# 不轻信
# 不转账
# 不上当

# 携手反电诈
# 聚力保民安

子孝媳贤家兴旺，一个电话打乱了这一切。一位“赵警官”发了“逮捕令”给我，说我涉嫌诈骗，让我把家里的所有积蓄全部打入指定的“资金清查平台”，为了证明清白，我把全家辛苦赚的五十多万打入了对方平台。然而这一切都是假的！我该如何回家.....

南京市公安局

扫一扫 学防骗

CONTENTS

# 目录


01 序言
什么是电信诈骗

02 刷单类诈骗案例

03 冒充公检法类诈骗案例

04 冒充领导类诈骗案例

05 冒充熟人类诈骗案例

06 冒充客服类诈骗案例

07 交友类诈骗案例

08 网络购物类诈骗案例

09 购物退款类诈骗案例

10 网络贷款类诈骗案例

11 信用卡类诈骗案例

12 网络投资类诈骗案例

13 网络预测彩票类诈骗案例

14 网络购票类诈骗案例

15 防电信诈骗“五不一打”

16 防电信诈骗“六个一律”

17 防电信诈骗“八个凡是”

# 序 言

近年来，电信网络诈骗案件持续多发高发，不法分子不断翻新犯罪手法，紧跟社会热点，精心设计骗术，针对不同群体量身定做、步步设套，对受害人进行欺骗、引诱、威胁、恐吓，严重危害人民群众财产安全，扰乱正常生产生活秩序。

## 什么是电信诈骗?

“电信诈骗是犯罪分子以非法占有为目的，利用移动电话、固定电话、互联网等通讯工具，采取远程、非接触的方式，通过虚构事实诱使受害人往指定的账号打款或转账，骗取他人财物的一种犯罪行为。”

# 01 刷单类诈骗案例

2018年2月13日，经常网购的市民王小姐收到一条短信，内容是：“你淘宝信誉良好，邀请你进行刷单任务，待遇每小时50到80元不等，适合宝妈，学生，上班族。”并留有一个QQ号码。

**刷单**

是指由店家付款请人在网店进行虚假购物，填写虚假好评，提高信用度，最终提高商品销量。

王小姐觉得这活不累报酬也不错，于是就添加了这个QQ号，不一会对方就给王女士发了个刷单流程和第一单的刷单任务，王女士看了之后就信心满满地开始起来。根据对方发来的转账付款二维码进行第一次付款，付了121元，第一单过后对方返给王小姐126元，王小姐尝到了甜头接着又刷了第二单任务，付完款后王小姐让对方返钱，对方说根据规定只有再完成几单任务之后才能返还佣金，并发了第三单任务，之后王小姐陆续又完成了多单任务，当提出让对方返还佣金时，对方还是以须继续刷单为理由不进行返还，王小姐觉得自己上当了，选择报警，但此时王小姐已经陆续做了12000元的任务，损失12000元人民币。

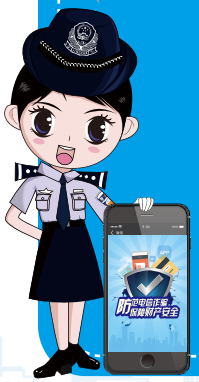
## 提醒

1、不法分子充分利用被害人想动动手指就可以赚钱的心理，以网店刷单、打字、网络发帖为名义进行诈骗，这些兼职消息会发布在各大论坛、网站，通常页面标题十分吸引人，例如“无任何要求”、“在家轻松日赚2000”等等。

2、不法分子会让你购买某个商家的商品，通常第一单金额较小，并且会给你返现，让你尝到甜头。接下来对方会让做大金额单子，并且不再返现金，以达到诈骗的目的。

3、还有些会提前收取押金或会员费，最后一并不再返还。

4、刷单属于违法行为，切勿参与类似刷单等兼职工作，做到不违法、不上当。





# 02 冒充公检法类诈骗案例

2018年3月23日，受害人刘女士在家中接到陌生电话，对方自称是南京市通信管理局的工作人员，说刘女士名下有一张电话卡发送了大量诈骗短信，现警方已介入调查。随后，“工作人员”将电话转到“某某公安局”。一位“赵警官”告诉刘女士，因其涉嫌一桩诈骗案，警方将逮捕刘女士，并通过QQ给刘女士发送了其本人“逮捕令”的图片，刘女士当即吓坏了。后按照“赵警官”要求，刘女士联系了办理案件的检察院“王科长”，“王科长”对刘女士说，要自证清白，需要将其名下所有资金全部转入“资金清查平台”进行清查。刘女士赶紧按照“王科长”的要求，在发来的链接里填下了自己银行卡的卡号、密码、U盾密码、手机验证码等信息。之后，在所谓的“资金清查”过程中，刘女士银行卡中先后存入的八十万元人民币被转出。

## 提醒

1、听到以下内容可以确认您遇到了“冒充公检法”诈骗！应当立即挂断电话并报警，向警方提供接听的电话号码。

(1) 说“我帮你把电话转接到公安机关”的；

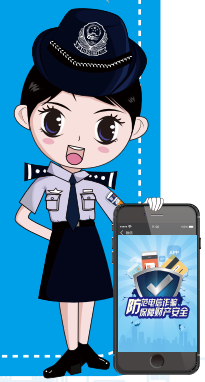
(2) 说“你可以拨打114，核实一下我的电话号码”的；

(3) 提出“我们这个是专案，保密性非常强，绝对不能跟任何人提到，家里人也不行，别的警察也不行”的；

(4) 要把全部财产转移到“公安机关安全账户”的；

(5) 让事主自己登录一个网址，查看自己通缉令的。

2、身正不怕影子斜，千万不要因为害怕轻信了骗子，有任何疑问请拨打110，南京市公安局会全力保障市民的人身、财产安全。



# 03 冒充领导类诈骗案例

2018年5月初，从事会计工作的张小姐在工作期间被拉进一个微信群，群主是自己公司老板的名字，群成员当中还有公司的其他股东，公司领导和同事，他们的名字、头像都是真实无误的。进群后，“老板”与其他所谓“股东”以及“公司领导”，你一言我一语的在谈论一个项目，过程中让张小姐查一下当天公司账上的流动资金还有多少，并且让他截一个明细的图片，张小姐没有多想就执行了，之后“老板”称这个项目需要立即启动，并给了张小姐一个账户号码，让她立即转入该账号36.8万，张某心想这是公司的内部群，没有任何怀疑就进行了汇款，直到公司内部审核资金时才恍然大悟，之前的一切都是骗局，后选择报警。

## 警方提醒：

**01** 受害人或由于职级的差距，不敢跟领导打电话、当面核实，或由于麻痹大意，犯罪分子则利用了这种心理实施诈骗。

**02** 企业要完善财务制度，须履行严格的财务审批手续，不要通过短信、微信、QQ等渠道传递转账指令。

**03** 会计人员收到陌生人发来的邮件、文件等，切莫轻易点击，当收到汇款指示时，不要轻易相信，必须主动换一种可靠的联系方式或当面与下达指令的领导进行确认。



# 04 冒充熟人类诈骗案例

2018年4月9日19时许，家住南京市鼓楼区的钱先生接到了一个电话。电话中一个操着北方口音的男子上来就问：“你知道我是谁吗？怎么连老朋友的声音都听不出来了。”当钱先生猜测地说出自己一个北方朋友的名字后，对方马上接过来说：“没错，就是我。”这位“朋友”告诉钱先生自己正在出差到南京的路上，到了就会去拜访他。

第二天上午，这位“朋友”又慌张地打来电话，说自己在苏州发生了意外，需要一些钱救急。此时还蒙在鼓里的钱先生立刻向“朋友”账号汇去5000元。不料，这位“朋友”却三番五次编织各种理由急需用钱，要求钱先生汇钱。当钱先生先后总共汇去了2万元后才开始有所怀疑，经过多方核实后发现自己被骗了，选择报警。

## 警方提醒：

**01** 此类案件中犯罪嫌疑人主要利用受害人，对熟人碍于情面，不好意思直接询问对方身份，抹不开面子去拒绝朋友求助的特点。

**02** 如果接到此类诈骗电话时，不要去猜而应直接询问对方姓名，并进行核实。

**03** 在无法确认对方身份时，可通过第三方亲朋进行核实或提出见面要求，如对方百般推脱，可以洞察其破绽。

**04** 当对方说自己遇到突发事件，急需用钱，这时要核实事件的真假，可以向相关办案部门了解，如有必要可以亲自前往或委托亲朋前往事发地，绝不轻易汇款转账。

## 05 冒充客服类诈骗案例

2018年7月17日，南京市民张某接到一个陌生电话，对方称是“南京银行”客服人员，亲切的问候完后，对方告诉张某“您的尾号938银行账户，有笔12000元的金额异常转出，现在和你核实，如果没有消费我们可以帮忙赎回，但过期不操作，会默认转出。”

张某的第一想法就是自己的银行卡被盗刷了，立即询问对方是否被盗刷。对方称“您的金额是异常转出，我们无法断定是不是盗刷，如果不是您本人操作，短时间内我们可以将该笔资金核实返回，超过时间将会默认转出。”张某心想客服都给我打电话了，那钱一定是少了，非常着急，连忙问客服怎么办，客服人员告诉他需要去ATM上操作才可以退到他的银行卡。

张某匆忙跑到附近的ATM机，对方又告诉张某必须将ATM机转换为英文界面，并声称只有在英文界面才可以进行退款操作，在对方的提示下张某操作至了一个密码输入界面，对方告诉张某只需要输入密码就可以将盗刷的钱退回。当张某输入密码后，返回中文查询界面查看余额，少了12000元。但此时已无法联系对方，于是张某选择了 报警。

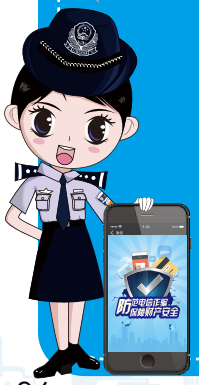
### 提醒

1、生活中要加强个人信息保护的意识。

2、收到该类电话，挂断可疑电话并且通过官方客服进行咨询。

3、在条件允许的情况下去柜面进行咨询及操作。

4、切勿在陌生电话的提醒下进行英文操作界面转换对自己银行卡进行操作。



## 06 交友类诈骗案例

5月15日，李先生提出见面吃饭的要求，谁料对方却一直推诿，这使李先生觉得事有蹊跷，于是提出就算不见面，大家视频一下的要求，万万没想到，对方直接将李先生拉黑，此时李先生感觉到可能是被骗了，于是选择报警。

28岁的李先生，独身一人在南京经营一家餐厅，2018年5月初，他在某征婚网站上认识了一名王姓女子。登记的信息显示这名女孩今年25岁，定居南京，并且从事的行业和财会有关，经过一周的微信联系，两人确定了情侣关系。

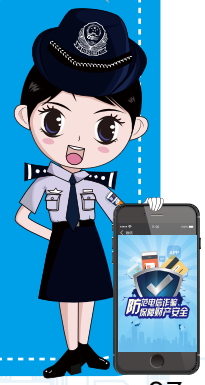
没多久，这名王姓女子给李先生发来一条私信，告诉李先生，声称自己的奶奶身患重病，需要很多钱去治疗，自己没有那么多钱，可能要去广州上班，他们两人可能没有机会见面了。 李先生出于想继续进一步发展的目的，因对方奶奶看病各种费用的理由，先后给所谓的“另一半”汇去了11万元。

### 提醒

1、婚恋诈骗案中，绝大多数犯罪嫌疑人利用被害人急于给对方留下良好印象的心理达到行骗目的，给受害人的身心带来极大伤害。

2、婚恋交友中要增强防范意识，要多方验证对方的身份。

3、当对方以各种理由借钱时，一定要高度警惕，不要轻易允诺。即使是验明了身份进行正常恋爱，借钱，也需要保留借条、汇款凭证及相关的聊天记录、短信等证据。



# 07 网络购物类诈骗案例

2018年3月9日12时许，王某在网页上看到广告，称可以用1044元的价格买一部苹果6手机，王某感觉很便宜，于是根据网页提示加了对方QQ好友进行联系，对方说要购买两部苹果6手机一共2088元，之后王某便给对方账户通过支付宝转账方式转账2088元。

转账后对方称如需发货还需要交2200元的保证金，并给了王某一个二维码，王某又扫了二维码付了2200元，汇款后对方又继续编织其他理由要求王某汇款，此时王某发现情况不对，觉得上当了，选择报警。

## 警方提醒：

01 天上不会掉馅饼，当一个商品的价格远低于零售价时，要特别留心，犯罪分子就是利用被害人贪小便宜的心理实施诈骗。

02 不随意扫陌生的二维码，不随意点开对方发的链接，链接则可能是填写身份信息后的付款链接或盗取银行卡密码的木马链接。

03 不要随便加陌生人微信，QQ号，在网上进行交易时一定要提高警惕，以免造成不必要的损失。

04 网络购物，请选择正规网站。



# 08 购物退款类诈骗案例

2018年5月26日，江宁大学城的小王，报警称其被骗，据了解：小王在某宝网上购买了一件棉衣，5月27日小王接到了一个陌生电话，对方声称自己是某宝网的店家，称小王买的东西缺货，现在要退款给小王，于是，小王根据对方的提示，加了一个支付宝账户来接收退款。

但对方告诉小王，小王的“信用额度”不够，需要让小王从支付宝上的“招联好期贷”里借款5000元提高“信用额度”才可以退款，然后再把这笔钱连同之前退款一并返还小王。小王按对方指示，通过对方发过来的支付宝二维码，支付了这借来的5000元，可是，对方说不成功，并谎称只用一个借贷平台可能不行，让其再从“蚂蚁借呗”借8000元，小王就又从“蚂蚁借呗”借了8000元并又转出去了，但对方还没有返款，此时，小王感觉上当，选择报警。

## 警方提醒：

01 所有退款相关事宜应通过官方购买渠道进行退款操作。

02 关于退款事项一定要多做了解，研究官方网站退款事项、致电客服询问等等。

03 第一时间联系之前购买物品的店家。

04 千万不要轻易扫描陌生人发来的二维码。

# 09 网络贷款类诈骗案例

2017年11月27日，小李在网络上搜索到一家名为“贷期贷”的网站，小李仔细看了看上面各种贷款的介绍觉得还挺靠谱，于是拨打了其所谓的“官方客服”电话。电话拨通后，小李便开始和对方交流起自己钟意的一种贷款方式，随后添加了其“客服”的QQ，对方先是和小李索要了各种个人信息，随后便告诉小李先交利息的10%作为手续费，就可以下款。

小李根据对方给出的账号汇去了1000元，汇款后，对方通过QQ发给小李一张“贷款合同”，小李填写完后，将“合同”传给对方，对方告诉小李，再过五分钟就可以收到钱。

五分钟过后，没收到钱的小李开始询问客服，为什么没有收到款项，对方则声称小李的信誉度较低，必须要再交2000元“公证费”，否则所贷款项和之前的1000元手续费都会打水漂，小李发现事有蹊跷于是报警。

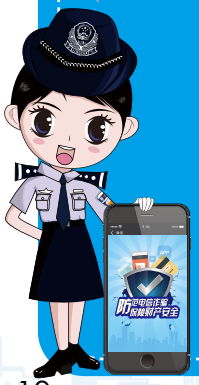
## 提醒

1、此类以无抵押贷款为名的电信诈骗主要作案形式都是网络小额贷款广告、QQ群信息。

2、嫌疑人将网页、QQ、陌陌等交友平台作为作案工具，寻找急需用钱的人群作为目标实施诈骗。

3、犯罪嫌疑人利用被害人急于拿到贷款的心理，又以预交保证金、月利息、送款担保费等名义达到行骗目的。

4、切勿轻易信任在网络上随意寻找到的贷款渠道。





# 10 信用卡类诈骗案例

2018年6月6日，家住南京的李先生在家中收到一条短信：“尊敬的用户您好！您的XX信用卡因（逾期还款）影响征信，现已冻结，请立即联系客服：00861-8449054528办理解冻。”【X银行】

李先生过短信留下的电话和对方联系后，对方称要用通过本人的储蓄卡协助解冻，之后李先生便按对方要求将自己的储蓄银行卡号发给了对方，并且要求储蓄卡内的余额达到一定数值才能满足解冻条件，李先生就通过支付宝向银行卡里转了11000元人民币，对方又要求李先生把手机上刚刚收到的几条所谓的“解冻”验证码发给对方，李先生也照做了。没一会，李先生收到短信得知，储蓄银行卡在京东上消费了两笔，以及通过POS机支取了人民币1000元。此时李先生才意识到被骗，其损失已经超过万元。后李先生选择报警。

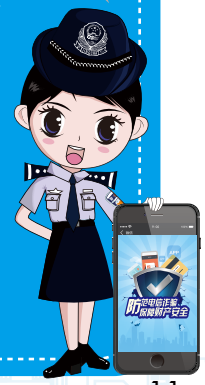
此案例中犯罪嫌疑人获得李先生的银行卡号，后将改卡绑定到预先准备好的京东账户进行消费，而所谓的“解冻”验证码实则是“京东消费”的银行卡绑定以及消费验证码，当把验证码提供给骗子李先生就上当了。

## 提醒

1、不要轻信来历不明的电话、手机短信和网络信息，不要轻易拨打短信中的所谓“客服电话”，从而进了不法分子设下的圈套，而是应该拨打银行的官方客服电话进行查证。

2、不要随意透露自己及家人的存款、银行卡卡号、密码、交易安全码等信息，特别是手机收到的验证码，千万不能轻易告诉陌生人。

3、当听到有关转账的要求后，要多思考、多核实，绝不轻易向陌生人汇款、转账，以保证自己的资金安全。



# 11 网络投资类诈骗案例

2018年6月，市民王先生在QQ上结识了一名网友，交流一段时间后得知这名网友在家中上网炒邮票赚了不少钱，王先生听说有这样一条发财的途径后，便请求网友教他炒邮票的方法，这名网友通过QQ给他介绍了一位专门从事炒邮票的林姓老师，并告诉他，自己一直在跟林老师炒邮票，自己赚的钱只是林老师的万分之一。王先生立刻与林老师取得联系，并从林老师处接收到一款名为XXXX的炒邮票操作平台手机软件，王先生花费了1500元在此软件注册了会员，在注册会员后，该软件送给了王先生10万元虚拟资金。经过几天的摸索与练习，王先生逐渐了解了这个平台的操作方法，并使用虚拟资金尝试投资，发现有很可观的收入，于是向该平台充值人民币28万元，在操作平台上炒邮票。

直至7月26日，王先生想把平台上赚到的钱提取出来时，发现无法提现，当晚20时，王先生再通过自己的用户名、密码已无法登录该平台，后选择报警，共损失28.15万元。

## 警方提醒：

**01** 切勿盲目购买网络投资产品，尤其对百分百有收益、无风险的投资理财产品，须保持高度警惕。

**02** 即使是大型网络平台上的网络投资推广链接，也应多方查证，多方验证，不可轻易相信。

**03** 切记天上不会掉馅饼，高额回报无风险的投资是不存在的。



# 12 网络预测彩票类诈骗案例

2018年2月27日，李先生在家上网时登陆了一个名为 “XX福利彩票3D专家预测网”的网站，该网站称其是由XX网络科技建立的专业彩票预测网，网站提供中国福利彩票双色球、福彩3D等彩票预测服务，预测命中率高达98%以上。李先生立即与该网站联系咨询。对方联系人自称叫“张大师”，他告诉李先生，如果要享受预测号码服务需先交纳2000元注册费成为会员才行，如果预测不准确，可以退还所有的费用。

3月2日，李先生按照“张大师”提供的工商银行账号汇去2000元。随后，“张大师”告诉李先生说他已经注册成为会员，须再交5000元保证金就能享受预测号码服务，3月5日，李先生如数汇去5000元保证金。然而，“张大师”提供的预测信息并不准确，李先生要求退钱，“张大师”称网站管理中心每月15日统一受理退赔事宜，如要退款，要等到15日。3月15日上午，李先生再次联系“张大师”，电话却成了空号。此时，李先生意识到自己被骗了，后选择报警。

## 警方提醒：

**01** 此类诈骗犯罪嫌疑人开设彩票预测网站、发布广告，声称彩票命中率高达90%以上，抓住被害人梦想发财、不劳而获的心理，进行诈骗。

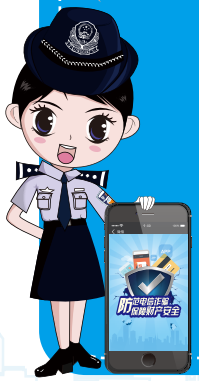
**02** 一旦受害人上钩，骗子就会以各种名义向受害人收取会员费、专家预测费、信息费、保证金等费用。

**03** 切勿相信“网络预测彩票”，人一旦产生贪欲，必然受骗！

## 13 网络购票类诈骗案例

2018年2月，大学生张某上网购买火车票准备回老家过春节，不一会就找到了一家声称可以代购特价票的网站，通过QQ张某联系上网站“客服”，在“客服”的要求下她用支付宝付款400多元，购买了一张高铁票，并留下个人信息。但是付款后，张某迟迟没等来车票确认的短信，她再次上网查询车票订单，网页仍然显示“未出票”。她再次询问“客服”是否购票成功，“客服”称正在出票，让她不要着急，只需耐心等待。随后张某又拨打了铁路的官方客服电话确认购票信息。官方客服却称系统内有她的购票登记信息，但显示还未付款。张某心想明明已经付款，为什么还不出票？她再次和“客服”联系。对方告知，她之前填写的乘车人身份信息有误，导致出票失败，可以办理退款，但需先缴纳1000元“保证金”防止退款后意外出票的情况。无奈之下，张某只得交了1000元，转账成功后张某的QQ立即被对方拉黑。此时张某意识到上当受骗，选择报警。

### 提醒



1、此类诈骗当中犯罪嫌疑人就是利用被害人急于开始行程而又无法购买到车票或希望能购买到低价车票的心理，实施诈骗。

2、网络购票一定要通过正规渠道购买，千万不要轻信所谓的代购“特价票”的广告及网站。

3、如若请别人帮忙代购，须一手交票、一手交钱，并当场验证车票的真伪。



## 防电信诈骗“五不一打”

### 不点:不明短信链接不要点

那些不明来路的短信链接,很可能就是骗子发送过来的。他们想尽办法引诱你点开链接,链接里面就是木马病毒。你点进去,手机绑定的银行卡、支付宝的账号密码,就被他们窃取啦。

### 不怕:冒充公检法诈骗

要记住公安局、检察院、法院等司法机关绝对不会电话办案,更不会设置安全账户,让你转钱过去证明清白。

### 不信:转账指令不轻信

现在的骗子,会潜入QQ或微信群,盗用老板的头像和名字,之后再假借老板的名义,要求财务人员转账,咱们遇到转账要求时,要当面或者电话核实清楚!

### 不贪:积分兑换现金不要贪

现在的骗子也懂高科技,他们可以利用改号软件,冒充任何单位的电话给你发送短信。

### 不转:不核实清楚,千万别转账

无论骗子表演了什么花样,他们的最终目的,就是让你给他们转账。广大市民朋友一定要记住,不核实清楚,千万不能转账。这可是守住咱们钱袋子的最后一道防线。

### 一打:发现被骗立即拨打110报警

被骗后,要尽快向警方提供骗子的银行卡号和手机号码,为银行部门冻结被骗资金争取时间。

# 防电信诈骗“六个一律”

只要一谈到银行卡
一律挂掉

只要一谈到中奖了
一律挂掉

一提到“安全账户”的
一律是诈骗

所有短信，让我点击链接的
一律删掉

微信不认识的人发来的链接
一律不点

只要一谈到“电话转接公检法”的
一律挂掉

# 防电信诈骗“八个凡是”

凡是自称公检法要求汇款的，都是骗子；

凡是叫你汇款到“安全账户”的，都是骗子；

凡是通知中奖、领奖要你先交钱的，都是骗子；

凡是通知“家属”出事要先汇款的，都是骗子；

凡是在电话中索要银行卡信息及验证码的，都是骗子；

凡是让你开通网银接受检查的，都是骗子；

凡是自称领导要求汇款的，都是骗子；

凡是陌生网站要登记银行卡信息的，都是骗子。