



## 合肥警方详解骗子惯用伎俩

# 都是新型电信诈骗的“套路”

冒充领导口气求财,号称“万事通”帮忙低息贷款,虚构股市内幕消息,子女遭绑架……随着电信诈骗手段的不断翻新,犯罪分子可谓“套路”满满,市民稍有不慎就会落入他们设定的圈套中,成为待宰羔羊。

如何预防电信诈骗、识破这些骗局成了关注的热点话题。为此,市场星报、安徽财经网记者专门来到合肥市公安局刑警支队,为读者揭露新型电信诈骗手段,请民警详细解析骗子的惯用伎俩。

■ 记者 王伟伟

### 套路一： 冒充领导口气求财， 迷糊老总乖乖汇款5万元

王某是合肥某公司的总经理秘书,上班时接到一个电话,电话中一男子声称是省某某厅的“伍处长”,让总经理接电话。公司总经理张某接电话后,该“伍处长”称“省某某厅的齐厅长”找总经理有事,并给其一个手机号码让张某打过去。张某得知,这位“齐厅长”老领导的亲戚在做礼品生意,希望其照顾,让张某拿50400元到“厅长办公室”买礼品。

张某也想通过此事与“厅长”建立友好关系,立即同意,并把该手机号码给了王某让其和公司的出纳办理此事。其间,“伍处长”又来电话,说“齐厅长”要送老领导去机场,希望在老领导登机前这笔钱能入账,让其把钱直接汇到某账号中,于是王某与单位出纳在银行将50400元汇出。随后,王某在与“伍处长”联系时发现对方电话再也无法接通,方知被骗。

**民警解析:**此类诈骗案,犯罪分子事先通过互联网或其他渠道非法收集事主信息,然后拨打电话冒充事主上级领导,以上级领导出国考察、孩子结婚,或亲戚做生意需要照顾等名义,要求事主向其指定账户打钱实施诈骗犯罪。

### 套路二： 自称炒股专家 有可靠内幕消息源

一名自称北方某投资咨询公司工作人员的男子赵某利用非法渠道获取了股民个人信息,随后,通过电话与股民曲某取得联系。开始,赵某先是向曲某推荐股票,在曲某的股票碰巧获得几次短线收益后,获取了曲某的信任。其后,赵某分别以“有内幕消息可以炒股赢利”“在公司做假账需先投入资金”等借口借款,分数次诈骗曲某80余万元。

**民警解析:**犯罪分子往往自称是某“投资公司”“金融咨询公司”或“某某私募公司”的工作人员,以推荐股票、提供内幕消息为由收取“服务费”“会员费”“收益分成”,或帮助代为操作、购买股票为由,对事主实施诈骗犯罪。

### 套路三： “妈妈救命！” 电话里传来子女呼救声

不久前,51岁的林某家中电话响起,接通后,电话里有人大声喊:“妈妈,救命!”好像是儿子的声音。然后就有一名男子接过电话,说林某儿子被绑架了,让赶快打钱,否则

“撕票”。林某当时就慌了连说可以。男子给林某一个账号,让林某抓紧汇4万元“赎金”,并让林某把家里电话听筒放在一边,不让挂电话;然后该男子拨打林某的手机,让林某接通后将手机保持通话状态,迅速到附近银行打钱。林某如数汇出“赎金”后,出了银行,对方就挂了电话。

随后,该男子又多次打电话来,以“老大”要求加2万元才肯放人,司机要红包等理由要求林某汇款,林某都一一照办。待林某回到家里,想起来应该拨打儿子的电话,这才知道其儿子一直在单位上班。林某因被诈骗损失72000元。

**民警解析:**犯罪分子利用非法获取的公民个人信息,拨打事主电话,谎称事主亲人(一般指事主的子女)被其绑架,犯罪分子的同伙往往会在旁边假冒被绑架者大声呼救,犯罪分子要求事主迅速向其提供的银行账户汇“赎金”,否则“撕票”。事主往往会因关心情急而信以为真,听从犯罪分子指挥,匆匆向其提供的银行账户汇“赎金”。

### 套路四： 朋友圈装“万事通”吸金 自称有门路低息贷款

市民钱先生是一家红酒销售公司的负责人,去年夏天,他被朋友拉进一个微信群,群里一位公认的“万事通”翟先生称有门路办低息贷款。急需资金周转的钱先生私下联系翟先生办一笔小额贷款,翟先生满口答应,称需要1.5万元保证金,再加1千元的好处费。钱先生二话没说将1.6万元打到翟先生提供的银行账户上。后来虽然贷款没办下来,钱也没能退回,但钱先生觉得自己因为这件事和“大神”混熟了,这些钱当投资了。

此后,二人日渐熟悉,一天,翟先生无意得知钱先生售卖的红酒进货价,便说自己有货源,价格比钱先生进货价便宜。钱先生一听心花怒放,转头就给胡先生转了10万元,等着翟先生为他进货。随后,翟先生又以朋友急需贷款为由,从钱先生这里拿走了5万元,随后就消失得无影无踪。

**民警解析:**此类短信,是骗子利用在银根紧缩的背景下,一些企业和个人急需周转资金的心理,以低息贷款诱人上钩,然后以预付利息等名义骗钱。

### 套路五： 你的信用卡扣除年费1200元 详情拨打电话……

女子李某手机接到一个短信“通知”,内容为“您的信用卡被扣除年费1200元,如有疑问请致电\*\*\*\*\*”。一看

银行卡被扣费,李某立即拨打该短信所留电话咨询。接电话的是一名30岁左右女性,自称是某银行工作人员。对方在电话中称有人以李某名义在某某银行开了一张可透支10万元的信用卡,并在珠宝店消费了23600元。该女子要求李某立即向所谓“公安局金融犯罪科”报警。

李某按照该女子所报电话号码打过去。接电话的是个40岁左右的男性,南方口音,自称“公安局金融犯罪科”民警,称李某涉嫌一宗洗钱犯罪,让其致电另一号码“设置银行卡监控功能”。就这样,李某转接了无数个电话,并按要求在自动取款机选择英文界面操作,按照对方要求输入大量的数字。随后,当李某发现自己银行卡内40000元存款被转到了一个陌生的账号上时,方才意识到自己被人骗了。

**民警解析:**犯罪分子利用短信群发器、伪基站等设备,发送事先编好的银行卡“扣年费”“购物消费”“透支”等虚假通知的短信,诱使事主与其联系,事主若按照短信所留联系方式打电话去“咨询”时,犯罪分子及其同伙便会分别扮演银行、银联中心、公安司法机关工作人员等角色,在确定事主银行账户有存款情况下,设下层层圈套,骗取事主银行账户资金。其中,伪基站发送的短信甚至可以冒充“110”“95588”“95533”等公共服务短号,危害性更大。

#### 警方提醒

除了上述的骗局,还有一些常见的诈骗手段:  
以“包裹内有毒品”等涉嫌犯罪为由,利用任意小号软件进行诈骗。  
高薪急聘员工,以“预收服装费、面试费、保证金”等名义诈骗。  
诱使回电“骗取”高额话费,一回拨即收费500元。  
虚构二手商品转让交易信息诈骗,以“缴纳定金”“交易税手续费”等方式骗取钱财。  
诱使关机实施诈骗,通过骗取对方亲友电话并通过短信诱使对方关机,然后在对方关机时以“在外出事故”“生病急需手术”等事由诈骗对方亲友。  
ATM机虚假告示诈骗,犯罪分子预先堵塞ATM机出卡口,并在ATM机上粘贴虚假服务热线告示,诱使银行卡用户在卡被吞后与其联系,套取密码,盗取用户卡内现金。  
盗用QQ号冒充好友进行诈骗。犯罪分子通过黑客手段,盗用某人QQ后,分别给其QQ好友,发送请求借款信息,进行诈骗。  
短信群发器发送“邮包投递未成功”“富家女重金求子”之类内容的短信,一旦事主拨打短信所留电话号码,犯罪分子便会布设层层圈套,实施诈骗犯罪活动。