

防范电信网络诈骗

三不一多

未知链接不点击 · 陌生来电不轻信
个人信息不透露 · 转账汇款多核实



国家反诈中心“APP”
(扫码或到各大官方应用商店下载)



国家反诈中心
微信视频号



国家反诈中心
抖音号



许昌市反诈中心
微信公众号



许昌市反诈中心
抖音号

电信诈骗案件的发生，有其偶然性，也存在必然性，及时关注许昌市反诈中心微信公众号及抖音号，了解本地诈骗案例，提高防范意识，保护好自身财产安全。

防范电信网络诈骗

宣传手册

十大类高发案件

典型案例

刷单返利类诈骗

易受骗群体 ▶ ◎学生、宝妈、待业、兼职群体。

作案手法

第一步：前期引流

通过短信、网站、社交软件、短视频平台等渠道发布兼职广告招募“刷单客”“点赞员”“推广员”，并将其拉入群聊，或以免费送小家电、免费技能培训等为幌子拉人建群。



第二步：小额返利

刷单群

任务未完成，需要连续做三个任务才可提现，需垫付2000元、12000元、30000元。

入群后，让受害人完成刷单、关注公众号、为短视频点赞评论、刷粉丝等任务，并发放小额佣金，获取受害人信任。

第三步：实施诈骗

安排“托儿”在群中散布其获得高额佣金的截图，以“充值越多、抢单越多、返利越多”为诱饵引诱受害人下载虚假刷单APP做“进阶任务”，以“任务未完成”“卡单”“操作异常，账户被冻结”等各种借口诱骗受害人加大投入进而骗取更多资金，直至受害人发觉被骗。

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。



警方提醒

◎“刷单、刷信誉”本身就是违法行为，并非正当兼职。

切记

◎不要被蝇头小利诱惑，所有刷单都是诈骗！



虚假网络投资理财类诈骗

易受骗群体 ▶ ◎有一定收入、资产，且有投资需求的群体。

作案手法

第一步：寻找目标

将受害人拉入所谓“投资”群聊，进而冒充投资导师、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；或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。

我也加入
发大财



第二步：怂恿投资

内部渠道
申购新股
中签率极高



委托受害人代为管理虚假投资平台账号，按照“导师”指令进行操作，骗子通过修改后台数据，向受害人分享虚假提现截图，引诱受害人开设账户进行投资。



第三步：实施诈骗

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，受害人被踢出群聊并拉黑。



典型案例

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，发现APP内余额无法提现并被对方拉黑，方得知被骗。



警方提醒

◎不要轻信非正规渠道推荐的投资理财。

切记

◎凡是标榜“内幕消息”“稳定高回报”的网络投资理财，都是诈骗！



虚假网络贷款类诈骗

易受骗群体 ▶ ◎有贷款需求的群体。

作案手法

第一步：推广引流

以“无抵押”“免征信”“快速放款”“免费提额套现”等幌子通过网络媒体、电话、短信、社交软件等方式发布办理贷款、信用卡、提额套现等虚假广告，引诱受害人下载虚假贷款 APP 或登录虚假网站。



第二步：洗脑引导



以贷款审核为由要求受害人缴纳“保证金”“手续费”或者“刷流水”，或向受害人发送虚假放贷信息，受害人发觉未到账后，再以受害人操作失误、征信有问题、流水不足等原因要求受害人缴纳各种费用。

第三步：骗取钱财

诈骗分子收到受害人的转账之后便关闭 APP 或网站并将受害人拉黑。



典型案例

樊某接到自称京东金融客服的来电，询问是否有贷款需求，樊某正好需要资金周转，便添加对方企业微信好友，并下载一款名为“京东金融”的 APP，在 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。樊某发现下载的贷款 APP 也已无法登录，才觉察到被骗。

警方提醒



◎如有贷款需求，建议通过正规渠道办理。正规机构在放款前不会收取任何费用！

切记

◎不要轻信网络贷款广告，凡是要求在放款前先交会员费、保证金等费用或要求转账刷流水的都是诈骗！

网络游戏产品虚假交易类诈骗

易受骗群体 ▶ ◎喜爱网络游戏的青少年群体。

作案手法

第一步：发布信息

在社交、游戏平台发布买卖网络游戏账号、道具、点卡的广告，免费、低价获取游戏道具、参加抽奖活动资格等相关信息。



第二步：实施诈骗

以在其他平台交易或私下交易更便宜、更方便为由，诱导受害人绕过正规的第三方平台，或者要求受害人添加所谓的客服账号参加抽奖活动。



第三步：诱导转账

以受害人操作失误、等级不够等为由，要求受害人支付所谓的“注册费”“解冻费”“会员费”等费用，随后将受害人拉黑。



典型案例

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觉被骗。

警方提醒

◎ 诈骗分子会以低价充值、高价回收、免费福利等引诱受害人点击虚假链接进行诈骗。

切记

◎ 买卖游戏账号、道具请通过正规网站平台操作，私下交易均存在被骗风险。



冒充电商物流客服类诈骗

典型案例

易受骗群体 ▶ ①经常网上购物或在电商平台开店的群体。

作案手法

第一步：获取信息

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”为由需要缴费，诱导受害人提供银行卡和手机验证码等信息。

你好，你的快递在运输途中被损毁，将对你进行经济赔偿……



第二步：诱导支付

屏幕共享
指导操作



声称误将受害人升级为VIP会员、授权为代理、办理商品分期业务等，以不取消上述业务将产生额外扣费；或不订购“保证金”“假一赔三”等服务将无法理赔退款、重新激活店铺，诱导受害人支付费用。

第三步：继续诈骗

以受害人在电商平台的会员积分、信用积分不足为由，让受害人申请贷款从而提高积分，并诱骗受害人将贷款汇入其指定账户。



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。稍后，杜某手机收到银行卡被转款2万元的短信，才意识到上当受骗。

您银行内
20000元已
被转出



警方提醒



①接到自称是电商、物流客服电话时，务必到官方平台核实。

切记

②正规网络商家退货退款无需事前支付费用，切勿点击陌生人提供的网址链接，切勿随意填写银行卡密码、短信验证码，更不要按照对方指示打开屏幕共享功能。

冒充公检法类诈骗

易受骗群体 ▶ ①防范意识较差、不了解公检法办案流程的群体。

作案手法

第一步：引诱目标

通过非法渠道获取受害人的个人信息，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，要求受害人配合工作。



第二步：威胁恐吓

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逼、恐吓，要求配合调查并严格保密，同时向受害人展示虚假通缉令、财产冻结书等法律文书以增加可信度。

第三步：实施诈骗

以帮助受害人洗脱罪名为由，诱导受害人到宾馆等独立封闭空间，阻断与外界联系，进而要求受害人配合调查或接受监管将名下所有资金转至“安全账户”，或下载指定 APP、引诱受害人从正规贷款平台借款转出，达到诈骗金额最大化的目的。



典型案例

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。对方以警务秘密为由要求杨某到无人的房间配合调查。对方称杨某想要解除嫌疑就需要把卡里的所有钱款转到“安全账户”，案件查清后这些钱款将返还，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，杨某才发觉被骗。

警方提醒

①如遇自称公检法人员主动联系，应及时与当地相关部门进行核实。

切记

①公检法机关工作人员不会通过微信、QQ 等形式发送逮捕证等文书，没有“安全账户”，凡是要求转账进行资金核查的都是诈骗！

虚假征信类诈骗

易受骗群体 ▶ ◎在校大学生、毕业生或经常网购的群体。

作案手法

第一步：假冒身份

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。

你注册过某金融的学生账号
需要注销 若不注销
要缴纳高额滞纳金
还会对个人征信有影响



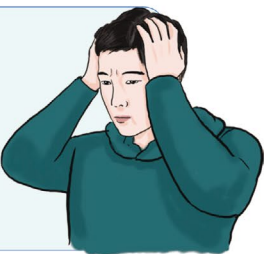
第二步：骗取信任



谎称受害人之前开通过校园贷、助学贷款等账号未及时注销，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。

第三步：实施诈骗

以消除不良征信记录、验证流水等为由，诱导受害人在正规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，从而诈骗钱财。



典型案例

王某接到一名自称银保监会处理高息贷款工作人员的电话，听到对方说有贷款逾期造成不良记录，将影响个人征信，经过一番交流，王某相信对方身份，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。

警方提醒



◎如果对个人征信存在疑问，应当通过官方渠道进行咨询，不要轻信陌生来电。

切记

◎凡是声称消除“校园贷”记录、升级学生账户或者清除不良记录，否则会影响征信，要求转账汇款或验资刷流水的，都是诈骗！

虚假购物、服务类诈骗

易受骗群体

◎喜欢在网购平台、微信群、朋友圈等渠道淘货或查找有关服务的人群。

作案手法

第一步：寻找目标

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，或者可以提供论文代写、私家侦探、跟踪定位等特殊服务的广告。



第二步：虚构交易



当与受害人取得联系后，诱导受害人通过微信、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等理由，要求私下转账。

第三步：实施诈骗

待受害人付款后，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

李某在网上看到出售茅台酒的广告，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。几日后，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。

警方提醒



◎通过社交网络平台交易时，一定要详细了解商家真实信息，多方面综合评估，交易时要有第三方做担保。

切记

◎一定要选择正规的购物、服务平台，对异常低价的商品提高警惕，不要相信所谓的论文代写、私家侦探、提供定位等服务信息！

冒充领导、熟人类诈骗

易受骗群体 ▶ ①政府、企事业单位人员、学生家长等群体。

作案手法

第一步：建立联系

诈骗分子使用受害人领导、熟人或子女老师的照片、姓名包装社交帐号，添加受害人为好友，或将受害人拉入特定群聊，或潜入受害人所在的群聊。



第二步：解除防备

领导找我帮忙，也是看重我，我得抓紧办妥。



诈骗分子以领导、熟人的身份对受害人嘘寒问暖表示关心，或模仿领导、老师等人语气发出指令，从而骗取受害人信任。

第三步：骗取钱财

诈骗分子冒充领导时，一般以有事不方便出面、不方便接电话等理由要求受害人代为转账，并发送虚假转账截图谎称已向受害人账户转账解除受害人防备，随后催促受害人尽快向指定账户转账；诈骗分子冒充企业领导或老师时，一般会模仿领导、老师语气，向受害人发出转账或缴纳费用的指令信息，并以时间紧迫、机会难得等借口催促受害人尽快转账。

典型案例

市民李某的QQ账号被拉入一个工作群，李某见群里成员的名字都是本公司工作人员便未加核实。几天后，李某收到群消息，“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，“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，后因公司总经理收到银行短信询问才发觉被骗。

警方提醒



◎如遇到自称领导、朋友添加好友或被拉入陌生群聊时，一定要多方确认对方身份！

切记

◎凡是接到自称领导、熟人要求转账的信息时，务必通过电话或当面核实确认，在核实确认之前切勿转账！

婚恋、交友类诈骗

易受骗群体 ▶ ◎单身、离异群体。

作案手法

第一步：包装身份

诈骗分子会通过网络收集大量“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。



第二步：建立信任

建立联系后，会进一步用照片和预先设计的个人经历丰富的虚假身份骗取受害人信任，并通过聊天和受害人建立恋爱关系。

第三步：实施诈骗

诈骗分子以遭遇变故急需用钱，或者以维持恋爱关系为由向受害人索要钱财，并且根据受害人财力情况不断变化理由要求转账，直至受害人发觉被骗或无力继续转账。

您已被拉黑



典型案例

谢女士在网上结识了一名“美国大兵”，对方自称是美国派驻中东某国的军医，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，“美国大兵”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，谢女士才发觉被骗。

警方提醒

◎网络交友需谨慎，虚拟世界难辨真。

切记

◎在涉及钱财问题时，不要轻信征婚交友对象的任何借口、说辞！



请记住这个号码，它很重要！

96110

如果当您接到“96110”打来的电话，那就说明您正在遭遇电信网络诈骗，请务必及时接听，耐心听取民警的劝阻，避免上当受骗。



国家反诈中心

国家反诈中心
APP使用指南

第一步 下载
第二步 安装

途径一
在手机官方应用市场搜索
“国家反诈中心”下载安装

途径二
扫描二维码



第三步 注册

点击“快速注册”输入手机号获取验证码

打开应用，选择河南省许昌市进行注册

完善信息并完善身份认证【人脸识别】

APP使用时需要点击
“诈骗预警”模块授权手机权限，如

照片访问
视屏访问
访问短信
访问通讯录

所有权限点击
“总是允许”

注意：如不开启诈骗预警权限，就不具备预警功能



国家反诈中心APP 功能介绍

主要功能一：涉诈来电、短信、网站预警提示。

可免费为您提供防骗保护，当收到涉嫌诈骗的电话、短信、网址或者安装涉嫌诈骗的APP时，可以智能识别骗子身份并及时预警，大幅降低受骗可能性。



主要功能二：涉诈线索一键举报。

在使用手机过程中，如果发现可疑的手机号、短信、钓鱼网站、诈骗APP等信息，可以在“我要举报”模块进行举报，后台会及时进行封堵预警。



主要功能三：

揭露诈骗手法，发布典型案例。

定期推送反诈宣传内容，及时发布权威声音，全面揭露诈骗手法，深入剖析真实案例，普及反诈防骗知识。



主要功能四：

可疑社交帐号、交易账号核验。

进行风险查询，在涉及陌生账号转账时，可以验证对方的账号是否涉诈，包括支付账户、IP网址、QQ、微信等，及时避开资金被骗风险。



主要功能五：可疑身份核验。

进行真实身份验证，在社交软件上交友、转账时，验证对方身份的真实性，防止对方冒充身份进行诈骗。



《反电信网络诈骗法》

将如何影响你的生活



多办？ 几张银行卡

不得超量

《中华人民共和国反电信网络诈骗法》规定

- ◎开立银行账户、支付账户不得超出国家有关规定限制的数量。
- ◎对经识别存在异常开户情形的，银行业金融机构、非银行支付机构有权加强核查或者拒绝开户。

多办？ 几张电话卡

不得超量



《中华人民共和国反电信网络诈骗法》规定

- ◎办理电话卡不得超出国家有关规定限制的数量。
- ◎对经识别存在异常办卡情形的，电信业务经营者有权加强核查或者拒绝办卡。

售卖个人信息 帮转账 ?

构成违法犯罪



《中华人民共和国反电信网络诈骗法》规定

◎任何单位和个人不得为他人实施电信网络诈骗活动提供下列支持或者帮助:

- (一) 出售、提供个人信息;
- (二) 帮助他人通过虚拟货币交易等方式洗钱;
- (三) 其他为电信网络诈骗活动提供支持或者帮助的行为。

制贩猫池、GOIP 设备 ?

构成违法犯罪



《中华人民共和国反电信网络诈骗法》规定

◎任何单位和个人不得非法制造、买卖、提供或者使用下列设备、软件:

- (一) 电话卡批量插入设备;
- (二) 具有改变主叫号码、虚拟拨号、互联网电话违规接入公用电信网络等功能的设备、软件;
- (三) 批量账号、网络地址自动切换系统, 批量接收提供短信验证、语音验证的平台;
- (四) 其他用于实施电信网络诈骗等违法犯罪的设备、软件。

买卖、出租、 出借“两卡” ?

纳入信用记录



《中华人民共和国反电信网络诈骗法》规定

◎任何单位和个人不得非法买卖、出租、出借电话卡、物联网卡、电信线路、短信端口、银行账户、支付账户、互联网账号等, 不得提供实名核验帮助; 不得假冒他人身份或者虚构代理关系开立上述卡、账户、账号等。

◎对经设区的市级以上公安机关认定的实施前款行为的单位、个人和相关组织者, 以及因从事电信网络诈骗活动或者关联犯罪受过刑事处罚的人员, 可以按照国家有关规定记入信用记录, 采取限制其有关卡、账户、账号等功能和停止非柜面业务、暂停新业务、限制入网等措施。

到境外参加 涉诈活动 ?

限制出境

《中华人民共和国反电信网络诈骗法》规定

◎对前往电信网络诈骗活动严重地区的人员, 出境活动存在重大涉电信网络诈骗活动嫌疑的, 移民管理机构可以决定不准其出境。

◎因从事电信网络诈骗活动受过刑事处罚的人员, 设区的市级以上公安机关可以根据犯罪情况和预防再犯罪的需要, 决定自处罚完毕之日起六个月至三年以内不准其出境, 并通知移民管理机构执行。