

## 疫情期间，反洗钱知识要了解

（漫画转自中国人民银行官网）

新型冠状病毒感染的肺炎疫情发生以来，全国上下同舟共济、众志成城，打响了一场没有硝烟的疫情防控战。位于疫情重灾区的天风股份有限公司作为反洗钱义务机构，一直全力做好疫情防控期间反洗钱工作，提醒广大人民群众和客户加强风险防范，保护自己、远离洗钱！

看看下面的漫画，你学到了什么？

## 1- 非法经营 POS 机提现

1



### 信用卡套现

黄先生

在线联系

手机:XXXXXXXXXXXX

网址:www.taoxianxinyongka.com

1.自2007年11月22日起,朱某利用伪造证件申办“××经营部”、“××服务部”、“××书店”POS机3台,并雇佣多名员工,在网上发布POS机套现信息。

2.朱某采用分散套现信用卡、分散交易金额及分散转入POS机“三分散”方式,试图掩饰非法套现犯罪活动。



2

3



3.朱某将套现资金从公司账户转入个人账户,立即通过网上银行转出或ATM提取,将套现资金付给“客户”,当天账户几乎不留余额。

4.朱某为十余名信用卡持卡人套取现金约672.4万元。2011年3月25日,山东省某市人民法院依法宣判被告人朱某犯非法经营罪,判处有期徒刑3年,缓刑3年,并处罚金8万元。



4

## 2-虚假的网上支付

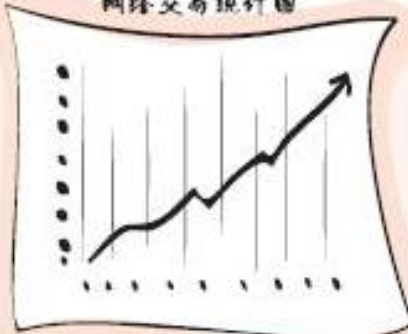
1



1. 王某在工作中获得了大量个人信息和信用卡申请表，通过伪造签名、篡改联系电话和账单地址，王某冒领他人数十张信用卡。

2. 王某指使梁某冒用他人身份证件开立多个网上支付账户和网上店铺，王某则以冒领的信用卡大肆刷卡“购物”。

网络交易统计图



2

3



3. 梁某收到资金后迅速转入多个第三方支付平台账户，再汇集到梁某、王某持有的银行卡账户中，完成洗钱。

4. 多名信用卡所有人收到银行催款通知或发现信用不良记录后，纷纷向公安机关报案。最终，王某因金融诈骗罪获刑，梁某因洗钱罪被起诉。



4

### 3-不翼而飞的网银巨款



1. 张先生的手机收到一条短信，提示他的网银需要升级。张先生立即登录短信提供的网址，进行操作。

一旦用户在“钓鱼网站”上进行操作，犯罪分子就可以通过木马程序窃取用户的账号和密码。

2. 两天后，张先生再次登录网银准备给家人汇款时，发现账户中的上百万元已不翼而飞！警方调查发现，这是一个典型的“钓鱼网站”诈骗案。



3. “钓鱼网站”与真正的银行官方网站非常相似。

4. 犯罪分子利用窃取的用户账号和密码登录网上银行，将受害者资金转到其所控制的账户，并通过ATM多次提现，完成洗钱。



#### 4-麻烦不断的网上钱庄汇款



1

1.2010年以来，杜女士在海外务工的丈夫因某地下钱庄手续费低廉，多次通过其将收入汇回国。

2.2011年杜女士的丈夫又汇出一笔钱，但杜女士却迟迟没有收到。同时，该地下钱庄在网上的频繁操作引起了警方怀疑。



2



3

3.警方调查发现，该地下钱庄利用海外汇款业务为犯罪分子清洗黑钱，杜女士也因涉嫌洗钱，多次受到警方询问。

4.虽然杜女士最终消除了嫌疑，但着实虚惊一场。



4

## 5-老乡熟人的网上洗钱圈套



## 6-网络诈骗的集资通道



1. 李某在网络上发布高息借款信息，谎称经营各种高收益项目。李某常在第一笔借款后按时偿还本金和高额利息，在获取他人信任之后，即以各种理由拒绝兑现借款承诺。

2. 赵某在明知李某进行网络诈骗的情况下，仍然将自己的账户交给李某使用，用于接收各种受骗款。



3. 赵某用银行账户的钱代李某购买别墅、商铺和住宅。

4. 案发后，李某因非法吸收公众存款罪被判入狱，赵某也因洗钱罪获利。

