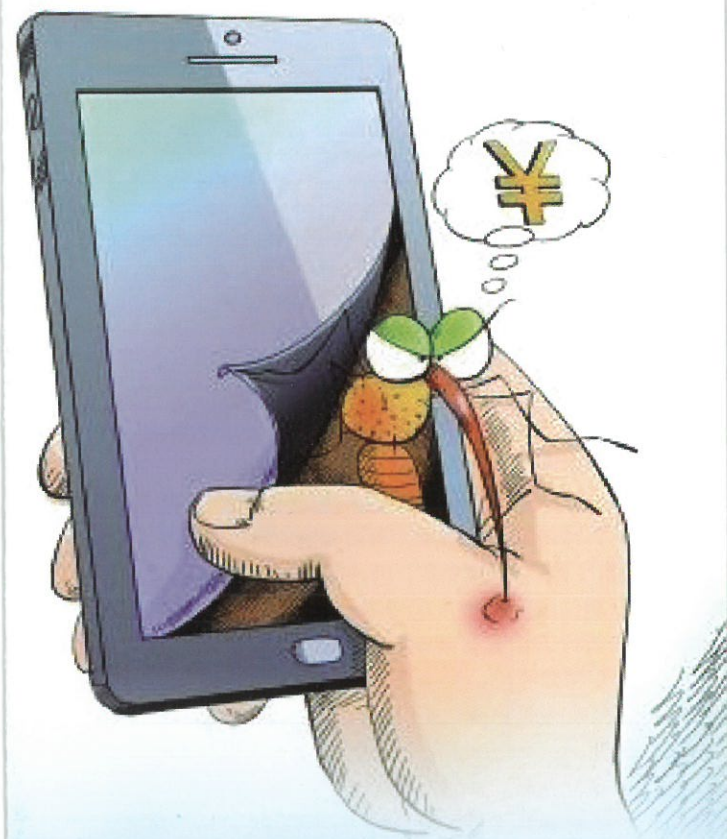


## 警惕诈骗陷阱 保护财产安全



为你详细揭秘五类典型诈骗手法,请擦亮双眼,提高警惕,加强防范,保护财产安全。

## 一、电话语音类诈骗

1. 冒充公检法诈骗。犯罪分子冒充公检法人员拨打受害人电话,以事主身份信息被盗用、涉嫌洗钱犯罪为由,要求将资金转入所谓的“国家账户”配合调查。



2. 医保和社保诈骗。犯罪分子冒充社保、医保工作人员,谎称受害人医保、社保出现异常,可能被他人冒用、透支,或涉嫌洗钱、制贩毒等犯罪,之后冒充司法机关人员以便于核查为由,诱骗受害人向所谓的“安全账户”汇款,实施诈骗。

3. 解除分期付款诈骗。犯罪分子通过专门渠道购买网站的买家信息,再冒充购物网站工作人员称:“由于银行系统错误原因,买家一次性付款变成了分期付款,每个月都得支付相同费用”,之后再冒充银行工作人员诱骗受害人到ATM机前办理解除分期付款手续,实施资金转账诈骗。

4. 包裹藏毒诈骗。犯罪分子以事主包裹内被查出毒品、涉嫌洗钱犯罪为由,要求事主将钱转到“国家安全账户”以便公正调查,实施诈骗。

5. 金融交易诈骗。犯罪分子以某证券公司名义通过互联网、电话、短信等方式散布虚假个股内幕信息,获取事主信任后,又引导其在虚假交易平台上购买期货和现货,骗取股民资金。

6. 票务诈骗。犯罪分子冒充航空公司客服人员,以“航班取消、可提供退票和改签服务”为由,将

事主引入诈骗圈套,要求进行汇款操作,实施连环诈骗。

7. 虚构事故诈骗。犯罪分子虚构受害人亲属或朋友遭遇车祸、亲友被绑架或子女或老人突发急病需紧急手术等各类事故为由,要求对方立即转账,实施诈骗。

8. 欠费诈骗。犯罪分子冒充通信或广电公司工作人员,向事主拨打电话或直接播放电脑语音,以其电话或电视欠费为由,要求将资金转到指定账户。

9. 购物退税诈骗。犯罪分子事先获取事主购买房产、汽车等信息后,以税收政策调整,可办理退税为由,诱骗事主到ATM机上实施转账操作,将卡内存款转入骗子指定账户。

10. 猜猜我是谁诈骗。犯罪分子获取受害者的电话号码和姓名后,打电话让其“猜猜我是谁”,随后根据受害者所述冒充熟人身份,并声称要来看望受害者,后又编造其被“治安拘留”、“交通肇事”等理由,要求受害者向其汇款借钱。

11. 破财消灾诈骗。犯罪分子先获取事主身份、职业、手机号等资料,拨打电话自称黑社会人员,受人雇佣要伤害事主,但受害人汇款就可以消灾,实施诈骗。

12. 冒充领导诈骗。犯罪分子假冒领导、秘书或工作人员等身份,打电话给基层单位负责人,以推销书籍、纪念币等为由,让受骗单位预付订购款、手续费等到指定银行账户,实施诈骗。

13. 提供考题诈骗。犯罪分子针对考生拨打电话,称能提供考题或答案,需将好处费转入指定账户,实施诈骗。



## 二、电子短信类诈骗

1. 娱乐节目中奖诈骗。犯罪分子以“我要上春晚”、“非常6+1”、“中国好声音”等热播节目组的名义向受害人手机群发短信,称其已被抽选为节目幸运观众,将获得巨额奖品,但需预交手续费、保证金或个人所得税等实施连环诈骗。

2. 引诱汇款诈骗。犯罪分子以群发短信的方式要求对方汇款,由于一些事主正巧准备汇款,收到汇款信息后,未仔细核实,即把钱款打入骗子账户。

3. 刷卡消费诈骗。犯罪分子群发短信,冒充银联中心或公安民警连环设套,以事主银行卡消费可能泄露个人信息为由,要求将其银行卡中的钱款转入所谓的“安全账户”,或套取银行账号、密码,实施诈骗。



4. 贷款诈骗。犯罪分子通过群发短信,称其可为资金短缺者提供贷款,月息低,无需担保,但需预付利息、保证金等名义要求汇款,实施诈骗。

5. 复制手机卡诈骗。犯罪分子群发信息,称可复制手机卡、监听手机通话信息,不少群众因个人需求主动联系嫌疑人,继而被对方以购买复制卡需预付款等名义骗走钱财。

## 三、非法网站类诈骗

1. 钓鱼网站诈骗。犯罪分子以银行网银升级为由,要求事主登陆假冒银行网站,获取事主银行账户、密码及手机交易码等信息实施诈骗。

2. 低价购物诈骗。犯罪分子通过互联网、手机短信发布二手车、二手电脑、海关没收物品等转让

信息，一旦事主与其联系，即以需“缴纳定金”、“交易税手续费”等方式骗取钱财。

3. 网购诈骗。犯罪分子开设虚假淘宝店铺，一旦事主下单购买商品，便称系统故障，需要重新激活。随后，通过 QQ 发送虚假激活网址，受害人填写好淘宝账号、银行卡号、密码及验证码后，卡上金额不翼而飞。



4. 虚构色情服务诈骗。犯罪分子在互联网上留下色情服务电话，受害人与之联系后，称需先付款才能提供上门服务，受害人将钱打到指定账户后发现被骗。

5. 冒充亲友利用 QQ 诈骗。利用木马程序盗取对方 QQ 密码，截取对方聊天视频资料后，冒充该 QQ 账号主人对其亲朋好友以“患重病、出车祸”等紧急事情为名要求汇款，实施诈骗。

6. 冒充公司老总利用 QQ 诈骗。犯罪分子通过搜索财务人员 QQ 群，以“会计资格考试大纲文件”等为诱饵发送木马病毒，盗取财务人员 QQ 号码，并分析研判出公司老板的 QQ 号码，再冒充公司老板向财务人员发送转账汇款指令，实施诈骗。

#### 四、纸质信件类诈骗

1. 冒充中奖诈骗。犯罪分子冒充三星、索尼、海尔等公司名义，将印刷精美的虚假中奖刮刮卡，通过信件邮寄或雇人投递发送中奖邮件，受害人一旦与犯罪分子联系兑奖，即以需缴纳“个人所得税”、“公证费”、“转账手续费”等理由要求受害人汇款，达到诈骗目的。

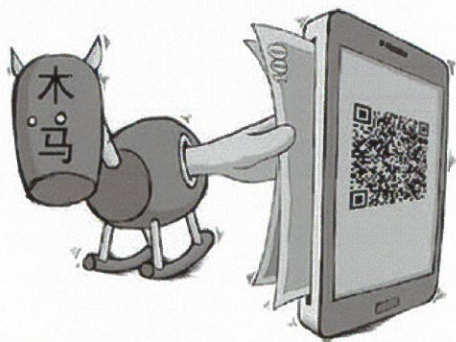
2. 办理信用卡诈骗。犯罪分子通过报纸、邮件等刊登可办理高额透支信用卡的广告，一旦事主与其联系，犯罪分子以“手续费”、“中介费”、“保证金”等形式要求事主转款，实施诈骗。

3. 收藏诈骗。犯罪分子冒充收藏协会的名义，印制邀请函邮寄各地，称将举办拍卖会并留下联络方式，一旦事主与其联系，则以需预交评估费、保证金、场地费等名义，要求受害人将钱转入指定账户，实施诈骗。

## 五、其他方式类诈骗

1. ATM 机告示诈骗。犯罪分子预先堵塞 ATM 机出卡口，并在 ATM 机上粘贴虚假服务热线告示，诱使用户在其银行卡被吞后与其联系，套取密码，待用户离开后到 ATM 机取出银行卡，盗取用户卡内现金。

2. 伪基站诈骗。犯罪分子利用伪基站向群众发送网银升级、10086 移动商城兑换现金的链接，一旦点击后便在其手机中植入获取银行账号、密码和手机号的木马，从而实施诈骗。



3. 伪装身份微信诈骗。犯罪分子利用微信“附近的人”查看周围朋友情况，伪装成“高富帅”或“白富美”，骗取感情和信任后，随即以资金紧张、家人有难等各种理由骗取钱财。

4. 代购微信诈骗。犯罪分子在微信圈假冒正规商户，以优惠、打折、海外代购为诱饵，待买家付款后，又以“商品被海关扣下需加缴关税”等为由

要求加付款项，实施诈骗。

5. “爱心传递”微信诈骗。犯罪分子将虚构的寻人、扶困帖子以“爱心传递”的方式发送朋友圈，引起善良网民转发，实则帖内所留联系方式绝大多数为外地号码，打过去不是吸费电话就是通信诈骗。

6. “点赞”微信诈骗。犯罪分子冒充商家发布“点赞有奖”信息，要求参与者将姓名、电话等个人资料发至微信平台，一旦套取个人信息后，即以需缴纳“手续费”、“公证费”、“保证金”等形式实施诈骗。



7. 利用公众账号微信诈骗。犯罪分子盗取商家微信公众账号后，发布“诚招网络兼职，帮助淘宝卖家刷信誉，可从中赚取佣金”消息，受害人信以为真，遂按照对方要求多次购物刷信誉，后发现上当受骗。

8. 二维码诈骗。诈骗分子以降价、奖励为诱饵，要求受害人扫描二维码加入会员，实则附带木马病毒，一旦扫描安装，木马就会盗取银行账号、密码等个人隐私信息，实施诈骗。

## 防范支付诈骗的“三不一及时”和“十个凡是”

不法分子实施诈骗的目的是骗取受害人钱财，而诈骗钱财是要通过转账支付来实现的，所以，广大群众只要做到认真学习支付知识，遇到不明支付要求不轻易支付钱款，骗子的阴谋就难以得逞。

### 三不一及时

一是不轻信。绝对不轻信来历不明的电话和短信。不管犯罪分子使用任何花言巧语或恐吓话语，都不要轻易相信，及时挂掉电话，不予回复，如确有担心可及时向亲友或公安机关咨询。

二是不透露。不因贪图小利而受犯罪分子诱惑，任何情况下，切忌向对方透露自己及家人的身份信息、存款、银行卡、密码等信息。如有疑问，可拨打 110 求助咨询，或向亲戚、朋友、同事核实。

三是不转账。绝不向陌生人汇款和转账，尤其是涉及到网银业务的，要格外谨慎。公司财务人员在汇款、转账前，需再三核实转账事由，明确对方银行账户情况。

四是及时报案。确实感觉自己已上当受骗，应第一时间向公安机关报案，提供骗子的银行账户、联系电话等详细情况，以便公安机关及时开展侦破破案工作。

### 十个凡是

1. 凡是自称公检法要求汇款的；
2. 凡是叫你汇款到“安全账户”的；
3. 凡是通知中奖、领取补贴要你预交手续费的；
4. 凡是通知“家属”出事要你汇款帮忙的；
5. 凡是在电话中索要个人信息和银行卡信息的；
6. 凡是叫你开通网银接受检查的；
7. 凡是叫你到宾馆开房接受调查的；
8. 凡是叫你登陆网站查看通缉令的；
9. 凡是自称“领导（老板）”要求汇款的；
10. 凡是陌生网站（链接）要求登记银行卡信息的。

