防范电信网络诈骗

下载国家反诈中心APP

网络违法犯罪信息举报：https://cyberpolice.mps.gov.cn/

国家反诈中心APP下载：各大应用商店搜索“国家反诈中心”

反诈劝阻电话：96110（务必接听）

反诈报警电话：110

反诈防骗校园行

宣传手册

反诈是门必修课 筑牢防线守好责

湖北省公安厅　湖北省教育厅　中国银行湖北省分行

防范网络诈骗

不要贪图小便宜

天上不会掉馅饼

致全省学生及家长的一封信

亲爱的同学们，尊敬的家长朋友们：

当前，电信网络诈骗犯罪手法多，翻新迭代速度快，让人防不胜防。同学们社会经验不足，防范意识薄弱，极易成为诈骗分子的侵害目标。全省青少年被诈骗案件时有发生。网络上“低门槛、高回报”兼职信息，熟人介绍的所谓“包机票酒店、月入数万”高薪出境工作邀约，以及“免费送游戏装备”都是披着糖衣的炮弹，其内核往往深藏致命诈骗陷阱。请一定提高警惕，具体做到：

1、了解诈骗手段，提高警惕性

电信网络诈骗手段多样，常常令人防不胜防。同学及家长们应充分了解常见的诈骗手段，如刷单返利类、虚假购物服务类、冒充熟人类、网络游戏虚假交易类、贷款、征信类诈骗等。我们要时刻保持高度警惕，不轻信陌生人的信息，不随意点击陌生链接，不向陌生人转账汇款。

2、加强个人信息保护

个人信息是诈骗分子进行诈骗的重要工具。因此，学生和家长们要加强个人信息的保护，不要随意在社交媒体上公开自己的姓名、电话号码、身份证号码、家庭住址等敏感信息。同时，对于要求提供个人信息的场合，要仔细甄别，确保信息的安全性和合法性。家长们要保管好个人手机、支付账户和支付密码。

3、培养正确的金钱观和消费观

对于学生来说，要树立正确的金钱观和消费观，不要盲目追求物质享受，不要轻信所谓的“赚钱捷径”“高薪招聘”。家长们也要加强对孩子的教育和引导，帮助孩子建立正确的消费观念，避免孩子陷入诈骗分子的陷阱。

4、遇到诈骗及时报警

遇到诈骗，要保持冷静，不要惊慌失措。第一时间收集相关证据，如聊天记录、转账记录等，并立即拨打110或96110向公安机关报案。同时，也要及时告知学校和家长；下载安装国家反诈中心APP，共同协助公安机关打击电信网络诈骗犯罪。

同学们，家长朋友们!反诈防骗，人人尽责。家长的每一次耐心提醒，是孩子识破骗局的关键指引。平时，请家长务必向孩子多灌输“不轻信陌生人，不随意转账，不透露身份证、银行卡等重要信息”的防骗理念。同学们遇到陌生人索要账户密码、要求屏幕共享时，应果断拒绝并及时请求家长帮忙处置。让我们大家携手共同擦亮识骗的“火眼金睛”，练就防骗的“铜墙铁壁”，早日实现天下无诈！

全民反诈，你我同行！

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

一、常见诈骗类案件

1、刷单返利类诈骗 01
2、虚假网络投资理财类诈骗 02
3、虚假购物、服务类诈骗 03
4、冒充电商物流客服类诈骗 04
5、贷款、征信类诈骗 05
6、冒充领导、熟人类诈骗 06
7、冒充公检法类诈骗 07
8、婚恋、交友类诈骗 08
9、网络游戏虚假交易类诈骗 09
10、机票退改签类诈骗 10
11、追星类诈骗 11
12、AI换脸类诈骗 12

二、不做电诈工具人

1、出租出借银行卡/手机卡 13
2、兼职采购洗钱类诈骗 14
3、境外“高薪”工作类诈骗 15
4、非法兼职类诈骗 16

三、用好八大反诈利器

八大反诈利器 17

四、二十个防诈关键词

二十个防诈关键词 23

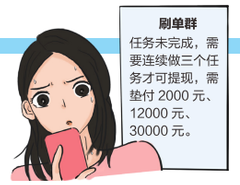
1、刷单返利类诈骗

第一步：建立联系

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”等，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

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：骗取钱财

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。

典型案例

张同学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。初期张同学投入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。

张同学完成转账后，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，于是按照客服要求再次向对方转账760元。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，在多重话术诱导下连续转账，最终累计损失2470元。

切记

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。

民警提示

“刷单、刷信誉”本身就是违法行为，并非正当兼职，千万不要被蝇头小利所诱惑。

2、虚假网络投资理财类诈骗

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；或通过交友平台与受害人确定特殊关系，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。

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

孙同学在网络上寻找兼职，发现一篇“轻松投入，稳定盈利”的帖子，加诈骗分子为好友后，对方给他推来一个APP，并宣称往里面投入资金购买“虚拟黄金”，每月固定有20%的收益，投入越多收益越多。

孙同学先尝试投入500元，并在月底顺利提现出600元，孙同学信以为真，果断再投入5000元，等到月底发现账号已失效，被诈骗分子拉黑。

切记

凡要求下载非官方APP的“理财顾问”均为骗子，投资理财需通过正规渠道，“高收益”背后必是高风险，发现异常立即报警。

民警提示

不要轻信任何宣称能稳定高额盈利的投资理财项目。

3、虚假购物、服务类诈骗

第一步：寻找目标

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

李同学暑假打工，赚了2100元，欲购买新手机，因贪图价格便宜，未通过正规官方渠道购买手机，而是选择在网络平台寻找私人卖家交易。

在转账2100元购款后，卖家未发货，并拉黑删除。

切记

网络代购风险高，空包诈骗需警惕！切勿轻信陌生人提供的身份资质，更不要脱离正规平台扫码转账。

民警提示

网上购物一定要选择正规的购物、服务平台。

4、冒充电商物流客服类诈骗

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、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

王同学通过扫描快递包裹中的二维码，诈骗分子谎称其网购商品存在质量问题，需退货，并可以赔偿高端产品，但需要“保证金”，王同学支付200元“保证金”后被对方拉黑。

切记

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”“远程操作”等功能。

民警提示

接到自称是电商、物流客服电话时，不要轻易相信，务必到官方平台进行核实。

5、贷款、征信类诈骗

第一步：寻找目标

诈骗分子冒充银行、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：虚构交易

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：实施诈骗

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

因曾在正规平台申请贷款未果，王同学接到自称“网贷客服”的微信好友申请。对方以“低息放款3万元”为诱饵，抛出“需预存30%流水激活额度”的话，诱导王同学登录陌生网购账户购买高价商品寄往指定地址。待王同学完成11833元支付后，账户突遭挤占下线，察觉异常的王同学在3小时后来到派出所报警。

切记

凡以“验证还款能力”“刷流水激活额度”为由索要转账的，100%是诈骗！

坚决拒绝登录他人账户、点击陌生链接、进行“屏幕共享”等高风险操作！

民警提示

发现异常立即拨打96110，转账后30分钟内报警可最大限度拦截资金！

6、冒充熟人、领导类诈骗

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。

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

某中学为方便新生家长沟通，将官方群二维码印在入学手册上随录取通知书寄出。骗子趁机混入群内，深夜冒充“群主老师”发布通知，要求缴纳“资料费、复印费”共495元，并附上支付二维码，还让家长备注学生姓名、截图接龙。流程看似正规，数额不大，导致9名家长在40分钟内扫码支付，共被骗4000余元。骗子甚至将已缴费家长拉入小群企图进一步诈骗。

切记

加入与学校相关的群聊后，立即与班主任、校方核实群管理员身份，并做好备注。对群内任何转账、收费、扫码支付要求保持警惕，切勿轻信！

民警提示

遇缴费通知，务必通过官方预留电话、线下找老师等方式直接向学校核实真伪！

7、冒充公检法类诈骗

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

陈同学在家中玩手机时下载了一款“名人朋友圈”的软件，被一陌生人添加“好友”。对方自称是“警察”，谎称其账号侵犯明星隐私权，并威胁“不配合调查将抓捕其父母”。陈同学按照对方要求添加“律师”，“律师”以“需要缴纳保证金，将钱转入安全账户”为由，通过视频通话指导陈同学将父母手机的余额共计转出13000余元。转账完成后“律师”指导小陈删除所有聊天记录，直到小陈父亲收到扣款短信后报警。

切记

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”。

民警提示

凡是要求转账进行资金核查的都是诈骗！

8、交友类诈骗

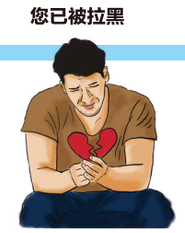
第一步：包装身份

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，然后在交友等网站发布个人信息。

第二步：建立信任

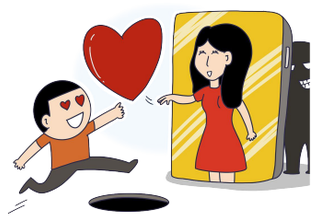
与受害人建立联系后，利用照片和预先设计的虚假身份骗取受害人信任，并通过持续的聊天和受害人建立好朋友关系。

第三步：实施诈骗



诈骗分子以遭遇变故急需用钱，或者以维持好朋友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



小丞同学在网购二手手机时，被伪装成女生的诈骗分子诱入圈套。骗子通过伪造清纯自拍照、身份证号及手写个人资料，虚构与受害者的共同爱好（如同一个明星演唱会、宠物狗同名旺财），迅速建立闺蜜关系。

随后以家庭变故为由，编造没钱吃饭生病住院母亲车祸学费不足等连环骗局。

切记

网络交友需谨慎，切勿轻易相信陌生人的甜言蜜语。对于那些以各种借口索要钱财的行为，更要保持清醒的头脑，谨慎对待。

民警提示

一旦发现任何可疑情况，应立即向警方报案，以便警方能够及时采取有效措施。

9、网络游戏虚假交易类诈骗

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

李同学把游戏账号挂在平台上出售。当晚有人私信称有购买意向。对方查看游戏账号内的装备后觉得十分满意，不久后便发来一个付款截图称已下单，随后发来一个链接，让李同学与客服联系。点开链接，进入一个人工客服界面。"客服人员"告知他需要缴纳"保证金"才可完成交易，若终止交易游戏账号有冻结风险。按照要求缴纳"保证金"后，却未收到交易完成的转账。再次点开链接时却发现已无法打开，也被拉黑了。

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。

民警提示

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游戏交易的，都是诈骗！

10、机票退改签类诈骗

第一步：发布信息

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：实施诈骗

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：诱导转账

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

罗同学接到一通陌生电话，对方自称是某航空公司工作人员，告知罗同学购买的航班因天气原因出现延误，询问她是否需要改签，还说改签成功后可以领取300元赔偿金。

罗同学同意改签，工作人员让她输入网址进入"某航空公司"页面，接着让罗同学按提示在"理赔申请"页面输入个人身份信息、银行卡信息，进入"认证会议"模式共享手机屏幕。不久，罗同学发现自己的银行卡被扣款4700余元。

切记

选择官网、12306官方APP等正规渠道购票，并及时查验客票状态，对于非官方渠道发布的票务信息或退改签通知，不要轻信，务必通过官方渠道核实。

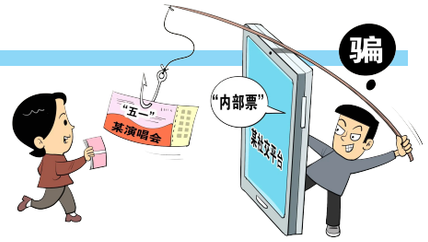
民警提示

官方渠道是王道，警惕陌生链接与信息。

11、追星类诈骗

第一步：发布信息

有的骗子会在网上兜售所谓的明星见面会门票、明星签名照、爱豆小卡、应援物料，吸引年龄小、防备心不强的未成年追星族。



第二步：诱骗信任

部分骗子为取得信任，会在二手交易平台挂出演唱会票务信息，并通过平台完成初步交易。在骗取首笔款项后，又以“加价升票”“系统确认”“押金解锁”等名义诱导受害人多次支付，直至最后通过“要求确认收货后再发票”等方式销号失联。

第三步：实施诈骗

受害人在质疑或反悔时，骗子会以“订单异常”“超时未支付”“退款需验证账户”等借口，让受害人添加新的“客服”或“财务”，进一步设计所谓退款流程，实际为再次实施诈骗的手段。

典型案例

张同学想购买某明星演唱会的门票，在搜索后，联系上了一位“卖家”，被拉入一个临时建的群。对方提出“各付一半，到票后再补余款”的方案，小张先行转账后，被告知“未备注需重转”。再次汇款后，对方又以“订单超时”之名引导添加客服，下载名为“Teams”的远程软件并共享屏幕。随后，对方以验证身份、提高银行卡流水等借口，诱导其不断转账。

切记

演唱会门票请认准官方渠道及认证票务平台，切勿轻信私信、视频评论等来源。

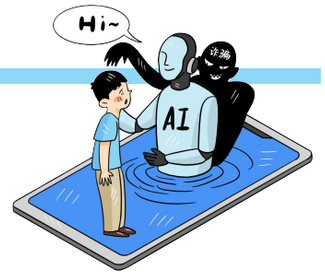
民警提示

爱豆私聊是陷阱，
理性追星莫沉迷。
涉及转账先停手，
陌生链接勿点击。

12、AI换脸类诈骗

第一步：获取信息

诈骗分子通过非法渠道获取受害人亲属、朋友的视频信息，并针对性的通过视频生成骗子需要的AI模型。



第二步：实施诈骗

联系上受害者，以各种理由编造需要金钱的状况，并表示事情紧急，要求受害者立即转账，并不得向外界求助。

第三步：变本加厉

收到资金后，继续编造各种理由如“坐牢”“判刑”等更严重的后果，威胁受害者继续转移更多资金，直至受害者无力承担。

典型案例

杨同学突然收到妹妹申请为好友的请求，通过后，接到妹妹发来的视频通话请求，视频中“妹妹”哭诉自己在外地因涉嫌违法被当地警方拘留，需要缴纳高额保释金，否则将被判刑。由于视频中的“妹妹”形象、声音与真实妹妹极为相似，杨同学心急如焚，在没有与妹妹、其他朋友或学校核实的情况下，分多次向对方提供的账户转账。直到后来与妹妹通话时，才发现自己遭遇了AI 换脸诈骗。

切记

如果接到“家人”“朋友”等转账、汇款的视频，一定要仔细甄别真伪。如有必要可以要求对方做快速地抬头、点头、转头的动作，进一步判断视频是否有异常的细节，来确认这个视频是真实的。

民警提示

尽量避免人脸、指纹等个人生物信息的过度公开和分享。
AI 语音也可伪造，陌生语音求助需通过视频验证或联系家属核实。

1、出租出借银行卡/手机卡

■ 第一步：诱导出借 ■

通过“高额佣金”、“兼职赚钱”等话术吸引目标人群，声称只需提供银行卡或手机卡即可轻松获利。

常见场景：社交平台广告、熟人介绍、线下“跑分”团伙招募。

■ 第二步：非法利用 ■

获取卡片后，用于洗钱、转账诈骗资金或注册虚假账号实施电信诈骗。

通过NFC功能盗刷银行卡、利用手机卡接收验证码实施诈骗。

■ 第三步：逃避追责 ■

资金到账后迅速转移，出借人因“证据不足”难以追责，甚至被警方列为嫌疑人。

法律后果：可能构成帮信罪（3年以下有期徒刑）或诈骗共犯。

■典型案例■

张同学网友要求帮其办一张电话卡，给450元报酬，张同学用自己的身份证去办理了一张电话卡并寄给对方，拿到了报酬，开心地买了游戏装备。结果，自己办理的那张手机卡被不法分子用于拨打诈骗电话，导致一群众被骗6万余元。

■切记■

公安机关严厉打击涉“两卡”违法犯罪，遇到情况可疑的“跑分”“洗钱”平台和个人时，市民应及时拨打110报警电话，向公安机关提供线索。

■民警提示■

警惕“跑分”“洗钱”陷阱。不要轻易被“朋友”或网络上承诺给予高额收入的招聘信息所诱惑。

2、兼职采购洗钱类诈骗

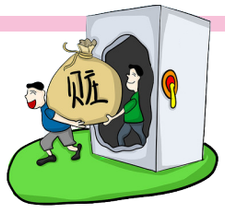
■ 第一步：发布信息 ■

诈骗分子在网上发布“高薪日结”“轻松采购”等虚假招聘信息，以“商场采购员”“代购员”等名义吸引求职者，承诺无需经验、报酬丰厚。

■ 第二步：诱骗工具 ■

要求求职者提供个人银行卡、身份证或收款码，谎称用于“公司垫付采购款”“代收货款”，实际用于接收诈骗资金。

■ 第三步：资金转移 ■



求职者账户收到赃款后，被要求取现或购买贵重物品（如黄金、名烟酒），再转交“指定人员”。完成后，诈骗分子以“佣金”名义支付少量报酬，随即失联。

■典型案例■

吉同学在求职公众号看到“商场采购员”兼职广告，日薪300元且包餐食。添加“周经理”后，对方要求其提供银行卡接收“采购款”并取现，由“张经理”指导操作。次日，小美账户收到15万元，取现后交给“张经理”，获得1500元报酬。随后“周经理”自称经营代购公司，要求小美带银行卡和身份证协助采购。实际“张经理”带其取现15万元后，以“今日缺货”为由中止交易。小美未等到后续通知，反被警方调查，才发现所谓“轻松兼职”实为洗钱陷阱。犯罪分子通过虚假代购名义，利用大学生银行卡进行资金转移，并以反常高额报酬诱导其参与。

■切记■

如今，新型洗钱犯罪手段更加隐蔽和复杂。大家要提高法律意识，警惕高额报酬的兼职，防止陷入“洗钱”陷阱或者遭遇电信网络诈骗。

■民警提示■

“轻松兼职”藏猫腻，护好证件拒当共犯。

3、境外“高薪”工作类诈骗

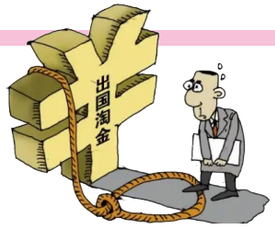
■ 第一步：发布信息 ■

通过社交平台（抖音/快手/兼职网站）发布“月入数万”、“包机票食宿”等广告，瞄准涉世未深群体。

冒充正规企业伪造营业执照、以“游戏代练”“客服兼职”降低警惕性、利用“好大哥”“热心网友”伪亲密关系。

■ 第二步：诱骗出境 ■

为受害者购买机票/酒店制造“合法出境”假象（实际不住），抵达后立即没收证件/通讯设备，通过边境偷渡转至境外电诈园区。



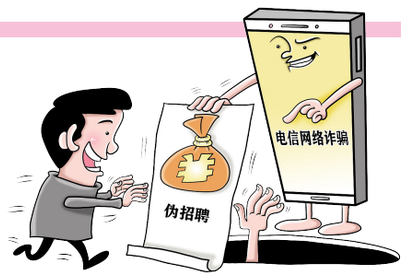
■ 第三步：强迫工作 ■

强迫从事电诈/赌博等非法活动，未达标者遭殴打/电击/勒索赎金，部分受害者被多次转卖至缅北/柬埔寨或其他园区。

■典型案例■

李同学轻信境外“月薪3万元、包机票食宿”的高薪行政岗广告，对方提供虚假电子合同并催促缴纳“岗位预留金”。李同学私自购票准备出境时，被校方发现并报警。

民警与家属劝阻时，骗子竟嚣张发来虚假国内定位“自证清白”，经警方核查，最终戳穿谎言。



■切记■

境外高薪工作往往是危险诱饵，看到境外招工信息，首先通过官方渠道核实，不可轻信“赴他国挣大钱、赚快钱”等诱骗信息，通过正规渠道求职。

■民警提示■

不要被境外高薪职位诱惑，更不要参与跨境电信网络诈骗和赌博、吸毒等违法犯罪活动。

4、非法兼职类诈骗

■ 第一步：发布信息 ■

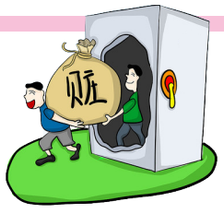
诈骗分子在网上以发布“高薪日结”等虚假招聘信息吸引求职者，承诺无需经验、报酬丰厚。

■ 第二步：提供信息 ■

诈骗分子为受害者提供账号或各类诈骗分子需要的信息，要求受害者在各类平台进行购买、交易，或者做一些很简单（或技术类、或不合常理）的任务。

■ 第三步：完成任务 ■

求职者接取任务后，按诈骗分子的要求完成任务。实际任务是诈骗分子完成诈骗（或资金转移）的一部分步骤。



■典型案例■

秦同学是某高校计算机系的一名学生，在网上看到一则兼职招聘，报酬很丰厚。小秦心动了，接下任务后根据骗子提供的信息，小秦发现骗子提供的代码是在某网站爬取相应的信息，秦同学完善代码，顺利完成任务，并取得相应报酬。

数月后，校方收到警方协助调查，最终秦同学被立案调查。

■切记■

明知违法不可为，不要因为一些小利误入歧途。

■民警提示■

“帮忙取现”可能是洗钱！
“技术支援”可能涉嫌犯罪！

八大反诈利器

1、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。

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。

2、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。

3、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。

根据国家反诈中心统计，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。

12381
涉诈预警劝阻短信
这个短信一定要看

4、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。

5、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

6、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。

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。

7、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。

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

8、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。

“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】

>>> 二十个防诈关键词 <<<

1、屏幕共享

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。

2、百万保障

“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。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。

3、安全账户

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。诈骗分子会百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。

4、NFC盗刷

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。

5、“两卡”

“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。

6、“帮信行为”

“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。

四、二十个防诈关键词

>>> 二十个防诈关键词 <<<

7、刷流水

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。

8、积分清零

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。

9、修复征信

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。

10、快递引流

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。

11、现金黄金

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。

12、购物卡

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。

>>> 二十个防诈关键词 <<<

13、内幕消息

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。

14、“电诈工具人”

“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”。

15、虚拟货币

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，利用虚拟市“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。

16、色情小卡片

“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。

17、刷单做任务

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。

18、未知链接、二维码

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。

>>> 二十个防诈关键词 <<<

19、小众聊天软件

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。

20、境外来电

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。

警方提示

以上关键词均有

各类衍生版本，

若遇到相关事件，

务必多次、多方位、

多人核实，

切勿受骗上当！