8月1日，本版刊发《防范打击电信诈骗 鹰城公安在行动》，在社会各界引起强烈反响。今天，市公安局民警为市民支招，继续揭穿电信网络诈骗套路，普及、解读防范措施——

鹰城公安民警支招 防范电信网络诈骗

本报记者 卢拥军 通讯员 董亚东 李宗铭

●新闻背景：

8月1日，本版刊发《防范打击电信诈骗 鹰城公安在行动》。报道刊发后，在社会各界引起强烈反响，市民纷纷来电咨询如何精准防范电信网络诈骗，希望公安民警为其支招。

当日，市政府党组成员、市公安局党委书记、局长石秀田作出批示，要求全市公安机关宣传部门加大宣传力度，进一步提高群众对电信网络诈骗犯罪的识别防范能力，力争反诈工作提升到一个新水平。

为此，记者专门走访了市公安局犯罪侦查支队的反诈专家，揭穿不同电信诈骗套路伎俩，普及、解读防范措施，进一步提高全民防诈识骗能力。

图为抓捕电信网络诈骗犯罪嫌疑人现场。 本报记者 卢拥军 摄

一、网络贷款诈骗

随着人们提前消费观念的流行和网络金融行业的兴起，“贷款”成了不少急需资金人群的首选方式。平顶山市反虚假信息诈骗中心民警经常接到群众电话：网络上的贷款中介可靠吗？无抵押、无担保、黑户可贷款的公司能考虑吗？签了正规合同的贷款应该没问题吧？其实，这很可能是不法分子精心设计的骗局。

■贷款诈骗“手段”

1.最纯粹的贷款诈骗：交完费、不放款

网上有很多“无抵押、无担保，正规公司、极速放款”的广告，而且很多都留有联系方式，当你开始网络办理贷款时，甚至可以收到对方发来的现金支票和银行交易流水，看起来好像一切都很正规的样子，但对方会忽悠你缴纳一定的保证金，否则不放款。一旦你把钱打过去，对方立即就会把你拉黑。

这种贷款诈骗被称作“纯骗贷”，即以低门槛发放贷款的名义收取保险费、保证金、激活费、服务费等，但到最后一分钱也不会给你，所谓的现金支票、银行交易流水都是事先伪造的。

2.最跨界的贷款诈骗：验流水

这种贷款诈骗主要是盗刷银行卡团伙跨界作案，他们会让你登录一个看起来很正规的网站，先搜集你的个人信息，随后以验资为由让你把钱打到自己账户，然后要求你提供银行卡号及短信验证码。

很多人认为把钱打到自己账户比较安全，殊不知，他们索要你的银行卡账号和短信验证码后，就可以通过盗刷或者网上购物将验资款占为己有。

■警方支招：

1.贷款并不需要交保证金、做银行流水账，一旦遇上了，一定是假的！

2.千万不要把自己的银行卡密码、动态验证码提供给陌生人!! 切记切记!!

3.不要随意在网络上申请贷款，不要随便在网络上提供个人信息！

如需贷款请一定到正规银行或知名网贷公司，按正规程序贷款。且不可听信各类贷款中介忽悠，陷入以上种种网络贷款诈骗。一旦确认自己被诈骗，一定要及时拨打110或到辖区派出所报警，保留相关证据。

二、冒充淘宝客服诈骗

淘宝客服在我们大家一般的认识中，是解决我们购物疑问、售前售后等问题的中间人。但是不法分子却利用我们对淘宝客服的信任冒充淘宝客服退款进行诈骗。

不法分子会冒充淘宝客服，以提交订单未成功需退款为借口，冒充淘宝客服退款进行诈骗。这些人会先冒充淘宝客服以取得买家的信任，然后再向其发送网站链接，骗取买家的信息，以此转走买家的钱财。

冒充淘宝客服退款的会从网上购买个人淘宝网购物信息，然后冒充淘宝客服谎称系统异常，订单未提交成功，需要退回支付款项。

买家们对淘宝客服的信任被不法分子冒充淘宝客服退款进行诈骗的事件不少，记者提醒大家，对外来网站链接要求填写个人信息的一定要注意，不要再被冒充淘宝客服退款这种骗局给骗了。

■警方支招：

淘宝客服联系会员，基本都是通过站内信形式发送。因此，如果有人给你发QQ信息或旺旺信息，说他是淘宝客服，你要提高警惕了！如果涉及先交钱或是预交保证金，就得注意了，网上类似这样的骗子很多。

为避免木马诈骗，网购要在正规网站进行，且一定要安装防木马病毒的软件，避免上当受骗。同时提醒朋友们要增强防范意识，不要轻易相信互联网上搜索的所谓“客服信息”，一定要通过正规渠道获取相关信息，以免上当受骗，造成不必要的损失。

1. 正规企业客服联系会员，基本都通过站内信的形式发送。如有人通过打电话或网络聊天自称客服的，请提高警惕！

2. 通话中可详询对方工号和相关事宜，挂断电话后反打网站官方客服电话求证。

3. 如果涉及先交钱或是预交保证金的，需反复核实，确保自身利益，谨防网上类似骗局。

4.一旦要求登录某个网站、填写银行卡信息的，肯定是诈骗无疑。记者有话说：天上掉馅饼，一定是陷阱。网购多小心，谨防被诈骗！

三、“杀猪盘”诈骗

■什么是杀猪盘？

杀猪盘，是业内的行话。受害者被称为“猪”；培养感情的过程叫“养猪”；沟通话术叫“猪饲料”；沟通工具叫“猪槽”；到了最后收网骗钱就叫“杀猪”。杀猪盘属于交友类诈骗中的“精准诈骗”，我们熟知的“卖茶女”也属于这一范畴。

杀猪盘内部有严密分工，一般分为话务组、供料组、技术组、洗钱组四类。其中供料组和技术组算是技术工种，一般不露面，供料组负责在婚恋网站物色对象提供给话务组；技术组主要是在国外租用服务器，每天搭建不同的赌博网站、彩票网站、投资平台，只要话务组有需求，就无限量供应。

■杀猪盘的诈骗流程是怎样的？

1.搭讪加好友，双方迅速坠入爱河，进入热恋期。一开始骗子会每天嘘寒问暖受害者，双方很快会建立关系。

2. 让受害人觉得自己出手阔绰，但其实和本身经济情况不符，激起受害人好奇心，顺势介绍虚假赌博网站。

通常，骗子会告诉受害者自己从事赌博网站技术维护工作，称自己近期发现技术漏洞，可以利用这个漏洞修改后台赔率，稳赚不赔。一开始会先引诱受害者投入小额资金，比如500元、3000元，不到一个小时让你赚100元、1000元，并且能成功提现。

感情诱骗也是惯用手法。若受害者表达不愿再投钱的想法，骗子就会打出感情牌，给受害者描绘赚钱之后一起买房、买车、养孩子、旅游的美好生活，受害者基于对美好未来的向往以及对“恋人”的信任，往往难以自拔。

3.受害者尝完甜头后，骗子称漏洞马上就要修复，来笔大的。

这个时候也是“收网”的时候了，骗子会要求受害者拿出所有积蓄，并怂恿受害者借钱、贷款。受害者在冲昏头脑、有利可图的情况下，借、贷凑个100万元一起投进去，之后第二天便会发现已经联系不上心目中的他(她)，受害者被骗子拉黑了。

■杀猪盘诈骗周期是多长？

相比一般诈骗周期比较长，因为感情培养需要时间，一般半个月以上。骗子会将受害者分为A、B、D三类，表示对博彩感兴趣的受害者被归入“A类”，是重点诈骗对象；表示有点意思的受害者被归入“B类”，是可发展对象；反应平淡的则被归入“D类”，骗子将放弃行骗。

■警方支招：

1.认识到网络永远是虚拟的世界。我们永远不知道网络那端是谁。网上交友一定要慎之又慎，时刻保持警惕，勿轻信“附近的人”，对网站上的信息认真审查，注意对方是否已通过实名认证，千万不要相信“有缘千里来相会”。所以交友也好、投资也好，都要提高警惕，天上不会白掉馅饼，任何人都是有可能上当受骗的。

2.规范自身行为。当对方对你提出金钱上的求助，或者指引你到某博彩、投资理财平台“赚大钱”的时候，一定要提防骗子已经下饵了。让自己远离网络上违法行为，确保诚信守法、洁身自好，能很大程度上避免交友类诈骗。

3.投资有风险，理财需谨慎。投资前应通过正规途径了解相关金融知识，面对各种标榜“专业指导”“高额回报”“稳赚不赔”等网络投资理财推销，要拒绝高息诱惑，谨防上当受骗。

4.一旦发现是骗局，要保留相关证据(双方联系记录、婚恋网站账号、手机号码、微信账号、汇款转账账号等)，然后立即拨打110报警求助。

在任何时候、任何环境下，都不要向他人轻易透露个人信息，不在网络上接受身份不明的人员为好友。最重要的，是要彻底打消借助特殊渠道一夜暴富的念头，对一切投资中介和网络平台打出的高额回报和利益诱惑，保持高度警惕和戒备心理。

四、冒充公检法诈骗

冒充公检法诈骗，会要求对个人全部财产进行验证，被害人一旦上当受骗，往往倾家荡产，社会危害巨大。

第一步：骗取信任

骗子通过网络购买的受害者个人信息，例如身份证号、住址等隐私来取得受害者的初步信任，同时会通过改号软件将来电显示为警方办公电话，让受害人拨打114查询验证，进一步增强受害人的信任。

第二步：震慑

骗子会通过严肃谨慎的语气，强势震慑并控制受害人。

第三步：恐吓

骗子让受害者彻底相信自己卷入了一个重大案件，随时可能被逮捕。为了增强恐吓，让骗局更加逼真，骗子会通过虚假政法机关官网或网络传真让受害人收到一份通缉令。

第四步：遥控转账

骗子声称要做资金调查，利用受害人的恐慌心理，缓和语气，诱骗受害人入局。实则是要求受害人把将银行卡插入ATM机，然后把卡内的资金转到指定的账户，或者要求受害人将所有资金汇集到一张银行卡，然后骗子通过骗取密码、验证码、网银等，直接通过对方提供的信息将该张银行卡的资金转走。

■警方支招：

1.公检法之间的电话不能直接转接

电话转接主要通过程控交换机来实现同一单位不同办公室电话的自动转接。公安局、检察院、法院都有自己独立的机构、人员，为了安全考虑，也都有自己独立的网络和通信系统，电话根本无法做到直接转接。

2.公检法移交案件必须依照规定的程序

公安、检察院、法院虽然都是国家政法机关的重要组成部分，但分工不同又相互制约。一般说来，除了国家机关工作人员犯罪，其他案件都由公安机关侦办，在侦办终结后才能移交检察院。检察院也需要做好全部的审查，才能移交法院。任何一个环节，短则几天，多则数月，绝不可能直接通过办案人员打个电话就能移交案件。

3.通缉令不会直接发给个人

除了重大案件通缉令会通过新闻媒体向社会公布，发动公众举报嫌疑人外，其他通缉令都只能由公检法内部人掌握，以方便抓捕，绝不可能专门把通缉令发给嫌疑人或者让嫌疑人自行查阅。

4.公检法机关没有“安全账户”

公检法机关在对违法当事人或被告人作出行政处罚或审判后，会告知其将罚款缴至相应的“对公账户”，但绝对没有所谓的“安全账户”。公检法调查资金往来会直接到银行调取相应流水，绝对不会动你的任何“钱财”。

5.任何人都没有权利要别人出示“验证码”

验证码和银行密码一样重要，任何国家机关和银行、他人都无权要求你出示“验证码”。当然，这里特别要说明的是，公检法等机关都可能通过电话联系当事人，询问或告知相关事项，但一般不会通过电话直接办案，更不会通过电话做笔录(一般会寻求当地公检法协助)，陌生人给你打完电话就要求告知“验证码”或者“转钱到安全账户”的，基本可以认定是骗子！

五、“机票改签”诈骗

如果你突然收到短信：“您所乘坐的航班取消或延误。”重要的是航班信息及个人信息百分之百吻合，你会怎么办呢？相信很多人都会选择按提示操作处理。可是，一旦按照短信的内容进行操作，你就落入了不法分子设下的机票退改签诈骗陷阱。

骗子先通过非法渠道获得乘客的航班信息，然后使用改号软件假冒航空公司电话向购票乘客发送短信，谎称因故取消航班。接着骗子就会通过冒充客服的电话，告知受害人航空公司会退还机票费以及赔偿相应的金额，同时要求受害人提供自己的银行卡号以及银行发送的验证码(其实是银行的支付验证码)，由于之前短信中的个人信息都是正确的，往往受害人在此时都不会起疑心，当受害人提供验证码后就会发现自己银行卡中的一笔资金不翼而飞，此时再拨打“客服”的电话，就会发现“客服”的电话已经无法接通了。

■警方支招：

1.购买机票应通过正规网站、正规途径。

2.骗子经常使用改号软件，因此，在收到类似“航班取消、航班变动、机票退签改签”等内容的短信时，应通过航空公司官方客服核实消息的真伪，不要盲目轻信来路不明的信息，不要拨打短信中提供的陌生号码，更不要按照对方的要求转账。

3.网络购票时要注意保护隐私，切勿向陌生人透露银行卡的卡号和银行发送的验证码等信息(特别注意：在操作过程中骗子让受害人提供的所谓的“验证码”，往往就是银行的支付密码)。

六、兼职刷单诈骗

上网就能赚钱？躺在家中就能日赚百元？这样无门槛、超回报、零风险的工作，真的有吗？

但是，你相信了就上当了，近日“兼职刷单”诈骗高发，每天都有数人被骗，这背后到底隐藏了什么骗局？

1.消费者在网购的过程中，会精挑细选货比三家，商家的信誉、商品销量、顾客评价都会成为重要的参考因素。不管哪个电子商务平台都存在虚假交易，于是催生了很多刷信誉需求。所谓的刷信誉，是指在购物网站中，卖方为提升网站或者商品的人气而采取的一种违规商业炒作模式。对于兼职的刷客来说，并不需要拥有此件商品，只需要帮助卖家完成交易获得佣金。兼职刷信誉本身就是一种非法行为，不仅破坏了诚信体系和市场的公平竞争，还可能构成违法行为，存在漏洞，容易被犯罪分子利用。

2.骗子通过短信、社交软件、电子邮箱发布网络刷单小广告吸引目标群体。

3.为了博取应聘者的信任，骗子通常会在线上给应聘者展示各种营业执照、企业注册文件、后台系统页面，来营造自己诚信经营者的形象。实际这些所谓的执照通过简单的PS即能够伪造出来。

4.骗子的专业化和细致分工也是导致人们受骗的原因。有专人通过论坛、招聘网站等渠道发布广告，有专人为前来应聘的人员介绍“兼职内容”，有专门的“客服”“业务经理”，各种角色轮番上演。用专业的术语和“贴心”服务来获得受害者的信任。

5.骗子会先给应聘者一两个比较小额的刷单任务，有时候还会按照“约定”返还本金和佣金，晒兼职的收益，付款截图，为的是“放长线钓大鱼”，充分赢得应聘者的信任。随后，骗子会逐渐加大刷单的金额和数量，同时利用各种系统问题、网络问题等理由，来诱骗应聘者加大投入，让被害人的付出成本不断加大，最后无路可退。

如此手法，周而复始。

■警方支招：

此类诈骗案件受骗的多为年轻人和家庭主妇，尤其是以大学生为主。很多情况下，都是受害者主动申请刷单兼职，他们判断力相对较弱，涉世未深，缺乏社会经验，但是自由支配的时间又较多。在接触到招聘刷单的信息时，一定要提高警惕，不要因小失大，切莫贪小便宜。此类“兼职工作”本身就是损人不利己的行为。帮助部分网店商家进行投机行为，伪造高质量、高评价的网店形象，损害了大部分网购者的利益。

骗子往往在开始给你返利，使受害者放松警惕。骗子展示的“晒单”未必真实，图片显示的转账记录、聊天记录、买家好评，都可以由软件自动生成。当你首次刷单后便会以各种理由(一般是此单由多个任务组成、做单时间过慢导致系统错误、完成大额才能返还)让受害者深陷其中。

七、冒充QQ好友诈骗

网络聊天软件传来一条消息，某好友称亲友正在住院，请帮忙转一笔钱应急。转还是不转？

近年来，类似的诈骗报道时常见诸媒体，当事人信以为真，立即转款，自己满以为是对好友仗义救急，却不知钱款进的是骗子的口袋，等到反应过来，求助的“好友”不见了，转出去的钱也很难追回。

受害者以年轻群体为主，安全防范意识弱。据了解，受害人绝大部分是大学生、高中生，以及刚走上社会的年轻人。他们是QQ平台的活跃用户，社会经验较少，防范意识也不强。诈骗团伙盗取QQ账号后，一般是向账号内联系人群发虚假求助消息，收到联系人回复后再步步引诱上套。由于学生的回复率比较高，骗子常常选择在特殊时间段作案，以降低被电话、视频等验证的可能性。

犯罪分子采用发送信息、文件、压缩包、网址等方式向他人电脑或手机植入木马病毒，通过植入的木马病毒盗取他人QQ账号，进而通过查看所盗得QQ账号的备注信息、聊天记录或视频，了解其人际关系、交谈方式、生活习惯等情况，再利用所盗得QQ号码冒充QQ账号使用者本人与其QQ好友聊天，采用截图、视频等方式取得对方信任后，最后以交学费、借钱、结账等方式要求对方汇款至犯罪分子指定账号。

■警方支招：

在用网络社交平台与好友联系时，若对方以紧急情况为由，发出帮忙付款、充值等请求，要通过电话、视频等渠道对好友身份进行核对确认，不能仅凭文字信息就配合转账。同时还要注意保护个人信息，不要随便泄露自己的银行卡号、身份证号码等信息，以防骗子利用软件生成虚假转账单实施诈骗。此外，在第三方支付平台进行大额转账时，可以设置延迟到账，为追回损失争取时间。

“遭遇诈骗一定要及时报案!”警方特别提醒，一方面，越早报案越有利于实现紧急止付和快速冻结，最大限度减少财产损失；另一方面，也有助于警方快速掌握案情，为打击电信诈骗犯罪活动赢得主动权。

八、冒充军警购物诈骗

冒充军警购物诈骗，此类诈骗案件主要针对个体工程承包商、私营业主。

惯用伎俩：冒充军警(武警、武装部等单位)人员，声称有工程项目、购买指定的罐头、军用帐篷、消防器材等。

诈骗过程：嫌疑人通过不法渠道查询到军警信息或军警工作人员的信息，然后嫌疑人员便开始冒充军警“领导”给工程承包商、私营业主打电话，首先会以需要订餐、承包项目等为由与工程承包商、私营业主联系，并称因近期部队里某某处要演习或汇演，需要从地方购买物资，让其介绍能够采购物资的人员。这时受害人往往认为是由熟悉的朋友介绍的赚钱项目，便主动联系冒充军警的嫌疑人，嫌疑人随后便以需要采购指定品牌的物资为借口并将指定厂家电话告知受害人，受害人再次联系需购物品的厂家时，对方以先打款后发货为由，让受害人将货款打入指定的银行卡内，进行诈骗。

该类案件中，因涉及朋友介绍、领导介绍，受害人上当受骗概率极大，且被骗数额巨大。一旦将钱款转入指定银行卡内，犯罪嫌疑人会在数分钟之内，借助互联网金融渠道将资金通过第三方支付给虚假商户进行转移。目前该种资金转移方式无法快速止付、冻结，资金追踪核查繁琐，侦破难度较大。

■警方支招：

1.广大商户在网上发布采购信息时不要透露过分详细的个人信息，对任何自称军、警方面人员的陌生电话都需保持戒心，任何军、警单位均不会轻易与个体商户合作，更不会要求群众汇款。

2.军警人员采购物资会履行严格的书面程序，切莫相信这种空对空的电话联系和转账方式。

3.遇到类似情况时需提高警惕，首先要核实其身份真伪，交易中如无法核实对方提供的供货厂商是否正规时，请立即中止交易，谨防上当受骗！

4.“切莫贪小便宜，天上不会掉馅饼”，如不幸被骗，立即拨打110报警。