白城日报

白城市公安局承办

公安专刊

2017年4月13日　第3版

本刊主编　武曼晖　编辑　王娅楠　孙泓轩

民警跨省千里侦办网贷诈骗案

“无息、低息”“无抵押、无担保”……上网搜索“网上贷款”四个字，其相关结果竟有千万之多，看得人眼花缭乱。其中“确有其事”还是另有“猫腻”？对此，白城市公安局温馨提示：急于贷款者千万不要“病急乱投医”！

今年2月，市民赵某在QQ聊天时看到一则可以办理贷款的小广告，急需用钱的他很快便与发布人取得了联系。

通过交流，赵某了解到，只要没有被银行列入“黑名单”，他便可以申请无抵押担保贷款，但前提是要先行交付“保证金”。

“你需要重新办理一张银行卡，将保证金存在新开的银行卡上，因为我们的业务绩效有办卡任务，所以开户的信息上要登记我的手机号码……”

虽说先交钱才能办贷款，让赵某有些犹豫，但钱款仍然在自己卡内，让赵某悬着的心落到了实处。

按照对方的要求，赵某先后将新办理的银行卡号及身份证号码等信息发送给了对方，然后便进入了漫长的等待。

每次，赵某询问、催促对方办理进程时，都被对方告知，由于“保证金”份额低，申请过程较慢，如果想加快流程，需要增加“保证金”。

赵某按照要求，多次向银行卡内存入指定金额，总额共计3万元。然而，其申请的贷款却迟迟“未通过审核”。感觉到“不对劲”的赵某，立即跑到银行查看信息才发现被骗了。

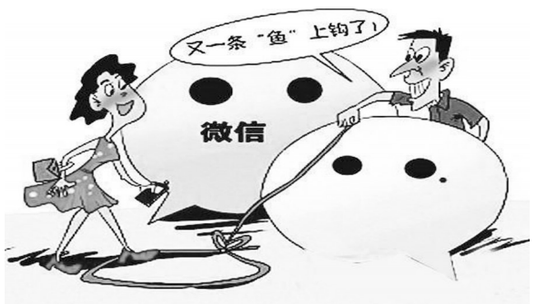
白城市公安局受理案件后，立即组织精干警力全力侦办。通过合成研判分析，民警发现赵某的银行卡被捆绑在某支付宝账号中进行恶意消费，地点是山东省泰安地区。

民警立即前往山东省泰安地区进行侦办，在当地警方支持下开展“地毯式”搜索。通过数日摸排锁定，民警最终在山东省新泰市一平房区内将犯罪嫌疑人李某抓获。

近年来，社会上电信诈骗案件频发，层出不穷的诈骗手段，给人民群众造成了严重的经济损失和精神伤害。为此，白城市公安局成立了反电信诈骗中心，抽调全市精锐警力全力攻克各类诈骗案件，揭秘不法分子的诈骗手段

让我们共同斩断电信诈骗黑手

●王少军　程威龙



“百变大咖”网聊骗取多人“感情债”

她自称自己叫“徐悦”，是标准的“白富美”，她还叫“徐岩”，是一名“高富帅”。其实，这都不是她。张某的真实身份只是一个普通的90后农村女孩，个子不高，长相一般，她包装出来的两个身份是为了周旋于多名男女朋友之间，骗取钱财。

去年2月，沈阳小伙韩某在微信群里认识了一个女孩，当时双方从贷款的话题聊开，越谈越投机。女孩说自己叫“徐悦”，父亲开了一家米业加工厂，家庭富裕，自己在白城一家风力发电厂当会计，平时工作很忙。

经过一段时间交流，两人相熟后开始“网恋”，在确立恋人关系没多久后，“徐悦”说自己父亲的米业加工厂因为被骗导致破产，现在有银行贷款还不上，希望韩某能帮自己渡过难关。韩某没有任何犹豫，立即给她汇款。后来，“徐悦”又说自己家人患病，韩某再次慷慨解囊，先后40余次给对方汇款、转账20余万元。

其实，“徐悦”仅仅是张某在网络里的一个身份。她同时还将身份演变成“男神”，化身“富二代”，在网络里找其他女孩聊天交往。

去年6月，张某改名换姓变成“徐岩”，在网络里结识了镇赉县某宾馆服务员臧某。臧某以为自己遇到了白马王子，两人在微信上确立了恋爱关系。

见时机成熟，“徐岩”故技重施，说自己有一大笔银行贷款到期，自己手头资金周转出现问题，希望臧某能帮他张罗点钱。臧某立刻拿出5000元转账给“徐岩”，但奇怪的是她并没有要这笔钱，而是使出了欲擒故纵的手段，后来臧某又给对方汇款两万元，“徐岩”才收下钱。

今年年初，臧某无意中得知“徐岩”家住嘎什根乡，便找到“徐岩”家中，还与其父母亲见了面。一切真相大白，臧某万万没想到自己的男友竟然是个女人。

臧某把“徐岩”找到家中，大发雷霆，两个人当即打了一架。臧某提出马上分手，一气之下臧某扣下了“徐岩”的一部手机。

臧某回家后，发现有人不断拨打“徐岩”的电话，接听后对方自称姓韩，原来他就是先前被骗的韩某，臧某感觉韩某也是受害人，便告知了“徐岩”也就是韩某口中的“徐悦”的真实身份。

今年2月，气愤的韩某立刻赶到镇赉县，和臧某一起到镇赉县公安局报了案。随后，警方立即成立专案组，并组织精干警力前往沈阳市及镇赉县各地进行取证。在大量的事实面前，张某对其网络诈骗行为供认不讳。

“警官”柔情恐吓 远程遥控支歪招

突然被“警察”打电话告知天降灾祸，任何人都会失去主心骨。而此时，“官方人员”又及时抛出了救命稻草，看似暖心之举，轻易相信一定会被痛宰。

今年3月，大安市民王某接到了“武汉市公安局民警”电话：“你涉嫌与一宗命案有关，在案发现场找到了你的银行卡。”

突然而来的电话让王某有些发懵。“我从来没出过吉林省，一定是有人盗用了我的身份信息。”他极力向对方解释并心理盘算着对方话语中的可信度。

然而，通过一轮交谈，对方非常详细地告诉了王某其“警官证编号”“办公室电话”，并要求王某在规定时限内到当地公安机关接受调查。

见到对方“义正言辞”的通知，并且办案所在地还在本市，王某信以为真，并主动与对方说好话意图套取小道消息。

“由于案件涉及金融资金较大，我们需要对你名下银行信息进行验证。”电话中，王某得知只要“公安机关”对他资金情况进行验证通过后，就能洗清嫌疑，便毫不犹豫地将银行卡信息告诉了对方。

在对方的忽悠下，王某将手机保持通话，并且不与任何人沟通联系。他很快来到辖区ATM取款机，将系统进入英文界面，并相继输入“办案时间”“案件编号”“验证号码”等对方告知的一系列“术语”。最终，王某终于“如愿”地避清了嫌疑。

当王某满足地回到家中，与家人提及此事后，方才恍然大悟。得知被骗的王某，立即跑到银行查看账户信息，发现8.8万已不翼而飞，随后报了案。

网络兼职“垫钱刷单”哄骗手段花样多

“会上网，就赚钱”“高薪酬、低门槛”“在家工作，日赚百元”……上网搜兼职时，满屏都是这种看似正规、极具诱惑性的招聘信息，其实十有八九都是骗子的钓鱼陷阱。

莎莎（化名）是白城师范学院的大一学生。今年3月，莎莎在寝室上网时收到表哥发来信息：某公司招聘网店信誉代刷员，通过帮助网店提高卖家信誉来赚取佣金。看到表哥发的信息，她没有任何犹豫，便与网店客服取得联系。

通过了解，莎莎得知该公司招的应聘者只要有开通支付宝功能的银行卡、能正常拍下商品就可以就职。

“我们是以任务的形式进行返款，一单一结。商家核对完成在3至5分钟之内，系统将自行识别任务货单，把本金和佣金一次性返还到你账户里。现在给你安排任务做，本次的任务是一单三组双数任务……”看到客服发来的信息，莎莎觉得坐在电脑前，点点鼠标就能赚钱，一天下来可以赚几百块，真的很划算。

很快，客服给莎莎发来一个网站，按照对方的指示，莎莎拍下了一组虚拟充值卡。但当莎莎向客服索要返利时，对方却向她强调，任务返款是一单一结，如果后面的任务不做完，不能返款。无奈，莎莎只好继续垫付资金刷信誉。

“姐，你电话多少，我给你打过去说。”随着任务不断进行，看着手中的生活费一点点被套牢，莎莎一时间慌了。

“姐，我不做了，把本金还给我吧，这是我的学费，我明天就得交，如果没了，我就完了……”尽管莎莎几经苦求，但客服仍然没有如愿将钱款返给莎莎，而是不停地对她进行劝说。

“姐，我任务都做完了，可以把钱退给我了。”终于，莎莎将最后一笔资金全部垫付后，任务显示结束，莎莎便急忙向客服索要本钱和佣金。然而，对方却告诉她“任务被系统冻结”，并要求莎莎继续投钱。直到此时，莎莎才感觉到不对劲。

“对方不会是骗子吧？”怀着忐忑的心情，莎莎继续与对方联系，可对方还是让她继续投钱。后来，莎莎在网上和对方说话，对方已经不回答，并把她拉入了“黑名单”，至此，莎莎已经垫资8640元。

意识到自己被骗的莎莎立刻跑到白城市公安局报了案。

什么是电信诈骗？

“电信诈骗”就是违法犯罪分子利用手机短信、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、朋友被人加害、出售致富信息、投资分红等，骗取受害人信任，让受害人将钱汇入到指定银行卡帐户骗取钱财的一种诈骗活动。

白城公安机关着重提示：

如您遭遇电信网络诈骗，不要慌乱，请依以下步骤将损失降至最低。

一、准确记录骗子的账号、账户姓名；

二、尽快拨打110或到最近的公安机关报案；

三、及时将骗子的账户、账号姓名提供给民警，由公安机关进行紧急止付。

当前，社会上的诈骗手段层出不穷，面对移动通讯和互联网上形形色色的诈骗信息，我们应当如何防范？对此，白城市公安局结合当前社会治安形势，深度解析16种常见多发诈骗手段，帮助广大人民群众避免电信诈骗陷阱。

典型案例之一：冒充公检法银行电信部门诈骗

案件分析：

1、犯罪分子通过欺骗性号码并自称公检法机关工作人员，称受害人涉嫌洗钱之类的金融犯罪活动，并要求其积极配合。

2、由于受害人无法及时到案配合调查，对方会以“电子资金审查”或存入“安全账号”为名，让其将资金转到一张银行卡上，以证清白。

3、按照他们发出的网址，接通互联网远程操作系统，在受害人登陆网银后，对其账户上的所有资金进行审查和监管，然后趁机转走款项。

警方提示：

1、公检法机关绝对不会使用电话对涉嫌犯罪等问题进行调查处理，公检法机关之间也不会相互接转电话。

2、公检法等部门不存在所谓的“安全账户”，凡通过电话、短信要求对存款进行银行转账或声称进行资金审查，请立即挂掉电话报警。

3、犯罪分子利用特殊计算机软件，可以模拟各类电话号码。

典型案例之二：发送虚假中奖信息诈骗

案件分析：

犯罪分子以《奔跑吧兄弟》《我要上春晚》《中国好声音》等热播节目组的名义向受害人手机群发短消息，称其已被抽选为节目幸运观众，将获得巨额奖品后，以需交手续费、保证金或个人所得税等各种借口实施连环诈骗，诱骗受害人向指定银行账号汇款。

警方提示：

一些来历不明的中奖提示，不管内容有多么逼真诱人，请千万不能相信，更不要按照所谓的咨询电话或网页进行查证，否则将一步步陷入骗局之中。

典型案例之三：虚构购车购房退税诈骗

案件分析：

嫌疑人事先通过其他手段获取购车、购房市民的详细资料，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、房退税，并留下所谓“服务电话”或“领导电话”以骗取事主信任，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。

警方提示：

在接到陌生电话或短信时，不要轻信所谓的汽车、购房等退税说辞，国家相关税务政策出台，将会通过新闻媒体报道告知，具体操作也是要到税务部门指定地点办理。切记，凡是到ATM机上进行任何名义的“退税”操作均为诈骗。

典型案例之四：招聘网购刷信誉度工作诈骗

案件分析：

网购刷信誉度工作由于网购的兴起而渐渐火热，犯罪嫌疑人利用此类工作虽新兴却很普遍，大多数人虽没见过却也听说过，这种新兴行业的状态，利用小恩小惠引诱一知半解的受害人，在受害人相信之后，进一步骗取受害人缴纳保证金，从而获利。

警方提示：

此类案件的受害者都是由于听说刷信誉度之类的工作，但又不十分了解，轻信了对方的承诺而上当受骗。无论对方的承诺多么诱人，但凡收取任何形式“保证金”的行为，都是典型的诈骗，请广大市民注意甄别。

典型案例之五：利用虚假网站诈骗

案件分析：

此类案件中，犯罪分子制作虚假网站，以“查询学生成绩”“个人信息泄露”“配偶出轨证据”等借口诱骗受害人点击登录该钓鱼网站，通过软件套取手机银行内钱款。

警方提示：

市民在收到来历不明的手机短信时，不要随意点击短信中的网络连接，建议广大用户安装专业的手机安全软件，在用户不慎打开钓鱼网站时，安全软件会及时拦截钓鱼网站，从而保障用户财产安全。

典型案例之六：冒充航空、铁路客服退票改签诈骗

案件分析：

诈骗分子通过非法渠道获取事主的订票信息，并冒充航空公司告知事主航班取消，让其退票或改签。当事主联系对方后，先是准确讲出个人信息和票务信息，在得到最基本的信任后，便问其账户余额并让事主前往柜员机操作。在操作过程中，诈骗分子利用事主对银行业务的生疏，诱骗其向诈骗分子提供的银行账户汇款。

警方提示：

警方提醒各位市民朋友，在收到机票改签或退票的信息时需谨慎，首先，在电话中询问对方的工作身份信息，告知稍后再联系，可马上拨打114查询官方客服电话与之核实该工作人员的真实性；其次，联系官方客服查询自己的订票信息是否异常，如已正常出票，则无需理会诈骗信息；再次，机票改签或退票均无需本人前往银行柜员机进行操作，使用相同诈骗手法的诈骗类型还有“社保退费”“购物退费”及“财政补贴”等要求均为诈骗。

典型案例之七：虚假贷款信息诈骗

案件分析：

犯罪分子针对急需资金周转的群体，通过互联网、电话、短信等方式发送虚假贷款信息，一旦有群众与其联系，则以收取贷款人保证金、利息，提供流水证明等名义，骗取受害人钱财。

警方提示：

防骗要做到“三不”。一是不透露，不向对方透露自己及家人的个人信息、存款、银行卡等情况；二是不轻信，绝不轻信来历不明的电话和手机短信；三是不转账，绝不向陌生人汇款、转账，尤其是涉及到网银业务的要格外谨慎，即可有效防止受骗上当。

典型案例之八：冒充亲友救急诈骗

案件分析：

这类骗术并没有任何高科技含量，主要在于利用受骗群众对亲人、朋友的紧张心理，实际上只要在汇款之前和当事人打个电话确认一下就可以识破骗局。但是因为受害人听到亲人、朋友出事紧张慌乱的情况下，盲目相信了骗子的话，导致骗子屡屡得手。

警方提示：

不要轻信陌生人的说辞，可以询问对方更详细的关于自己亲人朋友信息，如果是骗子不可能比你更了解他们，必然会露出马脚，如不能判断是否是骗子时，要第一时间联系自己的亲人，确认信息即可避免不必要的损失，切勿被激动的情绪冲昏头脑。

典型案例之九：虚假网络购物诈骗

案件分析：

当前，网络购物发展迅猛，很多年轻人更加喜欢这种足不出户的消费方式，但这种依赖于网络交易方式还没有建立一个足够完善的安全保障机制，行业监管难度大，买家交易信息泄露、病毒软件的攻击都能被犯罪分子利用，造成消费者财产损失。

警方提示：

网络交易尽量选择正规交易网站，购物之前要仔细对比买家信誉度，不轻易相信对方所述内容，应通过官方途径联系电商或支付平台的官方客服核实情况。不登陆来源不明的网页链接，不随意扫描非官网发布的二维码，资金操作要在官方交易平台进行。

典型案例之十：冒充单位领导诈骗

案件分析：

此类诈骗中，犯罪分子通过不法手段获悉受害人姓名及电话号码，或者盗取单位领导的网络帐号欺骗受害人，然后冒充领导让受害人汇款。虽然是针对少部分特殊群体进行诈骗，但是往往涉案金额巨大，对受害人职业生涯都造成了严重的影响。

警方提示：

在注意保存好个人信息的同时，也要做好公共信息的保密工作，为防止个人信息泄露，要慎重在公共场所电脑及网络上的QQ、微博、微信等留下自己以及单位的真实信息，也不要在手机上有过多名片标注，以防丢失时信息被骗子盗用。如果接到陌生QQ或微信要求加好友，自称是单位领导，且能准确叫出名字时，也应多方面核实真假。

典型案例之十一：虚假网络购物诈骗

案件分析：

犯罪分子利用伪基站设备，冒充银行客服、移动公司客服，大范围发送诈骗短信，声称银行卡、电话卡的积分可以兑换礼品、现金或话费，逾期作废，同时发送虚假客服网站，骗取受害人银行卡号、密码等信息，从而盗取卡内资金。

警方提示：

首先，要提高防范意识，办理银行、电信业务最好要到正规的营业厅现场办理，切勿轻易将自己的资料透漏给陌生人。

其次，在办理各种消费卡时，应特别注意保护好身份证号码、私人电话及住址类信息。

再次，要强化风险意识，必须确认证件及信息的用途与去向，不断增强自身抵御信用卡犯罪的能力。

典型案例之十二：盗用网号诈骗

案件分析：

犯罪分子通过技术手段盗号之后，向亲人朋友发送诈骗信息，往往让受害者误以为真。一些犯罪分子利用了国内外存在时差，国内的父母无法及时核实消息真实程度的特点，专门针对将子女送到国外读书的家长进行诈骗。

警方提示：

广大网民一定要不断增强网络安全防范意识，防止外人利用自己的网号进行诈骗活动，对自己的QQ号、微信号等网号要加强保密。如发现网号丢失或可能已丢失，第一时间通知亲友，以防受骗。有孩子在外的家长收到孩子网上发来的求助信息，一定更要第一时间电话确认，联系不到孩子时，要联系其所在学校的老师、同学等熟人确认。

典型案例之十三：投资理财诈骗

案件分析：

骗子投资公司利用受害人发布的自身真实信息获取受害人信任，然后用可观回报作为诱惑，诱骗受害人上当。

警方提示：

投资人不可轻信各种理财公司的高额回报诱惑，加强自身甄别意识，切莫贪图诱人回报而陷入诈骗陷阱，投资理财最好还是通过银行等正规金融机构。

典型案例之十四：彩票预测诈骗

案件分析：

嫌疑人通常是利用受害人的贪婪和急于发财之心，通过互联网散发虚构的预测彩票信息（例如：六合彩、福利彩票、体育彩票等），实行会员制，通过注册会员，预测中奖号码，收取会员费、保证金、税金等实施诈骗。其实，他们通过撒网式投放虚假信息抓概率，借其一步步诱导受害人以收取会员费、保证金、税金等为由让其向嫌疑人提供的账号打款。

警方提示：

福利彩票的发行部门是民政部门，其国家级管理机关只有中国福利彩票发行管理中心，彩票抽奖属于典型的“独立随机事件”，彩票预测只是一个明显违背科学常识的“陷阱”，警方提醒广大彩民，不要轻信所谓“预测中奖号码”的神话，更不能轻易汇款，对网站的内容可以向网站所属地公安机关电话咨询核实，不要轻易拨打网站上留有的电话，一旦轻信，追悔莫及。

典型案例之十五：冒充军人、武警采购诈骗

案件分析：

此类诈骗通常为团伙诈骗。犯罪分子利用人民群众相信军人、武警的心理实施行骗。以高利润的工程项目为诱饵，引诱受害人上钩，欺骗受害人代为向第三方采购物品。实际上，所谓的第三方也是诈骗团伙成员。

警方提示：

军队、武警等单位的工程项目同样需要履行正式的政府采购流程。同军队人员进行交易时，可以通过请其出示身份证件或到其所在单位证明其身份。

典型案例之十六：办理补助金诈骗

案例分析：

犯罪分子事先通过其他手段获取残疾人家庭情况，以残联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，受害人可享受残疾补助，以骗取事主信任，一旦受害人信以为真，即以交纳手续费等名义，诱导其到ATM机汇款。

警方提示：

家中有残疾人或低保家庭往往会遇到此类专门针对弱势群体的诈骗。在接到陌生电话或短信时，不要轻信所谓的国家出台新政策，可以办理补助的说辞。国家相关政策出台，将会通过新闻媒体报道告知，具体操作也是要到指定部门指定地点办理。切记，凡是到ATM机上进行任何办理操作均为诈骗。