谨防电信诈骗

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。

一、48 种常见电信诈骗犯罪案件

电信诈骗团伙中，有专门成员负责编写诈骗剧本，紧跟社会热点，针对不同群体，量身定做、精心设计、编制骗术，其犯罪类型多，手段变化快。

为有效开展预防打击工作，公安部刑侦局归纳出 48 种常见的电信诈骗犯罪案件，其中，使用电话类的占 63.3%，使用短信占 14.8%，使用网络的占 19.6%。

48 种案件类型如下：

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。

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,然后以资金到账查询为由,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账户汇入存款,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账户。

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账户,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账户;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。

二、近期高发的十类电信网络新型违法犯罪手段

骗术一：假冒公检法诈骗

犯罪分子假冒“警官”、“检察官”、“法官”等角色，谎称受害人涉嫌洗钱、贩毒等严重犯罪，诱导受害人将资金转入实为骗子持有的所谓“安全账户”，此类诈骗造成损失金额最大。

公安机关提醒：警方不会通过电话做笔录，逮捕证由警方在逮捕现场出示，不会通过传真发放，更不会在网上查到。公检法机关从未设立所谓的“安全账户”，更不会通过电话安排当事人转账汇款到“安全账户”。

骗术二：冒充熟人诈骗

犯罪分子通过非法渠道，获得受害人熟悉的亲友的手机号码、社交账号密码，并掌握受害人的社会关系，从而骗取受害人信任，进而编造“发生意外急需用钱”“资金周转”“代缴话费”等理由，诱使受害人转账。

公安机关提醒：凡是亲友间涉及借款、汇款等问题，一定要通过拨打对方常用号码，或者视频聊天等方式核实对方身份后再做决定。

骗术三：利用伪基站发送木马链接实施诈骗

犯罪分子使用“伪基站”，冒用银行、运营商等客服电话号码发送短信给受害人，以账户积分兑换奖品等为由诱导受害人点击短信中的木马链接。用户一旦点击，犯罪分子就能在后台获取用户的银行账户信息和密码，进而盗取其账户资金。

公安机关提醒：当收到“银行卡密码升级”、“积分兑换”、“中奖”等含有链接的短信时，要通过银行、运营商的官方网站或客服电话进行核实，不要轻易点击短信中的链接。

骗术四：兼职诈骗

犯罪分子许诺在各种网络平台刷得消费记录后，将返还本金并支付佣金。受害人在完成前几单任务后都会很快收到回报，而当做更多的任务时，骗子就会切断与受害人的联系，就此消失。

公安机关提醒：求职者不要轻信网络上“高佣金”“先垫付”等兼职工作，不要轻信没有留固定电话和办公地址的招聘广告。

骗术五：考试诈骗

犯罪分子通过非法手段获得考生信息，并有针对性的发送短信或邮件，声称“提供考题”“改分”“办假证”等，引诱考生汇款。

公安机关提醒：漏题、改分、改档案、伪造资格证等行为本身就是非法的，请坚持用自己的实力说话。

骗术六：校园贷诈骗

校园贷诈骗的形式主要有三种：一是用“免抵押、低利息”为诱饵诱导学生贷款，并要求缴纳贷款手续费、管理费、保证金等费用；二是声称能通过培训提高综合技能，夸大培训效果，签订培训合同，诱导学生贷款支付学费；三是与兼职诈骗结合，要求学生贷款购买手机等产品做“销售代理”。这些贷款的利息和滞纳金很高，学生如不能如期还款，将迅速背上难以承受的债务压力。

公安机关提醒：学生在申请借款或分期购物时，要衡量自己是否具备还款能力。对于关乎自身信息、财产安全的事，要多方求证，不要轻易相信他人的一面之词，轻易透露个人信息，甚至将身份证借与他人使用。发现危险,及时报警。

骗术七：民族资产解冻骗局

犯罪分子先编造一个民族资产秘密流落海外的故事，然后声称受国家委托对这些海外资产进行解冻，号召受害人缴纳手续费或资料费，称成功后每人可以拿到高额善款补助。除了“民族资产解冻”，犯罪分子还会编造所谓“养老”、“扶贫”等噱头来吸引投资实施诈骗。

公安机关提醒：此类诈骗的受害人多为中老年人，他们远离社会舆论，缺乏辨别诈骗的能力，年轻人要多关爱长辈，及时传达安全防范知识。此外，留意父母长辈的网络支付使用情况，保障财产安全，及时止损。

骗术八：投资返利诈骗

此类骗局通常标榜具有海外背景，从事的行业能赚取巨额利润，投资者将会获得高额投资回报。投资初期，犯罪分子会按时返利，让投资者尝到甜头，继续追加投资后，将会血本无归。

公安机关提醒：投资理财前，要对所投资的项目进行了解，多咨询评估，做到深思熟虑，谨慎对待。特别要警惕网络上各类标榜“低投入、高收益、无风险”的投资理财项目，切勿盲目追求高息回报，谨防被骗。

骗术九：保健品购物诈骗

犯罪团伙假扮医疗机构的顾问、专家、教授等，以为老年人“问诊”为名夸大病情，再以会员登记、免费体验、国家补贴、中奖等噱头诱骗客户购买各类保健品。而这些“保健品”基本上都粗制滥造，成本低廉却以高价出售。

公安机关提醒：经常给家中老人说一些老人被诈骗的例子，让他们不要相信保健品推销，一旦发现受骗要立即报警。

骗术十：引诱裸聊敲诈勒索

犯罪分子非法获得被害人信息后，通过社交软件建立联系，步步引诱受害人进行“裸聊”，从而获取受害人不雅照片、视频，以此敲诈受害人。

公安机关提醒：应远离网络不良行为，不向陌生人泄露身份和家庭等敏感信息。

三、如何防范电信诈骗

根据公安部有关发布信息，防范电信诈骗，社会公众应注意提高防范意识。

1、不轻信：不要轻信来历不明的电话和手机短信，不管不法分子使用什么甜言蜜语、花言巧语，都不要轻易相信，要及时挂掉电话，不回复手机短信，不给不法分子进一步布设圈套的机会。

2、不透露：巩固自己的心理防线，不要因贪小利而受不法分子或违法短信的诱惑。无论什么情况，都不向对方透露自己及

家人的身份信息、存款、银行卡等情况。如有疑问，可拨打 110 求助咨询，或向亲戚、朋友、同事核实。

3、不转账：学习了解银行卡常识，保证自己银行卡内资金安全，决不向陌生人汇款、转账。据公安机关所作抽样调查统计，从受害者性别上看，女性占 70%以上；从年龄上看，中老年人超过 70%。因此，中老年人和妇女同志要格外引起注意。还有一些公司财务人员和经常有资金往来的人群等，在汇款、转账前，要再三核实对方的账户，不要让不法分子得逞。

4、要及时报案：万一上当受骗或听到亲戚朋友被骗，请立即向公安机关报案，可直接拨打 110，并提供骗子的账号和联系电话等详细情况，以使公安机关开展侦查破案。

防范诈骗须做到“四要四不要”：

“四要”指的是:

转账前要通过电话等方式核实确认;

手机和电脑要安装安全软件;

QQ、微信要开启设备锁及账号保护，提高账户安全等级;

网上聊天时要留意系统弹出的防诈骗提醒。

“四不要”指的是:

不要连接陌生 WIFI，有些 WIFI 容易导致支付账号密码被盗;

不要向他人透露短信验证码;

不要将支付密码与账号登陆密码设为同一个;

不要将身份证等个人身份信息保存在手机里。

防范电信诈骗口诀

电信诈骗种类多，陌生来电需警惕，

积分兑换莫轻信，网银过期有猫腻，

欠费通知要核实，了解清楚也不迟，

短信链接慎点击，个人信息勿录入，

朋友借钱见面谈，未经核实不转款，

不给不要不贪心，电信诈骗不缠身。