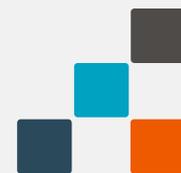


昆明三中呈贡学校（呈贡一中）

# 岁末年初防范非法金融活动宣传教育专题会

## 防范电信网络诈骗，守护幸福生活

2026年1月6日



# 昆明市教育体育局

## 转发上级部门关于做好岁末年初防范 非法金融活动宣传教育工作的通知

各县（市）区教育体育局，滇中新区、经开区、阳宗海、磨憨-磨丁合作区管委会社会事务（事业）局，各市属高校、直属学校（幼儿园）：

岁末年初是非法金融活动高发易发期，为切实筑牢教育体育系统防范非法金融活动安全防线，保护广大学生、家长及教职工合法权益，营造安全稳定的节日环境，现将《云南省防范和打击非法金融活动工作领导小组办公室关于做好岁末年初防范非法金融活动宣传教育工作的函》转发给你们，请结合本地区、本单位实际，认真贯彻落实，重点做好以下工作：

**一、提高思想认识，强化组织部署。**各单位要充分认识防范非法金融活动的重要性和紧迫性，加强组织领导，确保宣传工作有序有效开展。

**二、聚焦宣传重点，提升教育实效。**结合教育体育系统特点，通过校园广播、宣传栏、LED屏、微信公众号、主题班会等多种形式，普及非法金融活动识别方法、防范技巧和法律后果，引导广大师生及家长增强风险防范意识和自我保护能力。



1

什么是电信诈骗？

2

电信诈骗的常见形式

3

打击“两卡”犯罪，  
莫当电诈“工具人”

4

如何识别防范电信诈骗

Part

1

# 什么是电信诈骗

# 什么是电信诈骗？



手机  
短信

电话

网络  
电话

互联  
网

电信诈骗是指以非法占有为目的，利用手机短信、电话、网络电话、互联网等传播媒介，以虚构事实或隐瞒事实真相的方法，骗取数额较大的公私财物的行为（又称非接触性诈骗或远程诈骗）。

# 电信诈骗识别公式



人物：不能准确确认其身份+沟通工具：电话、短信、网络等+要求：汇款、转账

**如果遇到上述情况，请及时报警！**

# 电信诈骗的特点

1

## 诈骗手段日新月异，造成巨大损失

诈骗团伙有专门的研发团队，专门研究新的诈骗套路，诈骗手段日新月异。短短几年时间，电信诈骗已经发展出上百种诈骗套路。电信诈骗给群众造成巨大损失，占全部刑事案件半数左右，单起案件损失动辄数十、上百万。最大一起诈骗案损失2.5亿港元。

2

## 诈骗分子躲藏在境外，形式集团化

诈骗团伙为了逃避打击，大多躲藏在境外，并且形成集团化、职业化、产业化的特征，分工很细，各司其职。

3

## 破案难度大，追赃挽损困难

中国警察在国外没有执法权，必须依赖国际警务协作，不像国内这么顺畅。诈骗资金被迅速分散洗白，很难追查，大多数被骗损失无法挽回。

4

## 具有可防性的特征

电信诈骗利用了人们对网络、金融、法律等方面的认知差，补齐这方面的知识，提前了解诈骗的套路，可以有效预防被骗。



# 对电信诈骗的认知误区

反诈宣传铺天盖地，仍有很多人被骗，很多受害者甚至接受过反诈宣传。面对电信诈骗，不少群众存在一些认知误区，导致他们容易上当受骗：

1

**认为没钱就不会被骗：**真实案例证实，很多被骗的人都被诱导贷了网贷，或者向亲友借了钱。没钱不是不会被骗的理由。

2

**认为不贪就不会被骗：**除了贪婪，恐惧、对损失的厌恶也是诈骗分子常利用的人性心理漏洞。比如冒充公检法诈骗、冒充抖音客服诈骗、“百万保障”诈骗等

3

**认为不傻就不会被骗：**诈骗分子掌握了受害者个人信息，利用AI技术，定制诈骗脚本，理论上没有不会被骗的人。教授、博士、硕士、反诈专家、银行职工都有被骗的案例。



Part 2

# 电信诈骗的常见形式

# 骗术1：刷单返利诈骗

## 刷单就是诈骗



亲，您的双重任务已申请，本次任务为3单，每单佣金是7%（累计形式）任务将由系统随机安排，如果无异议我们将为您提交系统申请刷单！

好的。

没有异议，可以开始刷单

正式任务单 编号【JZ\_986853】按提示操作【一任务一结算】

任务完成3-5分钟后返款到您的淘宝账户

第一步：打开链接

第二步：购买数量6件，佣金201.6元

第三步：点立即购买

第四步：提交订单（物品信息请确认一下，以免出错）

第五步：其他信息自由选择

点击进入：[http://item.taobao.com/oiva\\_mhbjylmnb3usb9kuwqeo9u=123kjhdsiuqwb.html](http://item.taobao.com/oiva_mhbjylmnb3usb9kuwqeo9u=123kjhdsiuqwb.html)

任务已发布，请按照要求完成，哪里不懂请立即咨询

发布刷单信息

第一单返利

继续刷大单后拉黑

# 特别注意：公职人员在上班期间出现刷单情况，属于违纪行为！！！！

通过QQ群、微信群、微信朋友圈、微博、二手交易平台等发布刷单信息。

一开始刷第一单会返还一点小利，比如五块钱或者十块钱。

诱导你继续刷大单，必须做完连续任务才会返钱，以此为理由不返还本金及佣金，到最后直接把你拉黑。

接待员02号

现在有

- 1.垫付100元做完返130元以上(含本金)
- 2.垫付350元做完返400元以上(含本金)
- 3.垫付500元做完返650元以上(含本金)
- 4.垫付1000元做完返1300元以上(含本金)

接待员02号

选择一个你需要垫付的金额，然后告诉我开始任务。

## 骗术2：冒充公检法诈骗



### 案例写真

电信诈骗中，犯罪分子常用的手法就是冒充公检法机关“怀疑你涉嫌洗黑钱”“发送了诈骗短信”等为由，通过发送伪造的“通缉令”“逮捕证”，甚至穿上警服和你视频，让你深信不疑，陷入恐慌，从而言听计从，配合调查自证清白。随后以调查你的银行账户为由，让你把银行卡里的钱转到公安机关的“安全账户”，或者交给上门取现的工作人员。

2015年12月，贵州省都匀市经开区一名出纳被人以“冒充公检法”诈骗，配合进行“资金清查”，插入单位资金U盾，被转走1.17亿。2020年底，香港一名90多岁的富婆，遭遇冒充公检法诈骗，5个月内被骗2.5亿港币（折合人民币2.34亿元）。

给您来电1次，请方便时回复。【中国移动 和留言】



上海公安局  
嘉定分局  
刑侦队  
警员：陈■■■■  
编号：031220  
公务机：13520986234北京号

看到回拨  
北京党中央  
派发的公务手机  
陈警官

# 骗术3：“杀猪盘”诈骗



## 案例写真

诈骗分子冒充高富帅、白富美或者军人、白领身份，主动与受害者搭讪，嘘寒问暖迅速建立恋爱关系，然后让对方帮助其管理投资账户，以掌握内幕消息、平台漏洞可以赚大钱吸引受害者，怂恿受害者投资赚钱。并且还会利用PUA的手段，逼迫受害者网贷、借钱投资，最后还会利用受害者的银行卡“洗钱”。

2024年7月，杭州单身女性宋某在小红书上结识主动搭讪的王某。王某自称为部队现役军官，双方发展为恋人关系后王某称有稳赚不赔的内部投资平台，因工作原因让宋某代为操作平台账户。宋某发现盈利可观，在王某的怂恿下也注册账号投资。宋某首次充值投资50万便小有盈利，王某称购买黄金，由工作人员上门收取可获得更高返利，宋某多次购买价值人民币1850多万元的黄金，交给上门收取的陌生男子。8月2日，宋某因无法提现才发现被骗，共计损失1900多万元。

网络交友需谨慎。凡是主动提及掌握某网站系统漏洞、了解内幕消息，诱导你进行投资理财或网络赌博的都是诈骗。



P的军装照



骗子盗图

### 骗子冒充军人诈骗

# 骗术4：虚假投资理财诈骗



## 案例写真

叶某在刷手机视频时被一条投资理财广告吸引，其按照广告内容关注微信公众号学习炒股经验，并下载了一款投资APP。在“客服”引导下，叶某尝试在该平台进行投资，发现确有盈利。看着平台账户里不断增长的资金，叶某决定加大投资金额，连续转账13笔共计240万元。多次无法提现，叶某意识到被骗。

诈骗分子在网上发布投资理财的信息，寻找受害人群体，通过分享“投资经验”取得受害人的初步信任，然后以“高回报”“高盈利”等为诱饵，诱骗受害人在虚假投资平台进行投资。在受害人尝到甜头后，再诱骗受害人加大“投资”金额。当受害人提现受阻时，诈骗分子以继续投入大额资金，方可提取已投入本金为由，继续诱骗受害人转账，直至受害人意识到被骗。

不要轻信“高回报”“高盈利”等聊天内容，切记天上不会掉馅饼。



# 骗术5：冒充客服诈骗



## 案例写真

2月24日，四川乐山刘女士接到一陌生电话，对方自称是抖音“客服”，告知其开通了“抖音直播付费”功能，每月将自动扣除800元的手续费，如不需要该服务，可以指导其操作“取消”。为不被“自动扣费”，刘女士点击对方发送的链接，下载了一款名为“银联会议”的APP，同时打开了屏幕共享功能。在对方的诱导下，刘女士多次刷脸付款，先后向四个账号转账共计76万元。

**常见的冒充客服诈骗有：**1.冒充抖音客服称开通了某项服务要扣费；2.冒充微信、支付宝、拼多多或保险公司客服称开通了“百万保障”要扣费；3.冒充电商、快递公司客服称商品问题、损坏要赔偿；4.冒充航空公司客服称飞机延误要退改签并赔偿。诱导下载“银联会议”“抖音会议”“银办通”等涉诈软件，通过屏幕共享，远程控制、操作受害者手机，诱骗受害者转账或者获取受害者的银行卡密码、验证码等进行盗刷。



## 骗术6：冒充熟人诈骗（AI诈骗）



### 案例写真

2023年4月20日，福州某科技公司老板郭先生突然接到好友的微信视频电话，称自己的朋友在外地竞标，需要430万保证金，且需要公对公账户过账，想要借郭先生公司的账户走账。郭先生没有核实钱款是否到账，就把430万转到了好友朋友的银行卡上。事后，郭先生拨打好友电话才知道被骗。

冒充熟人诈骗的种类多样，骗子通常会冒充领导、老板、班主任、同学、闺蜜、在外读书的子女、孙子、孙女婿等进行诈骗。对于熟人来电涉及到钱的事项一定要多方核实。



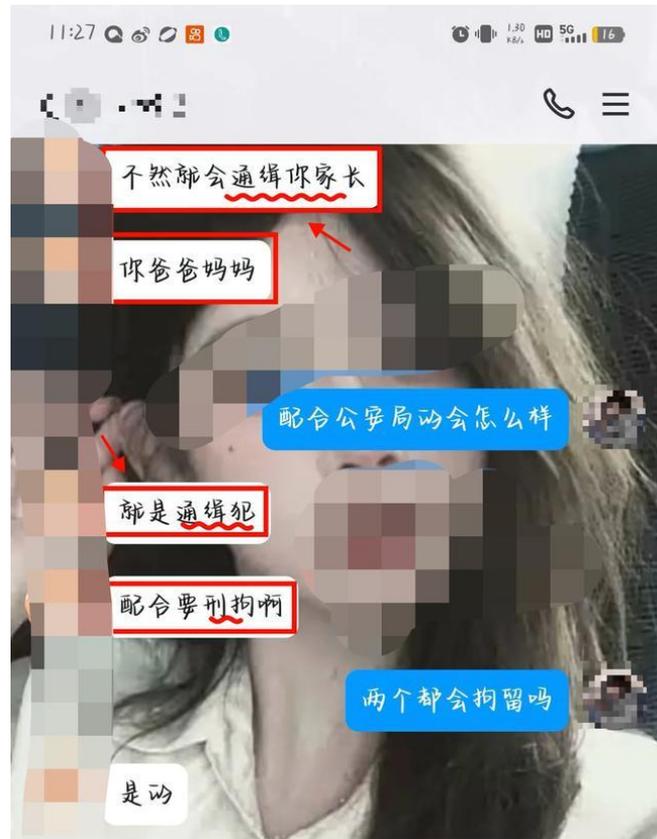
# 骗术7：冒充警察、律师诈骗学生



## 案例写真

长沙11岁小学生小雨玩手机时，刷到一条“扫码添加某明星QQ”的信息，便扫码添加了对方账号。不料对方自称该明星的律师，以明星隐私泄露为由要求小雨配合调查，否则就报警抓他的父母。小雨非常害怕，按要求接听了语音电话。对方说需要对小雨妈妈的银行卡进行核查，“指导”小雨向指定账户转账。小雨陆续转账90万余元，直到被小雨妈妈发现。

免费领取游戏皮肤、进明星粉丝群、领取学习资料等是骗子常见的引流套路，有的更是直接冒充警察加好友进行诈骗。学校和家长需加强学生的反诈教育。



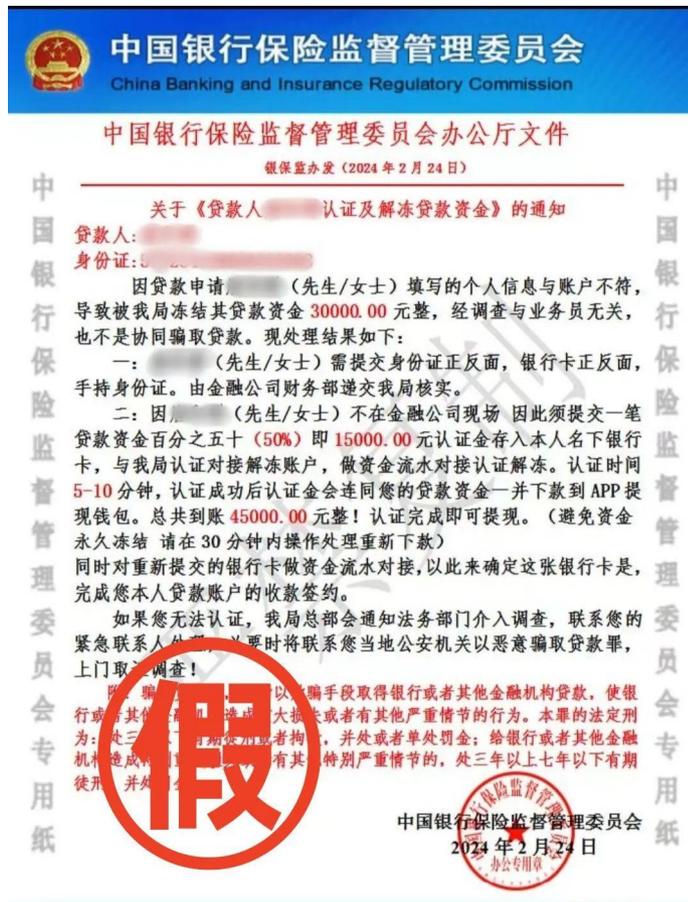
# 骗术8：虚假网络贷款诈骗



## 案例写真

宿迁的小范需要5万元周转，刚好看到一条网贷广告，便下载了一个“某呗”APP，申请了贷款。但放款时，系统提示其银行卡号错误。小范联系客服，对方说需要交纳15000元认证金，后来又说要交保证金、信用不够需要刷信用等，让小范转账。小范找亲朋好友和生意伙伴先后借款超百万转到指定账户，最终也没能提现成功。

诈骗分子利用冒充银保监会的虚假通知，以骗贷罪恐吓受害者，谎称不解冻也要还贷款，让受害者陷入拒绝沉没陷阱。贷款要选正规机构，APP要从应用市场或官网下载。



# 骗术9：虚假游戏交易诈骗



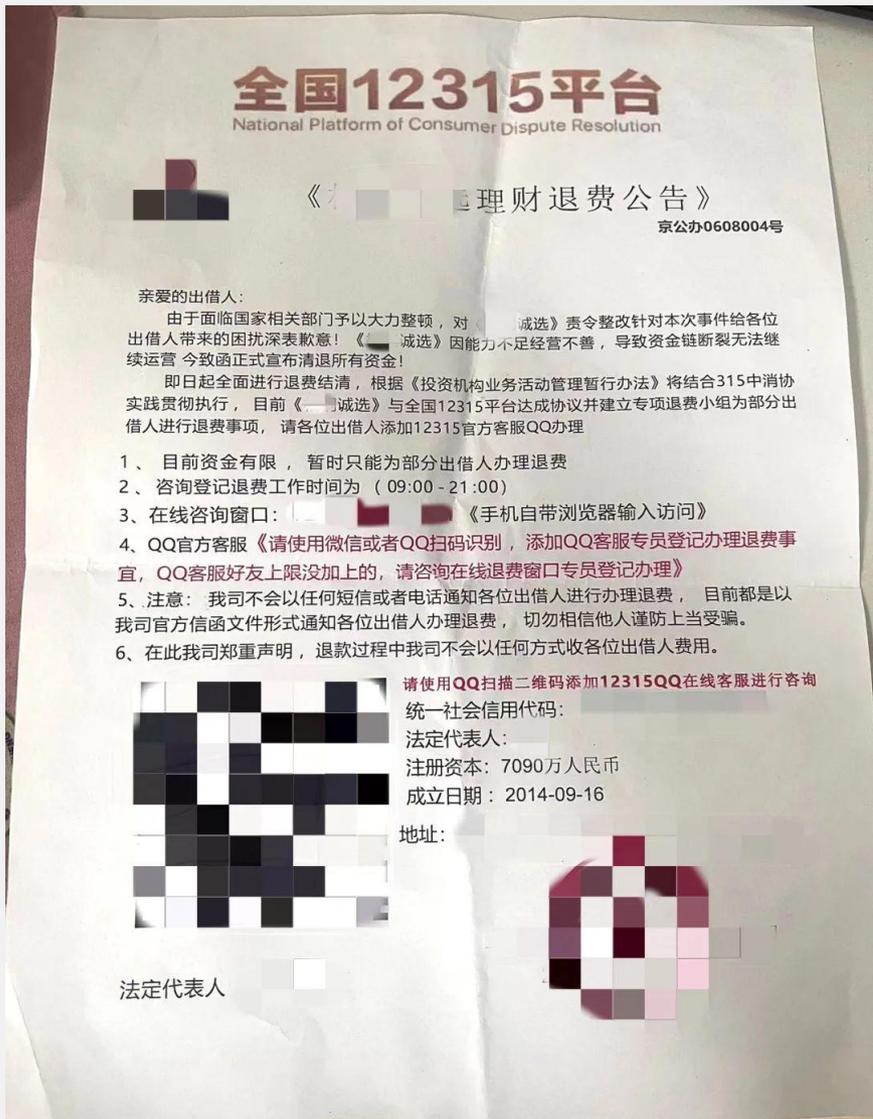
## 案例写真

2024年1月，一网友联系左某，想以10000元的价格购买其游戏账号。对方提出通过某游戏交易平台交易，并发来一个网站链接。左某点击打开网站，上传了交易信息，很快看到对方支付了10000元。但是，提现时平台却提示输错了银行卡号账户冻结了，必须交10000元解冻。左某交了一万元后，客服又说身份信息不完整，需要再交4万元。交完4万元后，还要再转12万元.....左某这才意识到遭遇了诈骗。



**钓鱼网站**是指伪装成正规网站（如银行、电商平台等），通过欺骗或窃取用户敏感信息（如账号、密码、支付信息）实施网络诈骗的虚假网站。

# 骗术10：虚假退费诈骗



## 案例写真

2023年3月，杭州姑娘小陈收到一条短信，通知他3月23日凌晨，她突然收到一条退费通知短信，告知她之前跑路的培训机构可以退费了。小陈加入了退费群，群里都是来退费的人，有人已经退费成功了。小陈按要求下载了一款“3.15”的APP，提供了收款银行卡号。“管理员”要小陈先交8000元保证金，承诺一并返还。小陈交完后，又以验证银行有效性账户为由，在平台上购买基金进行退费，转账6笔共计1552100元。

除了培训机构，P2P理财平台退费也是同类诈骗手段。退费应当原路返回，不可能通过购买基金的方式退还，所有要交钱的退费都是诈骗。

# 其他常见诈骗套路

01

## 一、虚假购物服务类诈骗

诈骗分子以低价发布商品、服务信息，诱骗受害者通过微信、支付宝或银行转账的方式直接购买，最后不发货或者以次充好。比如，疫情期间的口罩诈骗、某些二手平台上的低价手机、相机等数码产品等

02

## 二、裸聊诈骗

诈骗分子假冒美女，在网上主动向受害男性打招呼，通过暧昧的聊天勾引视频裸聊。期间，会以看照片、直播等理由诱骗受害人下载带木马的陌生APP，盗取受害人手机中的通讯录。最后，用录制的视频向受害人敲诈勒索。受害人交了一次钱后，再以不同的身份连续敲诈！

02

## 三、民族资产解冻类诈骗

不法分子伪造国家机关公文、证件，虚构“民族资产解冻”“扶贫”等项目，诱骗受害人缴纳“启动金”“会员费”或投资入股，承诺高额回报。针对中老年群体、社会危害大。

04

#### 四、虚假网恋交友诈骗

诈骗分子常伪装成“高富帅”“白富美”等形象，通过甜言蜜语快速建立信任，随后编造生病、投资亏损等借口索要钱财。或者伪装成“美国大兵”“外国军医”，专门针对中老年女性诈骗，骗子谎称准备来中国与女子共同生活，将巨额现金、贵重物品寄给受害人保管，再冒充海关、快递公司诱骗受害人缴纳清关费用、违约金、罚金等。

05

#### 五、虚假社保卡、ETC升级诈骗

诈骗分子以社保卡、ETC过期需要重新认证或者升级为由，发送虚假短信，诱骗受害人点击短信中的链接，打开假冒的网站，填写银行卡号、取款密码、验证码，盗刷银行卡内资金。

Part

3

打击“两卡”犯罪，  
莫当电诈“工具人”

# 打击治理涉案银行卡、手机卡、电话卡

## “两卡”用处

如果有人出售了自己的电话卡、银行卡，就会被卡贩子层层转卖  
最终被诈骗集团用于实施诈骗或洗白赃款

实名不真人

### 手机卡

既包括大家平时所用的三大运营商的手机卡，也包括虚拟运营商的电话卡，同时还包括物联网卡

“电诈高楼”地基的

### 银行卡

既包括个人银行卡，也包括对公账户及结算卡，同时还包括非银行支付机构账户，（微信、支付宝等）

“电诈高楼”的水管

# 电信诈骗相关罪名

最高检发布《刑事检察工作白皮书（2024）》，2024年起诉诈骗罪占刑事案件比为9.78%、掩隐罪7.92%、帮信罪5.06%，诈骗罪同比2023年上升25.4%。

1

**诈骗罪：**诈骗公私财物，数额较大的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金；数额巨大或者有其他严重情节的，处三年以上十年以下有期徒刑，并处罚金；数额特别巨大或者有其他特别严重情节的，处十年以上有期徒刑或者无期徒刑，并处罚金或者没收财产。

2

**帮助信息网络犯罪活动罪：**明知他人利用信息网络实施犯罪，为其犯罪提供互联网接入、服务器托管、网络存储、通讯传输等技术支持，或者提供广告推广、支付结算等帮助，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金。

3

**掩饰、隐瞒犯罪所得、犯罪所得收益罪：**明知是犯罪所得及其产生的收益而予以窝藏、转移、收购、代为销售或者以其他方法掩饰、隐瞒的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金；情节严重的，处三年以上七年以下有期徒刑，并处罚金。



# 惩戒措施

2024年12月1日，《电信网络诈骗及其关联违法犯罪联合惩戒办法》正式施行，对涉及电信网络诈骗及其关联违法犯罪的单位和个人，实行联合惩戒措施。

## 信用惩戒措施：

- (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。



# 第一类：“两卡”类



## 案例写真

2023年，浙江某法院审理了一起帮信罪案件，19岁的大学生小林因提供6张银行卡给“兼职中介”，涉案流水超800万元，被判有期徒刑1年6个月。

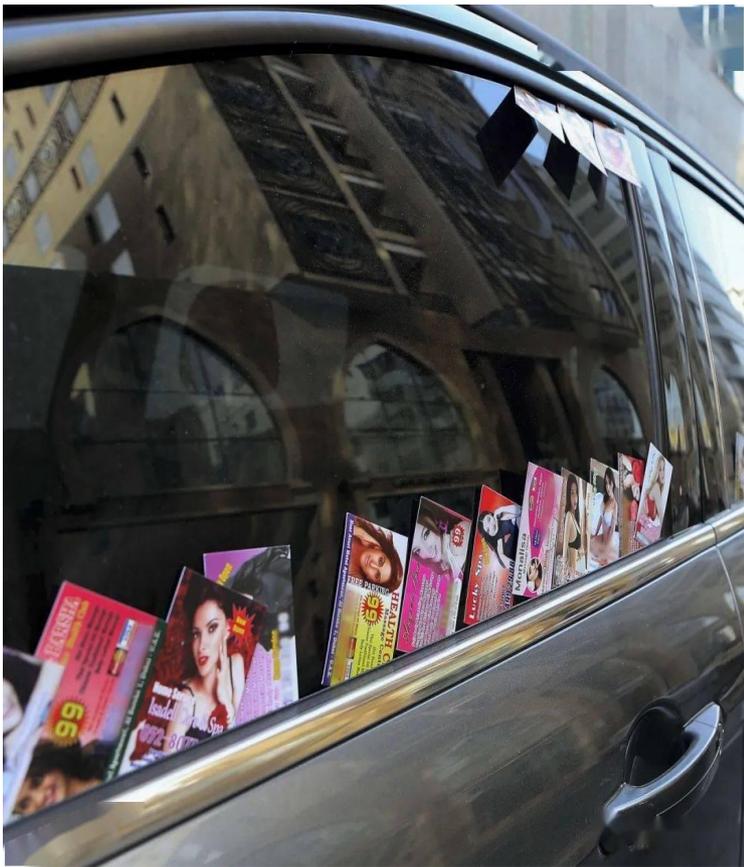
**“两卡”**是指**手机卡**（含流量卡、物联网卡等）和**银行卡**（含银行账户、非银行支付账户等）。出租、出借、出售“两卡”，涉嫌违法犯罪。



## 第二类：“引流”类



### 案例写真



一天，老吴在兼职群里得知，在社交平台发布推广引流信息就能挣钱。老吴心动了，拉上妻子小梅一起开始兼职引流。两人发现，其引流的网站是诈骗网站，但是并没有收手，还在网上找到4名下线，共投放虚假广告千余条，获利10万余元，很快被警方抓获并依法刑事拘留。

**常见的“引流”方式**还有：发送诈骗信息、地推、加好友、拉人入群、推广涉诈APP、替诈骗分子解封网络账号等。

## 第三类：“洗钱”类



### 案例写真

2024年9月，沙县警方打掉两个非法转移涉案资金的犯罪团伙，抓获犯罪嫌疑人黄某某、陈某某等6人。他们不仅在非法平台上承接“跑分”业务，还组织人员在ATM机上取现诈骗资金，采用“卡接回U”的方式进行洗钱。

**常见“洗钱”方式：**“跑分”平台、ATM取现、上门取现、购买黄金等贵重物品



## 第四类：“技术”类



### 案例写真

一天，有客户找到程序员小石，要他制作一批携带木马病毒的虚假交友软件。小石禁不住对方的高价诱惑，制作出20余款诈骗软件，出售后获利7万余元。不久，客户因涉嫌诈骗被警方抓获，小石也被依法刑事拘留。

**其他常见帮信行为：**架设虚拟拨号设备

(VOIP、GOIP、多卡宝、络漫宝等)、手机口网络、开发网络程序、制作运营网站等

Part **4**

# 如何识别防范电信诈骗？

# 电话诈骗的共同规律



诈骗分子无论花言巧语，手法如何翻新，最后都要落到一个点上，就是要钱。所以在此要提醒广大群众，千万不要轻信那种来历不明的电话、短信，不要轻易透露自己的身份和银行卡的信息，如果有疑问的话，要及时打电话给公安机关，哪怕向你的亲友、记者以及比较有见识的人询问一下、核实一下。

# 防电信诈骗十守则

## 1 手机短信内的链接都别点。

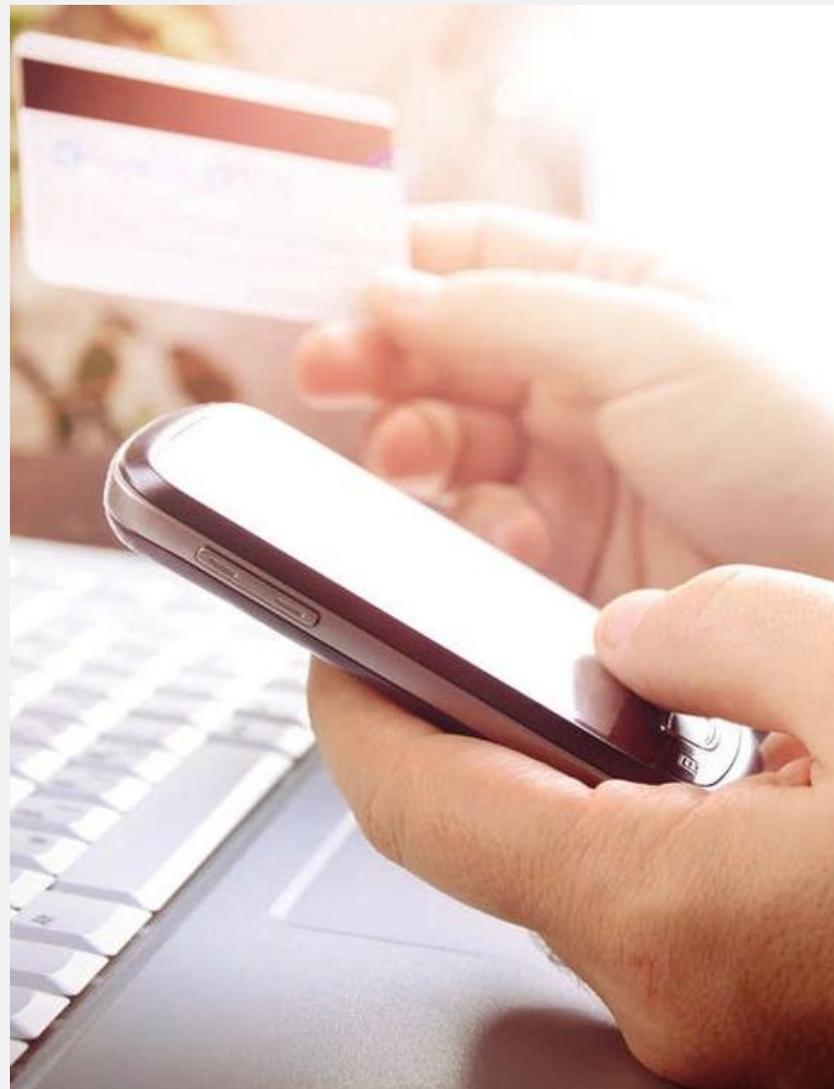
虽然手机短信中也有银行等机构发来的安全链接，但不少用户难以通过对方短信号码、短信内容、链接形式等辨别真伪，所以建议用户尽量不要点击短信中自带的任何链接。特别是Android手机用户，更要防止中木马病毒。

## 2 凡是索要“短信验证码”的全是骗子。

银行、支付宝等发来的“短信验证码”是极其隐秘的隐私信息，且通常几分钟之后即自动过期，所以不得向任何人和机构透露该信息。

## 3 凡是无显示号码来电的全是骗子

目前，除极少数军政方面人士还拥有“无显示号码”电话之外，任何政府、企业、银行、运营商等机构均没有“无显示号码”的电话，所以今后再见到“无显示号码”来电，直接挂断就好。



4

### 闭口不谈卡号和密码

无论电话、短信、QQ聊天、微信对话中都绝不提及银行卡号、密码、身份证号码、医保卡号码等信息，以免被诈骗分子利用。

5

### 不信“接的”，相信“打的”

为了防止遇上诈骗分子模拟银行等客服号码行骗，遇上不明来电可选择挂断后，再主动拨打相关电话(切勿使用回拨功能)，这样可以保证号码的准确性。

6

### 钱财只进不出，“做貔貅”。

任何要求自己打款、汇钱的行为都得长心眼，警方建议如需打款可至线下银行柜台办理，如心中有疑惑，可向银行柜台工作人员咨询。

7

### 陌生证据莫轻信

由于个人隐私泄露泛滥，诈骗分子常常会掌握有用户的一些个人信息，并以此作为证据，骗取用户信任，此时切记要多长个心眼——绝不轻易相信陌生人，就算朋友家人，如果仅仅是在网上，也不可轻信。



8

## 钓鱼网站要提防

切不可轻易信任那些看上去与官方网站长得一模一样的钓鱼网站，中病毒不说，还可能被直接骗走钱财，所以在登录银行等重要网站时，养成核实网站域名、网址的习惯。

9

## 新鲜事要注意

诈骗分子常常利用最新的时事热点设计骗局内容，如房产退税、热播电视节目等都常常被骗子利用。如果不明电话中提及一些你从未接触过的新鲜事，也切莫轻易当真。

10

## 一旦难分假和真，拨打报警电话最放心

如果真有拿不准的事，拨打110无疑是最可靠的咨询手段，虽然麻烦了警察，但必要时仍可以采取这种手段。



# 上当后如何补救

## 补救措施

### 五项应对措施

- 1 一旦汇款后发现自己被骗了，可在第一时间拨打银行客服请求帮助。
- 2 及时拨打报警或向派出所报案，提供对方收款的银行卡号、第三方支付账号信息，警方第一时间进行止付冻结。
- 3 整理聊天记录，转账流水，涉诈电话、APP、网站等等相关信息，提供给警方侦查办案。
- 4 切勿相信网上网警、律师、黑客等声称能够帮你追回被骗款的人，那些都是骗子。
- 5 调整好心态，正视被骗的事实，努力回归正常生活。主动学习反诈知识，防止被其他套路诈骗。

## 推荐关注、星标



国家反诈中心视频号



昆明反诈中心公众号



不明来电别轻信  
汇款诈骗别大意  
提高防范意识  
远离电信诈骗



# 演示完毕 感谢关注



呈贡反诈中心民警：XXX

