

1、冒充公检法诈骗：犯罪分子冒充公检法工作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，要求将其资金转入国家账户配合调查。

2、医保、社保诈骗：犯罪分子冒充社保、医保中心工作人员，谎称受害人医保、社保出现异常，可能被他人冒用、

透支，涉嫌洗钱、制贩毒等犯罪，之后冒充司法机关工作人员以公正调查，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购物网站的买家信息，再冒充购物网站的工作人员，声称“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，实则实施资金转账。



4、包裹藏毒诈骗：犯罪分子以事主包裹内被查出毒品为由，称其涉嫌洗钱犯罪，要求事主将钱转到国家安全账户以便公正调查，从而实施诈骗。

5、金融交易诈骗：犯罪分子以某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及走势，获取事主信任后，又引导其在自身搭建的虚假交易平台上购买期货、现货，从而骗取股民资金。

6、票务诈骗：犯罪分子冒充航空公司客服人员以事主“航班取消、提供退票、改签服务”为由，逐步将其引入诈骗圈套，要求多次进行汇款操作，实施连环诈骗。





7、**虚构车祸诈骗**：犯罪分子虚构受害人亲属或朋友遭遇车祸，需要紧急处理交通事故为由，要求对方立即转账。当事人因情况紧急便按照嫌疑人指示将钱款打入指定账户。

8、**虚构绑架诈骗**：犯罪分子虚构受害人亲友被绑架，如要解救人质需立即打款到指定账户并不能报警，否则撕票。当事人往往因情况紧急，不知所措，按照嫌疑人指示将钱款打入账户。

9、**虚构手术诈骗**：犯罪分子虚构受害人子女或老人突发急性病需紧急手术为由，要求事主转账方可治疗。遇此情况，受害人往往心急如焚，按照嫌疑人指示转款。

10、**电话欠费诈骗**：犯罪分子冒充通信运营企业工作人员，向事主拨打电话或直接播放电脑语音，以其电话欠费为由，要求将欠费资金转到指定账户。

11、**电视欠费诈骗**：犯罪分子冒充广电工作人员群拨电话，称以受害人名义在外地开办的有线电视欠费，让受害人向指定账户补齐欠费，否则将停用受害人本地的有线电视并罚款，部分人信以为真，转款后发现被骗。

又被忽悠了，

防不胜防啊！！



12、**购物退税**：犯罪分子事先获取到事主购买房产、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。

13、**猜猜我是谁**：犯罪分子获取受害者的电话号码和机主姓名后，打电话

给受害者，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。随后，编造其被“治安拘留”、“交通肇事”等理由，向受害者借钱，很多受害人没有仔细核实就把钱打入犯罪分子提供的银行卡内。

**14、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，受人雇佣要加以伤害，但事主可以破财消灾，随即提供账号要求受害人汇款。

**15、冒充领导诈骗：**犯罪分子获知上级机关、监管部门单位领导的姓名、办公电话等有关资料，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，让受骗单位先支付订购款、手续费等到指定银行账号，实施诈骗活动。



**16、快递签收诈骗：**犯罪分子冒充快递人员拨打事主电话，称其有快递需要签收但看不清具体地址、姓名，需提供详细信息便于送货上门。随后，快递公司人员将送上物品（假烟或假酒），一旦事主签收后，犯罪分子再拨打电话称其已签收必须付款，否则讨债公司或黑社会将找麻烦。

**17、提供考题诈骗：**犯罪分子针对即将参加考试的考生拨打电话，称能提供考题或答案，不少考生急于求成，事先将好处费的首付款转入指定帐户，后发现被骗。

**18、中奖诈骗—娱乐节目中中奖诈骗：**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消息，称其已被抽选为节目幸运观众，将获得巨额奖品，后以需交手续费、保证金或个人所得税等各种借口实施连环诈骗，诱骗受害人向指定银行账号汇款。



**19、引诱汇款：**犯罪分子以群发短信的方式直接要求对方汇入存款，由于事主正准备汇款，因此收到此类汇款诈骗信息后，未经仔细核实，不假思索即把钱款打入骗子账户。

**20、刷卡消费：**犯罪分子群发短信，以事主银行卡消费，可能系泄露个人信息为由，冒充银联中心或公安民警连环设套，要求将银行卡中的钱款转入所谓的“安全账户”或套取银行账号、密码从而实施犯罪。

**21、高薪招聘：**犯罪分子通过群发信息，以月工资数万元的高薪招聘某类专业人士为幌子，要求事主到指定地点面试，随后以培训费、服装费、保证金等名义实施诈骗。

**22、贷款诈骗：**犯罪分子通过群发信息，称其可为资金短缺者提供贷款，月息低，无需担保。一旦事主信以为真，对方即以预付利息、保证金等名义实施诈骗。

**23、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、预付款等名义骗走钱财。

**24、冒充房东诈骗：**犯罪分子冒充房东群发短信，称房东银行卡已换，要求将租金打入其他指定账户内，部分租客信以为真将租金转出方知受骗。



**25、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的钓鱼网站，进而获取事主银行账户、网银密码及手机交易码等信息实施犯罪。

进而获取事主银行账户、网银密码及手机交易码等信息实施犯罪。

**26、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、海关没收的物品等转让信息，一旦事主与其联系，即以“缴纳定金”、“交易税手续费”等方式骗取钱财。

**27、QQ诈骗—冒充亲友诈骗：**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账号主人对其亲友或好友以“患重病、出车祸”等紧急事情为名实施诈骗。

**28、QQ 诈骗—冒充公司老总诈骗：**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，盗取财务人员使用的 QQ 号码，并分析研判出财务人员老板的 QQ 号码，再冒充公司老板向财务人员发送转账汇款指令。



**29、网购诈骗：**犯罪分子开设虚假购物网站或淘宝店铺，一旦事主下单购买商品，便称系统故障，订单出现问题，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。

**30、订票诈骗：**犯罪分子利用门户网站、旅游网站、百度搜索引擎等投放广告，制作虚假的网上订票公司网页，发布订购机票、火车票等虚假信息，以较低票价引诱受害人上当。随后，再以“身份信息不全”、“账号被冻”、“订票不成功”等理由要求事主再次汇款，从而实施诈骗。

**31、虚构色情服务诈骗：**犯罪分子在互联网上留下提供色情服务的电话，待受害人



与之联系后，称需先付款才能上门服务，受害人将钱打到指定账户后发现被骗。

**32、中奖诈骗—冒充知名企业诈骗：**犯罪

分子冒充三星、索尼、海尔等公司名义，预先大批量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。

**33、中奖诈骗—电子邮件中奖诈骗：**通过互联网发送中奖邮件，受害人一旦与犯罪分子联系兑奖，即以“个人所得税”、“公证费”、“转账手续费”等各种理由要求受害人汇钱，达到诈骗目的。



#### 34、办理信用卡诈骗

**骗：**犯罪分子通过报纸、邮件等刊登可办理高额信用卡的广告，一旦事主与其联系，犯罪分子以“手续费”、“中介

费”、“保证金”等形式要求事主连续转款。

**35、收藏诈骗：**犯罪分子冒充各种收藏协会的名义，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，则以预先交纳评估费、保证金、场地费等名义，要求受害人将钱转入指定帐户。

**36、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，诱使银行卡用户在卡被吞后与其联系，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。

**37、伪基站诈骗：**犯罪分子利用伪基站向广大群众发送网银升级、10086移动商城兑换现金的链接，一旦点击后便在事主手机上种植获取银行账号、密码和手机号的木马，从而进一步实施犯罪。

#### 38、海德诈骗—伪装身份诈骗

**骗：**犯罪分子利用海德“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。



**39、海德诈骗—代购诈骗：**犯罪分子在海德圈假冒正规微商，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，要加缴关税”等为由要求加付，一旦获取购货款则无法联系。

40、**海德诈骗—爱心传递诈骗**：犯罪分子将虚构的寻人、扶困的帖子以“爱心传递”的方式发发布朋友圈里,引起不少善良网民转发,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讯诈骗。

41、**海德诈骗—点赞诈骗**：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海德平台,一旦商家套取完足够的个人信息后,即以“手续费”、“公证费”“、“保证金”等形式实施诈骗。

42、**海德诈骗—利用公众账号诈骗**：犯罪分子盗取商家公众账号后,发布“诚招网络兼职,帮助淘宝卖家刷信誉,可从中赚取佣金”的推送消息。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。

43、**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

