成都银行
BANK OF CHENGDU

成都市西御街16号　邮编：610015
客服电话：028-96511 / 400-68-96511
服务网址：www.bocd.com.cn

成都银行
BANK OF CHENGDU

金融知识普及月
金融知识进万家
争做理性投资者
争做金融好网民

中国人民银行
中国证券监督管理委员会

中国银行保险监督管理委员会
国家互联网信息办公室

目录 contents

个人金融小知识

个人房屋按揭贷款

产品介绍

个人房屋按揭贷款是指成都银行向自然人发放的，用于购买住房、商业用房的房屋贷款。住房贷款同时支持公积金组合贷款。

产品特点

- 额度高：最高可贷住房价格的70%。商业用房价格的50%；
- 期限长：住房最长30年。商业用房贷款最长期限10年；
- 便捷高效：业务办理快捷，贷款发放及时。

个人综合消费贷款

产品介绍

个人综合消费贷款指成都银行向借款人发放的具有合法消费用途的人民币贷款业务。用途包括购买汽车、房屋装修装饰、购买大宗耐用消费品、旅游、出国留学等。

产品特点

- 用途多样：涵盖多种消费用途，满足您多种贷款需求；
- 担保多样：包括抵押、质押、保证等，供您灵活选择；
- 流程畅通：方便快捷，为您提供优质服务。

个人理财业务

什么是银行理财产品？

商业银行在对潜在目标客户群分析研究的基础上，针对特定目标客户群开发设计并销售的资金投资和管理计划。在理财产品这种投资方式中，银行只是接受客户的授权管理资金，投资收益与风险由客户或客户与银行按照约定方式承担。

银行理财产品面临的主要风险有哪些？

- 政策风险：国家经济政策及相关法律、行政法规、部门规章的调整与变化可能使理财产品不成立、收益降低；
- 信用风险：融资人经营活动受国家政策、法规、行业和市场因素影响，没有给投资者带来逾期回报；
- 市场风险：受市场利率影响，导致理财产品收益水平相对较低；
- 流动性风险：投资者购买理财产品后不能提前赎回或终止协议，导致资金不能随时变现；
- 其他风险：自然灾害、战争等导致理财收益降低或损失。

非保本浮动收益是什么意思？

非保本浮动收益理财产品是指商业银行按照产品说明书约定条件和实际投资收益情况向客户支付收益，并不保证客户本金安全的理财产品。

销售文件中的风险提示是什么意思？

根据中国银监会关于个人理财业务的规定，理财产品不是储蓄存款，购买理财产品是一种投资行为，存在投资风险。因此，理财产品只适合特定客户群体购买。客户填写“客户风险评估问卷”、仔细阅读风险揭示书中的“风险提示”内容并签字确认，以及抄写风险确认的相关字句，都是按照理财业务相关管理办法，本着“为客户负责”的原则，向客户充分披露本产品的风险，便于客户根据自身的风险承

受能力、风险偏好以及财务状况，做出正确的投资判断。银行也会根据产品特性和对客户的风险评估结果，为客户提供投资理财产品的建议以供参考。

信用卡知识

什么是信用卡

信用卡是指由金融机构发行的，授予持卡人一定信用额度，持卡人能够凭以支付所购商品账款、预借现金或支付其他费用的银行卡。

申请信用卡的基本条件

1. 年龄 18-60 周岁（含）；
2. 具有完全民事行为能力；
3. 具有中华人民共和国国籍的境内居民，或者具有在中国境内合法居留权的外国人和港澳台同胞；有合法而稳定的收入源；
4. 信用卡收件标准规定的其它条件。

附属卡申请的基本条件

1.年龄 18 周岁以上具有完全民事行为能力的自然人；
2.与主卡申请人的关系为父母、配偶、子女。

信用卡申领及还款流程

1.申请人本人携身份证原件以及其他我行认可的申请材料至成都银行各网点填写申请表；

2.审核通过后，卡片由我行递送至申请人指定地址；

3.持卡人收到卡片后，需由本人通过电话、网银或者柜面等渠道激活后即可使用；

4.发生消费后，持卡人可通过我行柜面、自助机具现金存入；本行网银、柜面、自助机具以及电话银行转入；他行网银转账存入等多种方式进行还款。

信用卡分期

信用卡分期是以信用卡为载体，由银行一次性代持卡人垫付消费资金后，按照与持卡人约定的期数、摊销方式将垫付资金和手续费摊销至信用卡各账单周期，由持卡人按期偿还的业务。

移动支付安全知识普及

条码支付安全知识及风险提示

知识普及

近年来，条码支付在小额便民支付领域受到消费者欢迎，为帮助大家更加安全便捷的使用条码支付，人民银行要求：

1.使用条码支付时采用不包括数字证书、电子签名在内的两类（含）以上有效要素对交易进行验证的，同一客户单个银行账户或在同一机构的所有支付账户单日累计交易金额不超过5000元。

2.采用不足两类要素对交易进行验证的，同一客户单个银行账户或在同一机构的所有支付账户单日累计交易金额应不超过1000元。

3.使用静态条形码的，同一客户单个银行账户或在同一机构的所有支付账户单日累计交易金额应不超过500元。

风险提示

1.静态码适用于小额便民支付，按规定超过500元请选择安全级别更高的支付方式；

2.条码在开放互联网环境下以图形化方式进行展示，不法分子可通过截屏、偷拍等手段盗取支付凭证，易被篡改和变造，商户宜采用防护罩等物理防护手段避免静态条码被覆盖或替换；

3.不法分子可将木马病毒、钓鱼网站链接制成条码，诱导客户扫描，窃取支付敏感信息，请不要轻易扫描来路不明的二维码；

4.条码支付对设备要求低，普通手机摄像头、超市简易的收银机扫描枪等不具备加密、防拆机等安全功能的设备均可识别条码，易被不法分子非法改装使用，单笔交易金额较大请谨慎使用条码支付。

“手机号码支付”知识普及

什么是“手机号码支付”？

“手机号码支付”是为进一步提升跨行支付服务水平，便利客户支付体验，依托网上支付跨行清算系统(IBPS)推出的新业务。“手机号码支付”支持通过提供接收人手机号码自动关联银行卡号完成跨行支付业务。

如何开通“手机号码支付”功能？

“手机号码支付”功能面向个人客户提供，客户通过开户银行的手机银行、网上银行、银行柜面(具体视各银行的开放渠道)，将本人预留手机号码与常用银行卡号关联绑定,即可开通“手机号码支付”功能。

注册“手机号码支付”功能应遵循哪些规则？

为便利客户使用“手机号码支付”，一个客户可以使用多个手机号码注册，但一个手机号码只能被一个客户注册；一个手机号码可以关联多家银行的银行卡，但在一家银行只可关联一张银行卡。

“手机号码支付”有哪些优势？

一是便捷，仅需提供接收人手机号码即可实现支付转账。免于输入银行卡号等繁琐信息。

二是快速，通过人民银行网上支付跨行清算系统处理，实时完成跨行收付款。

防范非法集资小知识

非法集资的定义、危害及主要手法等

非法集资的定义和基本特征

根据《最高人民法院关于审理非法集资刑事案件具体应用法律若干问题的解释》（法释〔2010〕18号），非法集资是违反国家金融管理法律规定，向社会公众（包括单位和个人）吸收资金的行为。非法集资行为需同时具备非法性、公开性、利诱性、社会性四个特征要件，具体为：

- 非法性：未经有关部门依法批准或者借用合法经营的形式吸收资金；
- 公开性：通过媒体、推介会、传单、手机短信等途径向社会公开宣传；
- 利诱性：承诺在一定期限内以货币、实物、股权等方式还本付息或者给付回报；
- 社会性：向社会公众即社会不特定对象吸收资金。

非法集资人的法律责任

我国《刑法》中，非法集资根据主观态度、行为方式、危害结果等具体情况的不同，构成相应的罪名，其中最主要的是《刑法》中第176条非法吸收公众存款罪和第192条集资诈骗罪。

《刑法》规定，犯非法吸收公众存款罪的，处三年以下有期徒刑或者拘役，并处或者单处二万元以上二十万元以下罚金；数额巨大或者有其他严重情节的，处三年以上十年以下有期徒刑，并处五万元以上五十万元以下罚金。犯集资诈骗罪，数额较大的，处五年以下有期徒刑或者拘役，并处二万元以上二十万元以下罚金；数额巨大或者有其他严重情节的，处五年以上十年以下有期徒刑，并处五万元以上五十万元以下罚金；数额特别巨大或者有其他特别严重情节的，处十年以上有期徒刑或者无期徒刑，并处五万元以上五十万元以下罚金或者没收财产。

非法集资的常见手段

一是承诺高额回报。不法分子编造“天上掉馅饼”“一夜富翁”的神话，许诺投资者高额回报。为了骗取更多的人参与集资，非法集资人在集资初期往往按时足额兑现承诺本息，待集资到一定规模后，便秘密转移资金或携款潜逃，使集资参与人遭受经济损失。

二是编造虚假项目。不法分子大多通过注册合法的公司或企业，打着响应国家产业政策、开展创业创新等幌子，编造各种虚假项目，有的甚至组织免费旅游、考察等，骗取社会公众信任。

三是以虚假宣传造势。不法分子在宣传上往往一掷千金，聘请明星代言、名人站台，在各大广播电视、网络等媒体发布广告、在著名报刊上刊登专访文章、雇人广为散发宣传单、进行社会捐赠等方式，制造虚假声势。

四是利用亲情诱骗。有些类传销非法集资的参与人，为了完成或增加自己的业绩，不惜利用亲情、地缘关系，编造自己获得高额回报的谎言，拉拢亲朋、同学或邻居加入，使参与人员迅速蔓延，集资规模不断扩大。

典型非法集资活动的“四部曲”

第一步：画饼。非法集资人会编织一个或多个尽可能“高大上”的项目。以“新技术”、“新革命”、“新政策”、“区域链”、“虚拟货币”等为幌子，描绘一幅预期报酬丰厚的蓝图，把集资参与人的胃口“吊”起来，让其产生“不容错过”“机不可失”的错觉。非法集资人一般会把“饼”画大，尽可能吸引参与人眼球。

第二步：造势。利用一切资源把声势做大。非法集资人通常会举办各种造势活动，比如新闻发布会、产品推介会、现场观摩会、体验日活动、知识讲座等；组织集体旅游、考察等，赠送米面油、话费等小礼品；大量展示各种或真或假的“技术认证”“获奖证书”“政府批文”；公布一些领导视察影视资料，公司领导与政府官员、明星合影；故意把活动选在政府会议中心、礼堂进行，其场面之大、规格之高极具欺骗性。

第三步：吸金。想方设法套取你口袋里的钱。非法集资人通过返点、分红，给参与人初尝“甜头”，使其相信把钱放在他那儿不仅有可观的收入，而且比放在自己口袋里还安全，参与人不仅将自己的钱倾囊而出，还动员亲友加入，集资金额越滚越大。

第四步：跑路。非法集资人往往会在“吸金”一段时间后跑路，

或者因为原本就是“庞氏骗局”人去楼空，或者因为经营不善致使资金链断裂。集资参与人遭受惨重经济损失，甚至血本无归。

如何有效识别和防范非法集资

● 如遇以下情形向公众集资的，务必提高警惕：

1.以“看广告、赚外快”“消费返利”为幌子的；
2.以境外投资股权、期权、外汇、贵金属等为幌子的；
3.以投资养老产业可获高额回报或“免费”养老、“以房”养老等为幌子的；
4.以私募入股、合伙办企业为幌子，但不办理企业工商注册登记的；
5.以投资虚拟货币、区块链等为幌子的；
6.以“扶贫”“互助”“慈善”“影视文化”等为幌子的；
7.在街头、商场、超市等发放投资理财等内容广告传单的；
8.以组织考察、旅游、讲座等方式招揽老年群众的；
9.“投资、理财”公司、网站及服务器在境外的；
10.要求以现金方式或向个人账户、境外账户缴纳投资款。

● 投资理财注意事项

1.不要轻易相信所谓的高息“保险”、高息“理财”，高收益意味着高风险；
2.不被小礼品打动，不接收“先返息”之类的诱饵，记住天上不会掉馅饼；
3.要通过正规渠道购买金融产品。不与银行、保险从业人员个人签订投资理财协议，不接收从业人员个人出具的任何收据、欠条；购买保险过程中要尽量做到“三查、两配合”，即通过保险公司网站、客户热线或监管部门、行业协会网站查人员、查产品、查单证，配合做好转账缴费、配合做好回访；
4.注意保护个人信息，关注政府部门发布的非法集资风险提示，遇到涉嫌非法集资行为及时举报投诉。

● 防范非法集资的“四看三思等一夜”法

四看。一看融资合法性，除了看是否取得企业营业执照，还要看是否取得相关金融牌照或经金融管理部门批准。二看宣传内容，看宣传中是否含有或暗示“有担保、无风险、高收益、稳赚不赔”等内容。三看经营模式，有没有实体项目，项目真实性、资金的投向去向、获取利润的方式等。四看参与集资主体，是不是主要面向老年人等特定群体。

三思。一思自己是否真正了解该产品及市场行情。二思产品是否符合市场规律。三思自身经济实力是否具备抗风险能力。

等一夜。遇到相关投资集资类宣传，一定要避免头脑发热，先征求家人和朋友的意见，拖延一晚再决定。不要盲目相信造势宣传、熟人介绍、专家推荐，不要被高利诱惑盲目投资。

网络安全法 - 这些内容你要懂

《中华人民共和国网络安全法》是我国第一部全面规范网络空间安全管理方面问题的基础性法律，由全国人民代表大会常务委员会于2016年11月7日发布，自2017年6月1日起施行。

《网络安全法》的基本原则

第一，网络空间主权原则。网络空间主权是国家主权在网络空间中的自然延伸和表现，《网络安全法》第1条明确规定要维护我国网络空间主权。

第二，网络安全与信息化发展并重原则。《网络安全法》第3条明确规定，我国既要推进网络基础设施建设，鼓励网络技术创新和应用，又要建立健全网络安全保障体系，提高网络安全保护能力，做到“双轮驱动、两翼齐飞”。

第三，共同治理原则。网络空间安全需政府、企业、社会组织、技术社群和公民等网络利益相关者的共同参与。

《网络安全法》立法禁止哪些个人的网络行为？

不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家，破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉，隐私、知识产权和其他合法权益等活动。

发现他人有危害网络安全的行为时，我们应该如何处理？

向网信、电信、公安等部门举报。

发现网名运营者违反《网络安全法》相关规定，侵犯个人权益的，我们有哪些权利？

有权要求网络运营者删除个人信息，发现网络运营者收集、存储的个人信息有错误的，有权要求网络运营者予以更正。

安全攻略及典型案例

警惕电信诈骗

电信诈骗是近年来比较普遍的一种网络犯罪行为。不法分子通过电话、网络和短信方式，编造虚假信息，设置骗局，对受害人实施远程、非接触式诈骗，诱使受害人给不法分子打款或转账的犯罪行为。

案例一：短信欢乐购诈骗

李先生手机收到短信，称其获得980元抢购苹果6S的机会。李先生通过转账下单购机后发现，手机各种功能都非常不好使，是山寨货。

案例二：贫困助学诈骗

某大学新生徐某某，由于家庭条件不好，曾接到教育部门的电话，让她办理助学金的相关手续。正在等待助学金下发的她接到一个电话，这通电话称，有一笔2600元的助学金需尽快领取，并要求她通过ATM机将9900元学费汇入自己的账号，声称会在半小时内将

学费连同助学金一起汇款回来。完成操作后，对方电话关机，徐某某才反应过来自己上当了。万分难过的她当天晚上突然晕厥，最终经医院抢救无效去世。

安全提示：

●凡是谈到银行账户信息，一律挂掉；
●凡是谈到中奖了，一律挂掉；
●凡是短信让点击链接的，一律删掉；
●凡是微信发来的莫名链接，一律不点；
●凡是谈到“电话转接公检法”，一律挂掉；
●凡是自称领导、同事要求汇款的，一律不管；
●凡是告知“家属”出事需要先汇款的，一律举报；
●不要打开不明邮件，防止电脑、手机中毒。

防范伪基站

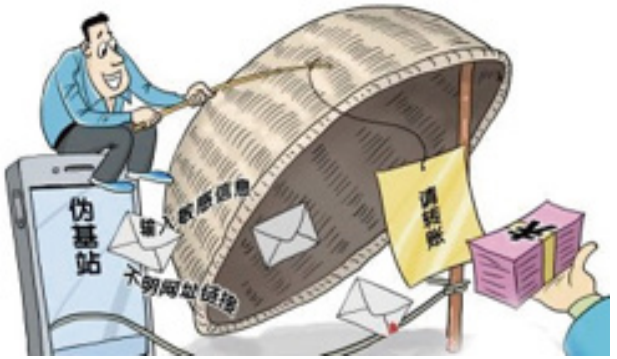
“伪基站”是不法份子利用现代计算机通讯技术伪装成运营商的基站，并向周边的手机发送伪装为银行、运营商、党政部门的信息。伪基站设备运行时，用户手机信号被强制连接到该设备上，导致手机无法正常使用运营商提供的服务，手机用户一般会暂时脱网8-12秒后恢复正常，部分手机则必须重启才能重新入网。在排除周边信号不好或者存在信号死角之外，当通话中信号突然中断时，很可能是被伪基站强制“吸”走，信号被“切断”。

案例三：短信诈骗

市民张先生收到“10000”发来的一条短信，称张先生有大量积分，可以兑换一笔金额不小的话费。张先生随后点击短信上的网址链接，进入了一个兑换话费的网页，并按提示输入了自己的银行卡账号和支付密码。张先生等了几天，说好的话费却迟迟没有到账，更蹊跷的是，他发现自己银行卡内的资金莫名减少，共被转走两万余元。事后追查，张先生是中了“伪基站”的诈骗。

案例四：“伪基站”诈骗

李女士正在玩手机，突然收到XX银行发来的短信，没有多想就点开了链接，按提示输入了自己的身份信息和银行卡信息，手机页面在运行几秒后出现输入验证码的对话框，随即手机又收到XX银行发送的一条含有验证码的短信。李女士看到验证码后，立即把验证码输入进去。没想到短短数十秒后，李女士手机又收到一条短信，是一条转款99998元的短信，这才意识到自己被骗了。



安全提示：

●不打开不明短信链接；
●发现手机信号突然中断的时候，提高警惕；
●遇到中奖、抽奖等字样时格外警惕；
●在手机上被要求输入银行、支付宝等账号及密码时要格外小心，尽量不要在非官方APP或网页上进行操作。

防范钓鱼Wi-Fi泄露隐私

不法分子在公共场合部署与免费Wi-Fi相似的钓鱼Wi-Fi。受害者访问钓鱼Wi-Fi时，他的所有数据信息都可能会被钓鱼Wi-Fi记录下来，从而盗取QQ账号、微信账号、游戏密码等个人隐私信息，甚至导致严重的财产损失。

案例五：钓鱼Wi-Fi诈骗

公共场所免费Wi-Fi来越多，人们进入酒店、餐馆、商场等公共场所后习惯先打开Wi-Fi功能，看一下是否有免费的Wi-Fi信号。市民张先生使用公共场所的Wi-Fi后，电脑被黑客入侵，在U盾、行卡均未丢失的情况下，网银被他人在两天内盗刷69次，卡上的6万多元仅剩下500元，与此同时他的手机也被黑客做了手脚，接收消费提醒

短信的功能被屏蔽，所发生的69次交易他根本没收到任何短信提示，钱在不知不觉中被转走了。

安全提示：

●关闭手机自动连接Wi-Fi的功能；

●在公共场所，不要连接未知的Wi-Fi；

●不要将自己家的Wi-Fi密码共享，定期修改密码；

●在未知的Wi-Fi信号下不要输入QQ、微信、游戏、银行卡、支付宝等账号密码；

●谨防手机在外充电、维修时信息被窃。

识别假二维码网络诈骗

不法分子虚拟一个网站并生成带有木马病毒的二维码，受害人扫描二维码后，不法分子通过云端软件获取身份证号、银行账号、手机号码等重要信息，并截取购物网站发送的验证码等，便可转走卡里的资金。有的还将这些个人信息再次出售给其它渠道，从中二次获利。

案例六：二维码诈骗

广西柳州经营快餐生意的覃先生接到一个订餐电话，电话里有人要订35份快餐，总共要消费499元钱。点好餐后，对方说钱要打入覃先生的微信里，还在电话里指挥覃先生，打开微信的收付款二维码来收钱。脑子一个不清醒，覃先生就把自己微信付款码上的数字，报给了对方。没过一会，覃先生收到一条支付成功的信息，微信里的499元钱被对方转走。覃先生这才意识到自己上当受骗了。

案例七：扫码违法停车单诈骗

有网民收到一张带有二维码的“违停罚单”，扫码后即向相关“个人账户”发起转账。一旦付款，也就等于直接转账给了骗子。

安全提示：

●不要贪图便宜随便扫描未知二维码；

●扫描后若要求填写个人账户信息，应当坚决拒绝，不要犹豫；

●手机安装正规防病毒软件，定期扫描手机安全性。

警惕充电设备中的病毒

不法分子将植入木马程序的“病毒充电宝”设置在公共场所或其他地点，读取充电手机信息，不法分子就可以借助电脑连接的互联网将此前收集到的个人信息隐蔽传输至任何地方，从而达到自己的非法意图，给受害者带来损失。

案例八：病毒充电宝诈骗

市民任女士某次出差途中，手机没电了，恰巧周围没有充电插口，只得借用一名男士的充电宝。次日，任女士便接到一通陌生电话，对方称手里有任女士手机中所有信息，包括一些重要的客户资料，向任女士索要赎金。经调查，任女士的信息泄露源头是借用他人的充电宝充电后，手机感染病毒导致的。

安全提示：

●从正规渠道购买移动充电设备；

●尽量不借用他人充电设备；

●最好使用直充电源，谨慎使用公共场所提供的免费充电接口；

●手机在连接“问题"充电宝后，不要点击提示的“信任”选项。

安全使用移动支付

随着移动支付盛行，为广大群众带来众多便利与快捷的同时，也给个人信息及财产的安全带来更多威胁。不法分子很容易在其中钻到空子，利用伪基站等手段获取动态口令，进而对群众的财产实施盗窃。

案例九：手机ID被盗

犯罪分子先通过“黑客”技术，攻破机主的注册邮箱篡改iPhone ID密码，再用该ID登录iCloud更改账户名，最后通过“查找我的iPhone 远程锁定手机。接着，盗号者将勒索邮件发到ID绑定的邮箱，称要解锁就得先交钱，以此达诈骗的目的。

案例十：微信好友色诱诈骗

小张通过陌生女子好友申请，该女子提出要小张发0.88元至88元不等红包，会给小张惊喜。小张支付0.88元后，发现账户被盗了。

安全提示：

●手机、身份证和银行卡，尽量不要放在一起，避免同时丢失造成损失；

●第三方平台的支付密码与银行卡的支付密码不要相同；

●如果银行卡丢失，请第一时间到公安机关和银行办理挂失，并及时关闭无线支付业务；

●手机和第三方支付平台设置不同的解锁密码，手机内不要存储身份证及银行卡信息；若丢失，及时补办手机号。

指纹识别安全防范

虽然指纹支付摆脱在一大堆卡中选择的烦恼，只需轻轻一按，3秒即完成支付；也不用再担心卡丢失、忘记密码，促使消费可以更简单；但每一次使用指纹时都会在指纹采集头上留下用户的指纹印痕，而这些指纹痕迹存在被用来复制指纹的可能性。

安全提示：

●若手机发生摔碰，及时检查指纹触摸键是否受损，试用未录入的手指进行解锁，若成功解锁，应立即关闭指纹支付/解锁功能；

●尽量避免使用“指纹贴”；

●在使用指纹验证前，检查指纹触摸键是否有其他异物图案；

●手机支付软件开通指纹支付业务后，一定要限额，以免被人盗用；

●对于设置过的支付方式，随时查看是否有变动。若发生变动，要进行必要的修改；

●尽量避免让他人的指纹录入到自己的手机中。

遭遇诈骗后的应急措施

●保存好汇款或转账时的凭证并立即拨打110报案,或到当地公安刑警队、派出所报案；

●向警方说清被骗经过,准确提供受害人姓名、受害人转现金的账户及开户行信息；

●向警方准确提供骗子的账号、账号用户名及户开户行(银行柜台及银行客户均可以帮助查询)；

●向警方提供汇款凭证或电子凭证截图。

提升安全意识，培养良好习惯

●提升安全意识、养成良好的安全用卡习惯，是应付层出不穷诈骗犯罪的有效方法；

●经常用于网络支付的银行卡不要存太多资金，或设置每日最高网络消费限额，减少损失；

●签约一些短信通知服务和盗刷保险服务，可以为资金财产保驾护航；

●不同网络支付账户建议设置不同密码；

●用于网络支付的电脑、Pad、手机等工具要安装杀毒软件，并定期查杀病毒；

●不要点击来历不明的网址，在进行网络支付或退款等操作时请登陆正规网站；

●不要告诉他人网络支付的动态校验码等关键银行卡信息；

●不要登录一些非法网站，避免电脑或移动终端被植入木马病毒。

金融知识问与答

A：什么是金融IC卡？

Q：金融IC卡是由商业银行发行的，采用集成电路技术，遵循国家和行业标准，具有消费信用、转账结算，现金存取，全部或部分金融功能，可以具有其他商业服务和社会管理功能的金融工具。

它具有数据存储容量大，安全性高等特点，可实现非接触式（闪付）应用，是基于传统金融支付并可无缝延伸至其他行业小额支付的智能化产品。多应用金融IC卡能够实现政府公共服务管理功能和金融支付功能，可以支持跨行业、跨平台、多功能的应用。

A：如何使用金融IC卡？

Q：金融IC卡分为接触式与非接触式（闪付）两种。接触式金融IC卡，可通过插入受理终端的读卡槽实现在POS和ATM上的使用。非接触式金融IC卡（或称闪付卡）用户可在支持“闪付”的非接触式支付终端上轻松一挥便可快速完成支付。

A：什么是小额免密免签？

Q：小额免密免签是中国银联为持卡人提供的一种小额快速支付服务。当持卡人使用具有“闪付“功能的金融IC卡或支持“银联闪付”的移动设备，在指定商户进行一定金额（境内1000元人民币，境外以当地限额为准）及以下的交易时，只需将卡片或移动设备靠近POS机等受理终端的“闪付”感应区，即可完成支付。支付过程中，持卡人不会被要求输入密码，也无需签名。

A：开通了小额免密免签功能的银行卡遗失怎么办？

Q：

1.与正常的卡片挂失一样，拨打发卡银行服务热线进行电话挂失或者前往行柜台办理挂失手续；

2.对于挂失之前72小时内发生的小额免密免签交易盗刷，在挂失后按照发卡行流程申请赔付；

3.发卡银行于接收到持卡人申请赔付的5个工作日内向银联提交补偿申请；

4.对于审核确认的情形，中国银联于2个工作日向持卡人入账。

A：银行个人账户分类管理是什么？

Q：自2016年12月1日起，个人银行账户实行分类管理，分为Ⅰ类、Ⅱ类、Ⅲ类账户，不同类别账户有不同的功能和权限。新政落地后，个人在银行开立账户，每人在同一家银行只能开立一个Ⅰ类户，如果已经有Ⅰ类账户的，再开户时，则只能是Ⅱ、Ⅲ类账户。

Ⅰ类账户I类户是“钱箱”，个人的工资收入等主要资金来源都存放在该账户中，安全性要求较高，主要用于现金存取、大额转账、大额消费、购买投资理财产品等。

Ⅱ类账户相当于“钱夹”，个人日常刷卡消费、网络购物、网络缴费通过该账户功理，还可以购买银行的投资理财产品。

Ⅲ类账户就相当于“零钱包"，主要用于金额较小、频次较高的交易，比如移动支付、二维码支付等。

A：个人账户转账业务的新增规定有哪些？

Q：增加转账方式——自2016年12月1日起，银行和支付机构提供转账服务时，向存款人提供实时到账、普通到账、次日到账等多种转账方式选择，存款人在选择后才能办理业务。

调整转账时间——除向本人同行账户转账外，个人通过ATM（自助员机）转帐的，发卡行在受理24小时后办理资金转。在发卡行受理后24小时内，个人可以向发卡行申请撤销转账。受理行应当在受理结果界面对转账业务办理时间和可撤销规定做出明确提示。

A：什么是银联二维码支付？

Q：银联二维码支付是银联联合成员机构推出的移动支付产品，可以提供消费、转账及取现等服务，包括用户主扫和用户被扫两种模式。持卡人只需一台普通的智能手机，通过出示二维码或扫描二维码完成支付，无需在受理终端输入密码，免去刷卡消费后的签名流程，操作简便、支付顺畅。

其优点在于：

1.国际标准，全球通用：遵循国际芯片卡及支付技术标准组织EMVCO二维码技术标准。发卡机构一次接入即可境内境外统一使用，收单机构一次接入即可实现内外卡统一受理；

2.支持广泛，功能丰富：支持所有智能手机和满足安全资质的APP加入并开办相关业务，用户入口类型丰富且覆盖面广泛；

3.安全可靠，风险可控：小额交易免输密码、交易免签名，操作便捷，带来全新移动支付体验；采用支付标记化(TOKEN)技术，进一步保护用户隐私信息安全；采用生物识别、设备指纹，风险实时监控及拦截等技术确保风险可控和资金安全；

4.接入简便，受理广泛：发卡机构简单改造即可快速上线。收单机构接入模式灵活，收单系统及受理终端无需改造即可开通主扫消费业务，系统改造完成后，亦可开办更丰富的业类型。支持的收单场景既包括线下实体商户收单，也包括线上移动互联网商户收单。支持的受理场景十分广泛，覆盖范围既包括商超、便利店在内的大中型商户，也包括到菜场、水果店等小微商户。

征信知识小课堂

如何保护个人信息安全

要做到：

1.妥善保管身份证件及复印件；
2.对外提供身份证复印件注明用途；
3.保管好信用报告,不随意乱放,不提供给他人使用；
4.保管好互联网查询信用报告的用户名、密码；
5.不要做:把身份证借给他人、乱扔信用报告,在公共网吧、使用公共WIFI查询、保存信用报告等。

信用报告

信用报告是什么？

是您信用历史的客观记录。
记录您借债还钱、合同履行、遵纪守法等信息。

信用报告有啥用？

是您的“经济身份证”！

●用处多：
货款、信用卡审批,任职资格审查,员工录用等。

●作用大：
记录良好,快速获得贷款、信用卡,享受低利率；
记录不好,不利于获得贷款、信用卡,利率可能较高。

信用报告记了啥?

五类信息详记录。

- 基本信息：包括身份信息、居住信息、职业信息等;
- 信贷信息：指借债还钱信息,信用报告中最核心的信息;
- 非金融负债信息：先消费后付款形成的信息,如电信缴费;
- 公共信息：社保公积金信息、法院信息、欠税信息、行政执法信息等;
- 查询信息：过去2年内,何人何时因为什么原因查过您的信用报告。

信用报告的信息哪里来?

放货机构、公用事业单位、法院和政府部门等。

“不良信息”指什么?

违约信息、欠税信息、法院和行政处罚信息。

信用信息存多久?

信息不同,时间不同。
不良信息:自不良行为或事件终止之日起保留5年。

谁能查您的信用报告?

您授权谁查谁就能查。
金融机构最关心您的记录,查的最多。
法院和政府部门可依法查询,无须告知或取得您的同意。

为什么说“您的信用您做主”?

征信中心，收集信息，整理信息，客观公正;
放贷机构，与您交易，报送信息，实事求是;
信用报告，记您所报，记您所为，记错改正;
好也是您，坏也是您，您若守信，无人能黑。

如何养成良好的信用习惯?

尽早使用信用卡,财富积累须及时,不当信用“空白户”;
还款日期记清楚,按时足额把款还,认真履约记录好;
量入为出好传统,精打细算好规划,过度负债要不得;
关注央行调利率,还款金额问银行,不当逾期冤大头;
对外担保也是债,他若不还您要还,否则逾期进报告;
发生逾期心莫慌,立即还钱是上策;若您真是有难处,
联系银行好商量,展期重组办法多,死马也当活马医;
还款谨慎用中介,还给中介不算还,钱到银行才算还;
联络方式有变化,通知银行莫耽误,不当信用“失联户”。

警惕钓鱼网站

时常有看上去很像但却是假的征信中心网站,目标是以各种名义骗取您的信息或钱财,切勿上当！！！

“三要”:要手动输入网址、要核对网站域名、要收藏征信中心官方网站;

“一不要”：不要点击陌生电子邮件、手机短信中的链接网址。