



雷霆出击 与诈骗分子拼速度

全市公安机关严打通讯(网络)诈骗

4月11日，一篇名为《实录亲历网络诈骗，互联网是如何让我身无分文？》的文章作者“趣火星”称，由于一条短信，他的支付宝、银行卡及百度钱包内的所有资金，被骗子彻底洗劫。

如果不是亲身经历，很多人在报纸上、电视上、网上看到各种诈骗案件新闻时，往往就像在看故事一样，觉得离自己的生活还很遥远。

然而，有数据显示，2015年全国公安机关共立通讯(网络)诈骗案件59万起，同比上升32.5%，共造成经济损失222亿元，个案被骗最高金额接近4000万元，令人咋舌。

而在我们浙江，在过去的一年中，全省公安机关共受理通讯(网络)诈骗案件10万余起，涉案金额15亿多元。

通信(网络)诈骗，离我们的生活并不远。

众所周知，通讯(网络)诈骗一旦发生，时间是最宝贵的，如果能将账户及时冻结，犯罪嫌疑人就无法把钱转走，被骗群众的经济损失也能得到减少，甚至及时挽回。因此，与犯罪分子“拼速度”，成了挽回损失最为重要的一件事。

记者 石承承 通讯员 刘益 杨熙瑾



社区民警向市民介绍最新通讯(网络)诈骗防范知识。

记者 王鹏 摄

【典型案例】

市反欺诈中心： 及时冻结 178 万余元

今年3月21日早上9点半左右，李先生在北仑小港新家村一家油品公司内上网时，误入钓鱼诈骗网站，在输入U盾密码后被转走50万元。

发现被骗后，李先生立即赶到北仑公安分局小港派出所报案。

接警后，小港派出所民警带着李先生一起到当地的光大银行开展查询工作。大约两个小时后，光大银行向小港派出所反馈，该笔50万元涉案资金已被转至招商银行一账户内。

这条信息立即被推送至市反欺诈中心，该中心和招商银行宁波分行联络员联系，采取应对举措，随即该涉案账户内的1781214元的余额被依法冻结，为案件的后续侦办赢得了时间。

江北： 单笔金额小一样不放过

今年2月17日，一群众向江北警方报案称，去年12月在网上看到一转让美图手机的信息，通过加对方为微信好友谈好价格后，收到对方发送的快递单照片和寄送快递打包视频后信以为真，通过支付宝转账2500元，却一直未收到手机，微信也被拉黑，才发现被骗。

江北警方坚持落实每起通讯(网络)诈骗案件的初侦初查工作。因为本案案件价值较小，为获取更多犯罪嫌疑人的信息，民警进行了大量的回访，串并了多起案件，涉案金额的不断高叠使民警意识到该案极有可能为系列性诈骗案件。

今年3月8日，江北公安分局民警

在温州警方的配合下，在温州市瓯海区抓获犯罪嫌疑人黄某某，缴获作案手机3部，银行卡3张，扣押赃款50余万元，现场勘查发现作案用的微信、微博、支付宝等虚拟账号70余个。通过调查取证，警方查明黄某某自2014年起，利用新浪微博、淘宝闲鱼平台，发布虚假的美图手机低价出售信息进行诈骗，疯狂作案300余次，诈骗所得50余万元。

鄞州： 三天三夜快速抓获犯罪嫌疑人

今年3月5日，鄞州公安分局集士港派出所接群众报案，受害人通过互联网找到一不锈钢材料公司，按照合同规定，汇款给对方30%定金共计8.5万余元，后联系不上对方，怀疑被骗。

案发后，鄞州公安分局刑侦大队、集士港派出所等部门迅速成立专案组，及时开展调查取证、信息研判等工作。3月8日，专案组赴江苏无锡开展抓捕，经过三天三夜的连续奋战，顺利抓获犯罪嫌疑人张某、蔡某。

经审讯，二人如实交代了在互联网上发布虚假出售钢材信息，签订虚假购销合同骗取钱财的犯罪事实。目前，该2人已被刑事拘留，案件正在进一步审理中。

镇海： 以动制动“伪基站”诈骗团伙

今年3月14日，镇海公安分局接群众报警称，收到“95588工商银行”发来的积分换现金短信，根据提示操作后发现银行卡被盗刷。

接报警后，镇海警方立即抽调警力

组成专案组开展侦查。其间，依托视频侦查、实地走访等手段，成功锁定涉案人员的车牌号，并查清其身份。3月17日上午，专案组在余姚阳明西路附近成功将犯罪嫌疑人朱某抓获。3月28日，分局专案组又破获一起3月25日接报警的类似诈骗案件，成功抓获犯罪嫌疑人郑某、林某等人。经审讯，三人对上述利用伪基站实施诈骗的犯罪事实供认不讳。

镇海警方共收缴伪基站设备2套，破获辖区通讯(网络)诈骗案件6起，串并宁波市大市范围内案件20余起，涉案金额10万余元，现已追回赃款2万余元。目前，朱某等3人已被分局依法刑事拘留，案件正在进一步审理中。

奉化： 发案增幅同比下降 65.7%

今年4月11日下午3点半左右，家住奉化岳林街道陈家岭村的裘先生接到“民生银行工作人员”的电话，称可提高其所使用的民生银行信用卡额度。见裘先生很是心动，对方遂提出要其先向指定账户汇款，以证明其还款能力。

在对方的步步诱惑下，裘先生最终向对方指定的账户汇过去36万元。直到钱汇出去后，裘先生才发现自己上当受骗。在接到市公安局指挥中心推送的警情后，市反欺诈中心立即对涉案账号和资金进行操作，在10多个涉案账户中成功止付18万元，为案件下一步侦查赢得了时间。

【应对举措】

通过上述案例，不难发现通讯(网络)诈骗存在一些显而易见的规律。

从“猜猜我是谁”到“我是你领导”，从“航班信息变更”到“银行卡透支”，通讯(网络)诈骗的招数不断翻新，让人防不胜防，深恶痛绝。

在各种诈骗手段中，又以冒充当事人公司的老总、财务经理，冒充公检法等国家机关谎称受害人“涉案”或发布假通缉令等手段实施诈骗，最容易使受害人上当，诈骗损失通常也最为严重。

通讯(网络)诈骗依托电话、网络进行，一天往往可以打成百，甚至上千个电话，这其中哪怕只有少数人上当受骗，也足以让犯罪嫌疑人“发一笔横财”。因此，此类案件具有潜在受害者广泛，发案频率高的特点。

受害人一旦上当受骗，犯罪嫌疑人一般会立即把账户里的钱取走。同时，为躲避追踪，犯罪嫌疑人往往会大量开设账户，将钱在几个，甚至十几个账户间“腾挪挪移”。

迅速冻结嫌犯账户，实现“零延误”才能在最大程度上将受害人的损失减到最轻。

为此，全省各地纷纷建立反欺诈中心，建立公安、银行、通信运营商的联动反应机制。公安机关一旦接到报警，将通过联动反应机制将警情通报给银行，在最短时间获得授权，快速止付、冻结涉案账号；若遇到涉案资金已被转走的，也可迅速开展跟进、查询工作。与此同时，银行也将对同一客户在同一商业银行开立借记卡的数量进行限制，对异常账户加强甄别，切断犯罪嫌疑人的“财路”。另一方面，相关警情也将通报给通信运营商，针对涉案手机号码、网络等信息采取的措施，进行追查。

民警提醒，遇到通讯(网络)诈骗，最根本还是公众应当提升防范意识，对汇款、转账等信息多留个心眼。虽然通讯(网络)诈骗的理由很多，但其最终目的就是骗取钱财，因此当听到要“输入身份证号”“提供取款密码”，或者点击链接，下载软件时，就要格外谨慎，不要给犯罪嫌疑人可乘之机。