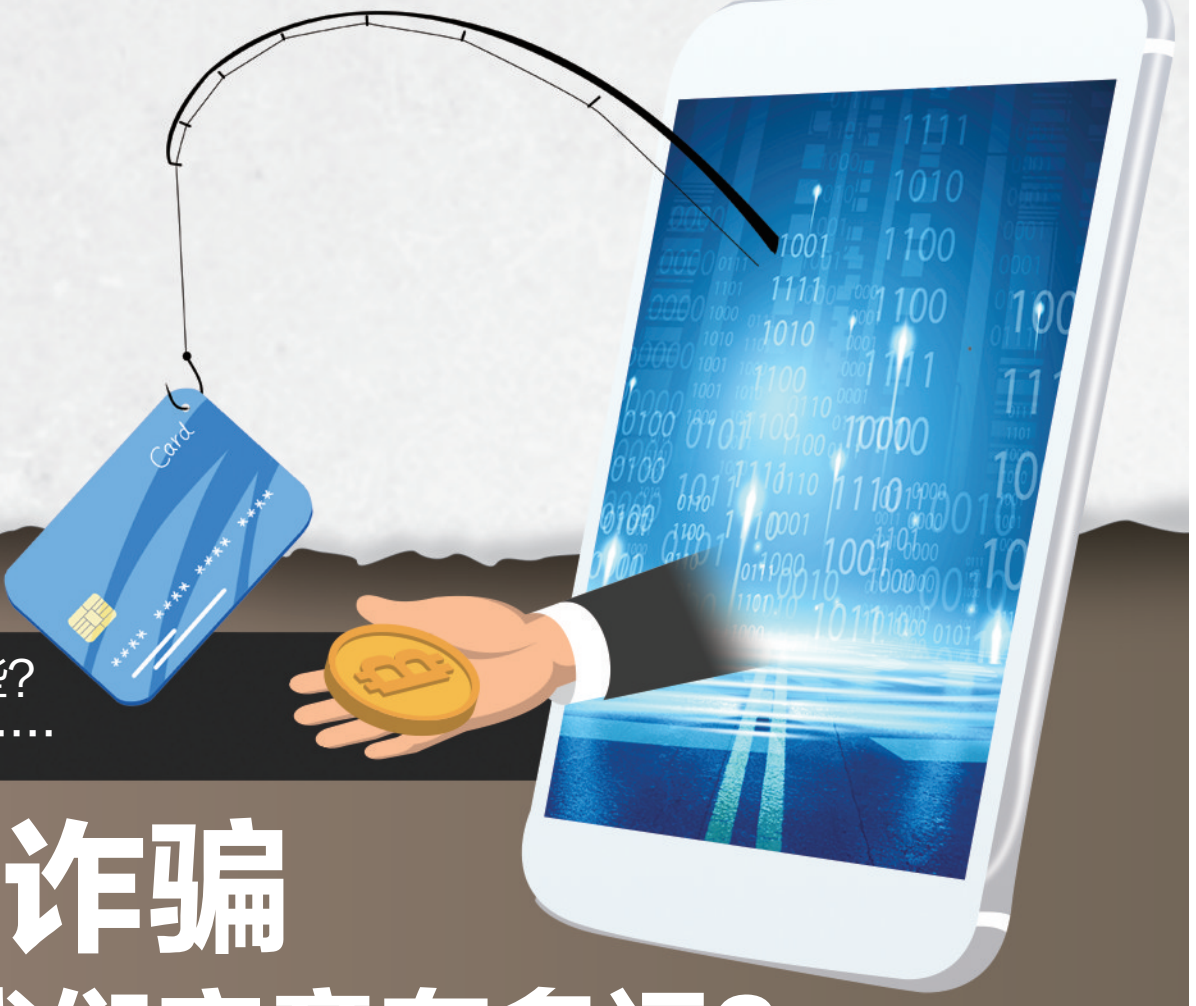
电信网络诈骗离我们究竟有多远？常见诈骗形式有哪些？如何更好地防范电信网络诈骗？带着大家关心的电信网络诈骗话题，近日，记者来到我市电信部门进行了采访。

■融媒体记者 秦艳艳 通讯员 李栋



电信网络诈骗常见形式有哪些？哪些群体易受骗？如何防范……

电信网络诈骗离我们究竟有多远？

何为电信网络诈骗？

在我们日常生活中，大家有没有接到一些陌生来电呢？这些来电号码所属地一般显示为非本地，多为全国其他不同城市，同时还会被手机自动标注上“疑似诈骗”“骚扰电话”等红色字样。市电信部门工作人员提醒广大市民，这些陌生来电一般多为电信网络诈骗分子的诈骗来电，不要轻易接通。如不小心接通后，市民更应保持高度警惕，小心上当受骗。

那么，何为电信网络诈骗？市电信部门工作人员解释，电信网络诈骗，是以非法占有为目的，利用电信网络技术等手段，通过远程、非接触的方式，骗取公私财物的行为。记者从市电信部门获悉，2023年度我市电信网络诈骗涉案涉诈数量呈明显下降趋势。据介绍，淮安电信部门上半年向公安反诈中心提供电信网络诈骗线索134条，打击18次，抓获36名诈骗嫌疑人。

典型诈骗类型有哪些？公安部公布十类高发电信网络诈骗案件，分别是刷单返利、虚假投资理财、虚假网络贷款、冒充电商物流客服、冒充公检法、婚恋交友、网络游戏产品虚假交易、虚假购物服务、虚假征信、冒充领导熟人类诈骗。市电信部门工作人员表示，在我市发生的电信网络诈骗案件中，典型诈骗类型有刷单返利诈骗、“杀猪盘”诈骗、冒充电商物流客服诈骗、冒充领导熟人诈骗、冒充“公检法”诈骗、虚假购物服务诈骗、注销“校园贷”诈骗等。其中，刷单返利诈骗发案占比最高，虚假投资理财诈骗涉案金额最多。

如何防范电信网络诈骗？

如何更好地远离电信网络诈骗？市电信部门工作人员建议广大市民，在日常生活中，为了快速甄别来电情况，可在手机中下载安装“国家反诈中心”App，并打开“来电预警”功能，同时还要做好个人信息安全防护，不断提高反诈意识和辨别能力。

注意避免个人资料外泄。妥善保护好个人姓名、身份证号码、电话号码、银行卡号等基本信息，对不熟悉的金融业务尽量不在ATM机上操作，应直接到柜面现场办理，切勿相信“银行账户涉及犯罪”等谎言。及时提醒家里的中老年人要保护好家庭各类信息，中老年人遇到不明白的事不要急于做决定，可先和家人联系、沟通，防止受骗。

不要轻信陌生电话和短信。当接到疑似诈骗电话或短信时，注意核实对方身份，尤其是对方要求向指定账户汇款时，不要轻易汇款，应第一时间告知家属商量解决或咨询公安机关。接到陌生电话、短信或不良信息，要主动向属地公安机关或电信监管部门举报。未成年人使用手机时，建议不外借给不熟悉的人，不以发送陌生短信而赚钱，不扫描陌生二维码。

注意陌生来电电话类型。对于冒充各类工作人员直接打电话进行诈骗的，一定要注意来电显示的电话类型。对于一些不熟悉、非正常手机号码的电话，尤其是境外电话号码，须谨慎接听。以95开头的电话号段，只要不是银行客服电话，建议直接拒接。以400、800开头的电话号段，也是骚扰电话重灾区，很多企业或个人常利用这些电话进行推销，要谨慎接听。

正确辨别96110来电。96110为反电信网络诈骗专用号码，专门用于对群众的预警劝阻和防范宣传等工作。然而，96110有可能会被诈骗分子加上前缀、后缀、引号或其他符号等来混淆，应注意甄别。另外，地区区号+96110，如哈尔滨0451-96110，这样的来电大家请放心接听，耐心听取劝阻员的劝阻，避免上当受骗。“12381”为劝阻短信号码，短信应仔细阅读。

新闻多一点

典型电信网络诈骗类型

为方便广大市民在日常生活中对照辨析，市电信部门工作人员梳理出以下常见网络诈骗类型基本情况及作案手法，希望引起广大市民警惕。

类型1：刷单返利诈骗

作案手法：第一步，诈骗分子通过网页、招聘平台、QQ、微信等渠道发布兼职信息，招募人员进行网络兼职刷单，承诺在交易后立即返还购物费用并额外提成，并以“投入无风险”“日清日结”等方式诱骗；第二步，刷第一单时，诈骗分子会小额返款让对方尝到甜头，当刷单交易额变大后，诈骗分子就会以各种理由拒不返款，并将对方拉黑。

类型2：“杀猪盘”诈骗

作案手法：第一步“寻猪”，诈骗分子伪装为成功人士，通过婚恋网站、网络社交工具寻觅、物色诈骗对象，与其聊天交友，确定男女朋友、婚恋关系，甚至远程下单赠送昂贵礼品，取得对方信任；第二步“诱猪”，诈骗分子推荐博彩网站或赌博App，谎称系统存在漏洞、有内幕消息等，投注便能稳赚不赔，甚至先提供账号让对方帮忙管理体验，从而诱导对方投注；第三步“养猪”，当对方少量投注时，回报率高，提现快，让对方逐渐产生贪婪欲望，进而加大投注金额；第四步“杀猪”，对方在投入大额资金后发现网站或App账户里的资金无法提现，或在投注过程中全部输掉，此时才发现自己已被拉黑。

类型3：冒充电商物流客服诈骗

作案手法：第一步，诈骗分子冒充购物网站客服工作人员给对方打电话，说出对方个人信息，谎称对方购买的产品质量有问题，需要为其进行退款赔偿；第二步，诱导对方在虚假退款理赔网页填入个人银行卡号、手机号、验证码等信息，从而将其银行卡内的钱款转走，或利用对方对支付宝、微信等支付工具中借款功能的不熟悉，诱导对方从中借款，然后转给诈骗分子。

类型4：冒充熟人或领导诈骗

作案手法：第一步，“领导”主动添加好友，诈骗分子通过非法渠道获取对方的手机通讯录和相关信息，冒充相关“领导”，通过微信或QQ添加对方为好友；第二步，“暖心关怀”骗取信任，诈骗分子用关心下属的口吻，降低对方的戒备之心，甚至还会主动提出帮助对方解决困难，让对方对个人事业发展浮想联翩；第三步，花式理由要求转账，当对方感觉与“领导”更亲近时，诈骗分子趁势而为，向对方提出转账汇款要求，转账理由多种多样，比如借钱、送礼、请客等。

类型5：虚假投资理财诈骗

作案手法：第一步，诈骗分子通过网络社交工具、短信、网页发布推广股票、外汇、期货、虚拟货币等投资理财信息；第二步，诈骗分子与对方取得联系后，通过聊天交流投资经验，拉入“投资”群聊，听取“投资专家”“导师”直播课等，以有内幕消息、掌握漏洞、回报丰厚等谎言取得对方信任；第三步：诱导对方在其提供的虚假网站或App投资，初步小额投资试水，回报利润高，取得进一步信任，再诱导对方加大投入；第四步，当对方在投入大量资金后，发现无法提现或全部亏损，在沟通交涉时发现被拉黑，或投资理财网站、App无法登录。