

《防范电信网络诈骗宣传手册》

为进一步扩大反诈宣传覆盖面，提高广大群众防骗意识，国家反诈中心制作2023版《防范电信网络诈骗宣传手册》，向广大人民群众介绍了“电信网络诈骗中的十大高发类案”、“防范电信网络诈骗七大反诈利器”及《中华人民共和国反电信网络诈骗法》等重要内容，揭批了诈骗犯罪手法、解析了典型案例、宣贯了法律法规，同时进行了防骗提示。下一步，将以《防范电信网络诈骗宣传手册》为载体，通过新闻宣传报道、新媒体平台、组织线下宣传等方式向全社会开展广泛的反诈防范宣传。

防范电信网络诈骗 · 提高全民反诈意识

国家反诈中心

防范电信网络诈骗宣传手册

2023版

国家反诈中心

牢记八个凡是构建全民反诈新格局

国家反诈中心提醒

凡是要求预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、解冻费或者转账刷流水的，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！

目录

十大高发类案

刷单返利类诈骗 /02

虚假网络投资理财类诈骗 /04

虚假网络贷款类诈骗 /06

冒充电商物流客服类诈骗 /08

冒充公检法类诈骗 /10

虚假征信类诈骗 /12

虚假购物、服务类诈骗 /14

冒充领导、熟人诈骗 /16

网络游戏产品虚假交易类诈骗 /18

婚恋、交友类诈骗 /20

七大反诈利器

国家反诈中心APP /23

96110预警劝阻专线 /26

12381涉诈预警劝阻短信 /28

全国移动电话卡“一证通查” /30

防范电信网络诈骗 · 提高全民反诈意识

防范电信网络诈骗 · 提高全民反诈意识

10大高发类案

防范电信网络诈骗 · 提高全民反诈意识

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。

典型案例

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！

防范电信网络诈骗 · 提高全民反诈意识

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。

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！

防范电信网络诈骗 · 提高全民反诈意识

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”“免费额度提现”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，便添加了对方的企业微信好友，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能满足不放贷，随后便失去联系。樊某发现下载的贷款APP也无法登录，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！

防范电信网络诈骗 · 提高全民反诈意识

冒充电商物流客服类诈骗

易受骗群体 ▶ 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。

第二步：诱导支付

屏幕共享指导操作

声称将受害人升级为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。

典型案例

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账2万元的短信，才意识到上当受骗。

警方提醒

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 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。

防范电信网络诈骗 · 提高全民反诈意识

冒充公检法类诈骗

易受骗群体 ▶ 群众防范意识不强，轻信公检法机关以办案为名实施的诈骗。

作案手法

第一步：冒充公检法工作人员

冒充公检法工作人员，以受害人涉嫌洗钱、银行卡涉案等为由，要求受害人将资金转入所谓的“安全账户”或“核查账户”，以配合调查。

第二步：诱导转账

在电话中不断催促受害人转账，并声称转账后可以退还保证金，否则将追究法律责任。

第三步：实施诈骗

受害人按照指示将资金转入指定账户后，诈骗分子便切断联系，受害人发现被骗时，资金已被转走。

典型案例

王某接到自称是公安局民警的电话，称其身份信息涉嫌被盗用，需要配合调查。王某按照指示将资金转入所谓的“安全账户”，结果被骗走2万元。

警方提醒

公检法机关不会通过电话办案，更不会要求转账。

切记 凡是自称公检法工作人员，要求转账的都是诈骗！

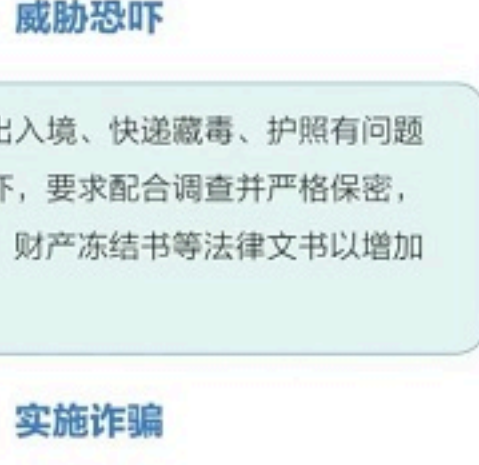
冒充公检法类诈骗

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

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、传递毒品、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，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，称杨某名下有一个银行账户涉嫌非法洗钱，让其到上海某公安局处理。杨某称去不了，对方让其添加QQ好友并发送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



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

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！

- 10 -

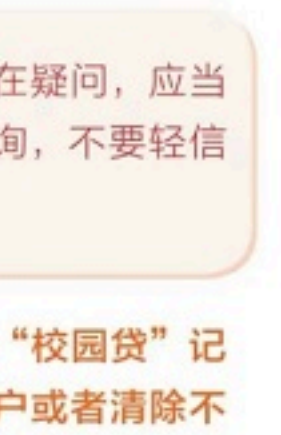
虚假征信类诈骗

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。



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，否则将严重影响个人征信。

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流水的，都是诈骗！

- 12 -

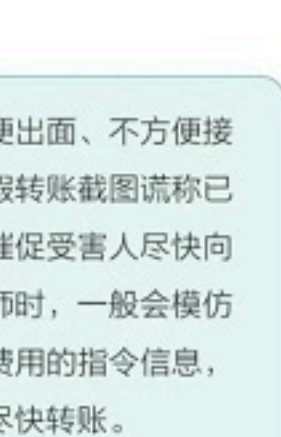
虚假购物、服务类诈骗

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折扣、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、交易费、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！

- 13 -

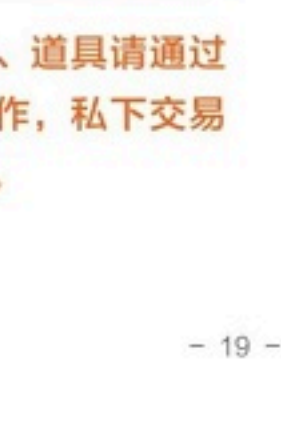
冒充领导、熟人类诈骗

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

诈骗分子使用受害人领导、熟人或子女老师的照片、姓名包装社交账号，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

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经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，李某进群后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”要求李某支付对方工程款，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！

- 14 -

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、道具请通过正规网络平台操作，私下交易均存在被骗风险。

- 15 -

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。

典型案例

谢女士在网络上结识了一名“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！

- 21 -

严密防范电信网络诈骗违法犯罪活动

全民反诈在行动

7大反诈利器

防范电信网络诈骗，提高全民反诈意识

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是一款官方手机防骗保护软件

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。

国家反诈中心APP您下载了吗？

下载国家反诈中心APP要进行实名认证，打开预警功能。

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



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。



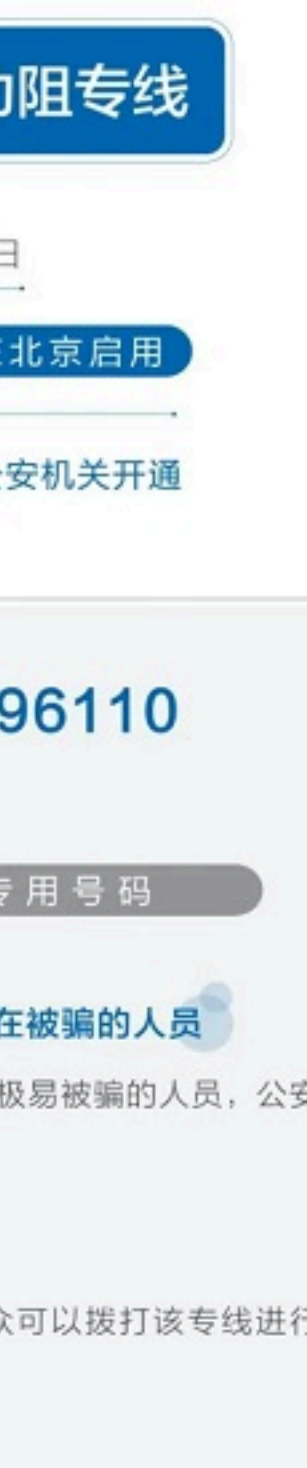
主要功能二：涉诈线索一键举报。

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。



7 全民反诈在行动 大反诈利器

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 29 个省区市的公安机关开通

96110 预警劝阻专线 96110 功能介绍

96110 是反诈预警劝阻专用号码

紧急劝阻预警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

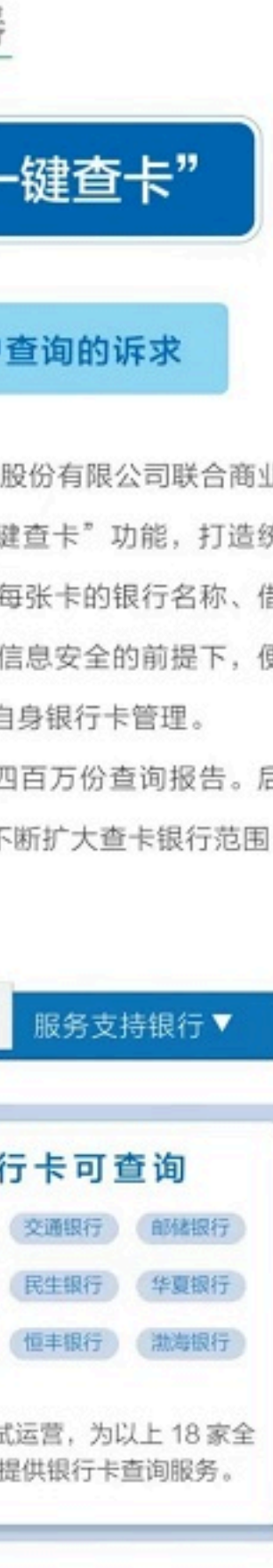
如果发现涉诈线索，群众可以通过该专线进行举报。

这个电话一定要接

1 警方提醒

全民反诈在行动

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。



7 全民反诈在行动 大反诈利器

3 12381 涉诈预警劝阻短信

2021年7月14日

工信部联合公安部推出 12381 涉诈预警劝阻短信系统

第一时间向潜在被骗用户发送预警提示

涉诈预警劝阻短信 12381 功能介绍

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。

1 警方提醒

如果收到来自 12381 的预警短信，说明很可能遭遇了电信网络诈骗。

这个短信一定要看

预警发现实时化
预警对象精准化
短信预警自动化
预警范围全国化
亲情联防联控
闪信霸屏预警



7 全民反诈在行动 大反诈利器

4 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。

“一证通查”服务打通了 93 家省级基础电信企业和 39 家移动通信转售企业相关数据，群众只需要使用自己的居民身份证，即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，专用短信端口 10699000 将在 48 小时内向预留手机号反馈结果，真正实现了全国移动电话卡的统一便捷查询。

工信部推出的全国移动电话卡“一证通查”服务
截至 2022 年 10 月底数据统计

1 处置涉诈高风险电话卡 亿张
1 接收用户查询量 亿人次

9000 关联互联网账号 万个

防范诈骗 · 保护你我

全国移动电话卡“一证通查”服务
查询方式
严密防范电信网络诈骗违法犯罪活动

一键查询

核验身份证信息后，便捷查询名下所有移动电话卡数量

全国范围
基础电信企业
移动转售企业

短信告知

48 小时内专用短信端口（10699000）反馈查询结果

绿色通道

提供本企业号码清单查询、关停、异地注销等便捷服务

企业营业厅
1. 基础电信企业、移动通信企业网上营业厅。
2. 基础电信企业线下自有营业厅。

国家政务服务平台
1. 添加微信小程序“国家政务服务平台”
2. 点击“一证通查”。

工信微报
扫描或者微信搜索公众号“工信微报”

工信部反诈专班
1. 扫描或者微信搜索公众号“工信部反诈专班”
2. 通过网页、微信 https://getsinnum.caict.ac.cn

CAICT 中国信通院 中国电信 China Telecom 中国移动 China Mobile 中国联通 China Unicom

7 全民反诈在行动 大反诈利器

5 云闪付 APP “一键查卡”

解决群众对于跨行银行卡账户查询的诉求

2021 年 12 月，人民银行指导中国银行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 2022 年 11 月，已累计生成超过四百万份查询报告。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 100 余家区域性银行提供银行卡查询服务。

云闪付 APP “一键查卡”功能操作流程

1. 下载登陆云闪付 APP，APP 内搜索“一键查卡”。

2. 选择查询银行核验本人身份

“一键查卡”功能试点、试用阶段，暂仅向身份证实名认证用户开放。其他证件实名认证用户进入后将有弹窗提示。

3. 生成查询报告短信通知

在用户授权及验证通过后，云闪付向各商业银行发起查询请求，同时在申请成功页面中告知用户在 24 小时内会生成报告，并提示用户注意短信通知。

4. 验证支付密码查询报告内容

用户在云闪付 APP 内点击“查看报告”，输入 APP 支付密码，验证通过后方可浏览报告内容。

1、报告内容根据银行反馈数据生成，卡片状态异常、证件过期等特殊情况下暂不支持查询。

2、请勿向他人透露“一键查卡”服务验证码，7 个自然日后系统将自动删除报告。

7 全民反诈在行动 大反诈利器

6 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，常被误认为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，严重影响了预警劝阻工作的预期效果。

“反诈名片”的作用

手机用户在接听国家反诈部门的预警劝阻电话时，同步弹窗显示国家反诈中心、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的发生。

“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！

1 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。

7 全民反诈在行动 大反诈利器

7 全国互联网账号“一证通查 2.0”

为防范用户不知情注册互联网账号等带来的涉诈风险，切实为群众排忧解难，工信部推出全国互联网账号“一证通查 2.0”服务，用户凭借手机号码和身份证号码后六位，便可查询本人名下手机号码关联的互联网账号数量。

有异议怎么办

当用户查询到本人手机号码关联的互联网账号数量与个人掌握的情况不一致时，可按照下列步骤解决：点击查询页面下方的“解绑与明细查询”，了解企业的明细查询和解绑处理机制。

警方提醒

您名下的手机号关联了多少互联网账号？赶快查一查！千万不要让您的互联网账号成为诈骗分子的犯罪工具。

全国互联网账号“一证通查 2.0”查询方式
严密防范电信网络诈骗违法犯罪活动

一键查询

核验身份证信息后，查询名下手机号关联互联网账号数量

全国范围
基础电信企业
移动转售企业
互联网应用

短信告知

48 小时内专用短信端口（10699000）反馈查询结果

可通过扫描下方二维码查询互联网账号

工信微报 工信部反诈专班

中国信息通信研究院 支付宝小程序

目前支持查询的互联网企业及应用

支付宝 淘宝网 拼多多 钉钉 微信 QQ 抖音 Bilibili 京东 美团 快手 敬请期待

全面准确实施 《反电信网络诈骗法》

查询方式

严密防范电信网络诈骗违法犯罪活动

一键查询

核验身份信息后，查询名下手机号关联互联网账号数量

互联网应用

短信告知

48小时内专用短信端口
(10699000) 反馈查询结果



可通过扫描下方二维码查询互联网账号

工信微报

工信部反诈专班

中国信息通信研究院



目前支持查询的互联网企业及应用

支付宝

淘宝网

拼多多

钉钉

微信

QQ

抖音

Bilibili

京东

美团

快手

敬请期待

- 37 -

全面准确实施
《反电信网络诈骗法》
坚决打击电信网络诈骗违法犯罪活动

2022年9月2日十三届全国人大常委会第三十六次会议表决通过
自2022年12月1日起施行



《反电信网络诈骗法》是什么？



2022年12月1日，《中华人民共和国反电信网络诈骗法》正式施行，这是我国第一部专门、系统、完备规范反电信网络诈骗工作的法律，是党中央部署打击治理电信网络诈骗工作的标志性成果，是中国特色反电信网络诈骗犯罪制度的成功探索和具体实践。

《中华人民共和国反电信网络诈骗法》
共七章50条

第一章
总则

第二章
电信治理

第三章
金融治理

第四章
互联网治理

第五章
综合措施

第六章
法律责任

第七章
附则

《中华人民共和国反电信网络诈骗法》旨在预防、遏制和惩治电信网络诈骗活动，加强反电信网络诈骗工作，保护公民和组织的合法权益，维护社会稳定和国家安全，根据宪法，制定本法。

- 39 -

《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、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。

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；没有违法所得或者违法所得一万元以上的，处一万元以上十万元以下罚款。

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，情节严重的，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，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、虚拟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，情节严重的，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，可以由有关主管部门责令暂停新增业务、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，情节严重的，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，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，情节严重的，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，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。

六个月内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。

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

