## “无货，可退款”，就这样被骗走8000元

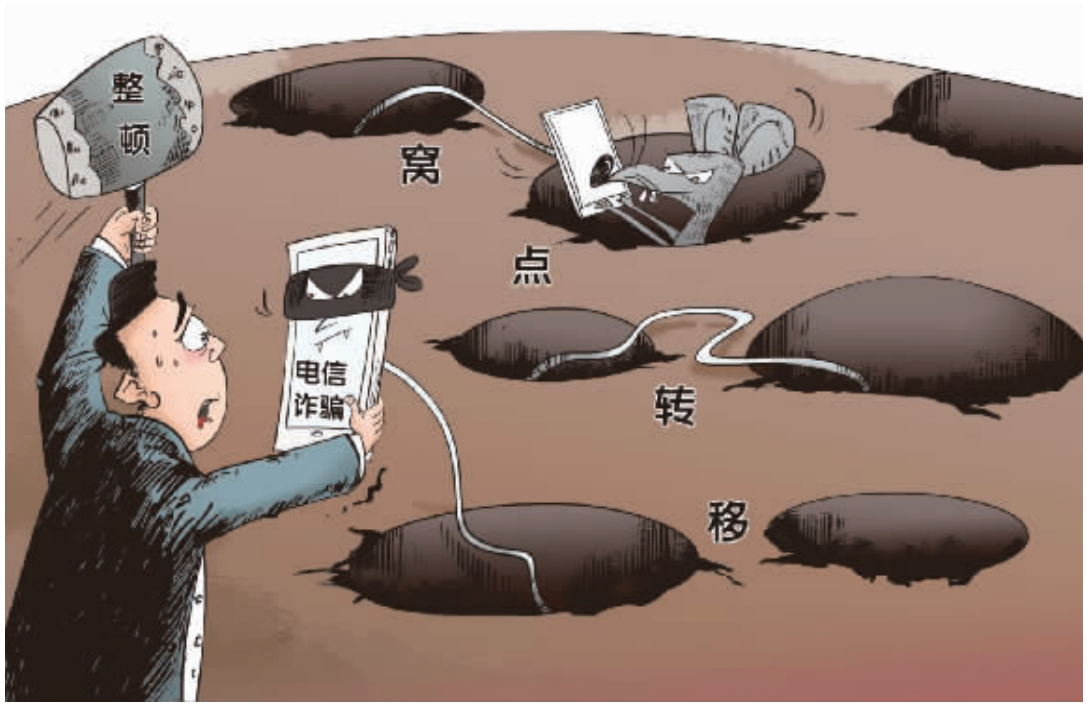
# 电信诈骗太“精准” 小心几大“套路”

“幸好我打电话问了航空公司，不然就着了骗子的道了。”日前，市民张哲在微信朋友圈发布消息，在乘坐从昆明飞往长沙的航班之前，接到短信称“您乘坐的航班因机场流量控制取消，请及时退票。”张哲立刻打电话咨询航空公司发现航班并未取消。正如张哲所言，“我走过最深的路，就是电信诈骗的套路”。

日前，《2016中国电信诈骗形势分析报告》发布，如今的电信诈骗，已经不只是发个短信通知中奖，或者“领导”打电话让你去办公室简单的伎俩。诈骗人掌握的信息精准，让人防不胜防。

12日，记者盘点了发生在我们身边的电信诈骗的几大“套路”，帮助消费者擦亮双眼，看穿骗局。

■记者 蔡平



近年来，持续高压打击下，不少福建安溪籍诈骗分子逃向其他省份甚至境外，设立窝点，广泛实施诈骗。新华社 图

### 【套路一】
### 莫名其妙“买了”贵金属产品

家住长沙市芙蓉区的市民刘先生接到了一个号码归属地为福建厦门的陌生来电，对方声称自己是某贵金属公司的工作人员，告知刘先生在其公司购买了价值37600元的贵金属，问是不是自己操作。

刘先生立刻登录了自己的网上银行，结果令他大吃一惊：卡上37600元不翼而飞，刘先生慌了。

对方表示他们可以帮助取消订单，但需要刘先生在自己的银行卡密码器上输入对方提供的单号，再把显示的数字提供给对方来取消订单。

对方开始催促，刘先生意识到如果把密码给对方，对方就能取走那37600元钱，因此并未执行。

**怎么破：**此类诈骗环环相扣。骗子以限时退款为由，要求受害者提供自己手机收到的验证码或者密码器验证码，受害者一旦把密码或者验证码提供给了对方，骗子就得手了。所以，关于银行的密码和验证码都不能告诉任何人。遇上此类情况，立即拨打银行官方客服电话核实，别相信任何主动呼入的、自称是客服的电话。

### 【套路二】
### 推荐牛股 骗取高额入会费

2015年10月，长沙市民朱先生接到一个陌生来电，对方给朱先生推荐了一个名为“投资交流群”的炒股QQ群，并声称群里会提供每日进仓的股票名称和买卖点等“内幕消息”，按照这些信息交易便可获利。

朱先生信以为真，在缴纳4万多元的“会员费”后，按照该QQ群的推荐购买了一只股票。结果，这只股票持续下跌，导致朱先生亏损并被“套牢”。朱先生立即与该QQ群负责人沟通，要求退还会费，却被对方“拉黑”并踢出该群。

**怎么破：**正规的证券公司一般是不会向股民提供付费荐股服务的，更不会以此为名向用户收取押金或保证金。骗子通常发来所谓公司的营业执照、工商证明或组织机构代码等的照片或图片，只要拨打证券公司的官方客服进行询问就能清楚。不要相信任何荐股、选股信息，不论这些信息是来自网站、QQ、短信还是电话。

### 【套路三】
### 冒充公检法 称“你涉嫌违法了”

日前，北京海淀警方证实，海淀区蓝旗营小区清华大学一老师，被冒充公检法电信诈骗人民币1760万元。

目前，“你涉嫌洗钱”、“你涉嫌非法集资”、“你信用透支需负刑事责任”，这些都是冒充公检法实施诈骗的由头。这种手法并不新鲜，但由于其极具恐吓性，不了解此类诈骗的人还是很容易上当。

**怎么破：**不要轻易相信陌生人打来的电话，如果有人说自己涉嫌犯罪，应当首先拨打110询问，或向身边的亲友询问一下，一般都能很快识破骗局。

### 【套路四】
### “您乘坐的航班取消 请及时退票”

市民张哲日前从昆明坐飞机回长沙时就遭遇了退机票诈骗。骗子取得张哲的航班信息，然后假冒客服发送短信，“您乘坐的航班因机场流量控制取消，请及时退票。”一旦张哲打开链接就会进入钓鱼网站，掉进诈骗陷阱。张哲打了航空公司客服电话才躲过这一陷阱。

《腾讯2016年第二季度反电信网络诈骗大数据报告》显示，这一诈骗类型占比高达44%，成为网络诈骗主流。骗子能够准确说出受害者的姓名、航班信息，多以可以获得改签补偿金的名义进行诈骗。

**怎么破：**机票退改签业务通过航空公司、票务代理商等正规渠道的网站、电话、服务厅办理，别相信任何电话、短信，即使与本人信息完全相符。

### 【套路五】
### “你购买的商品断货 可申请退款”

8月28日，市民刘小姐在网上购买了一个价值19元的收纳盒。29日9时许，刘小姐接到了一个自称是“售后客服”的电话。

对方准确地说出了自己的姓名、所支付的订单、价格等详细信息。紧接着，“客服”告诉她，她订购的货物目前没货，现在将货款退回给她。骗子设法套取刘小姐的银行卡号、密码和短信验证码，结果刘小姐卡上8000多元被骗子转走。

**怎么破：**遇到商品交易出现异常、断货等情况，应当首先向购物网站的官方客服电话进行咨询，不要轻易相信主动呼入的、自称是客服的人。网购账号、支付账号应当单独设置密码，并且密码要足够复杂，定期更换。

### 【套路六】
### “我换号码了，请惠存”

“我是××，我换号码了，你记一下……”收到这样一个陌生号码的短信，你可能并不会在意，立刻将号码存为你熟悉的朋友。过几天，新号码又会发来短信：有事请你帮忙。一看是朋友或亲戚的名字，警惕心自然松懈。接下来，各种老套骗术上场，稍有不慎就会上当受骗。

**怎么破：**收到这类信息后不要立刻保存新手机号码作为联系人，特别是非常熟悉的亲人或好友需要第一时间通过原号码、微信或其他共同联系人等方式确认是否换号。与熟人之间涉及到直接的资金来往要特别小心，不要未经多种方式确认对方身份就轻易转账。对一切通过电话、短信要求进行的资金操作，务必保持警惕。

**数据**

### 一个月拦截各类骚扰电话34.3亿次
### 金融理财诈骗是重灾区

360日前发布的《2016中国电信诈骗形势分析报告》数据显示，今年8月份，360手机卫士共拦截各类骚扰电话34.3亿次，其中拦截诈骗电话4.45亿次，平均每天拦截诈骗电话约1435万次。

360首席反诈骗专家裴智勇介绍，目前电信诈骗形势非常严峻，诈骗手法也非常多样，金融理财诈骗是重灾区，占比达43.2%。

还有很多是身份冒充，呈现出10大主要类型。报告数据显示，在所有的身份冒充诈骗中，冒充运营商的占26%，冒充领导的占21.2%，冒充快递的为14.3%，冒充医保社保机构的为12.5%。

而在诈骗电话的号码源类型中，固定电话呼出的诈骗电话数量最多，占所有诈骗电话呼叫量的56%；其次是400/800电话，占比为27.1%。

## 央行等六部门联合整治 非法买卖银行卡信息

记者12日从中国人民银行获悉，为保护银行卡持卡人合法权益，人民银行等六部门近日发布通知，决定于2016年9月至2017年4月在全国范围内开展联合整治非法买卖银行卡信息专项行动。

人民银行有关负责人表示，近年来，不法分子通过电信技术、黑客技术和改造银行卡收单受理终端等手段，窃取银行卡信息进而盗取卡内资金的违法犯罪活动日益猖獗，对社会公众利益和金融体系安全造成了严重威胁。

据介绍，专项行动将采取六方面的行动：破获一批非法买卖银行卡信息的犯罪案件；集中整治用于非法采集银行卡信息的钓鱼网站、恶意程序（APP）；检查银行、支付机构、银行卡清算机构的账户信息保护内控管理措施和支付业务系统安全性，排查存放大量公民个人信息的互联网站和重点行业、单位和企业的信息保护制度和系统的风险漏洞；组织开展对银行和支付机构布放的POS机具的安全性和标准符合性检查；依法关停一批发布银行卡信息非法买卖交易的网站和网络账号；加强社会公众安全使用银行卡的宣传教育。

人民银行有关负责人表示，社会公众在日常生活中应当加强对银行卡信息的保护，包括妥善保管好自己的身份证件、银行卡、网银U盾、手机；开通银行账户变动短信提醒；不随意丢弃银行卡刷卡消费或使用ATM设备的交易凭条；不轻易向外透露身份证件号码、账号、卡片信息；不轻信、不回拨收到的异常信息或电话；谨防木马病毒；妥善设置银行卡密码；使用资金额较少的银行卡或开立个人Ⅱ类、Ⅲ类户专门用于办理网络支付；将银行卡磁条卡更换为芯片卡等。

■据新华社