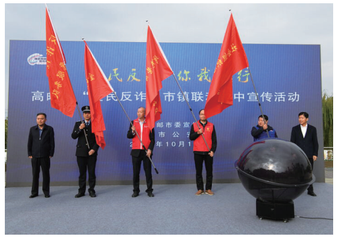

今日高邮微信
高邮日报手机报
在线投稿:http://tg.gytoday.cn 新闻热线:84683100 QQ:486720458
详情请浏览“今日高邮”网站 http://www.gytoday.cn




今日高邮微信
高邮日报手机报
在线投稿:http://tg.gytoday.cn 新闻热线:84683100 QQ:486720458
详情请浏览“今日高邮”网站 http://www.gytoday.cn

# 全民反诈 你我同行



为切实营造全社会防骗识诈反诈的良好氛围，增强人民群众反诈意识，近日，我市分别在净土寺塔广场主会场、各派出所分会场举行以“全民反诈 你我同行”为主题的全市“全民反诈”市镇联动集中宣传活动启动仪式。市委常委、宣传部部长杨文喜，副市长、公安局局长万圣托出席净土寺塔广场主会场活动。

在主会场，市公安局相关负责人详细说明了“全民反诈”市镇联动集中宣传活动的背景、重要意义，并动员号召全社会利用一切资源和力量，迅速掀起“全民反诈、全社会反诈”新高潮。市“红星平安哨工队伍”队员代表市反诈宣传社会组织作表态发言。市委常委、宣传部部长杨文喜，副市长、公安局局长万圣托分别向反诈宣传公安志愿服务队、反诈宣传金融机构志愿服务队、反诈宣传通信运营商志愿服务队、反诈宣传社会组织志愿服务队授旗，并与市委宣传部、市公安局负责人共同启动水晶球。

整个活动采取拉横幅、设立咨询台、竖立戗牌、摆放宣传展板、播放专题宣传片、现场咨询问答、发放宣传资料，以及组织开展进社区、进学校、进乡镇、进市场、进网站、进金融机构“六进”活动等多种形式进行。广泛传授讲解防范电信网络诈骗犯罪知识，揭露曝光“电诈”犯罪伎俩，警示叮嘱广大群众认清骗局，捂好自己的钱袋子，谨防上当受骗。通过此次集中现场活动，进一步扩大社会影响力，收到了良好的宣传效果和社会效果。

# 市公安机关多措并举 强力打击电信网络诈骗

近日，市公安局破获系列冒充老师收缴教材费实施诈骗的案件。嫌疑人将头像、昵称换成与班主任一模一样，非法进入班级群中实施诈骗，许多家长没细看便转了账。9月2日，接到报警后，市公安局刑警大队立即对该案进行立案侦查。因嫌疑人收完钱就退群，隐蔽性较强，诈骗资金流向层级多，案件侦破难度较大。办案民警抽丝剥茧，持清思路，经过不懈的努力，终于发现嫌疑人行动轨迹，迅速赶往广州市对嫌疑人实施抓捕。经过连夜蹲守，9月26日，警方将两名犯罪嫌疑人成功抓获。9月28日，犯罪嫌疑人将全部赃款退回。该起案件只是我市公安机关强力打击治理电信网络诈骗犯罪的一个缩影。

近年来，市公安局认真贯彻落实习近平总书记关于打击治理电信网络诈骗犯罪工作的重要指示精神，坚持以人民为中心，以党史学习教育“我为群众办实事”实践活动为载体，主动担当作为，不断夯实各项打防管控工作，全力遏制电信网络犯罪高发态势。截至目前，我市接报涉及电信诈骗案件由去年的升幅27.6%转为下降31.1%，取得了阶段性的成效。今年以来，警方又侦破一批有影响的案件，打掉电信网络诈骗犯罪团伙26个，依法对200余名涉嫌电信网络诈骗犯罪嫌疑人采取强制措施，为群众挽回经济损失400余万元。

在打击治理电信网络诈骗犯罪的同时，我市警方还通过加大宣传力度，强化源头预警，先后组织社区民警、平安哨工开展进机关、进学校、进店铺、进市场、进工地、进社区，利用“大篷车”“小喇叭”播放“防诈”语音，利用大型商场超市、公交站台、派出所、警务室的公告栏、宣传橱窗、LED显示屏等载体，发布防诈小知识、技巧，做到防范宣传处处可见。同时，充分运用现代融媒体手段，通过电台、电视台、公安门户网站、微博、微信公众号、抖音等媒介，发布防诈小视频、小案例，推广注册安装“国家反诈中心APP”，多维度、多层次向群众普及反诈防范常识。今年以来，我市警方共走访单位企业行业家庭6万余家次，利用快递包裹张贴宣传即时贴10万余份，发放各类反诈骗宣传单10余万份，通过公安短信平台发送防诈宣传短信90余万条。

市公安局反诈中心还建立常态化拦截封堵机制，开展全方位、有针对性的拦截阻断。发现正在被侵害人员，反诈中心及时开展短信提醒、电话劝阻，对尚未警觉、已被“洗脑”甚至准备转账的高危潜在被侵害人，立即指派社区民警上门开展见面劝阻处置工作。今年以来，已累计发送精准预警提醒短信1万余条，拨打劝阻电话3万余人次，社区民警上门见面劝阻4000余人次；定期召开三大通信运营商、人行等相关联席部门座谈会，加强对电话卡、银行卡“两卡”的开办、监管和惩戒工作。对国务院联席办下发的涉案“两卡”线索逐条组织人员查证，搜集证据，组织打击。据悉，截至目前共打掉“黑灰产”犯罪团伙12个，抓获帮信嫌疑人160余名，缴获手机卡、银行卡1000余张。

同时，针对电信网络诈骗案件高发势头，市公安局依托大数据，统筹反诈中心、刑侦、网侦等相关部门，利用优势资源组建研判、打击工作专班，创新打击模式，建立同步上案、快速反应工作机制。专班坚持“每案必研、每案必侦、每案必追”，集中力量形成工作合力，全力打打团伙、斩链条、端窝点、追赃款，进一步促进警种协同作战，提升打击效能。

# 电信诈骗防范小课堂

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。

尽管公安机关开展了持续不断地打击，但是受各种因素的影响，电信网络新型违法犯罪活动仍然快速发展蔓延，形势严峻，危害突出。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%。

**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。

**如何应对电信诈骗，高邮市公安局提醒广大市民：**

**八个“凡是”都是诈骗！ 切勿上当！**

1、凡是自称公检法要求汇款的都是诈骗！

2、凡是叫你汇款到“安全账户”的都是诈骗！

3、凡是通知中奖、领取补贴要你先交钱的都是诈骗！

4、凡是通知“家属”出事要先汇款的都是诈骗！

5、凡是索要个人和银行卡信息及短信验证码的都是诈骗！

6、凡是让你开通网银接受检查的都是诈骗！

7、凡是自称领导或老板要求打款的都是诈骗！

8、凡是陌生网站或链接要登记银行卡信息的都是诈骗！


**与此同时，我们还要做到七个“一律”：**

1、陌生人来电话，只要一谈到银行卡信息，一律挂掉！

2、只要一谈到中奖，先预付款，一律挂掉！

3、只要一谈到公检法税务或领导干部的，一律挂掉！

4、所有短信，但凡让我点击链接的，一律删掉！

5、所有微信不明链接，一律不点！

6、所有不熟悉的170开头的电话一律不接！

7、一提到“安全帐户”的一律不转！


**归根结底就是要做到“三不一及时”：**

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；单位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。