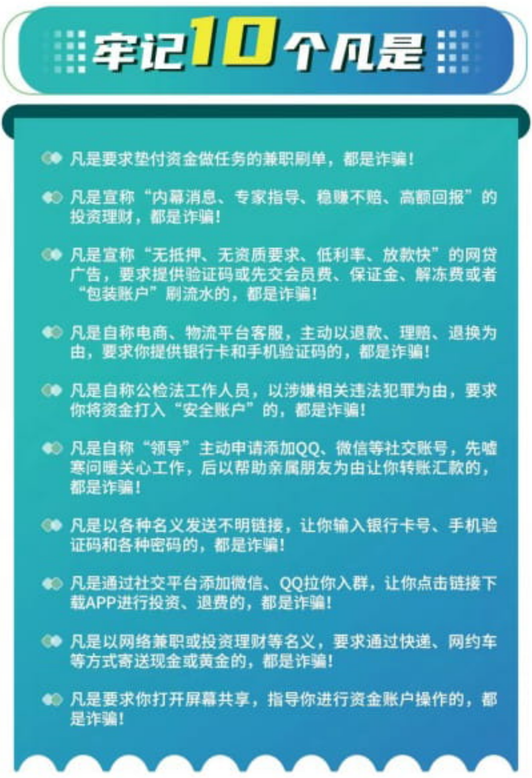
请查收 《2025版防范电信网络诈骗宣传手册》（全文）

防范电信网络诈骗
宣传手册

—— 反诈是门必修课 筑牢防线守好责 ——

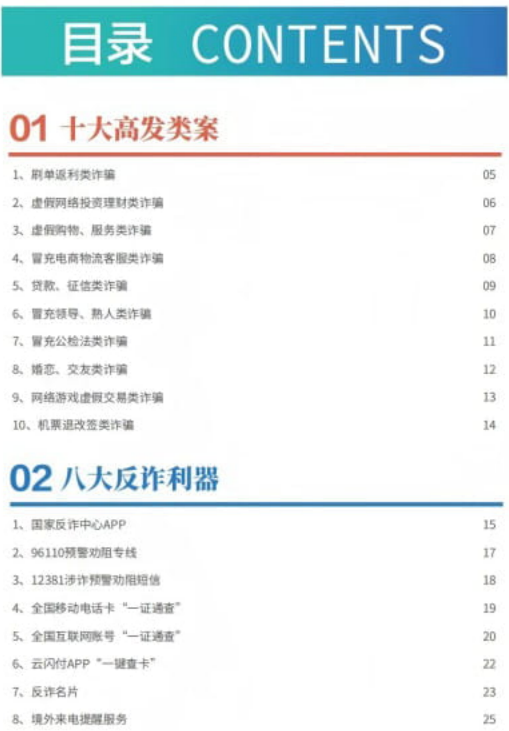
（2025版）

公安部刑侦局　国家反诈中心



牢记10个凡是

- 凡是要求垫付资金做任务的兼职刷单，都是诈骗！
- 凡是宣称“内幕消息、专家指导、稳赚不赔、高额回报”的投资理财，都是诈骗！
- 凡是宣称“无抵押、无资质要求、低利率、放款快”的网贷广告，要求提供验证码或先交会员费、保证金、解冻费或者“包装账户”刷流水的，都是诈骗！
- 凡是自称电商、物流平台客服，主动以退款、理赔、退换为由，要求你提供银行卡和手机验证码的，都是诈骗！
- 凡是自称公检法工作人员，以涉嫌相关违法犯罪为由，要求你将资金打入“安全账户”的，都是诈骗！
- 凡是自称“领导”主动申请添加QQ、微信等社交账号，先嘘寒问暖关心工作，后以帮助亲属朋友为由让你转账汇款的，都是诈骗！
- 凡是以各种名义发送不明链接，让你输入银行卡号、手机验证码和各种密码的，都是诈骗！
- 凡是通过社交平台添加微信、QQ拉你入群，让你点击链接下载APP进行投资、退费的，都是诈骗！
- 凡是以网络兼职或投资理财等名义，要求通过快递、网约车等方式寄送现金或黄金的，都是诈骗！
- 凡是要求你打开屏幕共享，指导你进行资金账户操作的，都是诈骗！



目录 CONTENTS

01 十大高发类案

1、刷单返利类诈骗 05
2、虚假网络投资理财类诈骗 06
3、虚假购物、服务类诈骗 07
4、冒充电商物流客服类诈骗 08
5、贷款、征信类诈骗 09
6、冒充领导、熟人类诈骗 10
7、冒充公检法类诈骗 11
8、婚恋、交友类诈骗 12
9、网络游戏虚假交易类诈骗 13
10、机票退改签类诈骗 14

02 八大反诈利器

1、国家反诈中心APP 15
2、96110预警劝阻专线 17
3、12381涉诈预警劝阻短信 18
4、全国移动电话卡“一证通查” 19
5、全国互联网账号“一证通查” 20
6、云闪付APP“一键查卡” 22
7、反诈名片 23
8、境外来电提醒服务 25

03《中华人民共和国反电信网络诈骗法》值得关注的3组数字

1、十五日以下拘留一至十倍的罚款 26
2、五万以上至五百万以下的罚款 28
3、六个月至三年以内不准出境 30

04《电信网络诈骗及其关联违法犯罪联合惩戒办法》的3种惩戒措施

1、金融惩戒 31
2、电信网络惩戒 31
3、信用惩戒 32

05 二十个防诈关键词

1、屏幕共享 33
2、百万保障 33
3、安全账户 34
4、NFC盗刷 34
5、“两卡” 35
6、“帮信行为” 35
7、刷流水 36
8、积分清零 36
9、修复征信 37
10、快递引流 37
11、现金黄金 38
12、购物卡 38
13、内幕消息 39
14、“电诈工具人” 39
15、虚拟货币 40
16、色情小卡片 40
17、刷单做任务 41
18、未知链接、二维码 41
19、小众聊天软件 42
20、境外来电 42

01 十大高发类案

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

诈骗分子通过短信、网站、社交软件、短视频平台、快递、街面小广告等渠道发布兼职广告招募“刷单客”“点赞员”“推广员”，更有甚者通过发布“约炮招嫖”广告并将受害人拉入群聊，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

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”，再以“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，进而骗取更多钱款，直至受害人发觉被骗。

典型案例：张女士在浏览短视频时下载了评论区推荐的所谓“赚钱软件”，注册后平台客服以“刷单返佣”为由诱导其垫资购物。初期张女士投入392元获得26元返利，随后客服提供支付二维码，要求其分七次扫码转账1344元，将获得204元佣金。张女士完成转账后，客服以做错任务为由，声称需要重新转账才能获得之前的返利，于是张女士按照客服要求再次向对方转账7600元。张女士照做后，对方又谎称账户因操作异常被冻结，需要继续充值才能解冻。张女士在多重话术诱导下连续转账，最终累计损失14万元。

警方提示

“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，不要轻信网络上高额报酬的兼职刷单信息，找兼职一定要通过正规渠道，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

诈骗分子冒充投资导师、金融理财顾问将受害人拉入所谓“投资”群聊，通过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、可获得高额理财回报等理由，骗取受害人信任。

内部渠道
申购新股
中签率极高

第二步：怂恿投资

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，又以“服务器异常”“操作失误导致账户冻结”等理由阻止提现，要求缴纳“保证金”“解冻金”等费用，造成大额财产损失。

典型案例：李先生在微信公众号阅读投资理财类文章后，扫码加入名为“投资-特训营”的群聊，并通过群内指引添加了自称“基金经理”的客服人员。该客服发送安装包要求李先生下载了指定的投资平台软件，并以“股票推荐”的名义诱导李先生向平台转账充值。初期账户持续显示盈利，面对账户余额不断增长，李先生放松警惕持续追加资金投入。数日后，该投资平台突然无法登录，客服人员也将其拉黑，李先生才发现被骗，最终造成82万元损失。

警方提示

不要轻信非正规渠道推荐的投资理财项目。

切记

凡是宣称“掌握内幕消息”“高额回报”“稳赚不赔”的网络投资理财，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群体。

作案手法

第一步：寻找目标

原价 5500 元
三折即可入手

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，或者声称可以提供代抢演唱会门票、订购预售产品、论文代写、代找工作、跟踪定位等特殊服务。

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或其他小众聊天软件添加好友进行商议，进而以私下交易可节约手续费或方便交易等理由，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：李女士通过社交软件结识了一位自称经营电脑业务的陌生网友，对方声称可以帮忙在电商平台代购电脑，并向李女士发送了身份信息和经营资质，以此获取了李女士的信任。随后对方向李女士提供了支付二维码，李女士扫码支付后，对方又称还有其他商品代购名额，而且优惠力度很大，李女士便继续转账让对方帮忙代购。几日后李女士收货时发现均为空包裹且无法与对方取得联系，遂发觉自己被骗。

警方提示

网上购物一定要选择正规的购物、服务平台。

切记

对异常低价的商品要提高警惕，避免脱离官方平台进行私下交易。

冒充电商物流客服类诈骗

易受骗群体 ▸ 经常网上购物、对网购退费流程不熟悉的群体。

作案手法

你好，你的快递在运输途中被损毁，将对你进行经济赔偿……

第一步：冒充身份

诈骗分子在快递包裹中附加小卡片、二维码，以扫码领取物品等为由引导受害人扫码添加虚假客服或加入群聊。冒充社交平台（如：微信、支付宝、抖音）、保险公司客服以误购买“百万保障”“升级会员”服务等为由与受害人建立联系，或是冒充电商平台或物流快递客服，谎称受害人网购商品存在质量问题或因违规被下架。

第二步：诱导配合

诱导受害人下载小众聊天软件，以帮助“退款理赔”或不取消相关服务将产生额外扣费等为由，诱导受害人支付费用或配合操作。

第三步：实施诈骗

诈骗分子以指导操作为名，以受害人电商平台网购的商品遗失理赔、存在质量问题、违规下架等理由，或者以会员积分、信用积分不足无法退费为由，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。诱导受害人开启屏幕共享，获取其银行卡密码、验证码，进而骗取资金。

典型案例：周女士网购了一件衣服，几天后，她接到自称是物流客服的电话，对方声称由于自己的失误，错将包裹丢失，要通过官方支付平台给她进行三倍理赔。随后，周女士添加了这位“客服”的好友，对方以“协助操作”名义要求下载会议软件并开启屏幕共享功能。对方引导周女士逐个点击银行App，并进行操作，没过多久，周女士收到银行发来的转账短信，其名下银行卡陆续转出4笔资金，共计损失13万元。

警方提示

接到自称电商、物流客服电话时，务必到官方平台核实。

切记

正规网络商家退款无需事前支付费用，切勿随意打开屏幕共享功能，切勿轻易点击来源不明的网址链接，更不要随意填写银行卡密码、短信验证码等信息。

贷款、征信类诈骗

易受骗群体 ▸ 有贷款需求、征信有问题难以正常申请贷款的群体。

作案手法

第一步：引流推广

诈骗分子冒充银行、抖音客服或是网贷平台工作人员，以受害人征信出现问题为由建立联系。通过网络媒体、电话、短信、社交软件等方式发布“无抵押”“免征信”“放款快”等虚假网络贷款广告，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

以受害人征信出现问题需要修复征信、贷款审核为由要求受害人缴纳“保证金”“手续费”，再以受害人操作失误、征信有问题、流水不足等为由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，以各种理由继续骗取钱财或直接消失不见。

典型案例：王先生在网上添加一陌生网友，对方称可以帮助其办理贷款，王先生随即向其咨询贷款流程。对方向王先生索要了相关个人信息和放款银行账户信息，随后便称王先生的贷款资质不足，提供的银行账户流水没有达到放款要求，声称可以帮助王先生免费“刷流水”。王先生便按对方指示分多次向指定账户转账共计5.2万元，但对方始终以各种理由拖延放款并要求继续转账。最终，王先生发现该网友失联，方知上当受骗。

警方提示

如有贷款需求，建议通过正规渠道办理，不要轻信网络贷款广告。个人征信由中国人民银行征信中心统一管理，任何单位和个人都无权删除修改。

切记

凡是在放款前要求缴纳手续费、保证金等费用，或诱导进行“刷流水”转账操作的，都是诈骗。

冒充领导、熟人类诈骗

易受骗群体 ▸ 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

诈骗分子盗用受害人领导、熟人或子女老师的照片及姓名，伪装社交账号添加受害人为好友，或诱骗受害人加入特定群聊，甚至直接潜入受害人所在的群聊之中。

领导找我帮忙，
也是看重我，
我得抓紧办妥。

第二步：解除防备

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，通常以有事不方便出面、无法接听电话等理由，要求受害人代其转账，并会发送伪造的转账截图，谎称已向受害人账户打款，解除受害人防备，进而不断催促受害人向指定账户转账；诈骗分子冒充企业领导或老师时，会刻意模仿领导或老师说话语气，向受害人发送转账或缴费的指令信息，并以情况紧急、机会难得等借口催促受害人尽快转账。

典型案例：公司财务孙先生被拉入一个工作群中，因群成员昵称均为公司员工便未加核实。几天后，孙先生收到群内消息，“老板”称需支付对方工程款，要求核对公司账户余额。在孙先生核对完账户资金后，群内的“老板”要求其将全部资金转至指定账户，并以紧急事由催促孙先生操作转账。因怕耽误工作，孙先生未经核实便将公司账上50万元全部转出，后因公司老板收到银行短信询问才发觉被骗。

警方提示

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。

冒充公检法类诈骗

易受骗群体 ▸ **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

诈骗分子通过非法渠道获取受害人的个人身份信息，冒充公检法机关工作人员，通过电话或微信、QQ等社交软件与受害人取得联系，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”，或缴纳高额的“取保候审金”。

典型案例：何女士接到一个自称是上海市公安局警察的电话，称何女士名下一张银行卡涉嫌非法洗钱，要求配合调查。对方添加何女士QQ好友，并发来“财产冻结书”，以案件涉密为由进行威胁恐吓，要求其到无人房间配合调查并禁止对外联络。随后让何女士将银行卡里的所有钱款转到“安全账户”，声称案件查清后将全部返还。在完成转账后对方失联，何女士方才意识到被骗。

警方提示

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法律文书，公检法机关没有“安全账户”。

切记

凡是要求转账进行资金核查的都是诈骗。

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，按照诈骗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

与受害人建立联系后，利用照片和预先设计的虚假身份骗取受害人信任，并通过持续的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，并且根据受害人的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。

典型案例：张先生通过网络交友平台认识了“穆女士”，对方自称因长期遭受丈夫家暴导致婚姻破裂，目前正在闹离婚。对方通过频繁倾诉婚姻不幸博取到张先生同情，期间还将离婚证发来，两人很快发展成为了恋人关系。在随后的交往中，“穆女士”先后以经营周转、信用卡还款、购置手机、住院治疗等理由骗取张先生10万余元。张先生再联系时发现已遭对方拉黑，随后按照对方此前提供的地址寻找，发现查无此人，张先生遂发现被骗。

警方提示

网络交友需谨慎，虚拟世界难辨真。

切记

在涉及钱财问题时，不要轻信网络交友对象的任何说辞。

网络游戏虚假交易类诈骗

易受骗群体 ▸ **喜欢网络游戏的青少年群体。**

作案手法

第一步：寻找目标

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，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：引导交易

以在其他平台交易或私下交易更便宜、更方便为由，请导受害人到指定平台或私下进行交易。

●第三步：实施诈骗

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：常先生在玩游戏时收到一条好友申请，对方提出想用3000元购买他的游戏账号，因对方出价较高，常先生觉得有利可图便欣然同意。对方发来网址链接声称需通过平台完成交易，常先生随即点击链接进入虚假游戏交易平台。注册登录后，系统显示账户内有3000元冻结资金，需要先交900元的解冻费才能开始交易，常先生通过扫码支付后，账号依旧显示被冻结。接着对方又以需要交手续费、认证金等各种理由诱骗付款3万余元后，常先生发现仍无法提现，才意识到被骗。

警方提示

买卖游戏账号、道具请通过正规网站平台操作。

切记

脱离官方平台或私下交易均存在被骗风险。

机票退改签类诈骗

易受骗群体 ▸ 购买机票的群体。

作案手法

●第一步：骗取信任

诈骗分子通过非法渠道获取受害人订票信息，冒充航空公司客服人员，通过电话或短信进行联系，以能准确说出受害人姓名、身份证号、登机时间、航班班次等信息来骗取信任。

●第二步：提出理赔

初步取得受害人信任后，诈骗分子谎称飞机故障、恶劣天气等原因造成航班延误或取消，需要受害人改签或退票，并主动提出给予赔偿金，诱导受害人下载视频会议类 App、指定软件或登录虚假网站。

●第三步：实施诈骗

以"转账验证账户安全""转账确保理赔通道畅通"等借口，通过屏幕共享等方式，套取受害人银行卡账户、密码、验证码等信息后转走资金，或诱导受害人转账完成诈骗。

典型案例：刘先生订完机票后不久接到一个陌生来电，对方自称是航空公司的客服，称刘先生订购的机票因飞机故障航班取消，办理退票或改签可获得300元的赔偿。对方能准确说出刘先生的航班信息，他信以为真，于是根据对方发来的链接下载了一款具有"屏幕共享"功能的App。对方称为了确保账户信息安全，妥善做好理赔，整个过程需要全程打开"屏幕共享"进行操作。刘先生开启"屏幕共享"后，对方要求打开手机银行App，并输入验证码等相关操作。最后，刘先生的银行卡被转账3次，共计被骗25万余元。

警方提示

当被告知航班延误或取消，应通过航空公司客服电话、官方网站等多方渠道核实，切勿轻易点击不明短信中的链接。

切记

如需办理理赔务必登录航空公司官网或购票平台进行操作。

02 八大反诈利器

国家反诈中心APP

2021年3月15日
公安部推出的国家反诈中心App正式上线

国家反诈中心APP基本介绍

国家反诈中心App基本介绍：国家反诈中心App是一款集诈骗预警提示、报案助手、线索举报、反诈宣传等多种功能于一体的手机软件，可以有效帮助用户预警诈骗信息、快速举报诈骗内容、高效提取电子证据、了解防骗技巧，切实提升用户的识骗防骗能力。

下载国家反诈中心App要进行实名认证，打开预警功能。

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。

国家反诈中心
APP正式上线

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。

96110预警劝阻专线

2019年11月8日
96110预警劝阻专线率先在北京启用
目前全国已有31个省区市的公安机关开通

96110
预警劝阻专线
这个电话一定要接

预警劝阻专线96110功能介绍

96110是反诈预警劝阻专用号码

紧急预警劝阻极易被骗人员或正在被骗的人员：发现群众正遭遇电信网络诈骗或者属于极易被骗的人员，公安机关将通过该专线及时预警劝阻。

- **防骗咨询**
  如果遇到疑似电信网络诈骗活动，群众可以拨打该专线进行咨询。
- **涉诈举报**
  如果发现涉诈线索，群众可以通过该专线进行举报。
- **警方提醒**
  96110是官方预警劝阻专线，如接到该号码来电，说明机主本人或家人正在遭遇电信网络诈骗，请一定及时接听并耐心听取民警的劝阻提示，避免上当受骗。

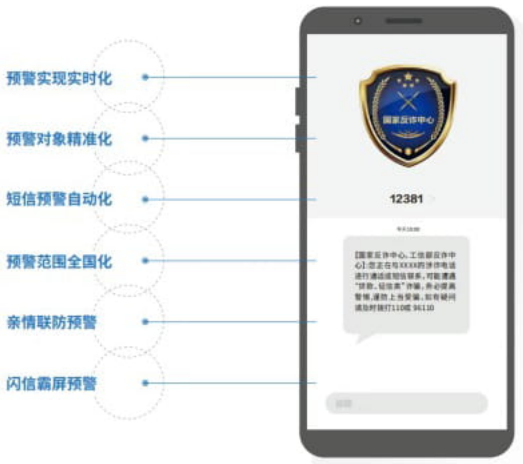
防骗咨询
涉诈举报
警方提醒

12381涉诈预警劝阻短信

12381系统可根据公安机关提供的涉案号码，利用大数据、人工智能等技术自动分析发现潜在被骗用户，并通过12381短信端口向用户发送预警短信，提示用户可能遭遇“刷单返利”“虚假网络贷款”“冒充公检法”等高发类型的电信网络诈骗。

12381
涉诈预警劝阻短信
这个短信一定要看

截至2025年5月底，12381涉诈预警劝阻短信系统累计发送预警信息共13.88亿条。其中，短信6.95亿条、闪信6.88亿条，预警劝阻成功率达到60%，直接避免约1940万用户受骗。

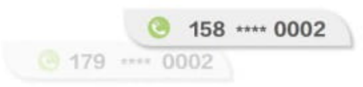


【国家反诈中心、工信部反诈中心】您正在与XXXX的涉诈电话进行通话或短信联系，可能遭遇“贷款、征信类”诈骗，务必提高警惕，谨防上当受骗，如有疑问请及时拨打110或96110

全国移动电话卡“一证通查”

诈骗分子冒用他人身份开办电话卡，严重侵害用户本人合法权益，广大群众对此深恶痛绝。

工业和信息化部指导推出全国移动电话卡“一证通查”服务，首次打通了124 家省级基础电信企业和39家移动通信转售企业相关统计数据，用户可通过线上、线下多种渠道查询本人名下持有的全国移动电话卡数量，“一证通查”服务将使用专用短信端口10699000，在48小时内反馈查询结果，真正实现全国移动电话卡的统一、便捷查询。



截至2025年5月底，一证通查已免费为广大手机用户提供查询服务2.26亿次，有效解决用户“记不清楚自己有多少手机号”等问题，精准防范“冒名办卡”“不知情被办卡”等安全风险，助力筑牢反诈防诈防火墙。

一证通查1.0已免费为广大手机用户提供查询服务 **2.6** 亿次

全国互联网账号“一证通查”

为有效防范用户“不知情被注册互联网账号”等带来的涉诈风险，切实为群众排忧解难，工业和信息化部指导“一证通查”服务升级，推出全国互联网账号“一证通查”，聚焦社交通信、购物出行、学习办公、休闲娱乐等人民群众高频生活场景，打通23家重点互联网企业共25款App相关账号统计数据，为广大用户提供本人名下手机号码关联互联网账号数量查询、解绑服务。

全国互联网账号
“一证通查”
2.0

截至2025年5月底，一证通查已免费为广大手机用户提供查询服务5629万次，有效解决广大用户“记不清楚手机号码绑定过多少互联网账号”等问题，为其快速、安全解绑互联网账号提供极大便利，成为人民群众喜闻乐见的“反诈利器”。

2025年5月底 **5629**万次

信息通信行业反诈中心二维码、互联网企业LOGO等相关信息，详见下图

扫描下列二维码进行一证通查

信息通信行业反诈中心二维码

一证通查支付宝二维码

国家政务服务平台小程序

支持查询的互联网企业LOGO

云闪付App“一键查卡”

2021年12月，中国人民银行指导中国银联股份有限公司联合商业银行基于银行业统一App云闪付试点“一键查卡”功能，打造统一查询途径，向境内公众提供银行卡数量、每张卡的银行名称、借贷记属性、脱敏卡号等信息的查询，在确保信息安全的前提下，便利公众直接掌握个人名下银行卡信息，强化自身银行卡管理。

截至2025年5月，已累计生成超过2300万份查询报告。后续随着试运营逐步完善、推广，中国银联将不断扩大查卡银行范围，优化查卡功能。

“一键查卡”已开放全国试运营服务支持银行18家全国性商业银行的银行卡可查询

工商银行 农业银行 中国银行 建设银行 交通银行 邮储银行 中信银行 光大银行 招商银行
浦发银行 民生银行 华夏银行 平安银行 兴业银行 广发银行 浙商银行 恒丰银行 渤海银行

目前，“一键查卡”已开放全国试运营，为以上18家全国性银行及487家区域性银行提供银行卡查询服务。

反诈名片

反诈名片是国家反诈中心、工信部反诈中心联合中国电信、中国移动、中国联通、中国信通院推出的一项反诈来电提醒服务。

电信网络诈骗是可预防性犯罪，实践表明，及时、有效地对与诈骗分子联系的潜在受害人开展劝阻能够大大降低犯罪实施的成功率。然而，公安机关在利用电话对潜在受害用户开展预警劝阻工作时，常被误认成骚扰甚至诈骗电话而遭拒接，从而错过最佳劝阻时间，耗费大量人力、物力、财力，严重影响预警劝阻工作的预期效果。

“反诈名片”的作用

手机用户在接听预警劝阻电话时，同步弹显国家反诈中心、工信部反诈中心温馨提醒信息，让手机用户能够有效甄别号码真伪，快速、安心接听反诈预警电话，大幅提升公安机关预警劝阻电话的接通率，更有效地预防电信网络诈骗犯罪。

“用户您好，该电话来自于国家反诈部门，请您接听！”

——【国家反诈中心、工信部反诈中心联合提醒】

国家反诈中心、工信部反诈中心联合中国电信、中国移动、中国联通、中国信通院创新推出“反诈名片”，权威提供来电号码认证提醒服务，助您安心接听反诈预警电话。信息通信行业又一反诈利器！守护您的财产安全，我们一直在行动！

国家反诈中心 × 工信部反诈中心

中国电信 CHINA TELECOM

中国移动 China Mobile

China unicom 中国联通

中国广电 China Broadnet

警方提醒

如果您收到带有“反诈名片”标记的预警劝阻电话，可以放心接听。

境外来电提醒服务

工信部组织基础电信企业全面推出了“境外来电提醒服务”，当手机用户在接听境外电话或收到境外短信时，同步弹显提醒，主动提示用户号码来源，帮助用户及时了解来电和短信的来源国家或地区，从而增强反诈防范意识。

提醒内容

“尊敬的用户，您好！您接听的号码是境外来电，请注意防范，谨防诈骗！”
“您接收到短信来源于境外，请注意防范，谨防诈骗！”

03 《中华人民共和国反电信网络诈骗法》值得关注的3组数字

这部法律中有哪些数字值得关注？

十五日以下拘留 一至十倍的罚款！

从事电信网络诈骗活动尚不构成犯罪的

第三十八条 组织、策划、实施、参与电信网络诈骗活动或者为电信网络诈骗活动提供帮助，构成犯罪的，依法追究刑事责任。

前款行为尚不构成犯罪的，由公安机关处十日以上十五日以下拘留；没收违法所得，处违法所得一倍以上十倍以下罚款，没有违法所得或者违法所得不足一万元的，处十万元以下罚款。

非法制造、买卖、使用GOIP、猫池等设备，为实施电信网络诈骗活动提供支持或帮助

第十四条 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。

第二十五条 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。

第四十二条 违反本法第十四条、第二十五条第一款规定的，没收违法所得，由公安机关或者有关主管部门处违法所得一倍以上十倍以下罚款，没有违法所得或者违法所得不足五万元的，处五十万元以下罚款；情节严重的，由公安机关并处十五日以下拘留。

提供实名核验帮助假冒身份开卡开户

第三十一条 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。

第四十四条 违反本法第三十一条第一款规定的，没收违法所得，由公安机关处违法所得一倍以上十倍以下罚款，没有违法所得或者违法所得不足二万元的，处二十万元以下罚款；情节严重的，并处十五日以下拘留。

五万以上至五百万以下的罚款！

对电信企业违反本法规定的处罚

第三十九条 电信业务经营者违反本法规定，有下列情形之一的，由有关主管部门责令改正，情节较轻的，给予警告、通报批评，或者处五万元以上五十万元以下罚款；情节严重的，处五十万元以上五百万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对其直接负责的主管人员和其他直接责任人员，处一万元以上二十万元以下罚款：

（一）未落实国家有关规定确定的反电信网络诈骗内部控制机制的；

（二）未履行电话卡、物联网卡实名制登记职责的；

（三）未履行对电话卡、物联网卡的监测识别、监测预警和相关处置职责的；

（四）未对物联网卡用户进行风险评估，或者未限定物联网卡的开通功能、使用场景和适用设备的；

（五）未采取措施对改号电话、虚假主叫或者具有相应功能的非法设备进行监测处置的。

对金融企业违反本法规定的处罚

第四十条 银行业金融机构、非银行支付机构违反本法规定，有下列情形之一的，由有关主管部门责令改正，情节较轻的，给予警告、通报批评，或者处五万元以上五十万元以下罚款；情节严重的，处五十万元以上五百万元以下罚款，并可以由有关主管部门责令停止新增业务、缩减业务类型或者业务范围、暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对其直接负责的主管人员和其他直接责任人员，处一万元以上二十万元以下罚款：

（一）未落实国家有关规定确定的反电信网络诈骗内部控制机制的；
（二）未履行尽职调查义务和有关风险管理措施的；
（三）未履行对异常账户、可疑交易的风险监测和相关处置义务的；
（四）未按照规定完整、准确传输有关交易信息的。

对互联网企业违反本法规定的处罚

第四十一条 电信业务经营者、互联网服务提供者违反本法规定，有下列情形之一的，由有关主管部门责令改正，情节较轻的，给予警告、通报批评，或者处五万元以上五十万元以下罚款；情节严重的，处五十万元以上五百万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，对其直接负责的主管人员和其他直接责任人员，处一万元以上二十万元以下罚款：

（一）未落实国家有关规定确定的反电信网络诈骗内部控制机制的；

（二）未履行网络服务实名制职责，或者未对涉案、涉诈电话卡关联注册互联网账号进行核验的；

（三）未按照国家有关规定，核验域名注册、解析信息和互联网协议地址的真实性、准确性，规范域名跳转，或者记录并留存所提供相应服务的日志信息的；

（四）未登记核验移动互联网应用程序开发运营者的真实身份信息或者未核验应用程序的功能、用途，为其提供应用程序封装、分发服务的；

（五）未履行对涉诈互联网账号和应用程序，以及其他电信网络诈骗信息、活动的监测识别和处置义务的；

（六）拒不依法为查处电信网络诈骗犯罪提供技术支持和协助，或者未按规定移送有关违法犯罪线索、风险信息的。

第二十五条　电信业务经营者、互联网服务提供者应当依照国家有关规定，履行合理注意义务，对利用下列业务从事涉诈支持、帮助活动进行监测识别和处置：

（一）提供互联网接入、服务器托管、网络存储、通讯传输、线路出租、域名解析等网络资源服务；

（二）提供信息发布或者搜索、广告推广、引流推广等网络推广服务；

（三）提供应用程序、网站等网络技术、产品的制作、维护服务；

（四）提供支付结算服务。

第四十三条　违反本法第二十五条第二款规定，由有关主管部门责令改正，情节较轻的，给予警告、通报批评，或者处五万元以上五十万元以下罚款；情节严重的，处五十万元以上五百万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站或者应用程序，对其直接负责的主管人员和其他直接责任人员，处一万元以上二十万元以下罚款。

六个月至三年以内不准出境

对涉电诈前科人员和重大嫌疑人员的管控措施

第三十六条　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。

04 《电信网络诈骗及其关联违法犯罪联合惩戒办法》的三种惩戒措施

1 对惩戒对象实施金融惩戒

（一）限制惩戒对象名下银行账户、数字人民币钱包的非柜面出金功能，与开立机构既有协议约定的代扣代缴税款、社保、水电煤气费等基本生活保障的款项除外；

（二）停止惩戒对象名下支付账户业务，支付账户余额向本人同名银行账户转账除外；

（三）暂停为惩戒对象新开立支付账户、实名数字人民币钱包，新开立的银行账户应遵循本条第（一）项要求。

2 对惩戒对象实施电信网络惩戒

（一）限制惩戒对象名下的电话卡、物联网卡、固定电话电信线路、短信端口等功能以及过户等业务；

（二）限制惩戒对象名下电话卡注册的存在涉诈风险的互联网账号功能及业务；

（三）不得为惩戒对象开立新的电话卡、物联网卡、固定电话、电信线路、短信端口，存在涉诈风险的互联网账号等以及提供网站、应用程序的分发、上架等业务；

» 以上涉及惩戒的通信业务、互联网应用等应当具备较高的涉诈属性和安全风险，具体惩戒范围由公安机关会同行业主管部门认定。在惩戒期内，惩戒对象在收到公安机关惩戒通知后10个工作日内可申请保留一张名下非涉案电话卡。

3 对惩戒对象实施信用惩戒

(一) 将有关惩戒对象纳入“电信网络诈骗”严重失信主体名单，共享至全国信用信息共享平台，并通过“信用中国”网站对严重失信主体信息进行公示；

(二) 将有关惩戒对象信息纳入金融信用信息基础数据库。

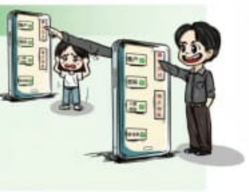
《电信网络诈骗及其
关联违法犯罪联合惩戒办法》
三种惩戒措施

05 二十个防诈关键词

1.屏幕共享

名词解释：

屏幕共享是指通过网络将一台设备（如电脑、手机）的屏幕画面实时传输给其他设备或用户的技术。其核心功能是让多人同步查看同一屏幕内容，广泛运用于远程协作、演示或教学等场景。在电信网络诈骗中，诈骗分子会诱导受害人下载具有屏幕共享功能的App，利用屏幕共享功能获取受害人的账户信息、银行卡号、验证码等，从而骗取钱款。



警方提示

在未确认对方身份和目的前，切勿随意点击对方发来的下载链接或开启屏幕共享，在涉及资金操作时需格外谨慎。

2.百万保障

名词解释：

“百万保障”是一些支付平台提供的保险服务，指当用户的支付账户因被他人盗用而导致资金损失时，按损失金额承诺不限次赔付，每年累计赔付金额最高为100万元的安全保障。这项保障措施是自动开启的，不论是微信、支付宝，还是抖音里的“百万保障”都是完全免费的，用户无需支付任何费用。在冒充客服退款类诈骗中这个词经常出现，诈骗分子通常以误开启“百万保障”为由，诱导受害人进行退款操作来实施诈骗。

警方提示

警方提示：如果对“百万保障”相关业务有疑问，应直接联系平台客服，通过官方渠道核实信息。只要接到陌生来电，无论对方以何种理由引导关闭“百万保障”功能设置的，均是诈骗行为！

3.安全账户

名词解释：

安全账户，也被称为担保金账户或保证金账户，是银行为了满足客户资金安全需求而设立的一种账户。这个词在冒充公检法类诈骗中经常出现。诈骗分子会冒充公检法国家机关工作人员，以“账户被冻结”“资金有风险”等各种理由要求受害人将资金转入所谓的“安全账户”中，并承诺资金核查完毕后进行返还，从而实施诈骗。

警方提示

公检法机关没有所谓的“安全账户”！凡是电话中自称公检法等国家机关工作人员要求把资金归集到指定账户，或要求提供银行账号、密码、验证码的，都是诈骗！

4.NFC盗刷

名词解释：

NFC全称为近场通信技术。它可以让两个设备在几厘米的距离内进行无线数据交换，就像给设备装上了“电子感应器”。目前，NFC技术应用广泛，如移动支付、公共交通、门禁卡等等。然而，这项便捷的技术也被一些不法分子所利用。诈骗分子会要求受害人将手机与银行卡贴靠，通过NFC功能，使银行卡信息与虚假App软件绑定，直接读取并转移卡内资金。

NFC
手机NFC功能
别乱用！

警方提示

切勿随意将手机与银行卡进行贴靠，谨慎通过NFC功能进行陌生支付操作。

5.“两卡”

名词解释：

“两卡”是指手机卡和银行卡。手机卡不仅包括我们日常使用的移动、电信、联通、广电四大运营商的电话卡，还包括虚拟运营商的电话卡以及物联网卡。银行卡包括个人银行卡、对公账户、结算卡以及非银行支付机构账户，如我们日常频繁使用的微信、支付宝等第三方支付平台。

不法
分子
售卖
“两卡”
法律惩处

警方提示

买卖或租借"两卡"均属违法行为。请勿将个人办理的手机卡、银行卡以及微信、支付宝等第三方支付平台账户买卖或租赁给他人。

6."帮信行为"

名词解释：

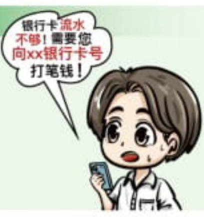
"帮信行为"是指帮助信息网络犯罪活动的行为，即明知他人利用信息网络实施犯罪，仍为其提供技术支持或帮助的行为。根据《中华人民共和国刑法》第二百八十七条之二规定，该行为可能构成帮助信息网络犯罪活动罪，情节严重的可判处三年以下有期徒刑或拘役，并处或单处罚金。

警方提示

帮信行为看似获利，实则可能沦为诈骗分子的帮凶，将面临法律严惩。任何出租、出借、出售"两卡"或参与引流、洗钱的行为均属违法犯罪，切勿贪小失大。

7.刷流水

名词解释：


银行卡流水不够！需要您向xx银行卡号打笔钱！

刷流水是指通过人为制造虚假的资金流动记录，以增加账户的交易流水的行为，通常用于提升信用评级或满足贷款审批要求。因此诈骗分子经常以刷流水为由，诱导受害人向指定账户进行转账。

警方提示

刷流水本身是一种违法行为，违反了金融法规和相关法律规定。如在办理相关服务时，遇到对方要求刷流水的，务必提高警惕，切勿直接向对方指定的账户进行转账。

8.积分清零

名词解释：

在生活中，有很多平台网站会对个人账户实行积分制管理，积攒一定积分可以享受相关服务或兑换相关礼品，这些积分通常是有一定期限，如没有使用将会过期或清零，诈骗分子通常以积分清零为由进行引流，诱导受害人点击相关诈骗链接。

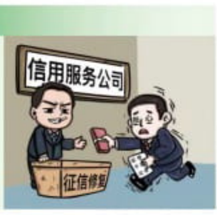
警方提示

切勿轻信非官方渠道发布的积分清零通知，避免盲目操作落入诈骗陷阱。面对积分兑换或清零提醒，应直接通过官方客服热线、官方网站或App等正规渠道进行核实。

9.修复征信

名词解释：

征信记录是个人或企业在信用机构管理下的信用活动记录，主要涵盖贷款、信用卡、按揭、担保等金融交易活动，以及逾期、欠款、违约等不良信用信息。如果征信出现问题对我们工作、生活有着重要影响。因此诈骗分子常常利用"修复征信"为由，利用受害人急于清除不良记录的心理实施诈骗。


信用服务公司
征信修复

警方提示

个人征信由中国人民银行征信中心统一管理，任何公司和个人都无权删除和修改。凡是声称提供消除不良征信记录的都是诈骗。

10.快递引流

名词解释：

我怎么不记得有一个快递

快递引流是指诈骗分子利用快递包裹作为媒介，通过在快递包裹里附加传单或小礼品吸引受害人注意，引导受害人扫码添加联系方式再将其拉入群聊中，为下一步实施诈骗进行准备。

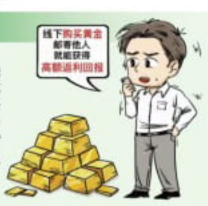
警方提示

不要随意扫描快递里的二维码，遇到邀请进群、转发可领取礼品等情况，务必要高度警惕。

11.现金黄金

名词解释：

这是一种新型洗钱手段，是指诈骗分子以各种理由诱导受害人通过线下取现、购买黄金或其他易变现物品，再通过跑腿、网约车、快递等方式将现金或财物直接交付给指定人员，以逃避资金监管和追查的行为。整个过程中，诈骗分子主要采用"线上诈骗+线下取钱"模式，一改过去"不见面""不接触"的套路，直接与受害人面对面交易，从而骗取信任。


线下购买黄金邮寄他人就能获得高额返利回报

警方提示

凡是要求取出现金或者购买黄金，并通过货运、网约车、邮寄或者跑腿等方式转交给陌生人的都是诈骗洗钱手法。

12.购物卡

名词解释：

商超购物卡因其具有匿名性、流动性的特点，诈骗分子将骗来的资金兑换成购物卡以逃避资金追查，他们通常会要求受害人将资金转换为购物卡，获取其卡号和密码后，再通过黑市渠道快速折价套现，完成洗钱。

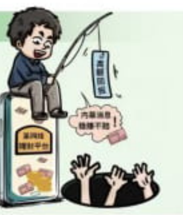
警方提示

凡是要求将资金用于购买大量购物卡，并要求提供卡号和密码的请务必提高警惕。

13.内幕消息

名词解释：

在电信网络诈骗案件中，“内幕消息”是诈骗分子常用的话术陷阱，指其虚构或夸大“内部消息”“独家情报”等概念，诱导受害人进行所谓“稳赚不赔”的投资或交易，最终实施诈骗的行为。


高额回报
内幕消息
稳赚不赔！
某网络理财平台

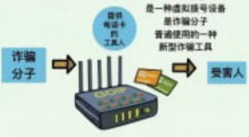
警方提示

凡是宣称“内幕消息、专家指导、稳赚不赔、高额回报”的投资理财，都是诈骗！

14.“电诈工具人”

名词解释：

“电诈工具人”是一种比喻，是对帮助电诈团伙实施违法犯罪行为相关人员的统称。在电信网络诈骗犯罪链条中，诈骗分子为完成违法犯罪行为，需要大肆收购、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成为“电诈工具人”。



警方提示

订购现金花束，扫码送礼品，帮助取现，出售电话卡、银行卡……你认为很平常的事情很有可能“埋雷”。面对花样百出的诱骗手法，增强自身“识骗、防骗、拒骗”能力，警惕诈骗新手法，不做“电诈工具人”。

15.虚拟货币

名词解释：

虚拟货币，也称为加密货币，是一种基于区块链技术发行的去中心化的、以数字形式存在的货币。它使用加密技术来确保交易的安全性和用户的隐私，通常不由任何中央机构发行，主要包括比特币（BTC）、以太坊（ETH）、泰达币（USDT）等，因其特殊性，利用虚拟币“洗钱”已成为犯罪分子实施诈骗以及转移涉诈资金的手法之一。诈骗分子通常以“虚拟货币”投资理财为名搭建虚假平台诱导受害人进行投资，并以线上交易存在风险等理由，扮演“币商”上门指导受害人操作，从而骗取受害人钱财。

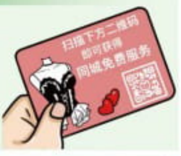
警方提示

虚拟货币交易本身不受法律保护，所谓“高额返利”“上门兑换虚拟币投资”均为诈骗。

16.色情小卡片

名词解释：

“色情小卡片”是刷单诈骗的变种引流手段，诈骗分子以色情信息为诱饵，在公共场所（如酒店、路边车辆）散发附有二维码或联系方式的小卡片，吸引受害人扫码。受害人一旦联系，会被诱导进入“刷单返利”“同城约会”等群聊或虚假平台，以“完成任务即可获取色情服务或高额报酬”为名，要求受害人垫资刷单、充值转账，最终卷款消失。


扫描下方二维码
即可获得
同城免费服务

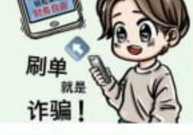
警方提示

传播色情信息及刷单均属违法，切勿因猎奇或贪利陷入诈骗分子的圈套。

17.刷单做任务

名词解释：

刷单做任务是一种虚假交易行为，通常指商家或个人通过组织“刷手”进行虚假的商品或服务交易，以达到提升店铺销量、信誉、排名等目的，在刷单诈骗中，诈骗分子通常以刷单做任务为由诱导受害人进行转账，前期给予小额返利，当受害人大额转入资金后实施诈骗。


急需
校园代理
无需经验
日赚千元
轻松实现
财务自由
刷单
就是
诈骗！

警方提示

刷单就是诈骗！网络刷单本身就是违法行为，不要轻信网络上“高佣金”“先垫付”等兼职刷单的信息。

18.未知链接、二维码

名词解释：

未知链接、二维码是指来源不明、无法确定其安全性和真实性的网络链接、二维码。这类链接和二维码通常通过电子邮件、短信、短视频平台、社交软件等渠道发送给用户，其中混入了大量的广告引流链接，当用户点击访问时可能引导至恶意网站，获取用户的个人信息，也可能下载病毒、木马或其他诈骗软件。

www.xxx.com
陌生链接

警方提示

谨慎对待未知链接和二维码，避免随意点击或扫描，保护个人信息和设备安全，防止财产遭受损失。

19.小众聊天软件

名词解释：

小众聊天软件指用户基数相对小、知名度较低的聊天类应用。部分小众聊天软件因具备强加密通讯、“阅后即焚”、私有化部署等功能，私密性过强，易成监管“灰色地带”，极易被电信网络诈骗分子利用来隐匿犯罪行为、销毁证据，有些软件甚至为实施诈骗而专门设计开发，社会危害性极大。

阅后即焚
加密通讯
私有化部署

警方提示

警惕小众聊天软件成为诈骗工具！切勿点击陌生链接下载陌生软件，如有下载安装软件需求请通过官方应用市场等正规渠道安装。

20.境外来电

名词解释：

境外来电指的是手机或电话接收到来自其他国家或地区的电话呼叫。境外来电是一种电信网络诈骗最常见的引流方式，电话号码通常以“+”或“00”开头，大多为虚拟号码，如果挂断电话再回拨该号码，经常会提示是空号或忙音。

+0014268
xxx458

警方提示

没有固定海外关系的情况下，频繁接到境外来电，几乎都是诈骗电话！在收到运营商跨境提醒服务弹窗提示信息后，一定要保持高度警惕，及时甄别号码来源。如确无境外通联实际需要，建议联系运营商开通拦截境外来电服务，从源头上防范电信网络诈骗。

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
个人信息不透漏 · 转账汇款多核实

国家反诈中心 APP
Android 下载

国家反诈中心 APP
ios 下载

公安部刑侦局
微信视频号

公安部刑侦局
微博号

国家反诈中心
人民号

国家反诈中心
微信视频号

国家反诈中心
微博号

国家反诈中心
抖音号

国家反诈中心
快手号

国家反诈中心
百家号

国家反诈中心
强国号

来源：公安部刑侦局