近年来，电信网络诈骗案件持续高发，引起社会高度关注。电信诈骗，让人不胜其害、也让人不
堪其扰，在受害者中有人倾
家荡产，也有人家破人亡。
骗子下了哪些套
子？钻了哪些空子？我们该怎样
识别，如何预防？今天小编为大家起底电信诈骗伎俩和反诈骗技能。

★ 63种诈骗伎俩 ★

1、QQ冒充好友诈骗

利用木马程序盗取对方QQ密码，截取对方聊天视频资料，熟悉对方情况后，冒充该QQ账号主人对其QQ好友以“患重病、出车祸”“急需用钱”等紧急事情为由实施诈骗。

2、QQ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。

3、微信冒充公司老总

诈骗财务人员

犯罪分子通过技术手段获取公司内部人员架构情况，复制公司老总微信昵称和头像图片，伪装成公司老总添加财务人员微信实施诈骗。

4、微信伪装身份诈骗

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”，加为好友骗取感情和信任后，随即以资金紧张、家人有难等各种理由骗取钱财。

5、微信假冒代购诈骗

犯罪分子在微信朋友圈假冒正规微商，以优惠、打折、海外代购等为诱饵，待买家付款后,又以“商品被海关扣下,要加缴关税”等为由要求加付款项，一旦获取购货款则失去联系。

6、微信发布虚假爱心传递诈骗

犯罪分子将虚构的寻人、扶困帖子以“爱心传递”方式发布在朋友圈里,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电信诈骗。

7、微信点赞诈骗

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微信平台，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。

8、微信盗用公众账号诈骗

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。

9、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提供服务，受害人将钱打到指定账户后发现被骗。

10、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。

11、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。

12、冒充知名企业中奖诈骗

犯罪分子冒充三星、索尼、海尔等知名企业名义，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，后以需交手续费、保证金或个人所得税等各种借口，诱骗受害人向指定银行账号汇款。

13、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。

14、冒充公检法电话诈骗

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等犯罪为由，要求将其资金转入国家账户配合调查。

15、冒充房东短信诈骗

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。

16、虚构绑架诈骗

犯罪分子虚构事主亲友被绑架，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。

17、虚构手术诈骗

犯罪分子虚构受害人子女或老人突发急病需紧急手术为由，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。

18、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。

19、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。

20、退款诈骗

犯罪分子冒充淘宝等公司客服拨打电话或者发送短信谎称受害人拍下的货品缺货，需要退款，要求购买者提供银行卡号、密码等信息，实施诈骗。

21、购物退税诈骗

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。

22、网络购物诈骗

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，卡上金额即被划走。

23、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。

24、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，犯罪分子则以“手续费”、“中介费”、“保证金”等虚假理由要求事主连续转款。

25、刷卡消费诈骗

犯罪分子群发短信，以事主银行卡消费，可能个人泄露信息为由，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。

26、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。

27、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。

28、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。

29、补助、救助、助学金诈骗

犯罪分子冒充民政、残联等单位工作人员，向残疾人员、困难群众、学生家长打电话、发短信，谎称可以领取补助金、救助金、助学金，要其提供银行卡号，然后以资金到帐查询为由，指令其在自动取款机上进入英文界面操作，将钱转走。

30、引诱汇款诈骗

犯罪分子以群发短信的方式直接要求对方向某个银行帐户汇入存款，由于事主正准备汇款，因此收到此类汇款诈骗信息后，往往未经仔细核实，即把钱款打入骗子账户。

31、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。

32、收藏诈骗

犯罪分子冒充各类收藏协会的名义，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。

33、机票改签诈骗

犯罪分子冒充航空公司客服以“航班取消、提供退票、改签服务”为由，诱骗购票人员多次进行汇款操作，实施连环诈骗。

34、重金求子诈骗

犯罪分子谎称愿意出重金求子，引诱受害人上当，之后以诚意金、检查费等各种理由实施诈骗。

35、PS图片实施诈骗

犯罪分子收集公职人员照片，使用电脑合成淫秽图片，并附上收款卡号邮寄给受害人，勒索钱财。

36、“猜猜我是谁”诈骗

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，一些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。

37、冒充黑社会敲诈类诈骗

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，然后提供账号要求受害人汇款。

38、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。

39、高薪招聘诈骗

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。

40、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。

41、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诈骗。

42、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。

43、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。

44、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。

45、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虚假链接，一旦受害人点击后便在其手机上植入获取银行账号、密码和手机号的木马，从而进一步实施犯罪。

46、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，又引导其在自身的搭建虚假交易平台上购买期货、现货，从而骗取事主资金。

47、兑换积分诈骗

犯罪分子拨打电话谎称受害人手机积分可以兑换智能手机，如果受害人同意兑换，对方就以补足差价等理由要求先汇款到指定帐户；或者发短信提醒受害人信用卡积分可以兑换现金等，如果受害人按照提供的网址输入银行卡号、密码等信息后，银行账户的资金即被转走。

48、二维码诈骗

犯罪分子以降价、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,木马就会盗取受害人的银行账号、密码等个人隐私信息。

49、假冒领导诈骗

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，让受害人单位先支付订购款、手续费等到指定银行账号，实施诈骗活动。

50、虚构羁押诈骗

犯罪分子虚构受害人子女嫖娼、打架等事由被公安机关羁押（无法直接通话，只能以短信方式联系），要求事主转账缴纳羁押保证金。受害人子女一般为大学生，犯罪分子多选用受害人子女考试期间进行诈骗，受害人在无法电话联系子女情形下，往往按照嫌疑人指示转款。

在诈骗犯罪中，还有一类非法集资型诈骗行为，由于其伪装成真人真事真项目，往往能够将人骗的血本无归。

51、以境外公司名义，虚假宣传所谓投资境外理财、黄金、期货等项目，有的在境外，如港澳台、东南亚国家的高档酒店召开“投资”推介会；

52、收款账户系以外国人名义在境内开立的账户，用于接收投资人的投资款；

53、许诺高收益的公司的网站注册地、服务器所在地在境外或公司高管系外国人，进行虚假宣传的；

54、以网络虚拟货币升值、现货交易、资金互助、黄金、贵金属、期货、外汇交易等为噱头，引诱投资人投资，尤其是鼓励发展他人并给予提成；

55、频繁变换网站名称、投资项目；

56、公司网站无正式备案；

57、以个人账户或现金收取资金、现场或即时交付本金即给予部分提成、分红、利息；

58、许诺超高收益率，尤其是许诺“静态”“动态”收益；

59、明显超出公司注册登记的经营范围，尤其是没有从事金融业务资质；

60、在街头、超市、商场等人群流动、聚集场所摆摊、设点发放“理财产品”广告，尤其以中老年人为主要招揽对象。

当然，我们更不能忽略了传销型诈骗。

61、编造或者歪曲的国家或

区域发展政策

比如“国家试点”“西部大开发”“北部湾建设”“资本运作”“1040工程”“阳光工程”等；

62、打着“改革创新”经营、

投资模式的幌子

比如“电子商务”“消费返利”“连锁销售”“连锁加盟”“特许经营”“网络游戏”“点击广告获利”“慈善事业”“爱心互助”“消费养老”“境外基金、原始股投资”、电子币买卖等；

63、声称高收益

包括：静态收益、动态收益、直推奖、层推奖、对碰奖、见点奖、领导奖、培育奖、报单奖、管理奖、小区业绩奖等。

★ 9大防诈骗技能★

1、查验“可信网站”

通过第三方网站身份诚信认证辨别网站真实性。不少网站已在网站首页安装了第三

方网站身份诚信认证——“可信网站”，可帮助网民判断网站的真实性。

“可信网站”验证服务，通过对企业域名注册信息、网站信息和企业工商登记信息进行严格交互审核来验证网站真实身份，通过认证后，企业网站就进入中国互联网络信息中心（CNNIC）运行的国家最高目录数据库中的“可信网站”子数据库中，从而全面提升企业网站的诚信级别，网民可通过点击网站页面底部的“可信网站”标识确认网站的真实身份。

网民在网络交易时应养成查看网站身份信息的使用习惯，企业也要安装第三方身份诚信标识，加强对消费者的保护。

2、核对网站域名

假冒网站一般和真实网站有细微区别，有疑问时要仔细辨别其不同之处，比如在域名方面，假冒网站通常将英文字母I被替换为数字1，CCTV被换成CCYV或者CCTV－VIP这样的仿造域名。

3、比较网站内容

假冒网站上的字体样式不一致，并且模糊不清。仿冒网站上没有链接，用户可点击栏目或图片中的各个链接看是否能打开。

4、查询网站备案

通过ICP备案可以查询网站的基本情况、网站拥有者的情况，对于没有合法备案的非经营性网站或没有取得ICP许可证的经营性网站，根据网站性质，将予以罚款，严重的关闭网站。

5、查看安全证书

大型的电子商务网站都应用了可信证书类产品，这类的网站网址都是“https”打头的，如果发现不是“https”开头，应谨慎对待。

2016年1月至2016年3月阿里云誉反欺诈系统共检出拦截钓鱼网站59567个，涉及钓鱼url总计81089个。钓鱼网站通常会在境外注册域名规避网络监管。

6、掌握官方联系方式

掌握余额宝、零钱宝、理财通等网络金融理财产品的官方客服联系方式，对通过百

度搜索出的官方网站或客服电话等信息保持谨慎态度。

7、慎点连接

余额宝等网络金融理财产品的用户不要点击陌生人发送的链接、压缩包；收到后缀为.apk的文件应警惕，不要点击下载。

8、注意保护个人密码

出售或外借电脑时，务必清理电脑中的个人隐私内容，特别是常用的账号和密码。

9、谨防电脑病毒手机木马

在日常使用中，勿保存网银、支付宝等账号密码；一旦电脑中木马，应立即在安全的电脑上(不要在已中木马的电脑上)修改账户密码，同时致电相关客服确认安全。