**警方防范电信网络诈骗提示**

为提高大家对电信网络诈骗的防范能力，我们根据警方提示，归纳了已发生的五大系列诈骗案件的特点及其防范建议，供大家在工作、生活中借鉴。
　　一、利用“分类信息门户网站”发布虚假信息进行诈骗
　　分类信息现已成为最具生命力的一项互联网应用，它开创了全新的信息传播途径，聚合了海量个人信息和大量商家信息，为网民解决日常生活中的焦点、难点问题提供了最便捷的解决途径。在我国比较典型的分类信息门户网站有百姓网、赶集网、58同城网等，此类网站为用户免费发布提供房屋租售、二手物品买卖、招聘求职、车辆买卖、宠物票务、教育培训、同城活动及交友、团购等众多本地生活及商务服务类信息等，这类网站给人民生活带来便利的同时，也给犯罪分子提供了犯罪温床。利用分类信息门户网站实施诈骗的主要类型有：虚假出售二手物品实施诈骗、网络交友诈骗、领养宠物诈骗等，上述网络诈骗已占到网络诈骗的15%左右，网民要睁大眼睛辨别，下面介绍一些代表性的诈骗常用手法及防范建议。
　　典型骗术一：以出售二手货为名实施诈骗
　　骗子通过“58同城”、“赶集网”、“百姓网”等知名二手商品交易网站发布虚假的二手货交易信息。由于上述网站日均访问量较大，作案人员在上述网站发布低价出售二手货的虚假信息，更容易吸引急需购二手货群众的注意。作案手段及方式：第一，以支付定金为名通过银行转账实施诈骗。当被害人主动联系作案人表明购车意向后，作案人会要求被害人通过ATM机将货款或定金转入指定账户，一旦收到钱款后作案人便以各种借口拖延或不再与被害人联系。第二，不明网民在购物网站进行二手货交易时，案犯利用群众贪小便宜的心理，在相关知名购物网站获取相关用户的资料然后利用电脑技巧将正在购物的群众引入圈套，然后以未收到单子为名向受害人提供相关网页，然后待受害人上此网页时一步步让受害人提供身份证号码银行卡号然后骗取受害人银行户头的钱。第三，作案人员以各种理由对被害人实施连环诈骗。部分作案人员在收到被害人的汇款后还会继续联系被害人，以需支付风险保证金、尾款才能取货为由要求被害人再次进行汇款操作，以达到对被害人实施二次或多次诈骗的目的。
　　【防范建议】广大网民要养成良好的网络购物安全习惯，选用具备反欺诈、反钓鱼的浏览器防护专业软件，拦截恶意网址，确保电子购物的安全；同时一定要办理好支付宝和网络银行卡的数字认证，把风险降低到最小；同时要提高防范心理，特别是对一些需要转账的交易链接，不要轻易相信，办理一些额外服务时需谨慎，以免财产受到损失。
　　典型骗术二：网络交友诈骗
　　骗子在交友、相亲网站上以找对象名义交友，编造自己“高富帅”身份，骗取对方的信任以及感情，然后编造各种理由（如生意资金周转不灵、偶遇突发事件等）骗取对方钱财财。网络交友诈骗，是利用了当前一些“大龄恨嫁女”的心态，一些情感脆弱、渴望被爱和闺中恨嫁的女性频频上当，不仅赔了“爱情”，又损失钱财。警方提醒，网络交友务必睁大一双慧眼，不要轻易被甜言蜜语迷惑。
　　【防范建议】首先，要提高警惕，不要刚刚联系就盲目将手机、QQ、姓名等信息透露给对方。可以试着申请一个专门用于相亲的手机号和QQ号，找到心仪目标后停用这个号码，这样就不必担心隐私的泄露；
　　第二，少量会员会假借交友的名义，寻找一夜情或提供性服务，当收到主动发来的QQ号或者电话号码时，可以先在网上搜索一下，一般假借交友名义提供性服务的不法分子都会在很多地方留下其联系方式。
　　第三，两个人正式见面前，最好问清对方的姓名和工作地点，并进行核实。见面后，最好要求对方出示身份证、学历证等相关证明；
　　第四，要警惕过于热情的异性，初次见面，警惕去酒吧、咖啡厅等高消费的地方，不要随便给对方买贵重礼品，更不要轻易借钱给对方，一旦发现对方有不良动机，最好录音、录像留证，并与公安机关取得联系。
　　典型骗术三：网络招聘诈骗
　　犯罪嫌疑人拨打受害人电话，先不讲明自己的身份，诱导被害人误认为骗子打着职业介绍所的牌子，未向求职者介绍工作就收取介绍费、押金，或是交了报名费就把求职者带到一个临时串通好的单位去做根本无用的工作，或是通过网银转账等方式交了各种名目的费用后，骗子就消失了。
　　【防范建议】第一，正规单位公司都不需要交任何费用。 第二，不要随意把自己的身份证之类的东西交给别人。第三，天上不会掉馅饼的，工资太高的工作记得问清楚你的工作内容，如是否带公关性质（也就是有饭局陪喝酒陪唱歌之类的）。
　　典型骗术四：领养宠物诈骗
　　骗子会在网站上发布信息帖子,一般以“本人有了身孕,把家中的宠物免费送给他人。有的网民正好要养宠物，看到对方还要免费送,就会通过QQ等与骗子联系。骗子一般会发来宠物的相片和视频,对宠物的生活习惯描述得头头是道,一下子就拉近了与受害人的距离。骗子一般会说:“我叫快递公司帮你运过去,不过运费得你出。骗子会给受害人一家快递公司的电话。受害人与快递公司取得了联系,被告知宠物运到需要800元,其中300元是笼子押金,收到狗不要笼子可当场退还,并要求先把钱打到快递公司的账户上。当受害人钱汇过去之后会有“物流人员”的电话:“银行当天系统升级,汇去的钱被冻结,无法显示汇过去多少钱,只有打一定的数额才能显示。”并会表示,只要钱显示出来,就立即把多余的钱转账回来。受害人虽心有戒备,但在对方软磨硬泡下又会汇钱过去。随后,“快递公司”又不断地以各种理由让受害人以网上转账的方式汇钱。
　　【防范建议】网上发布的赠送信息需要仔细核对,应格外小心。针对第三方要求支付担保付费或是预付物流费,民警建议尽量选择货到付款,不能轻信对方的种种理由,将钱打到个人账户上。实在没法避免,也最好将款项汇至企业名下账户。一旦发现被骗,要保存证据,立即报警。
　　典型骗术五：利用传播软件随机发送中奖信息进行诈骗
　　骗子利用传播软件随机向互联网QQ用户、MSN用户、邮箱用户、网络游戏用户、淘宝用户等发布中奖提示信息，当事人按照指定的“电话”或“网页”进行咨询查证时，骗子以中奖缴税等各种理由让事主一次次汇款，直到失去联系事主才会发现被骗。
　　【防范建议】如果接到类似中奖信息，一定要提高警惕，不要看到信息内容里是大家所熟知就掉以轻心，最好通过正规渠道进行确认，以防上当。与此同时要及时的更新杀毒软件。如果登陆某个网站时杀毒软件提醒你如下信息你一定要加强防范意识，不要忽略此警告，继续访问该网站。更不要盲目给对方汇钱。
　　典型骗术六：冒充QQ好友诈骗
　　骗子利用录制QQ视频的专用软件，与QQ用户聊天时截取对方视频；再使用木马或钓鱼链接等黑客技术盗取QQ号。随后伪装成该QQ用户与其好友聊天，并播放之前截取的视频，骗取受害人的信任后，以各种理由借钱，实施诈骗。由于骗子在作案过程中大多使用了“视频”聊天，作案成功率极高。
　　从前期案发的冒充QQ好友诈骗来看，骗子盗取QQ号码的主要对象是国外留学生及企业工作人员。犯罪嫌疑人利用国内外时差及其它通讯方式不便利的特点，盗取这些人的QQ号码，且通过修改QQ备注信息，有针对性的骗取其近亲属或是下属钱财。
　　【防范建议】第一，谨慎辨识对方身份，在遇到要求汇款等涉及财物问题时，一定要通过电话等方式联系对方，或在聊天时设置一些问题以辨明对方身份。据统计，去年下半年我市网络诈骗，被骗10万元以上的案件中，冒充QQ好友诈骗占到了46.6%，损失巨大。
　　第二，特别要提醒的是：有国外留学生的家长，遇到孩子请求汇款时，一定要谨慎。企业单位中的会计人员，当遇有上级领导指示给指定账号汇款时，一定要通过其它方式予以核实，谨防被骗。对于陌生人发过来的图片、链接等不要轻易接收，防止被植入木马程序。
　　典型骗术七：以 “网银升级”为名进行诈骗
　　【防范建议】一旦遇有网银升级等信息，一定要到银行网点咨询或是拨打银行的官方客服电话咨询，不要轻易相信短信，如果被骗请及时报警。
　　典型骗术八：网络购票诈骗
　　骗子利用虚假购票网站，提供虚假链接或网页，诱骗购票者输入银行卡账号、密码，窃取这些信息后盗取卡内的存款，或是以种种理由拒绝使用第三方安全支付平台，诱骗购票者直接汇款，进而获取钱财。
　　【防范建议】节假日前，围绕“车票”这一主题的网络购票诈骗迅速升温，为防止上当，警方提醒网络购票一定要通过正规的渠道购买，或是通过一些熟知的网站（如：www.12306.cn、去哪网、携程网、芒果网等）购买，切莫轻信低折扣或先付款、后送票等虚假交易。
　　典型骗术九：代办信用卡诈骗
　　网络上有人宣称不需要收入证明，不需要担保，就能够办理大额的信用卡，一旦受害人信以为真后，骗子就以收取保证金、手续费等名目向受害人索要钱财。当受害人付款后，骗子就会消失。
　　【防范建议】办理信用一定要到银行网点办理，这种不需要证明、不需要担保的信用是不存在的。同时也要提醒被骗的人，在办理不需要证明、不需要担保的信用卡时，自己的本意是什么，千万不要因小失大。
　　典型骗术十：以钓鱼网站形式诈骗
　　犯罪分子建立起域名和网页内容都与真正网上银行系统、网上证券交易平台极为相似的网站（即钓鱼网站），引诱用户输入账号、密码等信息，进而通过真正的网上银行、网上证券系统或者伪造银行储蓄卡、证券交易卡盗窃资金。
　　市民陶某在淘宝上开了一个出售各类电话卡的网络店铺，通过进销差价赚取利润。4月15日，一名淘宝用户主动与其联系称有低于市场价很多的优惠出售各类电话充值卡。于是，陶某便和对方联系，对方引诱陶进入一网站，要求其通过该网站利用网银支付1元钱的订单费，陶某登录网页后，登录支付界面，弹出一“工商银行网银支付界面”，陶某没有仔细核实，便输入自己工行帐号、密码以及电子口令卡密码，确认支付时，总是提示错误。陶某感觉不对，登录自己网银查询后发现自己的帐号被人以转帐的形式划走5000元。
　　【防范建议】第一，核实对方网站的真实性。通常可以通过查询网站底部的信产部备案号是否有备案，若有备案，是否与正在浏览的购物网站一致。若有异常，一般均为假冒购物网站。另外经营性网站可以通过工商部门的注册登记查询真伪。
　　第二，对网银支付界面进行核实。通常对方提供的支付界面与正规的网银支付界面很相似，可以通过核对支付界面网址的方式来辨别支付界面真伪，若不是官方支付界面，可以判定为诈骗网站。
　　第三，利用互联网搜索引擎进行搜索。如对网站上所留电话、银行帐号、公司地址、QQ号码、MSN帐号、邮箱等关键字使用百度、google进行搜索发现是否有人已经被骗。

　　二、利用当红的电视节目进行中奖诈骗

　　一段时间，《中国好声音》等电视节目，超高的收视率和观众认可度吸引了不少市民的关注，但与此同时，不少骗子也开始动起了歪脑筋，通过网站、手机短信群发等方式发布虚假中奖信息，设置钓鱼诈骗网站，已有一些观众上当。

　　一般犯罪嫌疑人会随机的发送一些短信称，对方被随机抽中，成为《中国好声音》等电视节目场外幸运星，并告知对方能领取不菲的奖金，收到的这条短信上，还公布了一个域名类似《中国好声音》等电视节目的真实网站，根据网站提示，对方需要输入短信上告知的验证码后才能领取奖品。当事人一般经受不住高额奖金的诱惑，信以为真的按照网站要求，依次输入了自己的手机号码、姓名、身份证号、联系地址和银行账号，一大堆个人信息输写完毕之后，网站又跳出一个对话框，要求缴纳税金、保险金等费用，如果继续按照对方的要求付款那么就上当受骗了。
　　【防范建议】在接到类似的陌生电话或短信时，要增强防范意识，不要轻信对方的身份，不要透露自己的身份信息和银行账号，更不要去银行转账，以免被假相蒙蔽而损失。如有疑问，可以拨打节目组的官方电话或是110进行咨询。特别是针对热播的《中国梦想秀》、《中国好声音》、《我要上春晚》、《星光大道》等热播电视节目进行中奖诈骗的要引起特别注意。
　　三、以淘宝“刷信誉”为名进行诈骗
　　骗子会在互联网QQ空间、论坛等部位发布帮助刷淘宝商家信誉的兼职信息，骗子是撒网式的，并以优厚待遇为诱饵，设立各种虚假名目、特定流程，刚开始会兑现承诺，赢得受害者的信任，当取得受害人信任后，就会让受害人去购买指定的商品，一般是购买充值卡、游戏点卡等，数额一般较大，这种实施连环诈骗，欺骗性强。当受害人按照骗子的要求做后，骗子便会消失。此类案件中，骗子利用ＱＱ、贴吧等发布虚假诈骗信息，不仅传播速度快、范围广，且具有虚拟性和不确定性。加之所谓“兼职刷信誉”对受害人学历及工作经验无任何要求，报酬丰厚，诱惑力较大，上当者大多为社会经验不足，防范意识差的年轻人。
　　【防范建议】网络兼职往往以高薪作为诱饵，工作量又小的工作，多为骗局。淘宝店的信誉是靠所有网购人员的评价所决定的，这中“刷信誉”的行为本身的合法性就有待研究，更不要盲目的参与。此类案件利用网络的虚拟性及不确定性，侵害对象多为经常上网的不特定人群，无固定职业年轻人及学生居多。希望广大网民提高识别能力，自觉抵制各种诱惑。坚信“一份耕耘，一份收获”， “天上不会掉馅饼”，尤其是对那些“高额回报”“快速致富”的项目或兼职进行冷静分析，不要盲目相信所谓的高薪。当遇到此类信息时，可以先咨询家人或朋友，切勿轻易相信，以防上当。万一被骗，要及时报警，并保存好相关证据。
　　【相关知识】第一，何为 “刷信誉”？“刷钻”、“刷信誉”、“刷信用”、“互拍”、 “群拍”或者“炒作信用度”，是指在淘宝、拍拍等购物网站中，买、卖双方以抬高信用为目的，或双方在无实际成交的情况下做出“满意”、“好评”评价的行为。
　　第二，这种行为是否违规？信用炒作是一种不道德的行为，对于其他卖家很不公平，这种以虚假的方式来提高本店铺信誉的行为本身的合法性有待研究，而作为网络交易平台本身的网站来讲，一旦查到这种行为后都会做出严厉处罚。
　　第三，何为以“刷信誉”为名进行诈骗？犯罪分子利用网络商户在交易平台中信誉等级提升的需求催生的“代刷信誉”为诈骗手段，以给予提成为诱饵，诱骗受害人为其“代刷信誉”，并将受害人“代刷信誉”时支付的相应款项据为己有或是购买虚拟产品后直接发给嫌疑人，并通过卡单、提高提成的手段或者威胁受害人，如果不继续为其“代刷信誉”，之前“代刷信誉”已支付的现金也不退还，骗取受害人钱财的行为。
　　四、以扫描“二维码”为名进行诈骗
　　随着移动终端的普及，一些便捷的网络支付方式也随即出现。近期网络购物中，出现扫描二维码进行支付的网络诈骗。在扫描二维码后，会自动登录一个网站下载手机插件，这个插件其实就是一个“木马程序”，他会窃取用户的支付密码，然后窃取相关支付方式的余额。
　　【防范建议】在网络购物时，一定要在正规的网站上购买，选择一些信誉好、评价好、销售量好的卖家，在交易的过程中尽量使用第三方支付平台来支付，保证交易的安全，对自己不熟悉的支付方式的使用一定要慎重。
　　五、冒充110电话诈骗
　　骗子利用技术手段，虚拟警方的电话号码，如110等，广泛撒网行骗。如果有人“上钩”后。骗子就会冒充警方人员，以“卷入毒品交易”、“银行卡非常危险”等理由让受害人方寸大乱，然后根据骗子的要求将钱打入所谓的“安全账户”，最终达到骗取钱财的目的。
　　由于网上转账有一定的限额，骗子往往会要求受害人到银行网点办理U盾，这样以便转出更大的金额。
　　由于受害人年纪较大者居多，电脑操作不是很熟练，骗子会要求受害人到骗子指定的网站上点击链接。其实这时受害人是下载了一个远程控制木马，骗子就像使用自己的电脑一样利用受害人的电脑把银行卡钱财转走。
　　【防范建议】警方提醒广大市民，警方绝不可能打电话向市民索取个人信息或要求“操作”银行卡。遇到这种情况，要冷静判断，多问几个问题，骗局很快就会土崩瓦解。无法判断真伪时，不要拨打对方提供的警方号码，而是直接拨打110咨询。
　　提醒广大网民，当对网银使用不是很熟悉的时候不要轻易使用； 当自己没有操作汇款时，U盾不要长时间插在自己的电脑上，同时不要轻易点击陌生人发过来的链接。