# 2026大学生防范电信网络诈骗安全手册

— 严防电信网络诈骗　拒触“帮信”犯罪红线 —



当前，电信网络诈骗犯罪手段持续翻新，诈骗分子捕捉AI换脸等新技术，不断迭代作案方式，防范难度日益加大。学生群体求知欲旺盛、学习能力强，对新鲜事物充满探索热情，然而由于社会阅历有限、风险辨别能力不足，往往容易被诈骗分子利用和蒙蔽。与此同时，诈骗分子以“高薪兼职”“勤工俭学”等为诱饵，引诱学生出租、出售电话卡和银行卡，或参与非法引流、跑分洗钱等活动，致其在不知不觉中沦为电诈“工具人”，甚至触犯“帮助信息网络犯罪活动罪”，面临刑事处罚和联合惩戒的严重后果。

本手册结合学生真实案例，围绕常见骗术手法、法律惩戒措施、实用防范工具及境外务工陷阱等内容，以案释法、以法示警。希望广大同学认真阅读，以案为鉴，切实提升识骗防骗能力，坚决不参与任何涉诈违法犯罪活动，守好自己的“钱袋子”和人身安全，共同营造清朗无诈的校园环境。

# 目录 CONTENTS

目录 CONTENTS

## 01 十大高发类案


1、刷单返利类诈骗 01
2、虚假购物、服务类诈骗 02
3、网络游戏类诈骗 03
4、冒充电商物流客服类诈骗 04
5、冒充熟人类诈骗 05
6、冒充公检法类诈骗 06
7、机票“退改签”类诈骗 07
8、网络交友类诈骗 08
9、网络贷款类诈骗 09
10、助学金、奖学金诈骗 10


## 02 常见电诈工具人表现形式及法律后果


1、地推式诈骗引流 11
2、短信引流 12
3、冒充客服电话引流 12
4、搭建手机口 13
5、架设GOIP、VOIP等虚拟拨号设备 13
6、出租出售出借银行卡、电话卡 14
7、购买并寄送黄金 14
8、取现寄递 15
9、实物洗钱 15
10、办贷款刷流水 16
11、话费、电费、燃气费充值 16
12、跑分 17
13、POS机套现和对公账户转账 17
14、法律后果 18


## 03 《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 19
2、电信网络惩戒 19
3、信用惩戒 20
4、典型案例 20


## 04 反诈利器全家桶


1、 12381涉诈预警劝阻短信 22
2、 96110预警劝阻专线 23
3、 国家反诈中心App 23


## 05 警惕境外高薪招聘陷阱


警惕境外高薪招聘陷阱 24

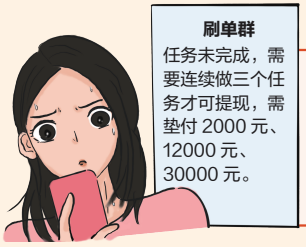
# 01 十大高发类案

## 一、刷单返利类诈骗

### 手段解析

诈骗分子会通过各种网络平台发布兼职广告，打着“足不出户、高额佣金”的旗号，或是以色情内容、免费礼物为诱饵拉人建群。




等受害者入群后，会让他们完成刷单、关注点赞等任务，并发放小额佣金，获取受害者信任。

随后他们会以“充值越多、返利越多”为由引诱受害者加大资金投入，或以“任务未完成、操作异常”等借口拒不返还资金，直至受害人发觉被骗。

**【典型案例】**大学生曹某被人拉入一微信群，发现群内有人发红包就抢了几个红包。随后，群里有人发链接诱导其下载APP，声称进入高级群可获取更大收益。加入所谓高级群后，曹某发现群内成员都在发收款到账截图，便在群管理员诱导下开始刷单。曹某连续做完多单任务领取佣金后，全部提现至银行卡中，正当其想继续做任务赚钱时，群管理员称其将做的任务是组合单，必须完成4单才能提现。曹某按照要求陆续加大投入后，群管理员以“操作失误”“账号被冻结”等为借口，诱骗其向指定账户累计转账42万元。因返现迟迟不到账，曹某遂发现被骗。

### 警方提醒



“刷单、刷信誉”本身就是违法行为，并非正当兼职。不要被蝇头小利诱惑，所有刷单（或披着做任务的“外衣”，实则还是刷单、刷信誉行为）都是诈骗！

# 二、虚假购物、服务类诈骗

## 手段解析

诈骗分子通过微信群、朋友圈、网购平台、短视频平台或其他网站发布低价打折、海外代购、0元购物等虚假广告，以及提供代写论文、私家侦探、跟踪定位等特殊服务广告。







在与受害人取得联系后，诈骗分子便诱导其通过微信、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为由，要求私下转账。

受害人付款后，诈骗分子再以缴纳关税、定金、交易税、手续费等为由，诱骗其继续转账汇款，最后将其拉黑。

**【典型案例】**学生林某被陌生网友拉入QQ群，诈骗分子称参加拼单购物能获得特大优惠，拼单不成功会退款。随后，林某拼单没有成功，诈骗分子就让林某下载了一款软件进行退款，并以林某的支付宝曾被冻结有风险为由，让林某从其母亲账号转钱到指定账户，并告知林某指定账户收到款后会全额退款。林某信以为真，导致被骗数万元。

## 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。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。

# 三、网络游戏类诈骗

## 手段解析

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，以及免费、低价获取游戏道具、参加抽奖活动等相关信息。





与受害人取得联系后，诈骗分子以私下交易更便宜、更方便为由，诱导其绕过正规平台进行私下交易，或诱骗受害人参加抽奖活动。

再以操作失误、等级不够等理由，要求其支付“注册费”“解冻费”“会员费”，得手后便将受害人拉黑。



**【典型案例】**学生王某拥有某游戏的账号，有诈骗分子添加其QQ询问是否愿意卖出该游戏账号，诈骗分子的报价超出王某的预期，王某当即表示同意。于是，诈骗分子通过QQ发给王某一陌生网址，要求其在该网站平台进行交易。随后诈骗分子以王某操作失误导致账号被冻结为由，要求王某向私人账户转账以解冻资金。王某信以为真，被诈骗2000元。

## 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。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。

# 四、冒充电商物流客服类诈骗

## 手段解析

诈骗分子通过非法途径获取受害人购物信息后，冒充电商平台或物流快递客服，谎称受害人网购商品出现质量问题、快递丢失需要理赔或因商品违规被下架需重新激活店铺等。







诱导受害人提供银行卡和手机验证码等信息，并通过共享屏幕或下载APP等方式逃避正规平台监管，从而诱骗受害人转账汇款。

**【典型案例】**学生杜某接到自称某网店客服的电话，称杜某前几日购买的物品有质量问题，现需向杜某进行退款理赔。杜某信以为真，在诈骗分子诱导下下载了一款APP，通过该APP打开手机屏幕共享功能并按照指示进行操作。随后，杜某收到银行卡被转款2万元的短信才发现被骗。

## 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。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。

# 五、冒充熟人类诈骗

## 手段解析

诈骗分子利用受害人熟人的照片、姓名包装社交账号，通过添加受害人为好友或将其拉入微信聊天群等方式，对其嘘寒问暖表示关心，或模仿老师、亲友等语气发出指令，从而骗取受害人信任，再以有事不方便出面、接电话为由，谎称已先将某款项转至受害人账户，要求其代为向他人转账。







为蒙骗受害人，诈骗分子还会发送伪造的转账成功截图，但实际上其未进行任何转账操作。随后，诈骗分子以时间紧迫等借口不断催促受害人尽快向指定账户转账，从而骗取钱财。

**【典型案例】**学生小李收到微博私信，对方和小李朋友用了完全一样的头像和风格相仿的昵称，小李以为是朋友的小号没再多问。对方称在亚马逊平台买了个包，但现在手机坏了没法结清尾款，若不及时支付则会取消订单，想让小李帮忙先垫付，同时对方发来支付宝转账截图称已经先给同学转账了，但因为银行问题到账会有延迟。随后小李通过对方提供的网页链接联系到平台的客服，客服称订单付款即将到期，要小李立刻转账。小李付款后给朋友打电话谈论这件事时发现被骗，损失6000元。

## 警方提醒



如遇到自称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！凡是接到自称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！

# 六、冒充公检法类诈骗

## 手段解析

诈骗分子冒充公检法机关、政府部门等工作人员，通过电话、微信、QQ等与受害人取得联系。




以受害人涉嫌洗钱、非法出入境、快递藏毒、护照有问题等为由进行威胁、恐吓，要求配合调查并严格保密，同时向受害人出示逮捕证、通缉令、财产冻结书等虚假法律文书，以增加可信度。



为阻断受害人与外界联系，诈骗分子通常要求其到宾馆等封闭空间配合工作，诱骗其将所有资金转移至所谓“安全账户”，从而实施诈骗。

**【典型案例】**大三学生小王接到一个自称是公安局民警的电话，对方准确说出了他的姓名、身份证号等信息，称他涉嫌参与一起重大洗钱案件，要求他将名下所有资金转到“安全账户”进行调查，否则将对他采取强制措施。小王被吓得不知所措，在对方的诱导下，分几次将自己的学费和生活费共计2万余元转到了指定账户，事后才发现被骗。

## 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。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！

# 七、机票“退改签”类诈骗

## 手段解析

诈骗分子假冒航空公司客服，发送退改签通知，引导受害者加QQ等即时聊天工具，私下通联，并通过诈骗链接让受害者填写银行卡号、密码、验证码等信息，非法获取受害者信息后，盗刷银行卡。




**【典型案例】**大学生孙某购买机票计划返校，随后收到一条短信称其预订航班因机械故障取消，可按信息内提供的方式联系客服办理退改签并补偿300元。孙某联系所谓客服后，按对方要求加了QQ好友。“客服”发送诈骗链接让孙某填写银行卡信息及验证码用于退款，孙某操作后，卡内2800元被盗转，再联系时已被拉黑。

## 警方提醒



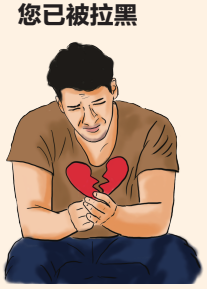
核实真伪第一时间通过所属航空公司官方购票程序或电话、网站进行确认。警惕链接不点击任何非官方链接，尤其是下载即时聊天软件、会议类软件的链接。拒绝透露提及个人隐私、银行卡信息的要提高警惕，切勿开启“屏幕共享”功能，谨防透露个人信息。

# 八、网络交友类诈骗

## 手段解析



诈骗分子通过在交友网站上打造优秀人设，与受害人建立联系，用照片和预先设计好的虚假身份骗取受害人信任，长期经营与其建立的恋爱关系




随后以遭遇变故急需用钱、项目资金周转困难等为由向受害人索要钱财



并根据其财力情况不断变换理由提出转账要求，直至受害人发觉被骗

**【典型案例】**某大学生小傅，1月中旬在网上结交了一名游戏主播，陪聊陪玩之后，双方很快发展成恋人关系，之后主播提出的任何要求小傅都尽量满足，从1月中旬起至2月底，小傅总共向主播刷礼物转账了30多万元。可令小傅万万没想到的是，自己那娇俏可人的“女神”，身份、照片居然都是假的。

## 警方提醒



网络交友需谨慎，虚拟世界难辨真。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！

# 九、网络贷款类诈骗

## 手段解析

诈骗分子通过网站、电话、短信、社交平台等渠道发布“低息贷款”“快速到账”等信息，诱骗受害人前往咨询。







甚至冒充银行、金融公司工作人员联系受害人，谎称可以“无抵押”“免征信”“快速放贷”等，引诱受害人下载虚假贷款APP或登录虚假网站，再以收取“手续费”“保证金”“代办费”等为由，诱骗受害人转账汇款。

诈骗分子还常以“刷流水验资”为由，诱骗受害人将其银行卡寄出，用于转移涉案资金。



**【典型案例】**樊某接到自称某金融客服来电，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，并根据对方发送的链接下载了一款名为“XX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也已无法登陆，才觉察被骗。

## 警方提醒

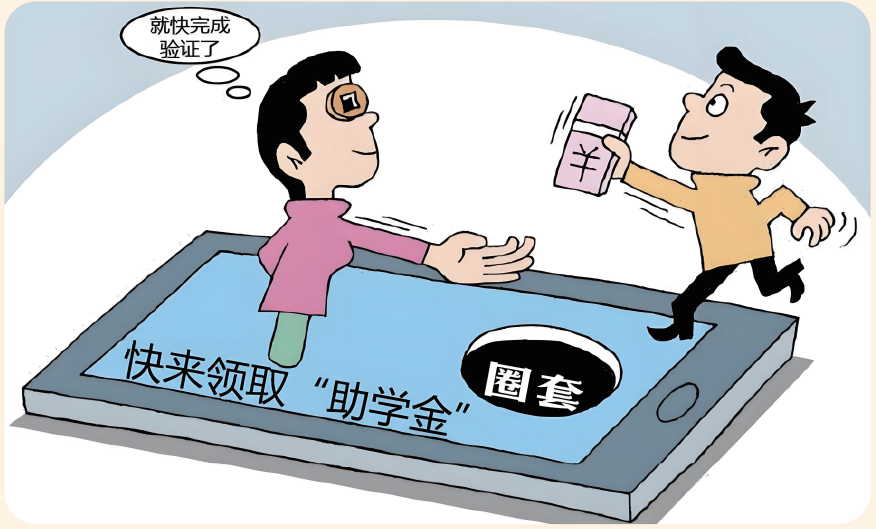


如有贷款需求，建议通过正规渠道办理。正规机构在放款前不会收取任何费用！不要轻信网络贷款广告，凡是要求在放款前先交会员费、保证金等费用或要求转账刷流水的都是诈骗！

# 十、助学金、奖学金诈骗

## 手段解析

诈骗分子冒充学校、教育部门工作人员，以“发放助学金”“学费减免”等为由，要求受害人提供银行卡信息或支付“手续费”“激活费”，最后制造紧迫感，谎称“名额有限”“逾期作废”，利用受害人紧张心理，逼迫其快速操作。




**【典型案例】**张同学是一名大二学生，平时学习刻苦，成绩优异。某日他收到一封自称来自“学校教务处”的电子邮件，邮件中称因其上学期表现突出，将获得一笔3000元的奖学金。邮件附有一个链接，要求张同学点击后填写个人信息和银行账户以便发放奖学金。张同学信以为真，立即点击链接，并按要求填写了相关信息。不久后，他收到了一条来自“银行”的短信，提示其账户已入账3000元，但需先支付100元的手续费才能解锁使用。张同学没多想，便按照短信提示向指定账户转账了100元。然而，当他再次查看银行账户时，却发现那笔所谓的奖学金并未到账，反而自己卡内余额被转走了3000元，这才发现自己被骗。

## 警方提醒



遇到涉及“奖金发放”“退费补贴”等信息，务必通过正规渠道进行核实，如工作单位、社区服务窗口、学校老师等，而不是轻信群消息。不点击、不转账、不透露验证码！

# 2 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。**



# 3 《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。

# 《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



## 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。



# 4 反诈利器全家桶

不听不信不贪恋，构筑反诈“心”防线



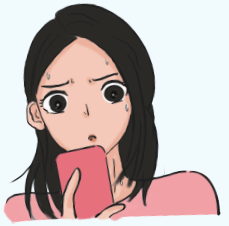



## 一、12381涉诈预警劝阻短信

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。**



## 二、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。




## 三、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。

# 5 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。**



# 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