10万贷款没拿到反被骗57万

诈骗团伙1个月转移500余万元，称“钱来得太容易了”

YMG全媒体记者 林媛
通讯员 宋佳 苏瑞刚
摄影报道

龙口市民王先生想办10万元的贷款，结果不仅贷款没有批下来，还被诈骗分子骗走了57万元。龙口市公安局刑侦大队民警们辗转1300余公里，顺藤摸瓜，将一“跑分”团伙抓获归案。

受害人：接到贷款电话，一步步掉入陷阱

2月初，受害人王先生接到一个电话，问他是否需要贷款。当时王先生正好缺钱，就说需要贷10万元。

对方特别热情，引导王先生办理：下载贷款软件，给了王先生一个银行账户，让其先打3万元的认证金。对方“信誓旦旦”，贷款下来以后，3万元认证金与10万元的贷款一起返还。

王先生信以为真，将3万元打入了对方提供的银行卡账户。“我本来是将信将疑的，但是看到贷款软件显示有3万元，我就放心了。”王先生说。

就在王先生安心等待放款时，一连串的问题却接踵而至。

“对方先跟我说操作流程不对，让我重新打钱。后来又说账户被冻结，让我打钱恢复账户。之后又说验资未通过，又让打钱。除了认证金，我又打了4次款，共计54万元。”王先生说。

没想到，对方还让王先生打款，这次王先生终于起了疑心，“我不贷款了，你们把我之前的57万元退给我！”结果对方销声匿迹，也不像以前那样“秒回”问题了。王先生一看不好，赶紧登录下载的贷款软件，却登录不上，才知道自己掉进了陷阱，立即报警。

连续5次打款，为啥没起疑？王先生说，每次打款，他都能在下载的贷款软件上看到转账金额，“感觉是正规机构，可以信任”。

“实际上该软件的信息是诈骗团伙在后台随意修改的。”龙口市公安局刑侦大队民警罗钧冈告诉记者。

侦查：犯罪团伙转移资金500余万元

接警后，龙口市公安局刑侦大队民警立即开展分析研判，很快确定了犯罪嫌疑人为王某某、牟某某。其中，王某某名下的银行卡还在进行资金往来，流水高达300余万元。

2月7日，民警根据掌握的线索，辗转1300余公里，先后奔赴济南、湖北等地，将犯罪嫌疑人抓获归案。

民警进一步深挖细查，追查到二人有上线，是以李某为首的“跑分”团伙，并锁定该团伙落脚点。2月9日，在河南洛阳市一酒店内，犯罪嫌疑人李某、文某某、侯某某等3人被抓获，现场缴获涉案资金8000余元。

经查，2023年1月以来，犯罪嫌疑人李某等3人先后组织多人利用银行卡、网络支付工具，为电信网络诈骗违法犯罪转移资金500余万元，目前，已冻结涉案资金近30万元。

嫌疑人：最小的18岁，“钱来得太容易了”

审讯时，嫌疑人唐某交待，他的上线是境外诈骗团伙。他们的任务是通过随机打电话的方式寻找需要贷款的人，让对方把钱打进指定的银行卡。收到钱后，再转移到10多个银行卡。

在被抓获的犯罪嫌疑人中，年龄最小的只有18岁，“感觉钱来得太容易了。我一个月的开销大概就得一两万，一般都去酒吧喝酒花掉了”。

目前，该犯罪团伙成员因涉嫌帮助信息网络犯罪活动罪、掩饰隐瞒犯罪所得罪已被龙口市公安局依法采取刑事强制措施。

警方提醒，大额度、低利息、零抵押的贷款往往是骗局的开始，大家要牢记，贷款前先交钱的都是诈骗。

新闻链接

“分”指的是钱，“跑分”就是让钱跑起来。对于诈骗得来的赃款，诈骗分子第一时间转出，才不能被公安机关察觉。“跑分”人员对赃款进行流动式洗钱，最终使钱变白，再回流到诈骗团伙手中。

谭希光 制图

冒充“公检法”诈骗升级
莱山区两人被骗18万元

YMG全媒体记者 林媛 通讯员 陈艳丽 摄影报道

从2月份开始，一个升级版的诈骗局在全国范围内高发。近4天来，莱山公安分局已连续接到多起群众报警。

“我是公安局的，你涉嫌洗钱犯罪”

“林XX吗？我是公安局的，你的护照被盗用，而且涉嫌诈骗洗钱犯罪，现在请配合调查。”2月19日中午，林女士接到自称是公安局户政警察的电话。由于对方准确地说出了她的身份信息，林女士没有产生任何怀疑。

“我们将把电话转接至受害人所在地公安机关，请你保持电话畅通。”话音一落，另一位“警察”接通了林女士的电话，表示要核实林女士资产，不要告知任何人。在对方的引导下，林女士先是在手机上下载了一款视频会议APP，又按照对方指示，开启屏幕共享。

“我们要核查你的名下银行卡是否涉嫌犯罪，现在请你把名下所有账号的钱统一转到你的一张银行卡上。”对方说。

“反正都在我的卡上，肯定没问题。”林女士在屏幕共享的情况下，完成了自己名下银行卡的互相转账。

之后，对方称要进一步核查，要求林女士下载一款名为“安全防护”的APP软件。下载过程中，林女士的手机不断冒出对话框，提醒这是一个危险的软件，是否继续下载。在“警察”的指示下，林女士一步步选择了“继续”。

下载完成并打开后，林女士按照对方的要求，又进行了几笔资金的转出转入，手机收到了资金往来的提醒。整个过程大概15分钟左右。之后，对方说已经完成核实，挂断了电话。

林女士查询银行账号，发现账上的8万余元全没了！

无独有偶，第二天，石先生也进行了同样的操作，银行卡内的10多万元被划走。

庆幸的是，正打算转账的李女士和修女士分别被警方及时劝阻。

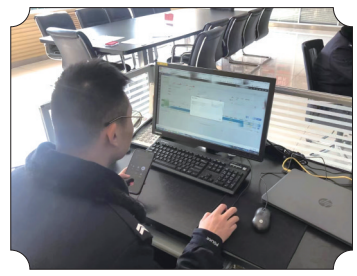
老手段使用新技术，“对方发来的链接都不可信”

这种诈骗是老手段使用新技术：冒充“公检法”诈骗升级。

“这是一种从2月份开始在全国范围内高发的诈骗类型。”莱山公安分局刑侦大队民警刘鹏告诉记者。

从目前接警的案件来看，受害人的共同点是在对方指挥下，都下载了两种手机APP：一种是带有屏幕共享功能的视频会议软件，被不法分子利用，在市民转账时，对方可以看到市民输入的账号密码和验证码。另一种是名为“安全防护”的软件，从下载这个软件的那一刻起，后台会窃取市民手机的通讯，包括来电、短信、微信、QQ等。然后，在市民不知情的情况下，从后台划走市民合并转到账上的所有的钱。

“必须提醒的是，‘安全防护’这个软件有很多个名字，但都是从对方发来的网页上下载的，不是正规渠道，而且很多安卓系统的手机会反复提醒这是危险软件，市民要瞪大眼睛注意辨别。”刘鹏说，“只要是对方发来的链接，都不可信！”



四大“要求”要拒绝

要求你绝对不能挂掉电话的

要求你必须开通网银或重新办一张银行卡或全部转到一张卡上

要求你绝对不能和别人透露通话内容的

要求你寻找隐蔽地方进行通话的

诈骗流程

第一步 亮明身份，自称某地公安局民警，告知受害人因身份信息泄露或曾经身份证遗失、被人冒用身份申领电话卡、银行卡、护照等，涉嫌刑事案件，需要配合警方调查。

第二步 电话会转接至“办案地公安局”“办案地检察院”“办案地法院”。在电话中，“警察”不断强调该案件涉密，不得向任何人透露信息。

第三步 “通缉令”“警官证”齐上场，受害人根据指示，添加“警察”的QQ或微信，对方发来虚假警官证或者通缉令等文书。

第四步 要求受害人下载软件配合“资金清查”，将所有钱转入一张银行卡。受害人按照指示开启了共享屏幕，在操作手机转账过程中，已被不法分子窃取了受害人银行密码，受害人卡上的资金已被全部转走。