了解防骗常识，提高防骗意识

一 当前电信诈骗犯罪几种常见手段：

1、冒充司法机关工作人员诈骗。

作案手法：嫌疑人 A 冒充电话局、邮局工作人员拨打事主家中电话，声称其家中电话欠费、有包裹没有签收等，然后称事主的身份资料与嫌疑犯有牵连，将事主电话转接给所谓的公安局或是其他司法机关，让事主核实；嫌疑人 B 假冒公安人员谎称事主个人信息泄露，银行帐号已被人利用进行犯罪（如贩毒、洗黑钱、涉嫌诈骗等），要求事主及时进行账户保护、清查，并将电话转给银行客服中心；嫌疑人 C 假冒银行工作人员，要求事主将存款转到“资产保护账号”等事先准备好的银行卡中。嫌疑人用电话指挥事主在银行 ATM 自动柜员机上操作，或指挥事主开通网银，获取网银密码后进行转账。

案例：2013 年 11 月 26 日，鞍山市居民马某在家接一个录音电话：“电话欠费，如不补款，三小时内强制停机，详情按 9 号键”。马某按了 9 号键，一个男人声音说有人用事主身份证在深圳罗湖区办理了一个座机电话，现电话欠费 3685 元，让其到深圳罗湖区公安局报案，事主称在鞍山无法去深圳报案，嫌疑人称提供电话转接服务，之后将电话转接给一个自称叫“孙国伟”的警官。“孙国伟”称事主涉嫌的案件较大，转接到一个叫“姜义”的警官，该人自称公安局大队长，称深圳罗湖分局抓了一个叫“王进”的人，“王进”将贩卖冰毒的非法所得转到了事主的账户里，为核实事主家中的合法来源，需要把家里所有的钱汇入所谓“国家刑事案件公用账户”里。事主按照嫌疑人要求，于当日 13 时许，将全部存款 60000 元通过银行柜面汇给嫌疑人提供的银行卡中后发现被骗。

2、QQ 冒充亲友诈骗。

作案手法：嫌疑人事先通过盗号软件和强制视频软件盗取 QQ 号码和密码，录制对方的视频影像，随后登录盗取的 QQ 号码与其好友聊天，并将所录制的 QQ 号码播放给其好友、亲属观看，以骗其信任，最后以急需用钱为名向其好友、亲属借钱，从而诈骗钱款。

案例：2013 年 6 月 8 日，大连市居民张某在出租房内上网，与朋友在网上聊天，聊了一会儿，“好友”把视频打开，张某一看是好友的影像，但此时视频马上就关闭了，“好友”

接着说，有点事，需要用钱，向事主张某借 20000 元人民币，张某信以为真，随后到附件银行向其“好友”帐户汇款 20000 元。6 月 10 日，张某与其朋友联系时，发现被骗。

3、退税诈骗。

作案手法：嫌疑人事先通过其他手段获取事主购车、购房、购农机等详细资料，以国税局或财政局工作人员名义用电话或短信方式联系事主，谎称根据国家最新出台的政策，事主可享受购车、购房、购农机退税，并留下所谓的“服务电话”，一旦事主与上述电话联系，即以交纳手续费、保证金等名义，诱导其到 ATM 机进行假退税、真转账的操作。

案例：2013 年 9 月 13 日，鞍山市台安县门某手机 1504076XXXX 接到手机 18816507970 来电:“我是政府农机办的，你的农机直补下来了，你给 13146318767 财政部门挂电话”。手机 13146318767 称:“我是财政部的，你的农机补助下来了，去银行领取”。到银行后，嫌疑人问看看银行卡上面有多少钱，一会给你打 5000 元钱，事主我说卡里有 7400 元钱。嫌疑人说你把卡插到提款机上，按我说的流程操作。之后再查余额，发现就剩 100 多元钱。

4、冒充熟人诈骗。

作案手法：嫌疑人通过拨打事主电话或发送短信等手段，冒充其外地熟人朋友，首次拨打往往以“你猜我是谁”、“怎么不记得我了么”等语言骗取事主信任后，谎称出差办事要去看事主。第二天，嫌疑人会以出车祸、嫖娼或赌博被抓、家人住院等理由，要求事主通过银行汇款达到骗取钱财的目的。

案例：2013 年 6 月 25 日，沈阳市皇姑区居民程某某在家中接一男子电话，对方自称是其外甥。事主程某某说“你是长宏的儿子天天吧”，对方说“是，在大连出差，明天到沈阳看你”。第二天，嫌疑人打来电话说，在大连嫖娼被抓，需要用钱保释，要求事主给其汇款 30000 元人民币。事主碍于情面，向嫌疑人提供的银行账户内分两次汇款 30000 元人民币后方知受骗。

5、冒充黑社会诈骗。

作案手法：嫌疑人通过非法渠道事先获得事主的个人信息后，冒充黑社会人员直接拨打电话，在通话中会说“事主家住在什么地方、开什么车、妻子和孩子的姓名”等，然后说事主得罪人了，有人花钱买事主一条腿，之后说同事主交谈感觉事主人不错，嫌疑人也是拿人钱财，替人消灾，如果事主拿钱就可以解决，利用事主恐惧心里进行诈骗。

案例：2013 年 6 月 9 日，朝阳凌源市居民王某某接到一陌生男子打来的电话，谎称自己是盘锦的黑社会“段老四”，称事主有两台车、车牌号为 XXX，然后称事主王某某得罪人了，

不拿钱当晚就要卸掉王某某胳膊和大腿，并向其索要 30000 万元人民币。事主王某某出于恐惧，将 3 万元人民币打入嫌疑人提供的银行卡中。后经朋友提醒，方之被骗。

6、“网络钓鱼”诈骗。

作案手法：嫌疑人通过设立假冒银行网站，当用户输入错误网址后，就会被引入这个假冒网站。一旦用户输入账号、密码，这些信息就有可能被犯罪分子窃取，账户里的存款可能被冒领。此外，嫌疑人通过发送含木马病毒邮件等方式，把病毒程序置入计算机内，一旦客户用这种“中毒”的计算机登录网上银行，其账号和密码也可能被嫌疑人所窃取，造成资金损失。

案例：2013 年 10 月 14 日，铁岭市居民蔡某手机 1384102XXXX 接到 106576595588 号发来的短信：“工行提示：您的电子密码将于次日过期请尽快登入我行网站：wap.icbcior.com 进行升级，给您带来的不便敬请谅解。”事主蔡某按照提示操作并输入了验证码。17 日，事主蔡某取钱时，发现自己工商银行卡上的 60000 元人民币没了，去银行核实后知道钱已被转走，发现被骗。

7、虚构绑架诈骗。

作案手法：嫌疑人给事主打电话，谎称事主孩子等亲属被其绑架，并模拟孩子、亲人的哭声、叫喊声，从而骗取事主钱财。

案例：2013 年 8 月 24 日。葫芦岛市居民董某某家中座机 0429-399XXXX 接到一陌生男子电话称其儿子被绑架，并威胁其汇款 1 万元，不然将其儿子腿打断。事主董某某将 1 万元钱汇入嫌疑人提供的银行卡中，后跟其儿子取得联系，发现并无此事，得知被骗。

8、虚假中奖信息诈骗。

作案手法：嫌疑人利用事主投机致富的侥幸心理，借助网络、短信、电话、刮刮卡、信件等媒介为平台发送虚假中奖信息，继而以收取手续费、保证金、邮资、税费为由，骗取钱财。

案例：2013 年 11 月 23 日，铁岭市居民孙某某接到一个电话（+8615657180493），自称北京中视购物中心，通知事主孙某某中了 28.9 万元大奖，并留下一个“李主任”的联系电话 13240757053。与“李主任”联系后，一财会人员给事主打电话，要求先交 1580 元公证费。事主到本地邮政储蓄所汇款后，财会又通知事主需交纳 2980 元转账费，后又提出需捐款等名义，总计诈骗事主 6 万元。

9、引诱汇款诈骗。

作案手法：嫌疑人先发送诸如“你好！请把钱汇到 xx 银行（或其他银行）；账号：XXXXXXX，谢谢！”之类的短信，事主误以为是商业伙伴或债权人的短信，即按要求把款项汇到某指定账户。再去核实时，就后悔莫及了。此种诈骗的嫌疑人往往是误打误撞，恰巧事主正准备办理汇款事项，因粗心大意不及多想，结果把钱款“汇”错了对象。

案例：2013 年 10 月 26 日，营口市居民张某在工商银行正准备给其朋友王某汇款 3 万元。此时，张某手机收到一条短信，内容是“卡号已换，请将钱打到 XXXXXX 这张卡中，户名李某某”。事主将钱汇入嫌疑人提供的银行卡后，告知朋友张某时，发现被骗。

10、股票内幕消息诈骗。

作案手法：嫌疑人以某某证券公司（多以 XX(如上海等)某某证券公司）的名义，通过互联网、电话、短信的方式散发虚构的个股内幕消息和个股走势，实行会员制，按照会员等级收取一定费用。若指定的个股走势碰巧吻合，则再以索要咨询费并许诺将继续提供个股内幕消息或走势的方式实施诈骗。

案例：2013 年 6 月 19 日，锦州市居民许某某报案，其于 5 月 20 日收到一封短信，内容是：加入海通证券会员可保证炒股盈利。事主许某某按短信给的网址联系上一个自称上海海通证券工作人员叫“王海明“的男子，该男子让事主加入会员。事主于 5 月 21 日向嫌疑人提供的银行卡汇款 6800 元，对方收到钱后传真了一份合同，让事主再汇 30000 元保证金，事主许某某认为上当，向嫌疑人索要汇钱无果，方之被骗。

11、低价购车诈骗。

作案手法：此类诈骗犯罪中，嫌疑人主要利用事主贪图便宜的心理，向事主发送低价出售二手名车等虚假信息，短信内容一般为：“本集团有九成新套牌走私名车（而出售价格只是市场价的零头）出售”。待被害人拨打联系电话想要购买时，不法分子提出必须交定金、托运费等费用才能进一步办理，要求其向提供的账户汇款，从而达到诈骗的目的。

案例：2013 年 11 月 4 日，盘锦市居民王某某报案，被自称是卖二手车的两名男子骗走 100000 元人民币。11 月 3 日，被害人手机接到一条短信“现有海关罚没走私车奔驰、宝马、奥迪 10 万元起，联系人张某，电话 XXXXX”。事主按照短信所留电话联系询问车辆价格并提出看车时，嫌疑人要求可以让事主找一个朋友代事主到嫌疑提供的一个地点看车，并索要了事主朋友的手机号码。此时，嫌疑人通过电话一直同事主朋友进行通话，另一名嫌疑人利用改号软件显示事主朋友手机号，并模拟事主朋友的声音给事主打电话，说“车不错，可以汇款”。事主将 100000 元汇入嫌疑人提供的银行卡后，再同朋友联系时发现被骗。

二 防范提示：

各种诈骗犯罪中骗子的目的是骗钱。上述诈骗者几乎都是通过银行转账、银行卡转账的形式达到骗取钱财的目的。无论骗子如何花言巧语、危言恐吓，他们真正的目的是让事主将自己的银行卡或存折内的钱转到骗子的手里。在这里警方重点提示：

1、催缴电话费是电信、通讯部门对于真正的电话欠费客户，通常是在每月缴费日起之前，使用正常客服电话通过电脑语音进行提醒按时缴费的一种商业服务手段。公、检、法机关作为执法部门是绝对不会使用电话方式开展此类所谓的“电话欠费”案件侦查工作的，请谨防上当。

2、对冒充各类工作人员打电话诈骗的，一定要注意来电显示上的电话类型，对于一些不熟悉，不像是正常座机手机号码的电话，尤其是电话前带有多个“0”的号码不要理睬。如接到类似欠费电话时，可拨打提供服务的电信部门的统一客服电话进行核对。如对方称是某公安分局民警，可以通过拨打 110 进行报案和咨询。

3、任何通过电话、短信要求您对自己的存款进行银行转账、汇款的，或者声称为您提供安全账户为您的存款进行保护的，首先要核对好对方身份和目的，千万不要轻信和疏忽大意。

4、要提醒在家里的中老年亲属、朋友，要保守家庭以及个人的各类信息，如银行账号、银行密码、家庭住址等。中老年同志遇到不明白的事不要急于做决定，要先和家人、子女等联系、沟通，防止受骗。

5、认真审视分析每一条信息和每一个来电，不轻信他人之言，遇事多与家人协商、或直接回拨号码等形式方法进行甄别。遇事冷静、多考虑一会可能就不会上当被骗。

6、有些犯罪嫌疑人能通过非法途径获取事主孩子或亲友的电话、姓名等信息，因此，在电话中有时能明确说出事主孩子电话或姓名，以强化事主对此事的相信程度，使事主在恐慌失措中上当受骗。当您接到此类电话时，不要慌张，要通过拔打孩子的电话或与其同学、朋友、学校联系等其它方式，证实情况。

7、凡以入会、提成为名义让股民交钱后为股民提供优质股票信息的、公司和网站均属非法。请不要相信虚假公司或机构及网站上标榜的优厚回报的虚假宣传，防上犯罪分子用“钓鱼”的方式行骗。

8、请您坚信无端的中奖短信都是诈骗分子设置的骗局。

9、任何陌生人通过电话、短信要求您对自己的存款进行银行转账、汇款的，或者声称为您提供安全账户为您的存款进行保护的，请一概不要相信，防止受骗。

10、近来电信诈骗犯罪嫌疑人利用特殊计算机软件能模拟各类电话号码，在事主电话上能显示事主家人手机以及政府有关职能部门的电话号码，使接电话事主误以真。对此，请您遇到陌生人打来电话时，一定要冷静、沉稳、思考，特别是涉及钱款转账时，要立即停止，把好最后一道防范关口。

三 应急挽救措施：

1、当您感觉上当受骗时，不要心存侥幸，应当迅速终止交易、保存涉案证据，并及时向公安机关“110”举报或咨询。

2、如果能准确提供涉嫌诈骗的银行卡号，可以拨打涉嫌诈骗的银行卡号所属的银行客服电话查询该卡的开户地点，并迅速到营业网点查清资金流向；如果不能准确提供银行卡号，可以到银行柜台凭本人身份证和银行卡查询骗子的账号。

3、通过冻结涉嫌诈骗的银行卡号为公安机关破案争取时间。通过电话拨打该诈骗账号所属银行的客服电话，根据语音提示，输入该诈骗账号，然后重复输错 5 次密码就能使该诈骗账号被冻结 24 小时，这项操作时为了防止嫌疑人手机银行转账。如果被骗的钱较多，一定要在次日的凌晨重复上述操作，则可以继续冻结 24 小时。进入网上银行页面，输入该诈骗账号，重复输错 5 次密码，同样可以使该账号冻结 24 小时，这项操作是为了防止嫌疑人网上银行转账。