

应急救援大队 2024 年 1 季度平安建设

防范电信诈骗知识宣传教育

紧绷防范之弦 远离诈骗之害

一、什么是“电信诈骗”？

电信诈骗就是违法犯罪份子利用手机短信、电话、传真和互联网等通讯工具，假冒国家机关、公司、医院、朋友等名义，谎称被骗人中奖、退税、家人意外受伤、朋友急事、有人加害或出售致富信息和投资分红等情况，骗取受害人信任后，叫其将钱汇入到指定银行卡账户的一种诈骗活动。

二、电信诈骗的各种手段和花样

1. 退税诈骗

犯罪份子通过非法渠道获悉购车人的电话号码后，冒充国家税务机关工作人员打电话给购车人谎称要退车购税，诱骗购车人到自动柜员机（ATM、CRS 等）上按其指令操作以此骗走购车人银行卡上的存款。

2. 中奖诈骗。

犯罪份子假冒公司工作人员或者公证处工作人员，以手机短信、打电话、电子邮件、QQ、MSN 等方式向受害人谎称其中大奖，叫受害人将“所得税”、“公证费”、“手续费”及“风险抵押金”等存入其指定银行账号，其再向受害人兑现支付“奖金”，以此骗取受害人钱款；部分犯罪团伙雇用人员到我市城乡推销奖票或附有刮奖的产品宣传单，受害人刮开后大多都会中 10 万或 20 万以上的巨额大奖，犯罪分子又慌称以“支票”形式全额兑现“大奖”，叫受害人将“中

奖所得税”、“公证费”、“手续费”及“风险抵押金”等存入其指定银行账号，以此骗取受害人的钱款。

案例 1

(1)、1月4日，牛某（女、21岁）报称：下载“交易猫”平台进行游戏账号收购操作，对方以出售游戏账号需缴纳保险和押金为由，诱骗其转账 3499.5 元。

(2)、1月4日，杜某（男、40岁）报称：下载“Mapat”刷单 APP，在对方诱导下做助力返现任务时，被骗 229507.5 元。已安装国家反诈 APP，接受过反诈宣传，接到预警电话后已完成转

(3)、1月4日，魏某（女、61岁）报称：下载“捷信”APP 申请贷款时，被骗 6000 元。

(4)、1月4日，王某（男、39岁）报称：通过“快手”APP 认识一男子学习股票，在对方的指导下通过下载“中证大户室”APP 向对方提供的银行账户转账 50000 元，后发现被骗。

3. 培训诈骗

犯罪份子假冒消防、税务、工商、海关等国家机关、伪造国家机关公文，以传真形式向公司、企业等单位发“培训通知”，要求其派员参加培训，并叫公司、企业将“培训费”打到其指定的银行卡账户上，以骗取钱款。

4. 家人遭遇意外诈骗

犯罪份子通过不法手段获悉受害人及其在外地打工、学习、经商的家人的电话号码，先故意电话滋扰身在外地的家

人，待其不耐烦而关机后，犯罪份子迅速打通受害人电话，假冒医院领导、警察、老师、朋友的名义，谎称其在外地的家人意外受伤害（如出车祸、被人打伤、被人绑架）或突然患疾病急需抢救治疗，叫受害人赶快将“抢救费用”或“赎金”打到其指定的银行账户上，以此骗取钱款。

案例 2

（1）、1 月 5 日，王某玉报称：1 月 5 日，其下载 360 借款软件，在客服的诱导下被骗转账 75000 元。（接受过反诈宣传，已安装国家反诈 APP，未收到预警）

（2）、1 月 6 日，石某（男，43 岁）报称：其下载“金川集团”刷单 APP 赚取高额佣金时，被骗 90256 元。（未接受过反诈宣传，曾经安装过国家反诈 APP、被骗时已卸载，未收到预警信息）

5. 亲友急事诈骗

犯罪份子通过不法手段获悉受害人的姓名及电话号码，打通受害人电话后以“猜猜我是谁”的形式，顺势假冒受害人多年不见的亲友，谎称其到受害人所在地的附近遇到嫖娼被罚、交通事故赔钱、生病住院等“急事”，以借钱解急等形式，并叫受害人将其打到指定的银行账户上，以此骗取钱款。

6. 虚假购物诈骗

犯罪份子以手机短信、打电话、电子邮件、QQ、MSN 等方式向受害人低价“推销”时尚商品或手枪、迷药、信号接收器、遥控监听器、特殊功能眼镜等违禁物品，以交“风险

抵押金”、“税款”、“手续费”或“先付款再发货”等名义，叫上当受骗者将现款汇入其指定的银行账户，以此骗取钱财。

7. 冒充黑社会杀手诈骗

犯罪份子通过不法手段获取受害人的姓名、移动电话、家庭电话等信息，以手机短信或打电话的手段向受害人谎称其受黑社会的雇请要加害于受害人及其家人（宰手断腿、挖眼割鼻等），给受害人造成心理恐惧，让受害人“出钱消灾”，诱使受害人将钱款汇入其指定的银行账户，以此骗取钱款。

8. 自动柜员机（ATM、CRS 等贴假提示诈骗

犯罪分子将银行自动柜员机的插卡口破坏，并在银行自动柜员机贴上假冒的“银行提示”，诱使取款人打其假提示上的假银行服务电话咨询求帮，由假银行工作人员套取得取款人银行卡号及密码后，骗走取款人的银行存款。

9. 冒充银行工作人员诈骗

犯罪分子捏造受害人在某商场的消费记录，冒充银行信用卡中心工作人员以电话或短信方式通知受害人，并提出要帮助受害人的信用卡升级，步步诱骗受害人泄露银行卡密码后，骗转走受害人存款

10. 虚假招工、婚介诈骗

犯罪分子以短信、电子邮件、QQ、MSN 等方式发布虚假的招工、婚介信息，以交报名费、面试费、服装费、介绍费、手续费、保证金等名义，诱使受害人汇款到其指定的银行账户，以此骗取钱款。

11. 虚假办理高息贷款或信用卡套现诈骗

犯罪分子通过短信、电子邮件、QQ、MSN 等方式发布可办理高息贷款或信用卡套现等虚假的业务信息，以提前交纳手续费、税款、利息、代办费等名义，诱骗受害人汇款到其指定的银行账户，以此骗取钱款。

12. 虚假致富信息转让诈骗

犯罪分子通过互联网或短信、电子邮件、QQ、MSN 等方式发布有快速致富及技术资料要转让的虚假信息，以提前支付定金、转让费、公证费等名义，诱骗受害人汇款到其指定的银行账户，以此骗取钱款。

13. 虚构信息威胁诈骗

犯罪分子利用手机短信或电话，以虚构投毒、公布隐私、绑架、爆炸或以举报受害人违法等为要挟，欺骗受害人汇款到其指定的银行账号内。

14. 虚构反洗钱、涉嫌刑事案件等诈骗

犯罪分子假冒公安、检查、法院工作人员，利用手机短信或电话向受害人谎称有人举报其银行存款涉嫌洗钱、贩毒等犯罪行为，假意为了受害人的资金安全，套取受害人存款开户行及银行卡（存折）卡号（存折账号）、密码号后窃转走受害人存款或以叫受害人将存款转到其提供的“安全账户”的手段，骗走受害人存款。

15. 冒充性工作者诈骗

犯罪分子通过不法手段获悉受害人的姓名、职务、工作单位及电话号码，假冒性工作者、坐台女，虚构自己曾经和受害人有嫖宿行为，谎称自己或家人遇到急事和困难，以要

求资助、不然就要举报相要挟，欺骗受害人汇款到其指定的银行账号内。

16. 冒充电信、公安、银行工作人员诈骗

近期，又有犯罪分子通过不法手段获悉受害人的姓名、电话号码后，分别假冒电信、公安、银行工作人员，打电话给受害人谎称其电话欠费。当受害人回答没有办过这个电话后，犯罪分子假冒的“电信局”工作人员就把电话马上转到所谓的“公安局”，假冒的“公安民警”就谎称：最近有一批诈骗案发生，诈骗人员盗取了很多老百姓的身份信息和银行信息，我们把电话转到银行，叫银行帮你查一下你的银行信息是否被盗了。之后转到“银行”，“银行职员”接电后一查，马上说“不得了，你的银行账户已经不安全了，马上把银行所有的钱转到我们指定的一个安全账户上”。老百姓一听，完了，就按“公安局”和“银行”的吩咐去办理，以此骗取受害人钱财。

17. 冒充党政领导及相关工作人员诈骗

犯罪分子通过不法手段获悉企业负责人姓名及其电话号码后，假冒政领导及其工作人员给企业负责人或办公室人员打电话，谎称要给企业解决困难或提供帮助，以要求企业赞助或借款解急等名义，要求企业将钱打入其指定的银行账号内，以此骗取钱财。

18. 新型网络 QQ 等即时通讯软件诈骗的作案手段

罪犯应为结伙作案，其中分工明确，有人负责和被害人聊天，实施诈骗行为，有人负责提款。犯罪分子一般先和网

友视频聊天窃取对方个人资料和真人视频，然后利用黑客程序秘密盗取其 QQ 号，冒充 QQ 号码的主人，诈骗 QQ 资料中的亲戚和朋友。

案例 3

(1)、1 月 3 日，吴某（女、39 岁）报称：在抖音认识自称现役军人的陌生人，通过聊天发展为恋人关系后，对方让其下载“北京中粮集团”APP 投资，被骗 118248.88 元。已安装国家反诈 APP，接受过反诈宣传，接到预警电话后已完成转账。

(2)、1 月 3 日，张某（男、42 岁）报称：通过快手添加微信好友，对方称可以代考驾照，其信以为真，先后通过支付宝给对方支付 26000 元的代考费，怀疑被骗。

三、如何防范电信诈骗？

诈骗犯罪份子都是利用受害人趋利避害和轻信麻痹的心理，诱使受害人上当而实施诈骗犯罪活动，为此广大人民群众在日常生活和工作中，应从以下几方面提高警惕，加强防范意识，以免上当受骗。

1、克服“贪利”思想，不要轻信麻痹，谨防上当。世上没有免费的午餐，天上不会掉馅饼。对犯罪份子实施的中奖诈骗、虚假办理高息贷款或信用卡套现诈骗及虚假致富信息转让诈骗，不要轻信中奖和他人能办理高息贷款或信用卡套现及有致富信息转让，一定多了解和分析识别真伪，以免上当受骗。

2、不要轻易将自己或家人的身份、通讯信息等家庭、

个人资料泄露给他人。对于家人意外受伤害需抢救治疗费用、朋友急事求助类的诈骗短信、电话，要仔细核对，不要着急恐慌，轻信上当，更不要上当将“急用款”汇入犯罪份子指定的银行账户。

3、多作调查印证，对接到培训通知、冒充银行、公检法机构等声称银行卡升级和虚假招工、婚介类的诈骗，要及时向本地的相关单位和行业或亲临其办公地点进行咨询、核对，不要轻信陌生电话和信息，培训类费用一般都是现款交纳或者对公转账，不应汇入过个人账户，不要轻信上当。对于来电声称是公安、检查、法院、银行等的电话号码，务必多方印证，尝试回拨电话核实，防止犯罪分子利用改号软件等手法冒充电话号码。

4、不作亏心事，不怕鬼敲门。如收到以加害、举报等威胁和谎称反洗钱类的陌生短信或电话，不要惊慌失措和轻信上当，最好不予理睬，更不要为“消灾”将钱款汇入犯罪份子指定的账户。必要时候，可以向当地公安机关等机构报告和核实。

5、购买违禁物品属于违法行为。对于广告“推销”特殊器材、违禁品的短信、电话，应不予理睬并及时清除，更不应汇款购买。对于要求先汇款后交货或要求预交定金、保证金、风险抵押金、公证费、手续费购物的陌生短信、电话，一定要小心谨慎，仔细甄别，千万不要轻信麻痹和上当受骗。

6、到银行自动柜员机（ATM、CRS 等）存取遇到银行卡被堵、被吞等以外情况，认真识别自动柜员机的“提示”真

伪，千万不要轻信和上当，最好拨打自动柜员机所属银行电话的客服中心了解查问，与真正的银行工作人员联系处理和解决。

7、日常应多提示家中老人、未成年人注意防范电信诈骗，提高老人、未成年人的安全防范意识。犯罪分子通常喜欢选择相对容易上当受骗的老年人、未成年人作为诈骗目标，作为子女或者父母，除了自己注意防范电信诈骗外，应积极主动向加重老人、未成年人传递防诈骗的知识，为我们敬爱的长辈和需要呵护的下一代筑起防诈骗的知识围墙。

四、遇到电信诈骗怎么办？

应及联系银行办理银行卡挂失、网上银行和手机银行密码修改等，防止可能的损失进一步扩大。同时，应尽可能及时记下诈骗犯罪份子的电话号码、电子邮件地址、QQ号、MSN码等及银行卡账号，并记住犯罪份子的口音、语言特征和诈骗的手段经过，及时向公安机关报案，积极配合公安机关开展侦查破案和追缴被骗款等工作。