附件2：

防范电信网络诈骗宣传材料

**一、电信网络诈骗——洗钱上游犯罪类型之一**

金融诈骗犯罪是指以非法占有为目的，采用虚构事实或者隐瞒事实真相的方法，骗取公私财物或者金融机构信用，破坏金融管理秩序的行为。电信网络诈骗属于金融诈骗犯罪的其中一类，主要是指：犯罪分子以非法占有为目的，利用电话、短信、网络为主要作案媒介，以通讯传播媒介和计算机网络信息系统为操作平台，采用虚构事实、隐瞒真相的欺诈手段，向社会不特定人群发布虚假诈骗消息，来骗取、非法占有他人公私财物，迫使被害人自愿交付财物、被骗数额较大的违法犯罪行为。

根据《中华人民共和国反洗钱法》，反洗钱是指预防通过各种方式掩饰、隐瞒毒品犯罪、黑社会性质的组织犯罪、恐怖活动犯罪、走私犯罪、贪污贿赂犯罪、破坏金融管理秩序犯罪、金融诈骗犯罪等犯罪所得及其收益的来源和性质的洗钱活动，依照本法规定采取相关措施的行为。电信网络诈骗的洗钱的上游犯罪类型之一，请大家警惕电信网络诈骗，同时切勿成为洗钱份子洗钱的工具。

**二、电信诈骗犯罪的特点**

（一）作案过程非接触化

诈骗案件与其他刑事犯罪相比，无现场、无痕迹物证，难以发现、固定和提取犯罪证据。在侦办传统诈骗案件中，往往采取比对嫌疑人体貌特征确定犯罪嫌疑人。而电信诈骗犯罪中，犯罪嫌疑人仅通过电话与受害人联系，与受害人不见面，受害人对犯罪嫌疑人了解仅限于电话号码、银行账号，不掌握犯罪嫌疑人体貌特征，难以确定犯罪嫌疑人。加之，电信诈骗犯罪嫌疑人通常采用网银系统转存及分解资金、自动柜员机提现等手段，与银行工作人员不接触，加大了确定犯罪嫌疑人、固定证据方面的困难。

（二）作案方式信息化

犯罪嫌疑人借助网络、电信“互联互通”科技便利，通过互联网服务器，使用任意显号软件、VOIP网络电话等技术手段，批量群发群拨短信、电话，落地接入本地电信、移动电话，实施诈骗行为，诱导受害人向指定账户转汇资金，随后通过网银系统短时间内转存、分解，利用自动柜员机多处分散提现，为案件调查、赃款控制、追缴带来相当难度。如在实际案例中，犯罪嫌疑人通过技术手段显示公安机关电话号码，骗取受害人信任，成功实施诈骗。

（三）作案手段智能化

犯罪嫌疑人利用受害人缺乏相关法律常识的特点，冒充电信局、公安局、检察院等单位人员，往往以受害人电话欠费、被他人盗用身份证号码涉嫌经济犯罪为名，以没收资金为威胁，以核对存款为理由，通过长时间语言跟踪对话进行心理暗示，环环相扣，令受害人短时间内无法认真思考、辨别真伪，直至被电话遥控转汇资金存款。实际案例中，犯罪嫌疑人常常冒充公安机关工作人员，以查办经济案件、涉毒案件为由进行诈骗。

（四）作案地域跳跃化

为防止受害人因报警及时造成账户资金冻结，犯罪嫌疑人往往选择异地作案，即甲地拨打乙地电话实施诈骗，遥控受害人向异地指定银行卡转汇资金，随后网上分解资金，丙地提取现金，给公安机关冻结资金流向、调查固定证据带来相当难度。如在一起电信诈骗案中，嫌疑人在山东乳山办卡，在湖北武汉诈骗，在江苏南通取款，地域横跨三省。

（五）作案目标不特定化

犯罪嫌疑人在某一段时间内集中向某一个号段或者某一个地区拨打电话、发送短信，侵害对象除地域集中外，无其他特定条件，受害者包括社会各个阶层，既有个体业主、公司职员、大学生，也有企业职工、普通民众。特别是大学生、中老年人由于信息相对封闭，对防范宣传不敏感，对骗子使用现代手段作案不了解，极易上当受骗，将绝大部分存款转汇，造成财产损失。

（六）犯罪组织职业化

电信诈骗犯罪往往由多人共同实施，相互间有明确分工，既有策划整个诈骗活动的“指挥组”，也有具体实施对话诈骗的“导演组”，同时还有专门负责网上转存、资金分解的“转汇组”及组织实施取款提现的“取款组”，各环节互不接触，这也给公安机关的打击带来很大困难。

（七）犯罪活动国际化

电信网络诈骗犯罪嫌疑人既有国内公民，也有境外人员，同时还有境内外相互勾结作案，隐蔽性很强，打击难度也很大。如实际案例中，诈骗集团在台湾运作诈骗过程，专门雇佣大陆居民在境内提款转存，造成了案件办理上的难题。

（八）赃款流动快速化

从银行转账汇款到对方账户资金到账，往往只需要15分钟的银行信息中心数据整理时间。电信诈骗实施成功后，犯罪嫌疑人会在银行资金到账的第一时间通过网络银行实行赃款的转移，按照ATM机提款上限分解到众多银行账号中，迅速组织人员提现。若受害人未能及时发现受骗，很难通过银行在被骗存款转存、分解、提现前采取控制措施。

**三、电信诈骗的主要作案手法和应对措施**

（一）假冒公职人员

犯罪分子冒充公检法工作人员，以事主电话欠费、查收法院传票、包裹藏毒等借口，谎称事主身份信息被他人冒用或泄露，银行账户涉嫌洗钱、诈骗等犯罪活动，为确保事主不受损失，将银行存款转至对方提供的所谓“安全账户”。

在此类作案手法中，近年新出现的比较典型的诈骗手段是“邮包涉毒”。犯罪分子冒充邮局或者公检法工作人员，谎称事主有包裹涉及毒品或违禁品，要求事主将资金转入“安全账户”进行验证。

对策：公检法等国家机关工作人员执行公务时，一定会持相关法律手续当面询问当事人，不可能通过电话要求转账，所谓“安全账户”也是子虚乌有，凡是自称国家机关要求把钱汇入安全账户的都是诈骗，对此切勿相信。

（二）冒充熟人（猜猜我是谁）

通过网络声讯电话语音冒充熟人编造谎话诈骗。犯罪分子打电话给事主冒充其同学、同乡、朋友或让事主猜其是谁， “你不记得我了、猜猜我是谁”，并称“好久不见，近期想见个面叙叙旧”套取信任，在赢得事主信任后，假称其在外地因嫖娼、赌博等违法犯罪受到处罚，或发生交通事故、家人住院等为由，请求事主向指定账户汇款实施诈骗。

对策：当接到自称“老朋友”“猜猜我是谁”电话时，要保持高度警惕，注意核实对方身份，必要时向老朋友电话核实或者向相关办案部门了解，不要轻易相信对方的种种理由而给其汇款。

（三）购车（房）退税

不法分子利用各种非法途径获知客户购房、购车信息后，冒充税务局、财政局、车管所或4S店工作人员拨打电话，以“国家下调购房契税、购车附加税率，要退还税金”为名，留下所谓“服务电话”，以交纳手续费、保证金等名义，要求事主汇入指定的账户实施诈骗。

对策：税务部门退税会在报纸、电视等媒体公告，而不会仅以电话方式通知，接到这样的电话即可认定是诈骗。

（四）银行卡消费透支

不法分子冒充银行客服人员，向当事人发送“银行卡刷卡消费”、“信用卡透支”等短信，称其身份证被人利用在外地办理了信用卡，此卡在某地方消费了几千元，详情联系XXX电话，否则银行人员将从其银行卡中扣除。如果当事人电话“垂询”时，犯罪分子便分别扮演“银行”、“银联管理中心”层层设下圈套，诱骗事主将银行卡内资金转移到“安全账户” 。

对策：收到类似信息应拨打正规的银行客服电话咨询，切记不要通过诈骗电话或短信提供的联系电话咨询。永远不要相信有“安全账户”。

（五）无抵押贷款

犯罪分子通过电话、手机短信、网络、报纸等媒介散布能够长期免担保贷款的虚假信息，如果当事人与之联系便会告知贷款必须预先支付1万至几万的保证金或者部分利息，同时要求当事人办理一张银行卡并要求存入金额不等的“风险金”，并开通电话查询功能，以证明当事人是否具有一定的还款能力，最后将事主的钱从卡中转出。

对策：谨防急需资金、无需抵押的心理被人利用。不要相信愿意垫付部分资金等假象信息，要辨识短信和网站的真实可靠性，可查询发送短信的联系电话查属手机的归属地，这些人的手机归属地往往在外省市，查询网站域名属地确认网站所在地，服务器不在我国境内的多为虚假网站。

（六）短信电话中奖

犯罪分子利用传播软件随意向互联网QQ用户、邮箱用户、网络游戏用户、淘宝用户等发布虚假中奖提示信息。当事人拨通电话后，犯罪分子通过“核实身份确认中奖”的手段要求当事人缴纳“手续费、保证金、税费”等费用进行诈骗。当事主按照指定的“电话”或“网页”进行咨询查证时，犯罪分子以中奖缴税等各种理由让事主汇款。

近年以来，使用此类手段进行诈骗的案件激增，主要方式是冒充“中国好声音”、“中国梦想秀”、“非常6+1”等比较火的选秀节目，拨打电话或发送短信，声称当事人中奖，让其登录“官网”进行确认和转款。

对策：对于收到的中奖、超低价商品的信息要保持警惕；对电话、短信、网站中透露的相关信息如有疑问，一定要通过正规渠道核实，不要急于转账或透露个人信息；绝不按照陌生人的指令在银行ATM机上进行转账操作。

（七）利用QQ等聊天工具

犯罪分子事先通过盗号软件和强制视频软件盗取他人QQ号及密码，并录制对方的视频影像，随后登录盗取的QQ号与其好友聊天，并将所录制的QQ号用户视频播放给其好友观看，以骗其信任，最后以急需用钱为名向其好友借钱，从而诈骗钱款。

对策：用户在上网时不要随便接收他人发来文件，防止因中木马病毒而导致QQ号码被盗；如有网友提出经济要求，一定要慎重，要通过电话进行核实和确认，如果电话联系不上，可以设置一些试探性问题辨别真假。

（八）虚假购物网站

网购诈骗主要有两种形式：一是钓鱼网站诈骗，受害者在进行网购时，网页出现钓鱼网站链接，受害人点击链接后，购物款直接转至嫌疑人账户；二是受害人付款时，嫌疑人谎称付款不成功而要求受害人多次进行付款操作，造成受害人重复付款，却根本收不到货物。

对策：网购时一定要选择有信誉度的购物网站，不要贪图便宜，不要轻信商家提供的图片和商品评论。尽量使用支付宝、U盾等安全支付工具，拒绝与店主私下交易。

**四、电子银行支付安全及防诈骗知识**

（一）电子银行安全使用小常识

一卡：

妥善保管好您的银行卡账户介质，同时，请您保管好您的网银盾安全产品，不要借予他人使用。

两码：

妥善保管好您的电子银行密码及短信验证码。同时，建议您不要“一套密码走天下”，将电子银行密码设置为数字+字母等复杂组合并定期修改；短信验证码是您的支付密码，绝不能以任何形式透露给他人。

三要素：

妥善保管好您的身份证号、账号、手机号等个人私密信息，切勿随意在网上填写。

四要：

官网网址要认准。要到苹果等正规的应用商店或我行官网(www.ccb.com或m.ccb.com)下载我行手机银行客户端等软件。账户变动要关注。推荐您开通账户变动短信、微信提醒服务，及时关注账户余额变动情况。手机电脑要杀毒，使用电子银行交易的手机、电脑要安装专业杀毒软件，及时升级、定期查杀病毒。

三不要：

公共网络不要使用。尽量不要在网吧等公共场所使用公共电脑登录使用网银。不明链接不要点击。遇到手机银行升级、积分兑换之类的短信，一定要拨打95533咨询，切勿轻信，不要随便点击其中的链接，以免造成资金损失。欺诈借口不要轻信。不法分子往往在电话、短信、QQ中使用贷款验资、司法协查、商品退款、积分兑换、中奖退税等借口进行欺诈，切莫轻信。

（二）客户安全支付建议

网络欺诈形势日益严峻，不法分子通过各种手段套取客户的有效信息进行诈骗，目前常见的通过钓鱼链接及木马病毒骗取客户身份证号码、卡号、密码及短信验证码等信息；利用虚假退款、公检法等诱骗原因骗取客户信任后套取信息；通过“撞库”等方式根据互联网已泄露的客户信息破解客户的注册用户名和密码等等方式均是不法分子套取客户信息的常用手段，在获取所需要的客户信息之后，不法分子以客户名义进行支付操作，完成客户资金的诈骗转移。因此，客户特别需要注重信息安全保护，时刻保持警惕，积极防范不法分子诈骗，主要可从以下方面加以防范：

1.加强个人私密信息保护

目前信息泄露日益严重，客户应注重保护自身信息，不要轻易相信来路不明的电话短信而主动泄露如身份证号、银行卡号、取款密码、短信验证码、授权码等安全信息。特别需要妥善保管短信验证码和取款密码等关键信息，这往往是支付验证的最后一道关卡，切勿向任何人透露。

2.警惕钓鱼链接和木马病毒

钓鱼链接是不法分子仿冒真实支付网站做出的虚假网页，往往与真实网站域名和网页内容相似，骗取客户在网页上输入身份证号、密码、短信验证码等关键信息；木马病毒是不法分子诱骗客户下载的app，植入客户手机移动终端，从而截取客户收到的短信，获取短信验证码等关建信息。因此客户应时刻警惕钓鱼链接，不要随意下载不明软件，以防被不法分子套取安全信息，诈骗资金。

3.切勿随意发送或回复不明系统信息

对部分需要客户上行短信完成的业务流程，不法分子会利用客户对业务流程不熟悉的特点，诱骗客户使用手机发送短信开通或解除相关操作，进而为其实施欺诈提供便利。因此客户需时刻警惕系统提示信息，仔细阅读短信内容，切勿随意发送或者回复来路不明的系统短信。

4.加强互联网各项服务密码管理

不法分子可通过“撞库”破解客户用户名及登录密码信息，从而登录客户电子银行账户进行资金转移。“撞库”是指黑客通过收集到的互联网已泄露的用户名和密码，尝试登录用户的其他网站账户。由于许多用户在不同网站上注册的用户名和密码一致，因此撞库的准确率往往相当高。建议客户加强互联网各项服务的密码管理，避免使用同一密码，以免遭到“撞库”侵害。

5.不扫来历不明的二维码

二维码支付方便快捷，然而也给不法分子提供了可乘之机，总有一些不怀好意的二维码暗藏风险，目前已成为木马病毒、钓鱼网站的传播渠道之一。客户在面对陌生人提供的二维码信息时需提高警惕，不能见码就扫，扫二维前应核实其来源，选择正规的途径和商家发布的二维码，切勿输入个人身份及银行账户信息，并在手机上安装防病毒安全软件加以保障。

6.牢记“七个凡是”

凡是遇到以下7种情况，都是骗子的伎俩：

1.凡是收到账户积分兑换现金、信用卡提额短信的。

2.凡是跟你索要个人及银行卡信息、短信验证码的。

3.凡是收到陌生网站（链接）要登记银行卡信息的。

4.凡是自称公检法要求你汇款到“安全账户”的。

5.凡是通知中奖、领奖要你先交钱的。

6.凡是通知“家属”出事要求先汇款的。

7.凡是自称领导（老板）要求打款的。