投资直至充值钱款全部被骗。还有部分诈骗分子通过网恋方式骗取受害人信任，再通过诱导虚假投资理财等进行诈骗。此类诈骗的受骗人群多为具有一定收入、资产的单身人士或热衷于投资、炒股的群体。

典型案例二

2024 年 5 月 16 日，郭某通过股票 QQ 群认识一个名叫“庞 XX”的人，添加 QQ 与对方联系后，对方声称自己是“大 X 证券”的工作人员，随后对方给被害人推荐一个名为“大 X 证券”和一个名叫

“企聊”的社交软件 APP，被害人下载注册登录并向“大 X 证券”APP 充值，随后被害人按照对方给出的“内部信息”开始在“大 X 证券”APP 内购买股票赚钱，第一次通过银行卡充值 50000 元建仓，后续充值时“在线客服”称可通过购买黄金来完成加仓，随后被害人按照对方要求购买黄金 19 次，共计 39 万余元。当被害人想将账户中的钱转出时，却被提示无法操作，被害人联系“庞 XX”询问原因，对方称他没有缴纳服务费所以无法提现，被害人遂向“庞 XX”提供的账户转账 33 万元，之后对方又称可以充值 52000 元开通一个会员通道，能够插队优先提现，被害人充值后，对方又以没有缴纳个人所得税为由拖延提现，被害人又一次转账 72000 元后，发现 APP 无法登录，才意识到自己被骗，遂报案，被骗总金额 885933 元。

虚假购物服务类诈骗

诈骗分子在微信群、朋友圈、网购平台或其他网站发布低价打折、海外代购、0 元购物等虚假广告，以及提供代写论文、私家侦探、跟踪定位等特

殊服务的广告。在与受害人取得联系后，诈骗分子便诱导其通过微信、QQ 或其他社交软件添加好友进行商议，进而以私下交易可节约手续费或更方便为由，要求私下转账。受害人付款后，诈骗分子再以缴纳关税、定金、交易税、手续费等为由，诱骗其继续转账汇款，最后将其拉黑。

典型案例三

2024 年 4 月，四川攀枝花女子王某在浏览网站时发现一家售卖测绘仪器的公司，各方面都符合自己需求，遂通过对方预留的联系方式与客服人员取得联系，客服称私下交易可以节省四分之一的费用。王某信以为真，与之签订所谓的“购买合同”。王某预付定金 1.3 万余元后，对方却迟迟不肯发货并称还需缴纳手续费、仓储费等费用，遂意识到被骗。

冒充电商物流客服类诈骗

诈骗分子通过非法途径获取受害人购物信息后，冒充电商平台或物流快递客服，谎称受害人网购商品出现质量问题、快递丢失需要理赔或因商品违规被下架需重新激活店铺等，诱导受害人提供银

行卡和手机验证码等信息，并通过共享屏幕或下载App等方式逃避正规平台监管，从而诱骗受害人转账汇款。此类诈骗的受骗人群多为电商平台的网购消费者或店铺经营者。

典型案例四

2024年10月，张某接到一个自称是“物流客服”的陌生来电，称因张某快递丢失需要进行理赔。张某随即查看某购物APP，发现一件商品未更新物流情况，便信以为真，添加了客服微信。随后“客服”发给张某一个链接，要求下载某聊天APP和银行APP，进行“理赔”操作。张某根据要求操作后，“客服”称其操作错误账户被冻结，需在银行APP里输入“代码”解冻，而这实际上是诈骗分子诱骗张某进行转账操作。张某收到银行转账短信后发现异常，遂发现被骗。

虚假贷款类诈骗

诈骗分子通过网站、电话、短信、社交平台等渠道发布“低息贷款”“快速到账”等信息，诱骗受害人前往咨询。后冒充银行、金融公司工作人员联系受害人，谎称可以“无抵押”“免征信”“快

速放贷”等，引诱受害人下载虚假贷款 App 或登录虚假网站，再以收取“手续费”“保证金”“代办费”等为由，诱骗受害人转账汇款。诈骗分子还常以“刷流水验资”为由，诱骗受害人将其银行卡寄出，用于转移涉案资金。此类诈骗的受骗人群多为有迫切贷款需求、急需资金周转的人员。

典型案例五

2024 年 5 月，江苏无锡男子王某在家中收到一条低息贷款的短信，王某点击其中的链接，根据操作指引下载了一款 App。王某在该贷款 App 上填写个人信息注册后，便想将贷款提现至银行卡。此时该贷款 App 显示银行卡有误，平台客服称贷款金额被冻结需要交解冻费。随后，王某向其提供的银行账户转账 6 万余元，但始终无法将贷款提现，遂意识到被骗。

虚假征信类诈骗

诈骗分子通过冒充银行、金融机构客服人员，谎称受害人之前开通过微信、支付宝、京东等平台的百万保障、金条、白条等服务，或申请校园贷、

助学贷等账号未及时注销，或信用卡、花呗、借呗等信用支付类工具存在不良记录，需要注销相关服务、账号或消除相关记录，否则会严重影响个人征信。随后，诈骗分子以消除不良征信记录、验证流水等为由，诱导受害人在网络贷款平台或互联网金融 App 进行贷款，并转到其指定的账户，从而骗取钱财。

典型案例六

2024 年 5 月 13 日，杨某接到一个自称支付宝蚂蚁金服工作人员电话，对方称被害人支付宝的花呗以及借呗都是在大学时期通过学生身份信息开通的，现在国家银监会要求进行成人信息实名，随后被害人根据指导进行个人征信修复，添加了对方 QQ 并下载“展 XX”APP，在更改信息时，按照对方要求将个人资金转入对方安全账户，被害人通过手机汇款十次，共计 184167.43 元后发现被骗，遂报案。

冒充领导熟人类诈骗

诈骗分子利用受害人领导、熟人的照片、姓名包装社交账号，通过添加受害人为好友或将其拉入微信聊天群等方式，冒用领导、熟人身份对其嘘寒

问暖表示关心，或模仿领导、老师等人语气发出指令，从而骗取受害人信任，再以有事不方便出面、接电话等为由，谎称已先将某款项转至受害人账户，要求其代为向他人转账。为蒙骗受害人，诈骗分子还会发送伪造的转账成功截图，但实际上其未进行任何转账操作。出于对“领导”“熟人”信任，受害人大多未进行身份核实便信以为真，以为“领导”“熟人”已将钱款转账至自己账户。随后，诈骗分子以时间紧迫等借口不断催促受害人尽快向指定账户转账，从而骗取钱财。此类诈骗通常利用受害人对领导熟人的信任心理，疏忽了对其身份进行核实。

典型案例七

被害人田某是某公司的会计，2024 年 5 月 29 日，一个陌生号码添加田某微信，对方自称是其公司老板。田某信以为真添加了对方的微信，之后对方让田某向其提供的某经销公司银行账户转账 460

万，且不断强调情况紧急，让田某尽快转账，田某转账后，对方继续提出要求向其他银行账户转账，田某心中起疑，向老板本人打电话确认，发现被骗，遂报警。

冒充公检法及政府机关类诈骗

诈骗分子冒充公检法机关、政府部门等工作人员，通过电话、微信、QQ 等与受害人取得联系，以受害人涉嫌洗钱、非法出入境、快递藏毒、护照有问题等为由进行威胁、恐吓，要求配合调查并严

格保密，同时向受害人出示逮捕证、通缉令、财产冻结书等虚假法律文书，以增加可信度。为阻断受害人与外界联系，诈骗分子通常要求其到宾馆等封闭空间配合工作，诱骗其将所有资金转移至所谓“安全账户”，从而实施诈骗。

典型案例八

2024 年 5 月，江苏无锡女子杜某在家中接到自称是无锡市公安局刑侦支队民警的视频电话。视频中，一身着制服的假“民警”称杜某的银行卡涉嫌洗钱犯罪，需要其配合调查。杜某按照要求下载会议软件进行屏幕共享，配合该“民警”核查银行卡内的资金情况。该“民警”称杜某需要将银行卡内资金转移至指定的“安全账户”内，才能证明清白。其间，为证明资金流水正常，该“民警”还让杜某通过银行贷款 15 万元，一并转到“安全账户”内。被家人发现后，杜某才意识到被骗。

网络婚恋、交友类诈骗

诈骗分子通过在婚恋、交友网站上打造优秀人设，与受害人建立联系，用照片和预先设计好的虚假身份骗取受害人信任，长期经营与其建立的恋爱关系，随后以遭遇变故急需用钱、项目资金周转困

难等为由向受害人索要钱财，并根据其财力情况不断变换理由提出转账要求，直至受害人发觉被骗。

典型案例九

2024 年 2 月 4 日，马某通过某视频平台认识了一个叫“潘 xx”的男子，对方自称是上海某工厂老板，经过聊天很快两人确认了恋爱关系，该男子称可以带着马某挣钱，马某通过对方提供的链接下载了一个名为“汇 x”的 APP，按照对方的指示购买期货，该男子还将马某拉入一个微信投资群，群内每日都有人分享在 APP 上的投资经验。马某根据该男子提示和群内消息共计充值投资 435500 元，直到某日发现微信群突然解散，且 APP 无法打开，才意识到自己被骗。

网络游戏产品虚假交易类诈骗

诈骗分子在社交、游戏平台发布买卖网络游戏账号、道具、点卡的广告，以及免费、低价获取游戏道具、参加抽奖活动等相关信息。与受害人取得

联系后，诈骗分子以私下交易更便宜、更方便为由，诱导其绕过正规平台进行私下交易，或诱骗受害人参加抽奖活动，再以操作失误、等级不够等理由，要求其支付“注册费”“解冻费”“会员费”，得手后便将受害人拉黑。

典型案例十

2024 年 10 月，家住东营利津县的小帅（化名）想要出售自己的游戏账号，一“玩家”有意购买，经协商以 1700 元的价格成交，对方要求走交易平台进行交易。小帅通过对方提供的网址下载了一个投屏软件，在对方的指导下，扫描二维码登录了某游戏交易平台，并发布账户出售信息。 很快，平台“客服”发来了订单支付成功的截图，告诉小帅因其操作失误导致账号冻结，让小帅向平台转账解冻费，并保证交易完成后全额退还。小帅信以为真，向“客服”提供的多个账户转账，共计 10000 余元，但仍无法提现，这才意识到被骗。