今年以来，全市公安机关紧紧围绕“两降两升”工作目标，以“雷霆”反诈行动和“云剑行动”为契机，充分利用“三合一”平台，坚持打防并举，对电信网络诈骗犯罪发起凌厉攻势——

防范打击电信诈骗 鹰城公安在行动

本报记者 卢拥军 通讯员 董亚东 李宗铭

●新闻背景：

为不断创新安全防范宣传新模式，7月18日上午，市公安局与美团点评集团签署战略合作协议，同时启动反电信诈骗集中宣传活动。当天，双方在美团外卖骑手协助开展防范电信网络诈骗宣传活动上达成战略合作协议。

市政府党组成员、市公安局党委书记、局长石秀田在启动仪式上指出，平顶山公安机关与美团达成战略合作框架协议，是顺应“互联网+”发展态势，主动探索提升社会治安防控智能化水平，是深化警企合作、推进社会共治、共同抵御和消除治安风险隐患的重要保障，必将对提高公安机关社会治理水平和打击刑事犯罪产生积极而深远影响。

据统计，今年上半年，全市公安机关共刑拘诈骗犯罪嫌疑人605人，同比上升205.6%；冻结涉案资金9304.7万元，同比上升624.2%；起诉电信诈骗犯罪嫌疑人158人，共破获案件1361起，处置涉案银行卡3509张，同比上升578.7%。

市公安局以维护群众合法利益为出发点，以推进反虚假信息诈骗中心建设为主线，不断完善打击、防范虚假信息诈骗犯罪工作机制，通过创新打击模式，持续加大打击力度，拓展反诈骗中心工作职能，加强与第三方支付平台协作，有力地提升了全市反虚假信息诈骗犯罪工作的能力和水平。

近日，记者深入市公安局，对今年以来打击电信诈骗工作进行了采访。现列举以下典型案例。

图为矿工路派出所打掉电信诈骗犯罪团伙现场 本报记者 卢拥军 摄

美女网友带来巨额资产？

突然接到陌生美女加微信好友的请求后，你会怎么办？其实，美女背后可能是一个电信诈骗团伙。他们的目标就是：掏空你的钱包。

今年5月22日，一男性张某到市公安局姚孟派出所报案称，自己被人骗了84000余元。事情的经过是，今年2月7日，微信昵称“阿丽莎”的人加张某为好友，闲暇时间两人聊天甚多，一来二去成了无话不说的“熟人”。3月的一天，“阿丽莎”突然告诉张某自己曾经的显贵身份目前在国外陷入困境，需要办理护照回到中国。到达中国后，就可以将在国外银行的1800万美元巨款转移到张某名下，而后便可以一起在国内投资，赚个“盆满钵盈”。

张某信以为真，随后将3万余元打到“阿丽莎”提供的银行账号上。之后，“阿丽莎”告诉张某办理护照费用已够，但是需要再交9万美元的庇护费用，就可以解困回到中国。得知张某没有足够现金，善解人意的“阿丽莎”就提供一个国外银行邮箱地址，张某只要按照其要求给银行写信，1800万美元就可以直接打款到他银行卡中。次日，银行回信，要求其限期在银行指定账户打款，之后就可以解冻资金。按照银行要求，张某先后以“授权费”“资金转移费”等名义，向对方转账5万余元。

5月22日，张某再次被要求以“手续费”“保管费”等转款。此时的张某已经囊中空空，他向亲戚借钱遭拒时才恍然大悟。

接报后，姚孟派出所政委宗健刚立即抽调精干力量成立专案组开展侦查。专案组民警深入研判，成功锁定犯罪嫌疑人系杨某萍，并获悉其最终落脚点为广州市番禺区某住宅区。办案民警迅速前往，果断出击，最终于6月3日在其租住房屋内将嫌疑人杨某萍成功抓获，查获银行卡17张。

据姚孟派出所案件侦办大队教导员朱晓轲介绍，今年初，嫌疑人杨某萍通过网络结识境外电信诈骗团伙人员。为非法获取利益，杨某萍先后利用多张银行卡，为电信诈骗团伙实施诈骗提供取现、转移服务收取“佣金”。警方发现，杨某萍银行卡经常有大量资金流入流出。

冒充女性微信交友诈骗

近日，市公安局北渡派出所打掉一个专门冒充美女网络交友进行诈骗的犯罪团伙。该团伙在两三个月的时间内累计诈骗金额30多万元，60多人受害。目前，6名团伙成员已被执行逮捕。

一个女孩的QQ头像在手机屏幕上闪烁，张先生点开一看，是一个网名叫“小依”的女网友要添加他为好友。抱着好奇的心理，张先生通过了好友请求。后来的一段时间，“小依”经常跟张先生聊天，张先生感觉对方是一个年轻、漂亮、小鸟依人般的女孩，便逐渐消除了戒心。

有一天，“小依”表示想去找张先生玩可惜自己没工作没路费。没想到女孩主动要来找自己，欣喜若狂的张先生当即就给对方转过去了几百元路费，心里美滋滋地等着对方上门。

一会儿，“小依”给张先生发来了一张河南洛阳火车站的照片，说在车站不小心把别人的苹果手机碰坏了却没钱赔。美女遇到困难岂能袖手旁观？张先生很快又给对方转过去了数千元。不一会儿，“小依”发来信息，问题已经解决，马上就要开车了。

两个小时后，“小依”说自己已经到了平顶山，但是怀疑张先生对她的感情是不是真的，正犹豫见不见面。既然美女都快到家门口了，为表明心意，张先生又给“小依”转了一笔款。可是，“小依”还是不肯见面。花了几千元却连美女的面都没见到，情急之下，张先生质问对方是不是骗子，没想到立即被拉黑了。这下，张先生醒悟过来：自己被骗了。

接到张先生报案后，市公安局北渡派出所所长姚明柱立即组织警力进行侦查。经过初步调查、分析，认为这是一起典型的网络交友诈骗案。考虑到嫌疑人通过QQ与受害人聊天、又通过微信接收转账，办案民警便以此着手，通过数据分析，选定了一个嫌疑最大的微信号进行了重点调查。巧合的是，这个微信号绑定了一张银行卡，持卡人是河南洛阳的中年女子张某某，而且调查显示张某某的儿子李某彬案发后在安阳市某地取走了被骗资金，李某彬的嫌疑陡然上升。

在河南安阳市某镇，办案民警苦等3天后，天降大雨，李某彬突然出现并帮张某某夫妇收烧烤摊。民警跟踪李某彬到其住处时立即将其控制，并起获了留有与受害人聊天记录的多部手机和电脑。

办案民警对起获的手机和电脑进行分析，发现这是个诈骗团伙，成员都是一个村的，涉案资金达到几十万元，受害人多达五六十位。

办案民警再次回到了安阳市，李某彬的同伙早已经闻风而逃。办案民警随即赶到李某彬等人的老家洛阳开展摸排。5月30日，办案民警在洛阳市下辖的两个县同时收网，一举抓获了该团伙的另外5名成员古某超、古某可、王某辉、王某阳（女）、赵某超。

据办案民警介绍，此案中犯罪分子借助聊天软件QQ的兴趣部落等搜索外地的陌生男性，团伙成员冒充年轻美女和受害人聊天培养感情或者假装谈恋爱，但绝不与受害人直接见面。等取得受害人信任后，犯罪分子再利用受害人急于见到“美女”的心理，借口没有路费、碰坏了别人的贵重物品没钱赔偿，或者要求受害人给钱以表明对女方的心意等等，让受害人给他们转账，一旦诈骗得手，便立即将受害人拉黑，而受害人往往被骗了钱却连“美女”的面都没见到。该团伙成员不仅进行了分工，还制定了“规章制度”：有人注册QQ号、微信号，有人冒充美女与受害人假装谈恋爱，有人专门取款，还有人专门统计诈骗金额大小据此发奖金。

假扮成功人士吸引单身女性

今年6月30日，引人关注的“2018·3·20”针对单身中年妇女实施的网络诈骗案已由检察机关正式向法院提起公诉，该案140名犯罪嫌疑人将受到法律严惩。

据侦破此案的市公安局矿工路派出所所长谢书军介绍，2018年3月份，矿工路派出所接到举报称：市区某电子商务有限公司涉嫌诈骗。为查清该公司的诈骗手段和资金流向，派出所派遣了一名精干的侦查员以业务员的身份应聘到该公司，展开卧底调查。

办案民警在调查中发现，每逢有新的业务员加入，便被公司要求先学会自我包装。所谓自我包装，就是在网络上搜集一些形象好、气质佳的40岁到60岁之间的男性照片，再配上打高尔夫、开豪车、品洋酒、在国外旅游等奢侈生活的照片，展示自己的成功形象。随后以假名在一些婚恋网站注册，专门加40岁到60岁之间的单身女性进行网聊。此案被骗的单身中年妇女达500人，分别来自全国20多个省份，涉案金额6000多万元。

网聊中，“成功男士”大打感情牌，对这些女性嘘寒问暖、关爱有加，赢得她们的信任，让她们误以为找到了可以依托的人生伴侣。等到时机成熟，“成功男士”就会向女方推荐一款名为“EA”的外汇交易软件，用这个交易软件炒外汇只赚不赔，每天可盈利数万元，谎称自己在“博美”“迈德汇”两个外汇交易平台上赚了大钱，以此引诱女方投资。一旦女方上钩，就必须先要购买这个“EA”外汇交易软件，价格从6800元到26800元不等，以一万美金起步，在第三方支付平台注资后即可操作。为了彻底打消女方的顾虑，“成功男士”还会向她推荐“迈德汇”平台的企业总监、技术员等3人共同为她服务。

经过外围调查，警方基本掌握了涉案团伙的作案手法及人员构成，遂实施集中抓捕行动。2018年3月19日，矿工路派出所组织警力，在位于市区佳田国际大酒店21楼的河南省某电子商务有限公司实施抓捕行动，当场抓获包括主犯焦某辉在内的犯罪嫌疑人101人，查获涉案电脑100台、诈骗所使用话术范本101份、所使用的QQ号102个。截至今年3月，在逃的其他犯罪嫌疑人也陆续被抓获归案。

经调查查明，2016年初，焦某辉、白某歌、张某兵、祝某斐、李某某注册成立河南省某电子商务有限公司，并通过市面以1万元的价格购买了一款名为EA的外汇自动交易软件，然后对软件进行简单包装维护。随后，这家公司大量招聘业务员，并要求他们以虚假的40岁至60岁单身离异或丧偶男性的身份，诱骗40岁至60岁的离异或丧偶中年女性。

“博美”平台实际为焦某辉等人所加盟代理的虚假平台，“迈德汇”为焦某辉等人实际控制的虚假平台。被害人所投入的资金均未真正进入国际外汇平台，而直接由第三方支付平台转移至焦某辉等人的个人账户。

这个涉案团伙骨干分工明确。马某系公司讲师部负责人，对新入职员工进行诈骗话术业务培训等，鼓励新招聘员工积极参与实施诈骗；李某伟系公司商务程序部负责人，负责修改EA软件参数，以增加客户交易量而导致客户大额亏损；刘某系公司风控部负责人，负责为迈德汇平台进行售后服务，以防被害人发觉被骗。

“其实骗术并不高明，先打感情牌，再通过小盈利获得女方的信任。”矿工路派出所副所长孙建峰说，由于软件本身无法帮助被害人盈利，焦某辉等人在公司设置风控部，以维护客户为名以防被害人发觉软件为虚假无用软件，便故意设置让被害人盈利的程序，一步步诱其投入大量资金。

犯罪嫌疑人张某系销售二部飞虎队组长，其取得两名女性的信任后，直接诈骗31万元。犯罪嫌疑人石某系销售一部光速队组长，与4名女性打得火热，直接诈骗客户153万余元。

“黑平台”以炒期货为名诈骗钱财

据市公安局青石山派出所党委书记朱平生介绍，该所经过近20天的缜密侦查，辗转千里，奔赴浙江、广东等地，打掉以期货投资为名、构建虚假平台实施网络诈骗的犯罪团伙，刑事拘留犯罪嫌疑人32人，查获作案用的电脑65台、手机118部、银行卡50余张，捣毁诈骗窝点两处，扣押涉案资金100余万元。

2019年4月2日16时许，市民卢某报警称，自己从2019年1月起，经朋友介绍，在网上被人以炒股投资等形式骗走人民币6万元。接警后，该所立即组织相关人员进行综合研判。经查证，这个虚假期货指数平台以高额回报诱骗受害人加入，有重大诈骗嫌疑。

该所案件侦办大队大队长马俊峰带领民警，围绕该期货指数平台资金流向开展侦查工作，发现各类线索均指向浙江省杭州市，随即指派侦查工作组赶赴杭州等地调查。在浙江警方的大力配合下，民警通过线上线下交叉核查，最终查明该案背后隐藏着一个公司化运营的电信网络诈骗团伙。

该团伙总部位于杭州市西湖区的一栋写字楼内，该公司负责人陈某冒用他人名义，首先通过微信以推荐股票为由拉人入群，团伙成员分工明确，在所谓“工作微信群”里散播赚取巨额利润的图片，吸引受害人上钩，然后再游说受害人投入更大资金到陈某的所谓“炒期货平台”进行层层诈骗，而钱款则进入陈某掌控的个人银行账户及其代理商的个人银行账户内，并未进入真正的期货市场。案发前，该团伙有两个公司在运营，分别在杭州市西湖区和广东省揭阳市两个窝点。

经过细致摸排、乔装跟踪，办案民警初步查清了整个诈骗团伙的组织架构、人员层级，集中收网时机成熟。5月17日，青石山派出所组成抓捕工作组，兵分两路挥师南下浙江、广东等地。在当地警方的大力配合下，于5月17日10时许，两省同时实施抓捕，并收缴作案用的电脑65台、手机118部、银行卡50余张。

5月18日下午，民警将涉案犯罪嫌疑人安全押解回平顶山。

返回平顶山后，专案组迅速组织精干力量对案件集中攻坚。经审讯，陈某等32人对其利用网络投资平台诈骗他人钱款的犯罪事实供认不讳，诈骗受害人30余名、金额600余万元。5月19日，32名犯罪嫌疑人因涉嫌诈骗罪被公安机关依法刑事拘留。

“贷款陷阱”频频得手

近日，市公安局东安路派出所成功打掉一个以“贷款陷阱”实施犯罪的电信诈骗团伙，8名团伙成员悉数落网，带破电信诈骗案件30余起。

今年4月4日14时，该所接到受害人报警，称其办理网络贷款时被骗。接报后，该所副所长宋晓鹏带领民警进行案情研讨，制定侦查方案，明确侦查方向，划定侦查范围。

经查，4月4日上午，报警人贾某某在上班时收到陌生人微信好友申请，添加微信后，对方以低利率网络贷款为诱饵使受害人掉入陷阱。犯罪嫌疑人以支付“贷款订单费”为名，先后通过微信收款二维码对受害人实施诈骗，金额共计3999元，支付成功后将贾某某微信拉黑。

经过大量工作，办案民警确定嫌疑人信息位置为广东省东莞市，并逐步掌握了该团伙的主要犯罪成员以及犯罪证据。5月20日，抓捕时机已成熟，派出所民警魏新峰、杨旸等人立即启程赶赴东莞市开展抓捕工作。5月23日，在当地警方的大力配合下，办案民警在东莞市西平社区一村庄内成功抓获嫌疑人李某某、杨某、覃某某。5月25日，在东莞市西平办公楼内将李某、何某某、孔某某、游某某、姜某等5人抓获。至此，该团伙成员全部落网。

经查，李某某等人对其于2018年11月以来，以办理网络贷款为名引诱受害人扫描二维码支付“贷款订单费”，先后骗取受害人贾某某等30余人的犯罪事实供认不讳。

目前，犯罪嫌疑人李某某等人已被刑事拘留。

●新闻链接：

16种常见的电诈类型

电信诈骗是犯罪分子以非法占有为目的，利用移动电话、固定电话、互联网等通信工具，采取远程、非接触的方式，通过虚构事实诱使受害人往指定的账号打款或转账，骗取他人财物的一种犯罪行为。

现将公安部门总结出的近年来发案较多的16种电信诈骗类型公布如下：

1.QQ冒充好友诈骗

利用木马程序盗取对方QQ密码，截取对方聊天视频资料，熟悉对方情况后，冒充该QQ账号主人对其QQ好友以“患重病、出车祸”“急需用钱”等紧急事情为由实施诈骗。

2.QQ冒充公司老总诈骗

犯罪分子通过搜索财务人员QQ群，以“会计资格考试大纲文件”等为诱饵发送木马病毒，盗取财务人员使用的QQ号码，并分析研判出财务人员老板的QQ号码，再冒充公司老板向财务人员发送转账汇款指令。

3.微信冒充公司老总诈骗财务人员

犯罪分子通过技术手段获取公司内部人员架构情况，复制公司老总微信昵称和头像图片，伪装成公司老总添加财务人员微信实施诈骗。

4.冒充公检法工作人员电话诈骗

犯罪分子冒充公检法工作人员拨打受害人电话，以事主身份信息被盗用涉嫌洗钱等犯罪为由，要求将其资金转入国家账户配合调查。

5.退款诈骗

犯罪分子冒充淘宝等公司客服拨打电话或者发送短信谎称受害人拍下的货品缺货，需要退款，要求购买者提供银行卡号、密码等信息，实施诈骗。

6.办理信用卡诈骗

犯罪分子通过报纸、邮件等刊登可办理高额透支信用卡的广告，一旦事主与其联系，犯罪分子则以“手续费”“中介费”“保证金”等虚假理由要求事主连续转款。

7.贷款诈骗

犯罪分子通过群发信息，称其可为资金短缺者提供贷款，月息低，无需担保。一旦事主信以为真，对方即以“预付利息”“保证金”等名义实施诈骗。

8.收藏诈骗

犯罪分子冒充各类收藏协会的名义，印制邀请函邮寄各地，称将举办拍卖会并留下联络方式。一旦事主与其联系，则以“预先交纳评估费”“保证金”“场地费”等名义，要求受害人将钱转入指定账户。

9.机票改签诈骗

犯罪分子冒充航空公司客服以“航班取消、提供退票、改签服务”为由，诱骗购票人员多次进行汇款操作，实施连环诈骗。

10.“猜猜我是谁”诈骗

犯罪分子获取受害者的电话号码和机主姓名后，打电话给受害者，让其“猜猜我是谁”，随后根据受害者所述冒充熟人身份，并声称要来看望受害者。随后，编造其被“治安拘留”“交通肇事”等理由，向受害者借钱，一些受害人没有仔细核实就把钱打入犯罪分子提供的银行卡内。

11.钓鱼网站诈骗

犯罪分子以银行网银升级为由，要求事主登录假冒银行的钓鱼网站，进而获取事主银行账户、网银密码及手机交易码等信息实施诈骗。

12.解除分期付款诈骗

犯罪分子通过专门渠道购买购物网站的买家信息，再冒充购物网站的工作人员，声称“由于银行系统错误原因，买家一次性付款变成了分期付款，每个月都得支付相同费用”，之后再冒充银行工作人员诱骗受害人到ATM机前办理解除分期付款手续，实则实施资金转账。

13.订票诈骗

犯罪分子利用门户网站、旅游网站、百度搜索引擎等投放广告，制作虚假的网上订票公司网页，发布订购机票、火车票等虚假信息，以较低票价引诱受害人上当。随后，再以“身份信息不全”“账号被冻”“订票不成功”等理由要求事主再次汇款，从而实施诈骗。

14.ATM机告示诈骗

犯罪分子预先堵塞ATM机出卡口，并在ATM机上粘贴虚假服务热线告示，诱使银行卡用户在卡“被吞”后与其联系，套取密码，待用户离开后到ATM机取出银行卡，盗取用户卡内现金。

15.金融交易诈骗

犯罪分子以某某证券公司名义通过互联网、电话、短信等方式散布虚假个股内幕信息及走势，获取事主信任后，又引导其在自身搭建的虚假交易平台上购买期货、现货，从而骗取事主资金。

16.二维码诈骗

犯罪分子以降价、奖励为诱饵，要求受害人扫描二维码加入会员，实则附带木马病毒。一旦扫描安装，木马就会盗取受害人的银行账号、密码等个人隐私信息。

（卢拥军）