

处置、打击、宣传三大模块组合发力 瑞安警方对通讯(网络)诈骗说不！

通讯员 赵小鸥 记者 陈丹丹

冒充公检法人员实施电话诈骗、在虚假短信中植入网络病毒链接、盗取QQ冒充熟人……近年来，通讯(网络)诈骗犯罪呈高发态势，不断翻新的诈骗手段令人眼花缭乱、难辨真伪。

据相关统计数据显示，我市通讯(网络)诈骗发案数量及被骗金额均位列温州全市各县(市、区)前三名。

近年来，我市警方全面开展通讯(网络)诈骗打防管控一体化建设，在处置、打击、宣传三大模块组合发力，成效显著。截至11月20日，全市通讯(网络)诈骗案件同比下降23.07%，打击诈骗对象221名，其中抓获2·20特大电信诈骗案同案人员166名，破案50多起，涉案金额3800多万元，止付止损被骗资金500多万元，其中冻结被骗资金398万元，追回资金130万元。

打击诈骗拼速度 止损止付 以快制快

猜猜我是谁、我是你领导、网上购物退款、中奖短信……名目繁多的各类诈骗短信、电话，在市民生活中不少见。

据警方透露，近年来通讯(网络)诈骗手段渐趋专业化、职业化，诈骗手法花样百出。

今年3月7日，家住塘下的市民周女士接到了一通冒充“公检法”的电话，差点被骗走银行卡里的170万元存款。当天，温州市反诈骗中心在对诈骗号码进行大数据分析时，发现其中一个诈骗号码与周女士存在异常通话。该中心随即回访周女士，判断分析了具体情况后确认为诈骗电话，劝阻她继续汇款并止付被骗资金40万元。

等到周女士止付后，瑞安市公安局反诈专班和塘下派出所及时冻结了该笔被骗资金，并办理了资金返还手续。6月15日，在温州市反诈骗中心的大力支持下，这笔被骗资金回到周女士手里。

据周女士回忆，当天中午，她在家接到一个自称“重庆公安局刘警官”的电话，对方说破获一起全国特大诈骗

案，有一笔200万元的诈骗赃款转到她的银行卡上，要对她进行调查。周女士对诈骗手段不了解，再加上“刘警官”的恐吓，精神防线很快被攻破，按照对方指示将银行卡里的100万元转到所谓的“安全账户”。正当她准备把另外一张银行卡里的70万元存款转给对方时，瑞安警方及时发现并拦截，才得以挽回损失110万元。

这是市公安局在温州市反诈骗中心直接办理案件被骗资金返还的首个成功案例。

无独有偶。今年10月11日下午，我市警方在大数据分析时，发现受害人甘女士疑似被冒充公检法的人诈骗，且电话关机。民警立即赶到甘女士所在的宾馆，但她已退房离开。民警判断她极可能去附近银行汇款，便兵分多路查找，所幸赶在她按下转账确认键的前一刻找到她，成功止骗止损。

据甘女士介绍，她接到一个自称某市公安局的电话，对方说她涉嫌严重犯罪，要求秘密配合调查，又要求她从银行卡里转账1万元到“安全账户”。所幸民警及时赶到，才让甘女士

如梦初醒。

4月17日，来自湖北宣城的王先生也遭遇了通讯(网络)诈骗：燃料油厂家打来电话联系业务，他信以为真，主动联系对方准备买油，按要求汇去定金22.4万元，后对方失联，王先生才发现被骗。

初步了解案情后，市公安局110指挥中心立即启动三方通话，温州市反诈骗中心对涉案账户快速止付。4月18日，塘下派出所所在温州市反诈骗中心的大力支持下，及时冻结该账户上的22.4万元被骗资金。

近年来，我市警方积极探索工作新机制，在快速处置上下工夫，着力提升诈骗案件紧急止付、快速冻结、信息查询和止损追赃能力。

通讯诈骗的特点是快，反制它的秘诀是“以快制快”，及时止损。受理相关案件后，警方第一时间指导受害人止付止损，联系温州市反诈骗中心开展相关处置工作，最大程度缩短流程，提高止损时效。

今年以来，我市累计止付止损被骗资金500多万元，其中冻结被骗资金398万元，追回资金130多万元。

打击犯罪拼力度 让诈骗团伙无处遁形

今年3月，一场抓捕行动在全国18省份56市开展，我市百余名民警在公安部直接领导和各地警方的配合下，参与统一抓捕行动。开展如此声势浩大的抓捕行动，目的只有一个：破获曾引起全国轰动的温州市2·20特大通讯网络诈骗案。

据了解，去年3月至今年2月，4名台湾籍人员在大陆境内招募186人，在柬埔寨、印度等地设立窝点，从事电信诈骗。他们集中吃住，经过专业培训，分工明确、各司其职，分别冒充大陆移动公司和“公检法”等单位工作人员实施诈骗。同时，他们特意设定一、二、三线话务员以及电脑手、管理人员等岗位，其中一线话务员负责

冒充被害人所在地的民警打电话，虚构被害人名下的银行卡在上海或北京涉嫌洗钱犯罪；二线话务员冒充上级警官；三线话务员充当检察官，诱骗被害人汇款。受害者当中，少则被骗走几千元，多则被骗上万元。

鉴于该案涉及对象多、涉案金额高，公安部门高度重视，公安部挂牌督办该专案。市公安局专门抽调精干力量组成专案组，以5+2、白加黑工作模式研判案情，深挖案件线索。

警方发现，该犯罪链条里存在招募环节，背后有26名藏身于印度的专业作案嫌疑对象。获取该线索后，市公安局高度重视、精心研判，并得到温州市公安局刑侦支队、反诈骗中心

等相关部门的支持，通过抓住一个对象带出一批同伙、审出一批案件的方式，从人到案、从案到人，反复研判、深度打击，逐步扩大战果。目前，专案组已经抓获嫌疑人109人，办理刑拘在逃54人，破案50多起。

在温州市公安局的统一部署和有关部门的支持配合下，我市公安局于3月和5月分别组织集中外出追捕行动，先后出动300多名警力，辗转吉林、黑龙江、湖南、广东、江西等地，将70多名对象抓捕归案。

10月22日上午，市人民法院公开宣判这起案件，以诈骗罪分别判处24名被告人有期徒刑10个月至11年不等，其中19名被告人获刑5年以上。

精准宣教求广度 防范预警更接地气

骗子花样再多，目的只有一个，就是要你汇钱！领个奖还要先付钱？那不是拿肉包子打狗吗？

说到我市反通讯(网络)诈骗宣传，不得不提“萌警官”张勇。这位上望派出所民警利用漫画，向市民开展普法教育和防范预警，深受欢迎。

由张勇及其团队创作的《谨防网络股票诈骗》、《谨防手机短信诈骗》、《谨防网络招聘诈骗》等预警作品，不仅在微信、微博、报纸上发表，还制作成展板巡回展出，简单易懂的语言配上生动的漫画，让市民和网友眼前一亮。走红后的张勇仍坚持进社区、进校园开展讲座，仅仅今年已经开课100多场次，被称为“萌警官”。

今年，他的团队还牵头筹建了全市“萌警”安防体验馆，集消防安全、交通安全、防诈骗、禁毒、反盗抢等防范题材于一体，目前已接待全市群众数万人，获得众多“点赞”。

除了“萌警官”，我市还有许多民警

为防范通讯(网络)诈骗宣传献计献策。

不仅如此，我市警方还通过案前主动做好各项防控工作，从被动应对向主动出招转型。面向中老年人、外来务工人员、教师、学生及其家长等易受骗群体，开展集中宣传，取得良好效果。

民警提醒，平时一定要保持清醒头脑，不要贪图小利、轻信谎言，始终保持警惕，对陌生人要求的汇款、转账电话和短信做到不听、不信、不转、不汇，避免钱财损失，必要时向警方报警。

假如已经落入骗子设下的诈骗圈套，那该怎么办？

民警介绍，很多诈骗团伙得手后，会迅速把受害人的钱转账到多个账户，再由专人取钱，有时几百万元的资金从转账到取现，最快只需要半个小时。

一般来说，被骗后1个小时内是报警的“黄金时间”。受害人越早报警，相关部门追查线索、追回被骗钱款的可能性越大。民警说。

[相关链接]

7类常见的通讯(网络)诈骗形式要认清

1. 网购、退款 诈骗

【案例】5月16日，王某接到“淘宝客服”的电话，对方说他网购的洗面奶有质量问题，已退款到支付宝账户。王某回复没有收到，“淘宝客服”称是王某支付宝芝麻信用分没有达到870分的原因，提出帮他提升芝麻信用分，让他在“趣店”、“蚂蚁借呗”、“安逸花”等手机APP上先后办理信用贷款2万多元，以支付宝扫描二维码形式转账给他。王某照做后，还是没有收到退款，又按对方要求用银行卡汇去几笔钱。一番折腾后，王某才发觉不对劲，询问正规淘宝客服后才发现自己被骗，损失28857元。

【案件分析】随着网购人群的日益庞大，网购退款类案件随之高发。诈骗方往往诱骗受害人通过微信微粒贷、支付宝借呗等系统，开通网上信用贷款、信用借款功能，再进行转账。

【警方提醒】消费者要选择正规网站网购。如果接到退款等短信，不要随意链接对方发来的网址或者回拨对方提供的电话号码，应登录正规网站，与商家客服核实。

2. 刷单兼职 诈骗

【案例】3月25日，吴某登录QQ，收到介绍兼职刷单的消息，信以为真，联系了对方的“对方介绍”了刷单流程，并发去网页链接。吴某登录网页，按对方的要求填写了数量，提交订单并截图，后用微信扫描对方提供的二维码陆续转账12960元，随后便联系不上对方。

【案件分析】此类诈骗信息多通过58同城和QQ群等平台发布，受害人年龄主要集中在17岁至30岁，以女性为主，大多在家中操作时被骗。诈骗方往往要求受害人刷二维吗转账，导致受害人不知道对方的银行账户。

【警方提醒】不管在现实中找工作还是“网上兼职”，应多方核实兼职单位的信息，不要被所谓“门槛低、时间短、高回报”的噱头蒙蔽。

3. 网购虚拟物品 诈骗

【案例】4月29日，蔡某报案，他在手机游戏“王者荣耀”里看到有人卖“皮肤”，就加了对方的微信，按约定转去430元，后被拉黑。蔡某在游戏中说对方是骗子，有人称可以帮忙把钱要回来，但是要知道蔡某的微信账号、密码，并要求蔡某把微信与母亲的银行卡绑定。蔡某信以为真，按照对方要求扫描二维码后，钱直接被刷走。受害人才意识到被骗，共损失1680元。

【案件分析】此类案件高发与手游的流行有关，个案案值普遍较小，中小學生受害人占比较大。诈骗者作案手法主要是谎称买卖游戏装备、账号，收到钱后就与受害人断绝联系。今年11月，马屿派出所接到一起小学生在手游“星球大作战”充值游戏币被骗2880元的案件，受害人年仅10岁，是我市年龄最小的通讯(网络)诈骗案件报案人。

【警方提醒】购买游戏币，应去正规的提供担保服务的购物网站。

4. 贷款担保 诈骗

【案例】4月18日，李某接到电话，对方询问是否需要贷款，且介绍了贷款流程。李某动了心，把银行卡号报给对方。过了一天，李某又接到电话，对方称银行卡里流水不够，要帮他走流水，需注册其公司的会员。李某按对方要求在“天天理财”平台上注册了账号，转入一笔钱，并将平台验证码告诉对方。

后对方称还需要李某转钱到其提供的一张银行卡内。李某信以为真，通

过网银转账。但对方称仍需要交保证金，李某感觉不对劲，就去查平台账号，发现里面已经没有钱了，前后被骗走29980元。

【案件分析】传统的贷款担保类诈骗案件，一般是冒充银行、贷款公司工作人员，要求受害人以交纳办理费、申请费、工本费或给特定账户转账进行刷流水的形式实施诈骗。近期，以开通微信微粒贷、支付宝借呗等信誉贷款的名义实施诈骗的情况有所增多。

【警方提醒】不法贷款担保最明显的特征，就是所谓的审批程序非常简单，但在办理过程中一步步要求交纳各种费用。一旦发现这种特征，市民要加倍小心。如果需要贷款，最好向正规银行申请。

5. 虚假投资理财 诈骗

【案例】5月2日，贺某报案：几个月前，他的QQ被拉进一个现货买卖群。经群友多方推荐，加了所谓的“长江开户专员”QQ，由对方远程操作，在上海长江联合金属有限公司开户，并转账10万元激活账户。小赚了一笔钱后，QQ群友建议贺某多做点。贺某加大投资后，平台开始莫名其妙地“卡盘”、连接中断，致使贺某亏损。QQ群友称是网络不好，让贺某加入一个在线培训班，投资额起步是50万元。贺某信以为真，在后期操作中又连续亏损，意识到被骗。

【案件分析】该类案件一般是犯罪分子在网上发布信息或通过网上聊天工具，和受害人直接联系，并以高额回报为诱饵，提供免费在线培训，鼓动受害人在网上平台注册账号，进行所谓的股票投资、证券投资、现货买卖。刚开始收益较好，但是随着投资额越来越大，受害人投资的物品价格突然暴跌或者平台无法操作。

【警方提醒】网络投资理财应选择正规渠道，不仅要看网站是否备案，还要尽量了解其背后企业是否具有资质、规模。尽量选择知名度高、规模大的企业，谨防小型企业跑路、关闭网站等事情发生。

6. 冒充银行工作人员 诈骗

【案例】5月17日，木某报案：平安银行工作人员打来电话，说他的信用卡被冻结，需要用另一张储蓄卡解冻。木某将银行卡卡号和密码报给对方，后收到银行短信，发现卡里少了14000元钱。

【案件分析】诈骗人员通常冒充银行工作人员，以信用卡还款逾期、办理信用卡、提升信用卡额度、银行卡涉案被冻结等由头，要求受害人交纳手续费、提供验证码、转账刷流水、缴纳保证金、转账到安全账户等形式实施诈骗。

【警方提醒】信用卡业务应当去柜台办理，拒绝一切非正规渠道的信用卡办理，不透露个人信息，尤其是银行卡信息。

7. 冒充公检法 案件

【案例】5月19日，万某报案，他在办公室接到自称“顺丰快递工作人员”的电话，对方说他的包裹被拦截，询问前几天是否在上海寄包裹，万某说没有。顺丰工作人员说万某的身份信息可能泄露，把电话转接到“上海虹口派出所”。

民警了解情况后，称万某在上海某银行账户内有大额资金，涉嫌洗钱，案件负责人是他们“队长”。“队长”接过电话，问万某是否办了银行卡出卖，万某说没有。“队长”就发了网站链接，让他如实填写自己的情况，并扬言要依法冻结万某银行卡内的资金，要求他将期间收到的手机验证码发还回去，并叫他发完后删掉验证信息。

万某操作完毕，发现银行卡内的钱被转走，损失139800元。

【案件分析】此类骗局中，犯罪嫌疑人往往冒充“公检法”工作人员，称受害人身份证被冒用，涉嫌严重犯罪，要对受害人采取强制措施或要求受害人自证清白，缴纳保证金或将钱转到“安全账户”进行验资。

【警方提醒】公检法机关不会通过电话进行所谓的情况核查、账户核实、安全转账等。不法分子的最终目的是要求转账或汇款，市民接到此类电话、传真等，一定要及时与身边人交流沟通，如遇被骗及时拨打110求助。



面对陌生通讯(网络)信息要警惕