# 我的网银去哪儿了？警惕网络新型诈骗！


漫画　沈欣

最近，银行卡新型诈骗全国各地上演，很多人甚至开始怀疑对网银使用的安全性。那么如何正确使用网银，才能防止陷入骗子的圈套呢？本期《警周刊》将结合案例，为你还原骗子是怎么一步步设计圈套，教你如何正确使用网银避免被骗。

姜方鸣

## 【案例介绍】

7月14日，家住江北庄桥的吕先生收到一条网银扣款短信，显示账户余额为0。此时，一个广东深圳的手机电话拨打过来，吕先生接起电话后，对方称是某保证金公司的工作人员，现有一笔保证金误入了他们的账户，需要吕某提供对方发送的一组验证码方能将保证金退回账户，吕先生警觉性较高，没有按照对方的指示做，并拨打了银行官方客服咨询，才发现之前所谓的保证金公司全为诈骗。

7月28日，江东区的刘女士收到了网银扣款短信，并显示账户余额为0，正当刘某疑惑时，一个可疑电话响起，对方声称是某网店的工作人员，刘女士在其网店购买了价值7600元的货物，并报出了她的银行卡号码及相关个人信息，问是不是确认购买，刘女士随即否认。“你这情况很可能是银行卡被盗刷，得赶快取消订单，否则钱会被转走的。”对方好心劝说，并表示会发一组验证码给刘女士，只要她把该验证码提供给对方，“交易”就能取消，钱就能返还。果断识破骗局的刘女士根本不睬对方，事后，在与银行工作人员沟通过程中得知，她网银内的钱款仍然在账户内，只是转到贵金属交易平台中，犯罪分子是利用了银行提供的一种账户内贵金属交易服务，这种交易因为不涉及向卡外转移资金，默认只要登录了网银就可以操作。

## 【作案分析】

为骗走钱财，一般情况下，骗子实际上是分几步走的。骗子会先用病毒木马等方法，获取当事人的网银资料（如账号、登录密码等）。而由于转账等操作需要有U盾验证和短信验证码，因此，骗子并不能直接把钱转走，但他们会用卡里的钱来购买贵金属等理财产品，因为这一步操作是无需U盾和验证码的。一旦购买，市民的手机会收到银行发来的短信：“您尾号为××××的银行卡，手机银行支出（如意积存）××元”。甚至还会收到银行卡开通“工银e支付”的验证短信和付款短信。

一般人收到类似短信都会比较担心——明明没有买理财产品，为什么会收到类似的短信呢？而骗子恰是利用了这种心理，迅速打电话给你（一般10分钟内）并自称是某网络平台的客服。骗子会问“您是否本人购买了如意积存的产品？”当你回答没有时，他便立刻告知：“如果不是您本人购买的话，我们可以帮忙拦截，但需要您手机短信上的验证码……”不少市民因为没有警戒心理，下意识的把验证码交出去，最终导致账户里的钱被骗子转走。

## 【民警支招】

**提醒一：妥善保管个人信息**

想要骗取市民的钱，骗子必须获取银行卡号、登录密码、交易密码、手机号、验证码等关键性个人信息，所以网银使用过程中，最重要的就是妥善保管上述个人信息。

在行骗前，骗子常常会千方百计通过各种方式获取上述信息。其中比较常见的方法有：向用户手机发送包含病毒链接的短信，在点击短信后即被植入木马，造成信息泄露；通过钓鱼网站套取客户的账户名和密码；而大家在公共场合登录一些不需密码验证的免费WIFI，并使用网上银行或手机银行，也极容易造成个人信息被盗。

对此，蜀黍们的建议是，妥善保管个人信息，对没有密码的WiFi谨慎使用。一旦察觉密码存在泄露可能，建议立即更改密码，不要存一时侥幸之心。

**提醒二：银行密码设置有技巧**

骗子会通过钓鱼网站甚至通过非法途径获取客户在其他网站的资料以“撞库”的方式猜测客户电子银行登录密码尝试登录。这种情况，一般骗子会通过非法途径获取用户在其他网站的注册资料、手机号等信息，利用部分客户将电子银行用户名、密码设置为与其他网站用户名、密码相同的习惯，以“撞库”的方式猜测客户电子银行登录密码尝试登录。

对此，蜀黍们的建议是，市民的电子银行密码设置专门的、不同于其他如会员密码、电子邮箱密码的密码，避免直接使用与本人明显相关的信息，如姓名、生日、常用电话号码、身份证件号码等作为密码。同时应将网银的查询、交易密码分开来设置，同时尽量做到每个银行都有独立的账号密码。

# 网络诈骗面面观

1. **电话欠费诈骗：**犯罪分子冒充通信运营企业工作人员，向事主拨打电话或直接播放电脑语音，以其电话欠费为由，要求将欠费资金转到指定账户。

2. **欠费诈骗：**犯罪分子冒充广电工作人员群拨电话，称以受害人名义在外地开办的有线电视欠费，让受害人向指定账户补齐欠费，否则将停用受害人本地的有线电视并罚款，部分人信以为真，转款后发现被骗。

3. **退税：**犯罪分子事先获取到事主购买房产、汽车等信息后，以税收政策调整，可办理退税为由，诱骗事主到ATM机上实施转账操作，将卡内存款转入骗子指定账户。

4. **我是谁：**犯罪分子获取受害者的电话号码和机主姓名后，打电话给受害者，让其“猜猜我是谁”，随后根据受害者所述冒充熟人身份，并声称要来看望受害者。随后，编造其被“治安拘留”、“交通肇事”等理由，向受害者借钱，很多受害人没有仔细核实就把钱打入犯罪分子提供的银行卡内。

5. **消灾诈骗：**犯罪分子先获取事主身份、职业、手机号等资料，拨打电话自称黑社会人员，受人雇佣要加以伤害，但事主可以破财消灾，随即提供账号要求受害人汇款。

6. **冒充领导诈骗：**犯罪分子获知上级机关、监管部门单位领导的姓名、办公电话等有关资料，假冒领导秘书或工作人员等身份打电话给基层单位负责人，以推销书籍、纪念币等为由，让受骗单位先支付订购款、手续费等到指定银行账号，实施诈骗活动。

8. **签收诈骗：**犯罪分子冒充快递人员拨打事主电话，称其有快递需要签收但看不清具体地址、姓名，需提供详细信息便于送货上门。随后，快递公司人员将送上物品（假烟或假酒），一旦事主签收后，犯罪分子再拨打电话称其已签收必须付款，否则讨债公司或黑社会将找麻烦。

8. **考题诈骗：**犯罪分子针对即将参加考试的考生拨打电话，称能提供考题或答案，不少考生急于求成，事先将好处费的首付款转入指定帐户，后发现被骗。

9. **娱乐节目中奖诈骗：**犯罪分子以“我要上春晚”、“非常6+1”、“中国好声音”等热播节目组的名义向受害人手机群发短消息，称其已被抽选为节目幸运观众，将获得巨额奖品，后以需交手续费、保证金或个人所得税等各种借口实施连环诈骗，诱骗受害人向指定银行账号汇款。

10. **引诱汇款：**犯罪分子以群发短信的方式直接要求对方汇入存款，由于事主正准备汇款，因此收到此类汇款诈骗信息后，未经仔细核实，不假思索即把钱款打入骗子账户。

11. **消费诈骗：**犯罪分子群发短信，以事主银行卡消费，可能系泄露个人信息为由，冒充银联中心或公安民警连环设套，要求将银行卡中的钱款转入所谓的“安全账户”或套取银行账号、密码从而实施犯罪。

张莉　李鑫文　孙红青美

# 公　告

## 机动车驾驶证作废公告

2015年8月份，我市有1070名机动车驾驶人因具有《机动车驾驶证申领和使用规定》第六十七条第一款第四项至第十项（第六十八条第一款/第六十九条/第七十七条第一款）所规定的情形，机动车驾驶证（驾驶证最高准驾车型资格/实习准驾车型资格/校车驾驶资格）已被依法注销，但未收回被注销（未在规定时间内办理降级换证业务/未收回签注校车驾驶资格）的机动车驾驶证，根据《机动车驾驶证申领和使用规定》第六十七条第二款（第六十八条第二款/第七十七条第二款）等规定，现公告作废。

## 注销机动车驾驶证（驾驶证最高准驾车型资格/实习准驾车型资格/校车驾驶资格）公告

2015年8月份，我市有158名机动车驾驶人因具有《机动车驾驶证申领和使用规定》第六十七条第一款第四项至第十项（第六十八条第一款/第六十九条/第七十七条第一款）所规定的情形，机动车驾驶证（驾驶证最高准驾车型资格/实习准驾车型资格/校车驾驶资格）已被依法注销，根据相关规定，现予以公告。

## 机动车驾驶证停止使用公告

2015年8月份，我市有1234名机动车驾驶人因在一个记分周期内累计记分已达到12分，经通知拒不参加学习和考试，根据《中华人民共和国道路交通安全法实施条例》第二十五条规定，现公告其机动车驾驶证停止使用。

## 机动车登记证书、号牌、行驶证作废公告

2015年8月份，下列在我局车辆管理所登记的机动车，因具有《机动车登记规定》第三十一条（第二十一条）的规定情形，根据《中华人民共和国道路交通安全法实施条例》第九条第一款、《机动车登记规定》第三十一条（第二十一条）等规定，公告下列机动车登记证书、号牌、行驶证作废。具体如下：

大型汽车2294辆，小型汽车5235辆，挂车33辆，教练汽车123辆，摩托车43361辆，警用汽车5辆

上述机动车从本公告发布之日起，仍上道路行驶的，我局将依法收缴，强制报废并依法予以处罚。

**以上公告详情请登录：**

宁波公安交管信息网（http：//wf.nbjj.gov.cn/affiche）查询，相关公告内容同时将张贴在宁波市公安局交通警察局车辆管理所（江东区中兴北路33号）的公告栏，机动车所有人或管理人可前往查询。

特此公告。

宁波市公安局交通警察局
2015年9月14日

微博二维码　微信二维码

想要了解更多新鲜资讯，
请扫一扫上方二维码，关注
“宁波公安”微信、微博。