

附件：

2023 年国家反诈中心《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。

防范电信网络诈骗 · 提高全民反诈意识



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 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！

目录

防
范
电
信
网
络
诈
骗
·
提
高
全
民
反
诈
意
识

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、熟人类诈骗	/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

严密防范电信网络诈骗违法犯罪活动

10大高发 类案



防范电信网络诈骗 · 提高全民反诈意识



~~骗~~

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，便添加了对方企业微信好友，并下载一款名为“京東金融”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！

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。

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。



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



◎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 ▶ ◎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，称杨某名下有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



◎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！

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。

原价 5500 元
三折即可入手



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 ▶ ◎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！

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。

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！

《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。

严密防范电信网络诈骗违法犯罪活动

《反电信网络诈骗法》

值得关注的 **3** 组数字

你我同心·反诈同行

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。



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。

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
企鹅号



国家反诈中心
强国号