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
快手号

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

防范电信网络诈骗宣传手册

(2026版)

不听不信不贪恋　构筑反诈“心”防线

公安部刑侦局　国家反诈中心

“全民反诈在行动”

不听不信不贪恋
构筑反诈“心”防线

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 02
2、虚假购物、服务类诈骗 04
3、虚假网络投资理财类诈骗 06
4、冒充电商物流客服类诈骗 08
5、贷款、征信类诈骗 10
6、网络游戏虚假交易类诈骗 12
7、网络婚恋交友类诈骗 14
8、冒充公检法类诈骗 16
9、冒充领导、熟人类诈骗 18
10、机票退改签类诈骗 20

02 反诈利器全家桶

1、跨境业务按需办理 23
2、全国移动电话卡和互联网账号“一证通查” 24
3、云闪付App“一键查卡” 25
4、“803反诈”智能体 26
5、境外来电提醒服务 28
6、反诈名片 29
7、12381涉诈预警劝阻短信 30
8、96110预警劝阻专线 31
9、国家反诈中心App 32

目录 CONTENTS

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 35
2、五万以上至五百万以下的罚款 38
3、六个月至三年以内不准出境 41

04 《电信网络诈骗及其关联违法犯罪联合惩戒办法》的3种惩戒措施及案例

1、金融惩戒 43
2、电信网络惩戒 43
3、信用惩戒 44
4、典型案例 45

05 常见电诈工具人表现形式及法律后果

1、地推式诈骗引流 49
2、短信引流 50
3、冒充客服电话引流 51
4、搭建手机口 52
5、架设GOIP、VOIP等虚拟拨号设备 53
6、出租出售出借银行卡、电话卡 54
7、购买并寄送黄金 55

目录 CONTENTS

8、取现寄递 56

9、实物洗钱 57

10、办贷款刷流水 58

11、话费、电费、燃气费充值 59

12、跑分 60

13、POS机套现和对公账户转账 61

14、法律后果 62

06 警惕境外高薪招聘陷阱

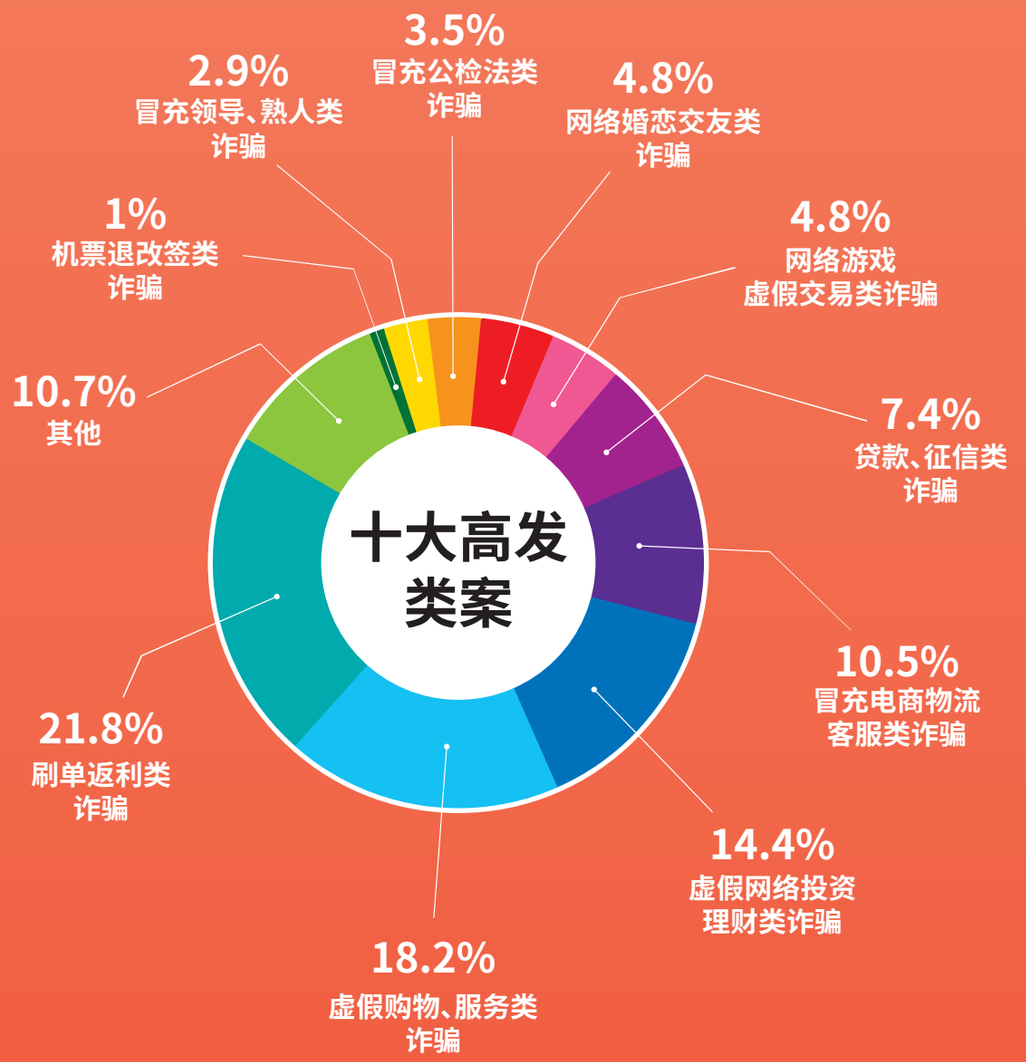
警惕境外高薪招聘陷阱 64

07 反诈最前沿

反诈最前沿 66

1 十大高发类案

不听不信不贪恋，构筑反诈“心”防线



1、刷单返利类诈骗（发案占比21.8%）

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、AI问答等渠道发布就业培训、招聘岗位、赚钱门路等信息，或通过涉黄网站、约炮App诱导被害人下载刷单App。

●第二步：小额返利

被害人完成垫资刷单、关注账号、点赞评论、投票冲榜、代付返现、积分返利、充值会员等任务后，诈骗分子会发放小额佣金，骗取被害人信任。

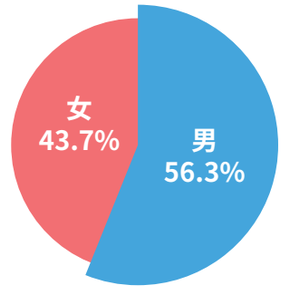
●第三步：实施诈骗

诈骗分子以“充值越多、抢单越多、返利越多”为诱饵引诱被害人做“进阶任务”，同时使用刷单App指导被害人进行大额垫资或充值，再以“任务未完成”“卡单”“操作异常”“账户被冻结”等各种借口诱骗被害人加大投入，进而骗取更多钱款，直至被害人发觉被骗。

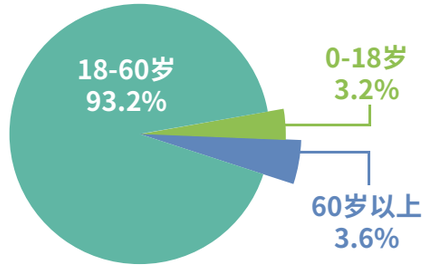
警方提示

“刷单、刷信誉”本身就是违法行为，并非正当兼职。

易受骗群体▶ 登录涉黄网站或App的、找兼职工作的、想开网店挣钱的人群。



受骗性别占比



受骗年龄占比

典型案例

乔先生在浏览短视频时点击了一个卖手机流量卡的直播广告，直播中声称只需8元就能获得256G的流量卡，乔先生认为价格实惠于是下单购买。

在收货后乔先生发现流量卡背后附有二维码，只有扫码添加客服后才能开通，乔先生照做后，客服诱导其下载“符号”App做广告任务，承诺完成后给予返利。

初期获得小额返利后，乔先生信以为真，持续追加资金投入，最终被诈骗分子以出现失误、操作异常、充值解除为由骗走9万元。

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。

2、虚假购物、服务类诈骗（发案占比18.2%）

作案手法

●第一步：寻找目标

诈骗分子在微信群、朋友圈、网购平台或短视频直播间等发布低价转让、海外代购等信息，或声称可以提供代抢演唱会门票、订购预售产品、代写论文、低价代买火车票或飞机票等服务。

●第二步：虚构交易

通过正规平台与被害人取得联系后，诈骗分子会通过微信、QQ或其他小众通联软件添加被害人为好友与其进行商议，以私下交易可节约手续费或方便交易等理由，要求脱离购物平台转账；或是通过发送仿冒的网购交易网站、App诱导被害人转账。

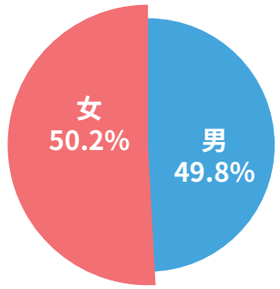
●第三步：实施诈骗

待被害人付款后，以缴纳定金、交易税、手续费为由诱骗被害人再次转账汇款，或者以需进行会员认证、未成年人验证等为由，要求被害人下载具有屏幕共享功能的App，通过语音通话或屏幕共享指导被害人操作手机，从而获取其账户信息及验证码，实现转款盗刷。

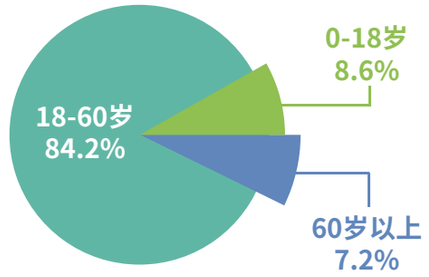
警方提示

网上购物一定要选择正规的购物、服务平台。

易受骗群体▶ 经常网购和进行二手交易，有购买演唱会门票、游戏皮肤装备需求的人群。



受骗性别占比



受骗年龄占比

典型案例

韦女士通过社交软件浏览到可以帮忙购买明星演唱会门票的消息，对方声称购买演唱会门票需实名，要求其提供身份信息，后对方以购票失败为由，诱导其通过小众通联软件语音通话并开启共享屏幕，韦女士按照对方指示操作手机，最终被骗12811元。

切记

对低价、代购商品要提高警惕，避免脱离官方平台进行私下交易。

3、虚假网络投资理财类诈骗（发案占比14.4%）

作案手法

第一类

诈骗分子冒充投资导师、金融理财顾问在短视频等互联网平台开播授课，以免费荐股、行情解读为噱头引流，引诱被害人加入专属群聊，通过群里的托分享虚假盈利、提现流水截图，营造稳赚不赔的假象，诱导被害人在虚假交易平台持续投入资金。

对被害人前期小额投资试水予以返利，一旦被害人加大资金投入，又以“服务器异常”“操作失误导致账户冻结”等理由阻止提现，并要求缴纳“保证金”“解冻金”等费用，造成被害人大额财产损失。

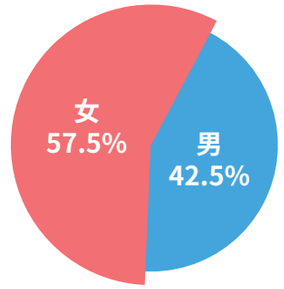
第二类

诈骗分子通过打造军人、高管等人设，在婚恋交友平台或社交软件与被害人结识并确立恋爱关系，再以有特殊内部渠道、可获得高额投资回报等为由骗取被害人信任。前期诈骗分子会委托被害人代为管理其投资平台账号，制造高额盈利假象，后期会诱导被害人一并开立账户投入资金。

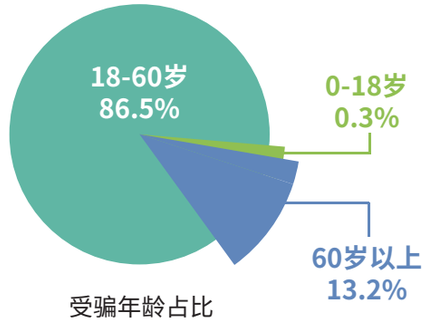
警方提示

此类案件中，诈骗分子会提前告诉被害人“投资项目高度机密不能对外泄露”或“正常转账也会被公安预警”，以此对抗公安机关预警劝阻工作。

易受骗群体▶ 有一定收入、资产，且有情感或投资需求的群体。



受骗性别占比



受骗年龄占比

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★38★”的群聊，并通过群内指引添加自称“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，一再追加资金投入。

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。

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。

4、冒充电商物流客服类诈骗（发案占比10.5%）

作案手法

第一类

诈骗分子批量开设低价网店，故意错发、漏发低价劣质货物，事后主动联系被害人理赔或退换，诱导其脱离正规平台建立联系，办理退费理赔实施诈骗。

第二类

诈骗分子通过大规模群发短信，冒充电商物流平台客服，以快件丢失、包裹破损、快递滞留、网购商品存在质量问题等为由，主动提出理赔补偿，诱骗被害人点击陌生钓鱼链接或添加虚假客服实施诈骗。

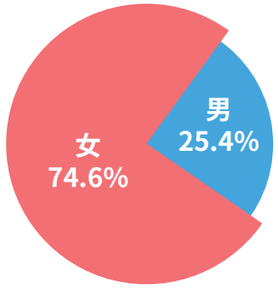
第三类

诈骗分子冒充互联网平台（如：微信、支付宝、抖音）或保险公司客服，与被害人建立联系，声称其已订购“百万保障”“会员续费”等服务，不解除相关服务将产生额外扣费，诱导被害人下载小众通联软件实施诈骗。

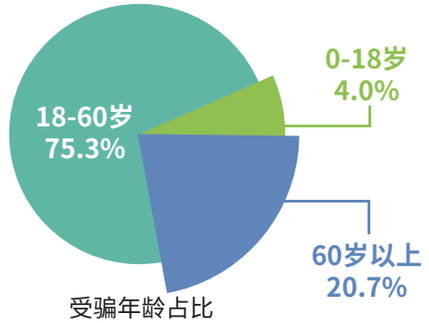
警方提示

自称电商、物流客服与您联系时，务必与官方平台核实，退费理赔切勿脱离官方平台监管。

易受骗群体▶ 经常刷短视频，网上购物，有课程退费，对理赔流程不熟悉的人群。



受骗性别占比



受骗年龄占比

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，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”为由要求周女士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。

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。

5、贷款、征信类诈骗（发案占比7.4%）

作案手法

第一类

诈骗分子通过网络媒体、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，引诱被害人下载虚假贷款App或登录虚假网站，再以银行卡信息填写错误、流水不足、征信有问题等为由，要求被害人缴纳保证金、手续费或向指定账户刷流水。

第二类

诈骗分子开发虚假贷款软件，包装成正规软件后上架到应用商店，软件中嵌入木马程序，可盗刷被害人账户资金。

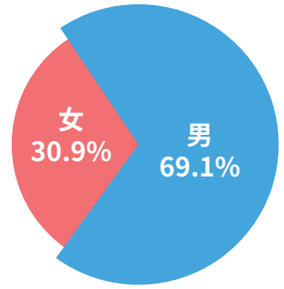
第三类

诈骗分子在正规贷款软件中内嵌弹窗广告，在被害人提交贷款申请时自动跳出，诱导被害人下载涉诈贷款App实施诈骗。

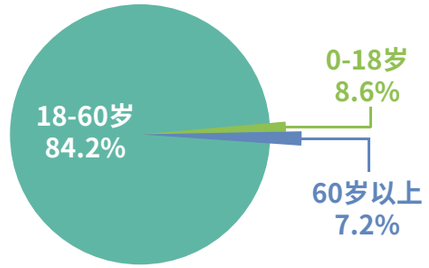
第四类

诈骗分子冒充银行、网贷、金融公司、短视频平台等官方客服，称被害人存在贷款未还、信用卡逾期的问题，如不及时处理将会被起诉、纳入失信名单，诱导其下载虚假贷款、征信服务类App进行“还款”“缴纳申诉保证金”“收取消除不良征信记录手续费”，以此实施诈骗。

易受骗群体▶ 有贷款需求、对征信政策存在认知误区或者已背负债务的人群。



受骗性别占比



受骗年龄占比

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个人和放款银行账户的信息，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，才知上当受骗。

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。

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。

6、网络游戏虚假交易类诈骗（发案占比4.8%）

作案手法

●第一步：寻找目标

诈骗分子在社交、游戏平台发布“高价收购游戏账号”“低价出售稀有装备、皮肤”“游戏代练”“免费送游戏皮肤、账号”等信息引流。

●第二步：引导交易

诈骗分子运用技术手段，仿冒正规的游戏交易平台，诱导被害人到仿冒的游戏交易平台或通过第三方交易平台私下进行交易。

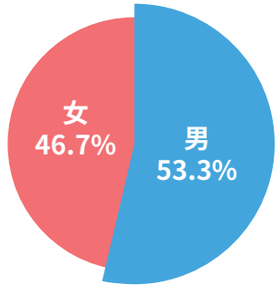
●第三步：实施诈骗

诈骗分子以被害人操作失误、等级不够等为由，要求被害人支付所谓的“注册费”“解冻费”“会员费”等费用，随后将被害人拉黑。

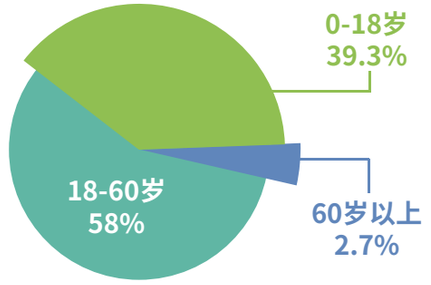
警方提示

买卖游戏账号、道具请通过正规交易平台操作。

易受骗群体▶ 喜欢网络游戏的青少年群体。



受骗性别占比



受骗年龄占比

典型案例

常先生在玩游戏时收到一条游戏好友申请，对方提出想用3000元购买常先生的游戏账号，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，系统显示常先生账户内有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导常先生付款3万余元，但仍无法提现，常先生这才意识到被骗。

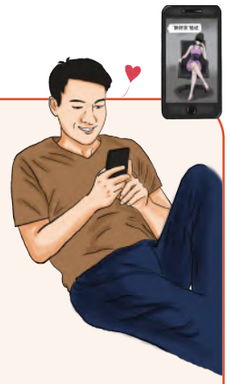
切记

脱离官方平台或私下交易均存在被骗风险。

7、网络婚恋交友类诈骗（发案占比4.8%）

作案手法

第一类



通过包装身份培养感情来诈骗钱款。诈骗分子会在社交软件、同城私聊、兴趣社群、直播平台中把自己包装成“白富美”或“高富帅”，以共同爱好为切入点，主动搭讪被害人，与被害人建立联系、培养感情，确立恋爱关系，再以家人生病、生意周转、生活遇困、奔现等突发状况为由，诱导被害人转账、发红包、赠送贵重礼品。

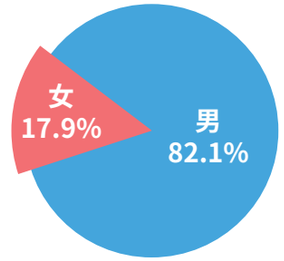
第二类

通过提供虚假色情服务来盗刷钱款。诈骗分子通过涉黄网站、线下约炮卡片、社交软件、短视频平台等渠道，以同城免费约炮、上门私密服务、一对一专属交友为噱头，诱导被害人下载虚假约炮App，此类App具有屏幕共享和远程操控的功能，通过窃取被害人银行卡账号、验证码、密码等信息实施盗刷。

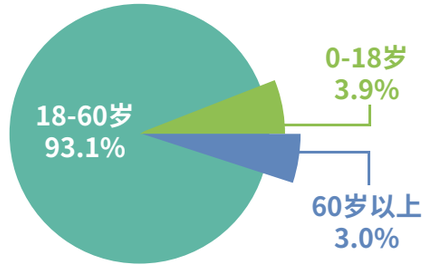
警方提示

网络交友需谨慎，虚拟世界难辨真。

易受骗群体▶ 单身、渴望交友的群体。



受骗性别占比



受骗年龄占比

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“穆女士”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。

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。

8、冒充公检法类诈骗（发案占比3.5%）

作案手法

●第一步：引诱目标

诈骗分子通过非法渠道获取被害人的身份信息，冒充公检法等国家机关工作人员，通过电话或微信、QQ等与被害人取得联系，要求被害人配合工作。

●第二步：威逼恐吓

诈骗分子以被害人涉嫌洗钱、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，同时向被害人展示虚假通缉令、财产冻结书等法律文书，甚至还会身着假警服，以仿冒的公安机关办公场所为背景与被害人视频通话以增加可信度。

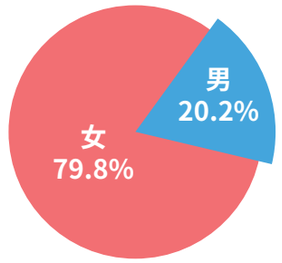
●第三步：实施诈骗

诈骗分子以帮助被害人洗脱罪名为由，诱导被害人到宾馆等独立封闭空间，阻断与外界联系，进而要求被害人配合调查或接受监督，诱导其安装具有屏幕共享和远程操控功能的诈骗App。以“洗脱嫌疑”“资金清查”为由，要求被害人将资金转至“国家监管账户、安全账户、验资账户”进行诈骗。

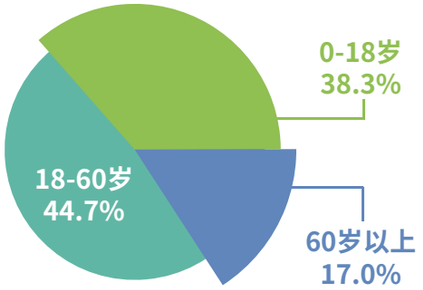
警方提示

公检法等国家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”。

易受骗群体▶ 防范意识较差，不了解公检法办案流程的群体。



受骗性别占比



受骗年龄占比

典型案例

周某（男，14岁）在QQ收到好友发送的一张图片，图片称其是未成年人，因为玩蛋仔派对已经被公安机关提醒，需要配合调查，如果不配合就要被拘留、罚款。

被害人添加图片中提供的QQ号后，对方自称是警察，需要进行“资金清查”，随后周某按照对方的要求打开父亲的微信、支付宝、手机银行等应用。

诈骗分子通过屏幕共享，实时看到了其父亲手机上的所有验证码，分批将账户内的4万元转走。

切记

凡是要求转账，配合国家机关进行资金核查的都是诈骗。

9、冒充领导、熟人类诈骗（发案占比2.9%）

作案手法

● 第一步：建立联系

诈骗分子盗用被害人老板、领导、亲朋、子女老师的头像及姓名，伪装其社交账号添加被害人为好友，或诱骗被害人加入特定群聊，甚至直接潜入被害人所在的群聊之中观察人员关系和动态。

● 第二步：骗取钱财

诈骗分子冒充老板、领导、子女老师的身份并模仿他们的语气发出转账或缴费的指令，并以情况紧急、有事不方便、尽快缴费等借口催促被害人尽快转账；或是冒充亲朋好友以“车祸事故代为支付医疗费”“代为订机票或支付购物款”等为由，向被害人实施诈骗。

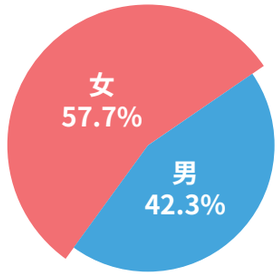
警方提示

识别假领导、假熟人的两个特征：

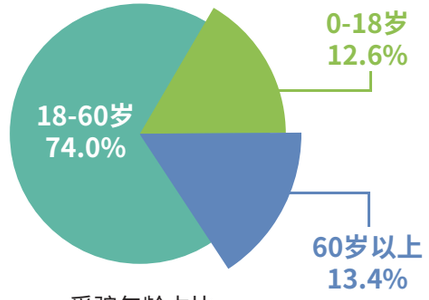
沟通方式奇怪：只打字，拒绝电话、视频联系。

需求紧急且涉及钱款：突然提出借钱、汇款、垫付费用要求。

易受骗群体▶ 财务会计、企事业单位人员、学生家长等群体。



受骗性别占比



受骗年龄占比

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才发现被骗。

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。

10、机票退改签类诈骗（发案占比1%）

作案手法

●第一步：骗取信任

诈骗分子通过非法渠道获取被害人订票信息，冒充航空公司客服人员，通过电话或短信进行联系，以能准确说出被害人姓名、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

初步取得被害人信任后，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，需要被害人改签或退票，并主动提出给予赔偿金，诱导被害人下载视频会议类App、指定软件或登录虚假网站。

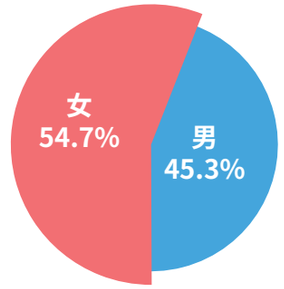
●第三步：实施诈骗

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，套取被害人银行卡账户、密码、验证码等信息后转走资金，或诱导被害人转账进而实施诈骗。

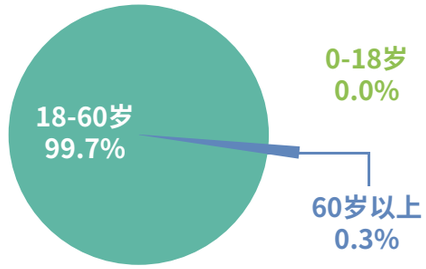
警方提示

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。

易受骗群体▶ 经常出差、旅行需购买机票的群体。



受骗性别占比



受骗年龄占比

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取消航班，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。

切记

如需办理理赔业务务必登录航空公司官网或购票平台进行操作。

2 反诈利器全家桶

不听不信不贪恋，构筑反诈“心”防线

业务办理及查询类的利器

一、跨境业务按需办理

为方便无境外通信需求的用户免受境外来电侵扰，工业和信息化部于2025年组织中国电信、中国移动、中国联通、中国广电推出“跨境业务按需办理”便民服务。对于没有国际及港澳台亲友、不从事跨境业务的用户，可结合自身实际通信需求，使用该服务关闭境外来电、短信接收功能。

当前“跨境业务按需办理”服务可通过两种方式办理

1、直接联系所属基础电信企业

四家基础电信企业专门开发了“跨境业务按需办理”短信办理功能，用户可通过发送短信到相关企业指定号码或拨打客服电话、前往线下营业厅等多种方式咨询办理。

2、使用“反诈公众服务平台”

工业和信息化部指导信息通信行业反诈中心归集四家基础电信企业办理入口，在“反诈公众服务平台”上线 “跨境业务按需办理” 功能。

用户可通过微信、支付宝搜索“反诈公众服务平台”小程序，选择自己手机号所属电信企业，一键关闭或重新开通境外来电及短信接收功能，一键触达、自主可控、灵活便捷。

“跨境业务按需办理”功能累计服务用户5.87亿。

点击跨境业务按需办理

选择电话所属的运营商

选择需要办理的业务

二、全国移动电话卡和互联网账号“一证通查”

为方便群众快速查询名下电话卡、互联网账号情况，工业和信息化部于2022年推出全国移动电话卡、互联网账号“一证通查”服务，联动124家省级基础电信企业和39家移动通信转售企业相关数据，以及23家重点互联网企业、共同提供查询支持。

广大用户可以使用该服务便捷查询本人名下持有的移动电话卡数量，以及本人名下移动电话卡关联的互联网账号数量。用户对查询结果有异议的，可以通过官方渠道及时联系电信企业和互联网企业沟通处理。

同时，“一证通查”服务提供了线上、线下多种使用渠道。用户可以通过“国务院客户端”小程序、“国家政务服务平台”小程序、“工信微报”公众号、各基础电信企业网上营业厅等进入查询入口，也可以持本人有效身份证件到相关电信企业线下营业厅查询本人名下所有电话卡情况。

全国移动电话卡和互联网账号“一证通查”服务已累计为用户提供查询服务超3.7亿次。

三、云闪付App“一键查卡”

为满足人民群众对于跨行银行卡账户查询的需求，2021年以来，人民银行指导中国银联联合商业银行推出“一键查卡”服务，打造统一查询途径，向公众提供银行卡数量、每张卡的开卡银行名称、借贷记属性、脱敏卡号等信息。

使用方法：

可在官方应用市场下载登录“云闪付”App，在首页顶部的搜索框中输入“一键查卡”进入功能页，申请查询并按提示完成人脸识别和短信验证。申请成功后约24小时内会收到短信通知，届时可打开上述页面查看报告，报告会在3天后自动删除以保护隐私。

云闪付App“一键查卡”，已累计生成超过3000万份查询报告。

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”已覆盖18家全国性银行及459家区域性银行。

四、“803反诈”智能体

2025年12月
上海市公安局率先推出
“803反诈”智能体App

“803反诈”智能体App基本介绍

“803反诈”智能体App是一款集智能问答、反诈辞典、反诈资讯、典型宣防提示于一体的移动端反诈软件，通过深度融合AI大数据模型，以真实案例和生活中常见诈骗场景为基础，打造反诈领域智能助手，为群众提供随时能用的反诈咨询服务。

目前，该App已在各大应用市场全面上架，同步推出微信小程序。

三大功能介绍

功能一

AI大模型智能问答模块

用户提问后，系统将从风险分析、诈骗类型识别、防范建议等多个维度回答，并同步关联“803反诈”相关视频案例，实时为用户提供反诈知识学习和涉诈场景判断服务。

功能二

反诈资讯模块

内嵌“803反诈”新媒体矩阵，定期更新发布反诈动态、高发诈骗类型预警及典型案例手法拆解等内容，以图文+短视频的形式让用户第一时间了解诈骗新动向。

功能三

反诈辞典模块

内嵌《防范电信网络诈骗宣传手册》电子版，用户可以通过分类浏览、关键词检索及语音朗读的形式，系统学习反诈知识。

预警提醒类的利器

五、境外来电提醒服务

为帮助群众第一时间甄别境外来源的电话、短信，工业和信息化部于2025年组织中国电信、中国移动、中国联通、中国广电全面推出“境外来电提醒”服务。当用户接到境外来电或收到境外短信时，手机将同步弹出提醒信息，告知来电、短信来源于境外，让用户自主决定是否接听或查阅，帮助用户提高反诈防范意识。

境外来电提醒服务累计提供跨境电话、短信提醒 **25.23亿次**

六、反诈名片

近年来，各级公安机关及时通过预警电话对正在遭受电信网络诈骗的群众进行预警劝阻，取得了显著成效。

为帮助广大群众轻松识别公安机关预警电话，放心接收防诈预警提醒， 公安部、工业和信息化部联合组织中国电信、中国移动、中国联通、中国广电推出了“反诈名片”服务，对各级公安机关的反诈预警劝阻电话号码进行标记，并在用户接听相关电话时弹出短信提醒，显著提高了公安机关预警劝阻电话接通率。

“反诈名片”助力
预警劝阻电话接通 **6.6亿次**　接通率提升 **32.8%**

“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】

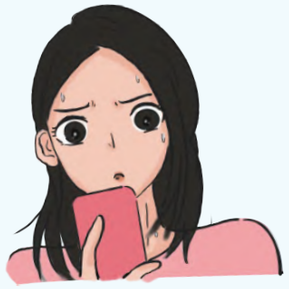
警方提醒

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。

七、12381涉诈预警劝阻短信

为提醒群众注意潜在诈骗风险，工业和信息化部联合公安部于2021年推出了12381涉诈预警劝阻短信公共服务，依托大数据、人工智能等技术及时发现潜在被骗用户，并通过12381短信端口第一时间向用户发送预警短信，提醒用户可能正在遭遇电信网络诈骗。

当用户收到12381涉诈预警劝阻短信时，应提高警惕，不轻信陌生信息、不点击陌生链接、不下载不明软件、不随意转账汇款，如有疑问可拨打110、96110号码进行咨询。



12381涉诈预警劝阻短信累计发送预警信息共17.26亿条。

八、96110预警劝阻专线

96110预警劝阻专线于2019年11月8日正式启用，目前全国31个省区市的公安机关全部开通使用。

预警劝阻专线96110功能介绍

96110是反诈预警劝阻专用号码

专门用于预警劝阻、防骗咨询和涉诈举报。

- **预警劝阻**

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**

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。

九、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是一款官方手机防骗保护软件，集预警提示、线索举报、涉诈App自检、AI内容鉴定、反诈宣传等多种功能于一身，是群众手机里的反诈“防火墙”。

功能介绍

主要功能一 高效预警劝阻提示

当用户收到涉嫌诈骗的电话或短信时，App会进行预警提示。

主要功能二 快速举报涉诈线索

当用户发现诈骗线索时，可以使用App一键举报功能进行举报。

主要功能三 全面了解反诈防骗知识

该App常态化发布防骗知识，拆解诈骗套路，提升用户识骗防骗能力。

主要功能四 涉诈App自检

可以检测目前手机中安装的各类应用程序和安装包，如发现疑似涉诈App和不明安装包，系统会自动提示并建议一键清理删除。

主要功能五 AI内容鉴定

可以检测用户上传的图片、视频、音频或文本是否存在AI生成痕迹，防止不法分子利用伪造内容进行诈骗。

3 《中华人民共和国反电信网络诈骗法》值得关注的3组数字

不听不信不贪恋，构筑反诈“心”防线

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：

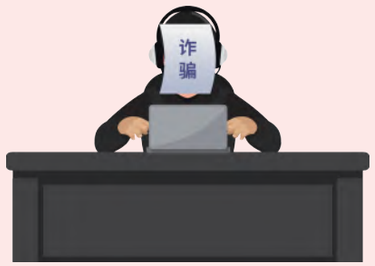
（一）出售、提供个人信息；

（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；

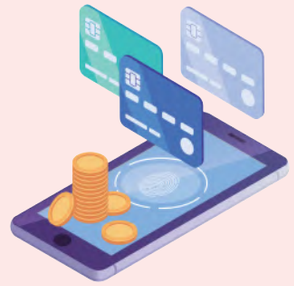
情节严重的，由公安机关并处十五日以下拘留。



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。

4 《电信网络诈骗及其关联违法犯罪联合惩戒办法》的3种惩戒措施及案例

不听不信不贪恋，构筑反诈“心”防线

《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

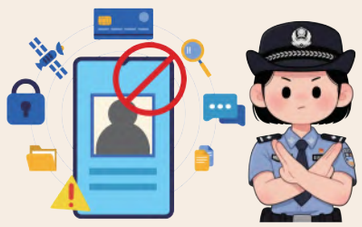
1 对惩戒对象实施金融惩戒

（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》典型案例

案例1 出借银行卡帮助诈骗团伙转移涉诈资金

何某将本人名下的一张银行卡提供给诈骗分子接收涉诈资金49985元，随后帮助诈骗分子提现49700元并从中获利。

经公安机关调查，其在明知收取到的是涉诈资金的情况下，仍帮助取现并送给犯罪团伙成员。何某因帮助信息网络犯罪活动罪被法院判处拘役四个月。

同时，何某被公安机关列为惩戒对象，3年惩戒期内，在金融方面，限制其名下的银行账户、数字人民币钱包的非柜面出金功能，限制其支付账户、实名数字人民币钱包等功能；

在电信网络方面，限制其名下的电话卡、物联网卡、固定电话，以及使用电话卡注册的互联网账号等功能；

在信用方面，被纳入“电信网络诈骗”严重失信主体名单，并在“信用中国”网站向社会公示。

案例2 利用微信、支付宝等帮助诈骗团伙转移涉诈资金

仇某将本人实名认证的微信账户提供给诈骗分子，转移涉诈资金56900元，从中获利4000元；高某将本人实名认证的支付宝账户提供给诈骗分子，转移涉诈资金135842元，从中获利6000元。

仇某、高某被公安机关列为惩戒对象，3年惩戒期内，在金融方面，限制其名下的银行账户、数字人民币钱包的非柜面出金功能，限制其支付账户、实名数字人民币钱包等功能；

在电信网络方面，限制其名下的电话卡、物联网卡、固定电话，以及使用电话卡注册的互联网账号等功能；

在信用方面，被纳入“电信网络诈骗”严重失信主体名单，并在“信用中国”网站向社会公示。

案例3 架设手机口为诈骗分子提供通讯支持

康某伙同侯某在明知诈骗分子正在实施电诈犯罪活动的情况下，仍通过搭建“手机口”的方式为其提供通讯传输，关联全国3起电信网络诈骗案件，两人非法获利共计59338元，构成帮助信息网络犯罪活动罪被法院分别判处有期徒刑十一个月和有期徒刑九个月。

同时，两人被公安机关列为惩戒对象，3年惩戒期内，在金融方面，限制其名下的银行账户、数字人民币钱包的非柜面出金功能，限制其支付账户、实名数字人民币钱包等功能；

在电信网络方面，限制其名下的电话卡、物联网卡、固定电话，以及使用电话卡注册的互联网账号等功能；

在信用方面，被纳入“电信网络诈骗”严重失信主体名单，并在“信用中国”网站向社会公示。

案例4 使用互联网社交App为诈骗团伙引流

陈某、李某、赵某等7人为非法获利，将邵某拉入介绍跨境电商项目的投资理财微信群中，帮助境外诈骗分子与邵某建立联系，最终造成邵某被骗。经查，陈某等7人每组建一个群聊即可获利4至6元，共计获利4万余元。陈某等7人在明知他人实施电信网络诈骗犯罪的情况下仍积极参与，因涉嫌诈骗罪已被公安机关采取刑事强制措施。

同时，上述人员均被公安机关列为惩戒对象，3年惩戒期内，在金融方面，限制其名下的银行账户、数字人民币钱包的非柜面出金功能，限制其支付账户、实名数字人民币钱包等功能；

在电信网络方面，限制其名下的电话卡、物联网卡、固定电话，以及使用电话卡注册的互联网账号等功能；

在信用方面，被纳入“电信网络诈骗”严重失信主体名单，并在“信用中国”网站向社会公示。

案例5 利用自己及家人支付宝账户帮助诈骗团伙实施诈骗

受电信网络诈骗团伙的指使，在2026年4月9日至15日期间，麦某怀伙同弟弟麦某一起使用两人名下的支付宝账户，并借用其父亲和妹妹的支付宝账户，在刷单返利骗局中给予被害人小额返利进而帮助诈骗分子实施犯罪，每天接单400起左右，获利转账的4%，共计获利1400元人民币。麦某怀因向电信网络诈骗活动提供帮助被处以行政拘留5日、罚款1000元的行政处罚。

同时，麦某怀被公安机关列为惩戒对象，2年惩戒期内，在金融方面，限制其名下的银行账户、数字人民币钱包的非柜面出金功能，限制其支付账户、实名数字人民币钱包等功能。

在电信网络方面，限制其名下的电话卡、物联网卡、固定电话，以及使用电话卡注册的互联网账号等功能。

5 常见电诈工具人表现形式及法律后果

不听不信不贪恋，构筑反诈“心”防线

电诈工具人常见形式①

地推式诈骗引流

警惕诈骗新手法　不做电诈工具人

诈骗分子雇佣地推人员，印刷张贴带有二维码的涉黄小广告，引诱受害人下载涉诈App实施诈骗的行为。

电诈工具人常见形式②

短信引流

警惕诈骗新手法　不做电诈工具人

通过传播虚假广告信息链接到微信群、朋友圈等，或是发送诈骗短信给指定电话，帮助诈骗分子引流实施诈骗的行为。

电诈工具人常见形式③

冒充客服电话引流

警惕诈骗新手法　不做电诈工具人

诈骗分子招募兼职“话务员”，要求以固定话术剧本，冒充客服人员拨打指定电话，并将受害者引流给诈骗分子的行为。

电诈工具人常见形式④

搭建手机口

警惕诈骗新手法　不做电诈工具人

同时打开两部手机扬声器，一部手机通过网络软件接通诈骗分子，另一部手机拨打指定电话，帮助诈骗分子完成电话转接的行为。

电诈工具人常见形式⑤

架设GOIP、VOIP等虚拟拨号设备

警惕诈骗新手法　不做电诈工具人

非法购买、使用GOIP、VOIP等虚拟拨号设备，为境外诈骗分子搭设通话转接通道的行为。

电诈工具人常见形式⑥

出租出售出借银行卡、电话卡

警惕诈骗新手法　不做电诈工具人

非法买卖、出租、出借电话卡、银行账户、支付账户和互联网账号等，并以此牟利的行为。

电诈工具人常见形式⑦

购买并寄送黄金

警惕诈骗新手法　不做电诈工具人

诈骗分子为躲避公安机关对涉诈资金的拦截和追查，以各种理由要求“工具人”购买黄金，随后交给指定人员，或将其藏匿在辣椒酱、电饭煲等物品中进行伪装，再邮寄转运的行为。

电诈工具人常见形式⑧

取现寄递

警惕诈骗新手法　不做电诈工具人

帮助诈骗分子取现后，按要求放置到指定地点，或通过跑腿、网约车、快递等方式把现金交付给指定人员的行为。

电诈工具人常见形式⑨

实物洗钱

警惕诈骗新手法　不做电诈工具人

通过购买电脑、手机、手表、烟酒等贵重物品进行大额消费套现，或在实体商户下单购买粮食、货物等大宗商品，以达到洗钱目的的行为。

电诈工具人常见形式⑩

办贷款刷流水

警惕诈骗新手法　不做电诈工具人

诈骗分子以贷款账户需要刷流水包装账户才能放款为由，要求贷款者出借或邮寄银行账户和密码，甚至帮助刷脸辅助验证来转移非法资金的行为。

电诈工具人常见形式⑪

话费、电费、燃气费充值

警惕诈骗新手法　不做电诈工具人

用户通过非官方平台的慢充方式充值话费、电费、燃气费时，诈骗分子会修改充值链接，将充值订单与涉诈充值订单进行替换，从而转移非法资金的行为。

电诈工具人常见形式⑫

跑分

警惕诈骗新手法　不做电诈工具人

使用自己或他人银行账户、第三方支付账户，为诈骗分子提供非法资金转移的“跑分”洗钱行为。

电诈工具人常见形式⑬

POS机套现和对公账户转账

警惕诈骗新手法　不做电诈工具人

诈骗分子以“刷流水、提升信用卡额度”“养卡、代还信用卡赚佣金”的幌子，吸引“工具人”申领POS机并绑定账户，或是声称“高价收购”“轻松获利”，引诱“工具人”办理营业执照并开通对公账户，最终通过POS机虚假交易、利用对公账户转账，将赃款“洗白”的行为。

法律后果

警惕诈骗新手法　不做电诈工具人

上述为电信网络诈骗犯罪活动提供帮助的行为，依据《中华人民共和国刑法》第二百六十六条、第二百八十七条之二、第三百一十二条规定。

构成犯罪的法律后果

涉嫌构成诈骗罪、帮助信息网络犯罪活动罪、掩饰、隐瞒犯罪所得、犯罪所得收益罪，将被依法追究刑事责任。

尚不构成犯罪的法律后果

尚不构成犯罪的，依据《中华人民共和国反电信网络诈骗法》第十四条、第二十五条、第三十一条、第三十八条、第四十四条等规定，由公安机关依法给予行政拘留、没收违法所得、罚款等行政处罚。

亦可依据《电信网络诈骗及其关联违法犯罪联合惩戒办法》，相关违法犯罪人员将被列为惩戒对象，实施金融惩戒、电信网络惩戒、信用惩戒。

公安机关提醒

任何为电信网络诈骗活动提供帮助的“工具人”行为，均是违法犯罪链条的重要环节，公安机关将予以严厉打击。

请广大人民群众增强法律意识，切勿贪图小利，避免沦为“电诈工具人”，以防遭受惩戒甚至牢狱之灾。

6 警惕境外高薪招聘陷阱

不听不信不贪恋　构筑反诈“心”防线

警惕境外高薪招聘陷阱

当前，在公安机关的严厉打击之下，境外电诈团伙出现了“用人荒”，他们瞄准想挣快钱的人群以高薪工作为诱饵，声称到境外打工、带货、当主播就能获得高额报酬“月薪过万”，并谎称可以提供食宿、包办机票签证。

有些人轻信了这些话术，一步步被诱骗出境，一旦出境，将被立即没收护照和手机、限制人身自由，强迫从事电信网络诈骗等违法犯罪活动。“业绩”不达标或试图逃跑者，会遭殴打虐待，甚至被绑架向家属勒索高额赎金。

国家持续加强国际执法合作，境外并非“法外之地”，偷越国（边）境、参与电诈活动均属违法犯罪，将承担相应的法律责任。

求职过程中，对境外高薪招聘应保持高度警惕，有境外务工意向的，一定要确定用工企业资质及招聘真实性、签订劳动合同、办理正规工作签证、查询入境国家对外劳务合作企业名录等，切勿听信招募方的一面之词。

如果身边有人突然要前往境外务工，一定要多加留意、帮助分辨，必要时及时报警求助。

特别是对于涉世未深的未成年人及学生群体，学校和家长要尽到教育监管责任，严防被骗出境、落入险境。

7 反诈最前沿

不听不信不贪恋，构筑反诈“心”防线

反诈最前沿

当前，电信网络诈骗犯罪形势依然复杂严峻，已经成为刑事犯罪中占比最高的类型。电诈危害程度大、打击治理难、群众反应强烈。公安部刑侦局联合中央广播电视总台《法治在线》栏目，重磅推出反诈专题板块《反诈最前沿》，带您直击反诈一线，拆穿最新电诈骗局。

播出时间 央视新闻频道CCTV13周一至周五中午12:35

央视法治在线微信视频号

央视频《反诈最前沿》专栏