揭开“积分兑换现金”的秘密——

破产老板长沙布“网”诈骗

今日女报/凤网记者 唐天喜 通讯员 吴虎

他曾是百万老板，一朝破产后，他奔赴长沙，看上了日赚2000元的行当。只是，这个行当，带给他的不是绝处反击，而是让他的人生充满了更多的悲剧色彩。

民警孙瀚向记者介绍案情。

A “积分兑换现金”？点击短信链接后5000元没了

9月23日，如果没有意外，正在长沙市韶山南路逛街的女大学生陈冬儿（化名）会觉得是个幸运日。这天，她突然收到了一条显示为“95533”的号码发来的短信。

内容是“积分兑换现金”的活动介绍：“您在我行已满5000积分，可兑现5%现金，请登陆我行手机网领取，http://m.cczh.cc，逾期不可兑现。[建设银行]”。陈冬儿拥有一张建设银行的卡，而且刚刚刷卡购完物，所以对于收到这样的银行短信，并没有产生怀疑，反而是“逾期不可兑现”这几个字让她有种紧迫感，于是，她立刻点击网址登录到一个手机银行界面，并按照提示，逐步填写了自己的银行卡号、身份证号码、银行卡密码等信息。

很快，她收到了一条建设银行发来的6位数验证码，她以为是验证自己的身份，也一并填写了。“接着，我就收到银行短信提示，说我支出了5000元。”陈冬儿回忆，她当时就觉得可能遭遇了骗子，因为她自己并没有支出这样一笔钱。一查账户，果然显示有一笔5000元的交易。陈冬儿知道受了骗，立即报警。

B 奋战十几个小时，民警从300多台车中找到嫌疑车辆

“接到陈冬儿的报案后，我们根据95533这条线索，分析可能是遭遇了电信诈骗，而且可能是使用了伪基站群发短信。”长沙市公安局雨花分局刑侦大队民警孙瀚告诉今日女报/凤网记者，有此遭遇的不止陈冬儿一人。

民警们开始搜集类似的电信诈骗短信案例，发现近段时间来报案的人有100多个。通过对他们接收到的诈骗短信地点和诈骗短信时间的分析，民警得出结论：每天上午9时到10时，伪基站的发射信号都经过长沙猴子石大桥。

“伪基站的发射距离是有限制的。”孙瀚解释，“通常，它只能给500米半径的所有手机发送短信，因此，它需要移动，或者到人群密集的地方，才能发送短信给更多的人。”

9月24日7时左右，孙瀚和几位同事来到猴子石大桥蹲守，9时46分，几位民警的手机同时响起短信铃声，他们收到了跟陈冬儿一样的短信息。显示号码为“95533”。

接下来，民警开始调阅9时46分左右猴子石大桥的监控视频，发现当时经过的车辆有300多台，民警察随后又翻查了前后两三天该时段的监控视频，最终从众多车辆中确定了一辆嫌疑车。“我们3位民警每人负责100多台车，每台车都要进行甄别和筛选。连续工作了十几个小时，才终于作出判断。”

9月25日，长沙市公安局雨花分局刑侦大队的民警，在队长李啸的指挥下，分为三组，一共三台车，每车3人，前往猴子石大桥进行跟踪、抓捕。当天10时左右，当嫌疑车辆出现时，民警们又再次收到了显示为“95533”的诈骗短信。民警兵分三路悄悄靠近、堵截。最终，当嫌疑车辆在长沙高桥大市场某处停下来时，民警将正在车上发送短信的刘虫鸣（化名）抓获。

C 百万老板破产后瞄上日赚2000元行当

在车内，民警发现了全套伪基站设备：一个手提箱、一根60厘米长的天线、一台笔记本电脑。

“伪基站可以给一定范围内的所有手机发送短信，它能模拟任何一个号码，还能抓取附近的所有电话号码，无论你是联通，电信，还是移动。”长沙市公安局雨花分局刑侦大队民警孙瀚说，这种伪基站可以模拟110、银行、通讯公司等任何号码，包括国外的号码，以及我们的亲戚朋友的号码，然后发送垃圾短信来进行诈骗。“我们当时发现其发送的诈骗短信有7万多条，设置的钓鱼网站有4个。”

孙瀚介绍，用这种伪基站发送垃圾短信，操作很轻松，一个人就行，几乎没什么技术含量。

而更让民警吃惊的是，刘虫鸣竟然曾经是一位百万老板。他为何要从事电信诈骗的勾当呢。

原来，出生在湖南邵阳的刘虫鸣2007年从中南大学土木工程专业毕业后，也有一份不错的工作。后来，他选择下海去广东创业，赚了几百万元。但好景不长，因为经营不善等多种原因，公司垮了，他辛苦赚的几百万全亏了。

但让人意外的是，刘虫鸣没有选择东山再起，而是转行了。他为一个利用伪基站发送诈骗短信的老板打工。

“他可能觉得这个收入不错，一天能赚2000元，而且隐蔽性强，人们难以发现。”孙瀚介绍，但是2014年末，刘虫鸣在惠州因此被抓，并被判处6个月的管制。管制对罪犯并不予以关押，但会限制其一定自由。刘虫鸣选择回到湖南接受管制。但他没有“浪子回头”，而是重操旧业。他买来各种零件，然后自己组装了一个伪基站。

“从他的交易开支来看，总共花了不到1万元。”孙瀚介绍，这个骗局能够完整实施，还有一个技术人员，负责设置形似银行界面的钓鱼网站。因为钓鱼网站很快会被屏蔽，因此，技术人员需要不断地设计钓鱼网站，骗子也才会在短信中提到“逾期不可兑现”。

此外，还有一个人负责操作银行卡转账。“骗子可以通过钓鱼网站看到你输入的任何信息。然后，他们用你的卡进行快捷支付，并自动转换一个要输入验证码的页面，当你输入验证码，就确认了支付。像陈冬儿就是这样被骗的。”孙瀚告诉今日女报/凤网记者，目前，这个团伙只剩下负责转账的骗子在逃。

孙瀚提醒，收到类似短信，千万不要点开，若不小心点开了，请及时对手机进行杀毒；如果想了解信息真假，请自己拨打相关单位官方电话进行咨询。

TIPS1 近来电信诈骗手法

1 假冒10086

今年5月底，大量用户投诉反馈收到10086积分兑奖诈骗短信。根据反馈信息，长沙移动联合警方，通过技术手段精确定位犯罪分子所在位置，将这个设在宾馆内的伪基站窝点捣毁。

2 响一声就断

响一声就挂机的电话，你如果回拨过去，一般是语音播放提示用户中奖、重金求子等欺诈信息。今年5月初，长沙县公安机关曾破获一起这样的案子。嫌疑人通过给大量手机安装自动拨号软件程序进行“随意”拨号，每小时呼叫可达万次。其诈骗方法为富婆重金求子，诱骗受害人交诚意金。

3 “我是公安局江警官，你涉嫌贩毒……”

在这种骗局中，对方通常会声称自己是警官，如果你要证明自身清白，必须立即去银行办一张新卡，将自己身份证名下银行卡上的钱全部转到新卡上，然后转入公安局的安全账户，就能证明她没有参与犯罪，这些钱3天后，公安局会自动返还到新卡上。最后，警官会警告你此事千万要保密，任何人都不能告诉，否则就要判刑。如果你信了，结果当然是被骗。

4 “你猜我是谁”，骗了5千万

据新华网报道，今年3月份，常德津市警方接到50多名受害人及多家企业报警称被电信诈骗，涉案金额达5000多万元。原来，有一个诈骗团伙购买了全国各地电话卡，随机拨打手机号码，接通后以“你猜我是谁”开始，冒充接听者熟人、上级领导逐步诱人上当受骗，以各种理由骗人汇款。

TIPS2 伪基站信号强过运营商

伪基站设备是一种高科技仪器，一般由主机和笔记本电脑组成，因为伪基站的信号强度远远大于运营商基站的强度，所以，它不是通过运营商的通信网络，而是强制其覆盖范围内用户从运营商网络切换到伪基站网络，然后通过短信群发器、短信发信机等相关设备，给一定半径范围内的手机发送垃圾广告短信。作为运营商来说，它们只能监测到这个区域内的用户信号短时受到干扰，到底是什么原因引起的，却无法准确判断。

9部门严打伪基站

据新华社，2014年以来，中央宣传部、中央网信办、最高法、最高检、公安部、工信部、安全部、工商总局、质检总局等9部门在全国范围内部署开展打击整治专项行动，严打非法生产、销售和使用伪基站设备的违法犯罪活动。据不完全统计，2014年，湖南省内电信诈骗发案近2万起，造成损失达3亿。