

公安部公布十大高发电信网络诈骗类型

近年来，公安部聚焦人民群众深恶痛绝的电信网络诈骗，全面加强“四专两合力”建设，组织全国公安机关以前所未有的力度和举措深入推进打防管控各项工作，有效遏制了案件快速上升势头，有力维护了人民群众合法权益。当前，电信网络诈骗犯罪形势依然严峻，刷单返利、虚假网络投资理财、虚假网络贷款、冒充电商物流客服、冒充公检法、虚假征信等10种常见诈骗类型发案占比近80%，其中刷单返利类诈骗发案率最高，占发案的三分之一左右，虚假网络投资理财类诈骗造成损失的金额最大，占造成损失金额的三分之一左右。

刷单返利类诈骗

网络刷单返利类诈骗已逐步演化成变种最多、变化最快的一种主要诈骗类型，成为虚假投资理财、贷款等其他复合型诈骗以及网络赌博、网络色情等其他违法犯罪的主要引流方式，被骗百万元以上的重大案件时有发生。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】邵某在微信群内看到“免费送礼品、点赞评论返佣金”的信息及二维码，扫码联系上客服并按要求下载了一款APP，随后在APP内“接待员”指导下做刷单任务。完成5单小额任务后收到了对应的佣金，并可全部提现到银行卡中。邵某遂开始认购金额更大的组合任务单，投入总本金11万元。但按要求完成任务后却发现已无法提现，APP“接待员”称因邵某操作失误造成“卡单”，要再做一次复合任务才能提现，邵某此时才发现被骗。

虚假网络投资理财类诈骗

此类案件中，有的诈骗分子通过多种方式将受害人拉入所谓“投资”群聊，然后冒充投资导师、金融理财顾问，以发送投资成功假消息或“直播课”骗取受害人信任；有的通过婚恋交友平台与受害人确定婚恋关系，再以有特殊资源、平台有漏洞等可获得高额理财回报等理由，骗取受害人信任。随后，诈骗分子诱导受害人在虚假投资平台开设账户进行投资，并对受害人前期小额投资试水予以返利，受害人一旦加大资金投入，就会出现无法提现的情况。受骗人群多为具有一定收入、资产的单身人员或热衷于投资、炒股的群体。

【典型案例二】于某在某直播平台上观看炒股知识直播时，收到自称是主播的好友请求，私聊后双方添加了 QQ 好友，对方又将于某拉入一投资交流群，于某在群内看见其他人在某款 APP 投资获利，便下载该 APP 并按照群管理员的指示在 APP 内进行投资操作，小额试验都成功盈利并顺利提现。于某感觉获利丰厚，便在 APP 内累计投资 347 万元。直至月底，于某发现 APP 内余额无法提现并被对方拉黑，才发现被骗。

虚假网络贷款类诈骗

诈骗分子通过网络媒体、电话、短信、社交工具等发布办理贷款、信用卡、提额套现的广告信息，然后冒充银行、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”，诱骗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。诈骗分子收到受害人转账后，便关闭虚假 APP 或虚假网站，并将受害人拉黑。受骗人群多为有迫切贷款需求、急需用钱周转的人员。

【典型案例三】樊某接到自称某金融平台客服的来电，询问是否有贷款需求。因樊某正好需要资金周转，便添加了对方面企业微信好友，并下载某款“贷款”APP。樊某在该 APP 上申请贷款后，对方以交会员费、解冻金、证明还款能力等为由要求其转账。樊某向对方转账 13.7 万元后，对方仍称贷款条件不满足不能放贷，随后便失去联系。樊某发现下载的 APP 已无法登录，才发现被骗。

冒充电商物流客服类诈骗

诈骗分子冒充电商平台或物流快递企业客服，谎称受害人网购的商品出现质量问题或售卖的商品因违规被下架，以“理赔退款”或“重新激活店铺”需要缴费为由，诱导受害人提供银行卡和手机验证码等信息，并通过屏幕共享或要求下载指定 APP 等方式，指导受害人转账汇款。受骗人群多为经常在电商平台网购的消费者或电商平台的店铺经营者。

【典型案例四】杜某接到自称某网店“客服”的电话，称其前几日购买的染发剂有质量问题，现需向杜某进行退款理赔，杜某信以为真。该“客服”诱导杜某下载一款 APP，通过该 APP 打开手机屏幕共享功能并按照指示进行操作。随后，杜某手机收到银行卡被转款 2 万元的短信，才发现被骗。

冒充公检法类诈骗

诈骗分子通过非法渠道获取受害人的个人身份信息，随后冒充公检法机关工作人员，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、护照有问题等违法犯罪为由进行威胁、恐吓，要求配合调查并严格保密，并向受害人出示“逮捕证”“通缉令”“财产冻结书”等虚假法律文书，以增加可信度。同时，要求受害人到宾馆等封闭空间，在阻断与外界联系的前提下“配合”其工作，将资金转移至“安全账户”，从而实施诈骗。

【典型案例五】杨某接到一个自称上海市公安局警察的电话，称杨某名下一个银行账户涉嫌非法洗钱，让其到上海市公安局处理。杨某称去不了，对方让其添加 QQ 好友并发来一个显示杨某照片的文件，里面有涉嫌洗钱要被判刑等内容，杨某心生恐惧。随后，对方以涉及警务秘密为由要求杨某到无人的房间配合调查，并称杨某要想解除嫌疑就需把卡里的所有钱款转到“安全账户”，待案件查清后将返还钱款，杨某遂向对方提供的银行账户转账 5 万元。后因对方要求删除所有聊天记录，杨某才发现被骗。

虚假征信类诈骗

诈骗分子冒充银行、银保监会工作人员或网络贷款平台工作人员与受害人建立联系，谎称受害人之前开通过校园贷、助学贷等账号未及时注销，需要注销相关账号；或谎称受害人信用卡、花呗、借呗等信用支付类工具存在不良记录，需要消除相关记录，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，并将钱款转到其指定账户，从而实施诈骗。

【典型案例六】王某接到一名自称银保监会处理高息贷款的工作人员电话，对方说王某有贷款逾期造成的不良记录，将影响个人征信。经过一番交流，王某相信了对方的身份，并按指引先后 3 次向所谓的“中国银保监会认证对接账户”的 3 个不同账号转账，共计 25 万元，其中 23 万元为王某从 3 个金融平台借贷的款项。“你还用过哪些银行卡和贷款 APP？”当对方一再问及该问题时，王某方才醒悟过来，意识到上当受骗。

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”等广告，或提供“论文代写”“私家侦探”“跟踪定位”等

特殊服务的广告，以吸引受害人关注。与受害人取得联系后，诈骗分子诱导其通过微信、QQ 或其他社交软件添加好友进行商议，以私下交易可节约“手续费”或更方便等为由，要求私下转账。待受害人付款后，诈骗分子便以缴纳“关税”“定金”“交易税”“手续费”等为由，诱骗受害人继续转账汇款，事后将受害人拉黑。

【典型案例七】李某在网上看到出售某名贵白酒的广告，遂按照对方留下的联系方式添加为微信好友咨询详情。对方自称为厂家直销，可提供内部价，但需私下交易。商定好价格后，李某向其账户转账 11000 元。数日后，李某向对方咨询物流配送信息时发现被拉黑，才发觉被骗。李某为找到骗子，在网上搜索私家侦探后，添加了一名自称私家侦探的人为好友。对方称可以通过手机定位为李某找人，但需先支付 1 万元劳务费，李某向对方提供的账号转账 1 万元后发现再次被拉黑，先后两次上当受骗。

冒充领导、熟人类诈骗

诈骗分子使用受害人领导、熟人或孩子老师的照片、姓名等信息“包装”社交帐号，以“假冒”的身份添加受害人为好友，或将其拉入微信聊天群。随后，诈骗分子以领导、熟人身份对受害人嘘寒问暖表示关心，或模仿领导、老师等人语气骗取受害人信任。再以有事不方便出面、不方便接听电话等理由要求受害人向指定账户转账，并以时间紧迫等借口不断催促受害人尽快转账，从而实施诈骗。

【典型案例八】李某的 QQ 账号被诈骗分子拉入一个工作群，见群里成员名字都是本公司工作人员便未再核实。几天后，李某收到群消息：骗子冒充的“总经理”称需支付对方工程款，要求李某核对公司账户上还有多少钱。李某核对公司账户资金后，骗子冒充的“总经理”要求李某把账上资金全部打给对方指定账户，并以事情紧急为由催促李某快点转账。因怕得罪“领导”，李某便将公司账上 40 万元全部转出。后公司总经理收到银行短信询问，李某才发现被骗。

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，或免费低价获取游戏道具、参加抽奖活动等相关信息。待受害人与其主动接触后，诈骗分子以私下交易更便宜、更方便为由，诱导受害人绕过正规平台与其进行私下交易；或要求受害人添加所谓的客服账号参加抽奖活动，并以操作失误、等级

不够等为由，要求受害人支付“注册费”“解冻费”“会员费”，得手后便将受害人拉黑。

【典型案例九】沈某在玩游戏时看到游戏聊天框内有一条“进群免费领取游戏道具”的消息，申请进群后，一位网名“派送员”的人告诉沈某扫描群内二维码便可领取大量游戏福利。沈某使用微信扫描二维码并填写了相关信息后，网页忽然显示微信将被冻结，沈某便联系“派送员”，对方称系沈某操作不当，并向其推送一个网名为“处理员”的人。“处理员”称需要通过转账证明微信是本人使用，验证后将如数退还所有资金。沈某便按对方要求，先后向指定账户转账18000元，后因被对方拉黑才发现被骗。

婚恋、交友类诈骗

诈骗分子通过网络收集大量“白富美”“高富帅”自拍、生活照，按照剧本打造不同的身份形象，然后在婚恋、交友网站发布个人信息。诈骗分子通过社交软件与受害人建立联系后，用照片和预先设计的虚假身份骗取受害人信任，并长期经营与受害人建立的恋爱关系。随后，诈骗分子以遭遇变故急需用钱、帮助项目资金周转等为由向受害人索要钱财，并根据受害人财力情况不断变换理由要求其转账，直至受害人发觉被骗。

【典型案例十】谢女士在网络上结识了一名“外国大兵”，对方自称是派驻某国的军医，非常喜欢中国文化，希望以后可以到中国定居。谢女士在与这名“大兵”聊天过程中逐渐被对方优雅的谈吐和日常的关心感动，在没见过面的情况下与对方确定了恋爱关系。“大兵”称要将自己的全部财产转移到中国，以便与谢女士共同生活，但因为遇到海关拦截，需要谢女士帮忙缴纳一笔费用才能通过。谢女士遂向其提供的账户转账5万元，后又因需缴纳“解冻费”“手续费”等向对方提供的银行账户多次转账40余万元，直至被对方拉黑，谢女士才发现被骗。

（来源：公安部，网址：<https://www.mps.gov.cn/n2253534/n2253543/c9077933/content.html>。
时间：2023年6月15日。访问时间：2023年6月20日14:01。）