



## 刷卡积分“免费”消费

小夏算是刷卡族中的“达人级”玩家了。作为公司采购,平时隔三差五出差,飞行里程数不断积累。公司让小夏自己预订机票然后报销。为订票和转账付款方便,他办了一张“牡丹上航国际信用卡”,只要出差搭乘上航或上航合作航空公司的航班,都可累积里程。一年下来,小夏去年底突然收到提示电话,说他的飞行奖励里程已达 1800 公里,可换 1800 元的机票——恰好是回家的全价机票。小夏说:“为公司卖命了一年,年底白来一张回家的机票,感觉就像是公司派送的福利。”

尝到了“刷卡积分”的甜头,小夏开始关注各家航空公司的积分派送消息,一口气办理了东航、国航联名信用卡,由于小夏出差频繁,里程数飞涨,不久就成为 3 家航空公司的金卡会员,不仅积分成倍累计,还能在贵宾室候机。另外小夏还发现,用信用卡刷卡预订酒

店,同样可累积积分,达到一定程度,有免费住店机会。现在小夏正谋划着用刷卡积分,为他和女朋友赚出一个免费国内游呢!

消费一定要花钱吗?或许不少人至今对刷卡积分还嗤之以鼻,认为那只是噱头,但是像小夏这样的“刷卡达人”告诉我们,如果合理利用积分,刷卡的同时其实已在为下次消费省钱了。但积分的关键在于消费意识的改变,“刷”字则是王道。要想多得积分,最好养成刷卡消费习惯,无论金额大小,一律刷卡买单。此外还要掌握银行卡积分窍门。

### 小贴士 节省跨行取款费

目前,多数银行对跨行取款要收取每笔 2 元的手续费,为了节省此项开支,可尽量选择网点和 ATM 机数量较多的银行,这样可以减少跨行取款的机会,节省开支。

## 手机银行安全性有保障

手机银行其便捷性不言而喻，不过也有很多朋友有安全性方面的担忧：“网上银行已经不够安全了，手机银行岂不是有更多隐患吗？”诸如此类想法非常普遍，不过，在对手机银行安全性做进一步调查后，可能你的想法会改变。

例如，工商银行的安全保障分为几层，首先是客户端手机号与手机银行绑定，对于没有开通手机银行即未绑定的手机号码，是无法使用工商银行手机银行的。其次，工商银行用户在开通手机银行时需要设定登录密码。另外，工商银行还将网上银行电子口令卡配置到手机银行上，在客户想要进行转账等资金交易时需要输入，并同时输入交易密码和验证码。为了进一步确保安全，你可以选择开通手机银行时不开通对外转账、电子商务、网上缴费等功能。

## 外币避险有“门道”

人民币不断升值，很多手里持有美元等软货币资产的人免不了为自己的资产贬值而苦恼。这里就为你介绍一些常用的外汇避险方法。

1. **及时结汇。**你可能有外币的收入，一个比较好的方法就是收到之后迅速结汇。避免资产在你持有之后继续贬值。

2. **兑换成欧元等比较坚挺的币种。**这样不仅在一定程度上避免了资产的进一步贬值，有时还可能由于人民币相对该币种贬值而带来一定的收益。

3. **利用外币进行投资以避免通胀、贬值对资产带来的侵蚀。**常见的有购买外币理财产品等。

4. **还有一种大家可能还不熟悉的产品就是外汇期权。**它不仅可以用于现有外币的保值，而且如果你未来有确定的外币流入，你可以从现在开始为其进行“保值”了。具体的方法是：当你持有软货币的时候，你可以买入未来以指定价格卖出该币种的期权，这样就锁定了你的资产价值或者未来流入的资产价值。这种方法尤其适用于较大外币数额的持有者。



## ATM 机欺诈的防范

一、要留意身边是否有陌生人偷窥密码或离自己距离太近,必要时提醒他人与自己保持一定距离;

二、不要转移注意力捡东西或向别处张望;

三、不要轻易接受“热心人”的帮助,被人转移注意力;

四、用手或身体挡住插卡口,防范不法分子调包;

五、提高安全用卡意识,对 ATM 机上张贴的各类通知、ATM 机的改动、卡被吞吃等情况提高警惕。如果不放心,请直接拨打银行的客户服务热线,或者到银行柜台询问,不要拨打张贴通知上所留的电话;

六、留意门禁是否有密码键盘或改装痕迹(一般自助区不设门禁密码);

七、留意是否有多余的装置或摄像头,键盘是否有改装过的痕迹或被贴上薄膜。同时,还要时刻关注账户内的资金变化,假如无暇关注,不妨为自己开通个余额变动提醒。不少银行都推出了余额变动短信提醒的服务,只要定制了该项服务后,市民存取款、转账汇款、刷卡消费或投资理财时,只要账户资金发生变动,就能在第一时间收到手机短信提醒,随时了解账户资金变动情况。



## 如何防范 网银被盗



1. 访问银行网站时请直接输入网址登录,建议将银行网站地址添加到浏览器的“收藏夹”中,不要采用超级链接方式间接访问。

2. 保护好密码。您是唯一知道自己网上银行密码的人。一旦卡号和密码被他人窃取或猜出,您的账户就有可能在网上被盗用,从而造成不必要的损失。

3. 将您的网上银行登录密码和用以对外转账的支付密码设置为不同的密码,多重验证以保证您的资金安全。不要在计算机上保存您的密码。不要将密码书写于纸张或卡片上。要定期更改密码。

4. 查看欢迎页面上的“上次登录时间”和实际登录情况是否相符,便于您及时发现异常情况。

5. 确保计算机安全,定期下载安装最新的操作系统和浏览器安全程序或补丁,将您计算机中的 hosts 文件修改为只读,不要开启不明来历的电子邮件。

6. 不要在公共场所(如网吧、公共图书馆等)使用网上银行,因为您无法知道这些计算机是否装有恶意的监测程序。

7. 在每次使用网上银行后,不要只关闭浏览器,请点击页面右上角的“退出登录”结束使用。

## 8 大骗术要看清楚

### 骗术 1: 短信欺诈。

冒充银行工作人员发出“在商场刷卡消费成功”类似短信,电话回复时指导存款人到 ATM 机转账,骗取存款。

### 骗术 2: 电话骗取密码。

电话告知“您的银行卡被人伪造或盗用,犯罪嫌疑人已抓获”,要求把卡号和密码报给假冒的银行工作人员,骗取密码。

### 骗术 3: 伪造非法网站盗取卡信息。

伪造与银行网址相似的非法网站,或通过某些网站打广告建立链接,存款人输入卡号和密码进入网站后,卡信息即被盗取。

### 骗术 4: 安装微型摄像机和刷卡槽。

在 ATM 机上安装微型摄像机、在 ATM 机门禁卡槽或插口上加装假刷卡槽,盗取卡信息。

### 骗术 5: 代办银行卡。

不法分子以高息回报、高额授信为诱饵,承诺代办银行存折、储蓄卡和信用卡,在办理过程中盗取卡信息。

### 骗术 6: 制造 ATM 机故障。

人为制造 ATM 机故障,并在 ATM 机上张贴“通告”称银行系统出现故障,指导存款人按“通告”上的流程操作,诱骗转账。

### 骗术 7: 在 ATM 机安装挡板。

在 ATM 机出钞口安装挡板,无法正常吐钞,待存款人离开后取走现金。

### 骗术 8: 调包盗取银行卡。

趁存款人操作 ATM 机时,利用拍肩膀等手段转移注意力后取走银行卡,同时在出钞口插入假卡造成卡已退出的假象,并以急需取钱为由催促存款人离开。



对此，我们提醒广大金融消费者从以下8个方面加强银行卡诈骗的风险防范：



## 8 大对策教你防范

- 对策 1：** 不要通过非银行工作人员办理银行卡；
- 对策 2：** 向银行提供准确的收件地址，确保亲自收到银行卡及账单，向发卡行申请开通账户资金变动短信及时提示服务；
- 对策 3：** 收到银行卡后及时修改密码，在卡背面签署姓名，记住发卡银行网站地址和客服电话；
- 对策 4：** 妥善保管银行卡及密码，卡遗失后立即挂失，密码设置避免使用生日、手机号码、6位相同数字；
- 对策 5：** 操作银行自助设备中如有人故意靠近，要引起高度警惕并注意不被他人看到密码，交易完成后核实取回的银行卡；
- 对策 6：** 遇到 ATM 机吞卡、不吐钞等故障，不要急于离开和轻信来历不明的电话；
- 对策 7：** 尽量不要在网吧等公众场所进行网上银行交易；
- 对策 8：** 任何情况下银行职员或警方都不会要求存款人提供银行卡密码或向其他不明账户转账，进入自助银行门禁系统不要输入密码，遇到此类情况及时报警。