合肥一周发生贷款诈骗52起

网络贷款诈骗高发，合肥警方发布预警信息

“网络办理小额贷款，无抵押，快速放款”“网络贷款，无需征信，当天放款”……这样的好事，对于资金周转困难的借款人来说，非常具有诱惑力，加上借款人急于筹钱的迫切心理，使得贷款诈骗犯罪分子能够屡屡得逞。今年二季度合肥市共发生贷款类诈骗案件658起，占全部电信诈骗案件的23.08%。7月1日至7日，合肥发生贷款诈骗案件52起，群众被骗98.17万元。网络贷款类案件已成为当前电信网络诈骗中发案量大且最具有欺骗性的一类。据介绍，当前，从作案手段来看，贷款诈骗案件总体上可分为两类：以收取“保证金、好处费、保险费、解冻费”等各种费用为由实施的贷款诈骗；以“验流水、过征信”为由实施的诈骗。 □合公新 记者 王玮伟

案例一

男子网上贷款被骗5万余元

6月29日上午，肥西男子陈某接到一个自称为某贷款平台客服打来的电话，称可以帮其办理贷款，刚好陈某近期急需用钱，在向对方简单了解后，便加了对方的QQ好友。

随后，对方通过QQ给陈某发送了一个他们的审核软件“沃钱贷”，陈某下载安装后，填写了个人信息，过了一会这个审核软件就显示审核成功。陈某把审核通过的截图发给对方，对方以缴纳“包装费”为由，让陈某转3600元。陈某按对方要求将3600元汇至对方提供的银行卡内之后，对方说陈某贷的6万元放在了“沃钱贷”软件里，但是陈某却始终无法提现，便联系了对方进行询问。而对方则称陈某填错银行卡号，导致账户被冻结，所以钱贷不下来，需要缴纳12000元的解冻费，并且承诺后期会返还给陈某。

陈某又将12000元转入对方提供的银行卡内，接着对方说要清除陈某之前的贷款记录，这样他们公司才能放贷给陈某，但要转14500元给他们，陈某又将14500元汇至对方提供的银行卡内；转过之后，对方发来一个清除贷款记录进度的截图，上面只显示清除了70%，剩下的30%要清除的话，需要再交纳21000元。陈某又将21000元汇至对方提供的银行卡，转完之后，对方还让陈某再转21000元的风险保证金，才可放贷下来。直到此时，陈某才意识到自己遇到了骗子，之后越想越不对劲，选择了报警。

警方分析：此类贷款诈骗，犯罪分子以低门槛发放贷款为诱饵，以收取“包装费、解冻费、激活费、保证金”等名义进行诈骗。受害人在被骗第一笔钱后，存在侥幸心理，被迫继续缴纳各种费用，同时作案过程中，犯罪分子往往会将事先伪造或者PS的所谓清除贷款记录、成功的现金支票、银行交易流水图片发给受害人作为进一步行骗的钓饵。

案例二

向受害人发送木马病毒链接

6月初，合肥市民王某接到一个电话，对方声称银行有关系，无抵押信用贷款，可以迅速发放贷款，感兴趣可以加微信洽谈。王某信以为真，就加了对方微信，并按对方要求，提供了自己的身份证号、手机号和银行卡等信息。对方在微信里说因为王某银行账户交易流水太少，无法证明还款能力，无法放款，要他马上存2万元到他自己的银行卡上。王某觉得银行卡和密码都是自己掌握，存钱没有风险，就马上去存了钱。这个时候对方发来一个暗藏木马病毒的网址链接，说是要验证银行卡资金，让王某填写姓名、身份证号、银行卡账号和短信验证码。点开链接后，王某一看还挺正规，于是信以为真毫不犹豫就填了银行卡卡号、密码和短信验证码。

过了一会，王某收到了2万元的扣款短信，王某正准备微信质问对方，发现微信被对方拉黑了。

警方分析：这种贷款诈骗，骗子通过无抵押信用贷款的噱头，诱骗受害人给其转账增加所谓的银行卡交易流水，完成诈骗，或者是要求受害人证明自己的还款能力在银行卡里存钱，其实是通过木马病毒网址链接获取受害人银行卡信息和短信验证码，完成对受害人银行卡资金的盗刷。很多人认为把钱打到自己账户比较安全，殊不知，紧接着骗子就会通过发送木马病毒的网址链接，要求受害人点击网址链接并填写银行卡账号、密码，不法分子在获取受害人银行账户、密码、验证码之后就可以通过盗刷或者网上购物将“验资款”占为己有。

剖析

1.不法分子通过QQ、微信、手机短信、网站网页等多种途径发布网络贷款广告。

不法分子在发布广告时为获取受害人信任，制作发布的广告往往打着“专业贷款公司”“投资咨询公司”的名义，有时甚至假冒一些知名金融网贷公司。广告中往往会出现“无抵押、无担保”“信用贷款、当天放贷”等极具诱惑性的标语。这些标语极其精准地切中了广大急需资金的受害人的要害。

2.不法分子针对急需资金而征信又比较差、不太了解银行贷款业务且网络知识匮乏的人实施精准诈骗。

一些受害人因为没有良好的抵押资产或担保，或者征信比较差，此类人群寻求正规贷款途径无法贷到款，所以遇到不法分子编织的无抵押信用贷款时，有饥不择食的迫切心理。

3.不法分子利用电话、短信及微信、QQ等即时社交工具实行普遍撒网和筛选急需资金而征信又比较差的受害人实施精准诈骗。

不法分子通过“无须担保、无须抵押”为噱头诱骗受害人先缴纳一定的保证金、手续费、解冻费、包装费等各种费用，并结合木马病毒网址链接，以验证受害人银行卡资金为由，对受害人资金进行盗刷。

谨记

1.声称“无需抵押、无需担保、放款速度快”，一律是骗子

2.要求缴纳“包装费”“解冻费”“保证金”等各种手续费的一律是骗子

3.声称银行卡资金流水不足的一律是骗子

4.要求验证还款能力的一律是骗子

“技术型”盗贼 手机里详记盗窃“笔记”

星报讯（唐放 记者 徐越蔷） 毛贼再细致，也难逃民警“火眼金睛”。近日，淮北警方抓获了一名格外注重细节的“蒙面盗贼”，破获跨省系列盗窃商超案件11起。

今年2月至4月，淮北市区多家超市被盗。淮北警方高度重视，经对嫌疑人轨迹及流窜路线的推演及侦控，7月4日凌晨3时许，专案组于亳州涡阳县一宾馆抓获涡阳籍犯罪嫌疑人郝某成，继而又在郝某成住处查获断锁钳、锡纸、特制U形针、点槽卡片等作案工具。

“亳州市谯城区魏武大道与光明路交叉口西南方300米处某超市，超市南200米处有一枪机（高清枪式摄像头），超市西北一岔路口有一球机摄像头，超市晚10点关门，TY320（锁具的类型）、无人值守、无联网报警……”据了解，郝某成每次作案前都会踩点，精心踩点后不急于出手，而是直奔50公里外的邻市抵达前几日已经踩好点的店铺，于夜深人静时蒙面实施盗窃，隔一段时间再到多日前已踩好点的商超实施盗窃，其手机备忘录里详尽细致记录着踩点完成的各项标注。

经审讯，犯罪嫌疑人郝某成如实供述了自去年12月起于安徽淮北、宿州、亳州，河南鹿邑、商丘，江苏徐州等三省六地实施盗窃商超11起的犯罪事实。郝某成通过技术性开锁的手段，于夜间专门盗窃街面商超，开锁最快只需25秒，进入商超后只窃取现金从不顺手取货。据其供述，这么做是为了安全、高效，把“动静”和“聚焦点”最小化。

自断手指“碰瓷” 短短月余作案30余起

星报讯（杨晓虎 记者 徐越蔷） 近日，繁昌县公安局通过缜密侦查，快速出击，打掉了一个碰瓷诈骗的犯罪团伙。

7月3日上午10点多，繁昌县繁阳镇居民秦某驾驶着电动三轮车经过某路段时，无意中“碰倒”了一个骑着自行车的小伙。小伙躺在地上，说自己手受伤了。秦某感觉不对劲，立即报了警。民警调取了路面监控，发现在“交通事故”发生之前，秦某的电动三轮车被一辆外地牌照的小轿车别了一下，在电动三轮车另外一旁的小伙骑着自行车顺势倒地。民警立即讯问受伤小伙陈某，陈某交代，小轿车上的人员是他的同伙。陈某被发现后，其他团伙成员立即驾车逃走。警方紧追不放，7月4日凌晨，民警在芜湖市某宾馆将该团伙其余成员悉数抓获归案。

经查，该团伙驱车从湖南出发，沿途伺机作案。团伙头目李某驾驶汽车别正在行驶的电动三轮车，在另外一旁骑自行车的同伙佯装碰擦倒地受伤，经医院诊断手指骨折，团伙其他成员与受害人进行协商，要求支付一定的医药费。三轮车车主通常迫于无奈，只好付给对方几千元至一万多元不等。而据民警调查，在此团伙中专门负责碰瓷受伤的嫌疑人俗称“骑手”，在外出诈骗前事先将手指砸骨折。

记者了解到，该团伙专门找电动三轮车下手，短短月余时间，就作案30余起，诈骗金额达20多万元。

“讨好”网红女主播 男子流窜诈骗老乡钱财

星报讯（周颐添 记者 马冰璐） 热衷于观看网络女主播视频的仲某某，为送礼讨好女主播，竟专挑老乡下手，诈骗他们的钱财。昨日，记者获悉，仲某某因涉嫌诈骗罪被合肥市瑶海区检察院批准逮捕。

年近50岁的仲某某是重庆人，离婚后沉迷于网络，热衷观看网络女主播视频。为花钱送礼讨好女主播，今年5月12日，仲某某来到合肥一农贸菜场，找到一家面店，谎称自己叫张某某，是合肥一家医院的食堂承包人，每天需要100斤鲜面条，希望与该店建立长期供货关系。面店老板郭某某见对方是重庆老乡，又是一笔“大生意”，于是把仲某某请进店内商谈。仲某某见对方没有防备，于是装模作样地提了一些卫生、时间、证件方面的条件，并将注意事项写下来让郭某某签字确认。获取郭某某的信任后，仲某某就多次以办理发票簿、医院门卡交押金、办健康证、交窗口税等理由让郭某某给其转钱。最终，郭某某分六次一共给仲某某转了8865元。此后，当郭某某再联系仲某某时，才发现其联系方式已被拉黑。