



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

2020 金融知识普及月

金融知识读本目录

| | |
|---------------|----|
| 个人信息保护..... | 3 |
| 防范电信网络诈骗..... | 8 |
| 理财知识..... | 20 |
| 支付安全..... | 35 |

个人信息保护

一、个人信息定义

个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

二、个人金融信息保护法律规定

目前，我国尚未出台专门的个人金融信息保护的专门法律，但在《中华人民共和国中国人民银行法》、《中华人民共和国商业银行法》、《中华人民共和国证券法》、《中华人民共和国保险法》等法律法规中，都有保护个人金融信息的条款。例如：

（一）《商业银行法》第六条规定：商业银行应当保障存款人的合法权益不受任何单位和个人的侵犯。第二十九条规定：商业银行办理个人储蓄存款业务，应当遵循为存款人保密的原则，对个人储蓄存款，商业银行有权拒绝任何单位或者个人查询、冻结、扣划，但法律另有规定的除外。

（二）《中华人民共和国反洗钱法》第五条规定：对依法履行反洗钱职责或者义务获得的客户身份资料和交易信息，应当予以保密；非依法律规定，不得向任何单位和个人提供。

（三）《刑法》修正案七规定：国家机关或者金融、电信、

交通、教育、医疗等单位的工作人员，违反国家规定，将本单位在履行职责或者提供服务过程中获得的公民个人信息，出售或者非法提供给他人，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金。

（四）《征信业管理条例》第十三条规定：采集个人信息应当经信息主体本人同意，未经本人同意不得采集。但是，依照法律、行政法规规定公开的信息除外。第十四条规定：征信机构不得采集个人的收入、存款、有价证券、商业保险、不动产的信息和纳税数额信息，但征信机构明确告知信息主体提供该信息可能产生的不利后果，并取得其书面同意采集的除外。第二十六条规定：信息主体认为征信机构或者信息提供者、信息使用者侵害其合法权益的，可以向所在地的国务院征信业监督管理部门派出机构投诉，信息主体认为征信机构或者信息提供者、信息使用者侵害其合法权益的，可以直接向人民法院起诉。

（五）其他规范性文件。《中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知》（银发〔2011〕17号）规定，银行业金融机构在收集、保存、使用、对外提供个人金融信息时，应当严格遵守法律规定，采取有效措施加强对个人金融信息保护，确保信息安全，防止信息泄露和滥用。特别在收集个人金融信息时，应当遵循合法、合理原则，不得收集与业务无关的信息和采取不正当的方式收集信息。银行业金融机构不得篡改、违法使用个人金融信息。在使用个

人金融信息时，应当符合收集该信息的目的，不得出售个人金融信息，不得向本金融机构以外的其他金融机构和个人提供个人金融信息（但个人书面授权同意、以及法律法规另有规定的除外），不得在个人提出反对的情况下，将个人金融信息用于产生该信息以外的本金融机构其他营销活动。

三、金融监管部门保护措施

2011年1月21日，中国人民银行印发了《关于银行业金融机构做好个人金融信息保护工作的通知》（银发〔2011〕17号），要求商业银行强化个人金融信息保护工作，并从商业银行自身建设、个人金融信息的收集和使用、外包管理、商业银行报告义务和法律责任等方面提出了明确规定。

2012年3月27日，中国人民银行印发了《关于金融机构进一步做好客户个人金融信息保护工作的通知》（银发〔2012〕80号），要求各银行业金融机构在制度、内控管理、信息安全防范、员工教育等方面采取措施，进一步加强个人金融信息保护，并在全国银行业金融机构开展个人金融信息保护自查工作。各级人民银行分支机构适时开展了对银行业金融机构个人金融信息保护工作的专项检查，对未履行客户个人金融信息保护义务，侵害客户合法权益的，根据有关规定严肃处理。

四、金融机构保护措施

（一）采取物理隔离、防火墙等措施加强技术防范，杜绝外部非法入侵系统窃取个人金融信息；

（二）建立内控制度，对可能出现的个人金融信息泄露的环节进行排查；

（三）形成相互监督和制约的管理机制，切实防范信息泄漏事件的发生；

（四）履行客户身份识别义务，依法使用、保存和销毁客户原始凭证资料；

（五）规范查询本人、代理查询他人金融信息的程序，审核客户有效身份证件或有关法律文书；

（六）建立员工行为准则，加强员工培训教育，与涉密岗位人员签订书面保密承诺书。

五、金融消费者要强化个人金融信息风险的防范

在金融业虚拟化和网络化程度不断提升的现代社会，个人金融信息安全面临着前所未有的挑战，除了金融机构加强个人金融信息安全管理外，广大金融消费者也应增强防范意识，妥善采取保护措施，确保自己的个人金融信息等隐私信息不受侵害。

（一）切勿把自己的身份证件、银行卡等转借他人使用。

（二）在日常生活中切勿向他人透露个人金融信息、财产状况等基本信息，也不要随意在网络上留下个人金融信息。

(三) 尽量亲自办理金融业务，切勿委托不熟悉的人或中介代办，谨防个人信息被盗。

(四) 提供个人身份证件复印件办理各类业务时，应在复印件上注明使用用途，例如：“仅供申报**信用卡用”，以防身份证复印件被移作他用。

(五) 不要随意丢弃刷卡签购单、取款凭条、信用卡对账单等，对写错、作废的金融业务单据，应撕碎或用碎纸机及时销毁，不可随意丢弃，以防不法分子捡拾后查看、抄录、破译个人金融信息。

(六) 不要轻信来历不明的电话号码、手机短信和邮件。警惕向您询问个人金融信息的电话及电子邮件，在任何情况下，法院、警方都不会要求您告知银行账户、卡号、密码或向来历不明的账户转账，如遇到此类情况，应予以拒绝，必要时立即报警。

防范电信网络诈骗

一、电信网络诈骗的概念

电信网络诈骗是指犯罪分子通过电话、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，诱使受害人给犯罪分子打款或转账的犯罪行为。

二、电信网络诈骗的特点

（一）作案手法变化快。犯罪分子作案手法翻新层出，千方百计编造各种虚假事实进行诈骗犯罪，从最初的“中奖”、“消费”虚假信息，发展到“绑架勒索”、“电话欠费”等虚构事实诈骗，甚至冒充电信工作人员、公安民警诈骗，欺骗性非常大，识别很困难，没有接收过诈骗信息的群众非常容易上当受骗。

（二）社会危害相对较大。一些群众多年的积蓄一夜之间被犯罪分子骗取，思想包袱很大，个别群众因被骗厌世轻生自杀，给社会治安管理工作带来了很大压力。

（三）受害群体不特定。通过梳理分析，受害群体按职业分，有在校学生、个体老板、下岗工人、打工人员、农民；按年龄段分，青年人、中年人和老年人均占一定比例。

（四）侦办难度大。由于电信诈骗犯罪往往是跨地区甚至是跨境作案，涉案资金账户和受害人遍布全国各地，地区协作成本高、破案难度大。另外，此类犯罪涉及互联网、电信、计算机等多个领域，加之银行具有开户方便、

销户方便、转账方便、取款方便等功能优势，犯罪分子转移赃款便捷迅速，证据固定难度大，追回赃款的可能性小，都加大了此类案件的侦办难度。

三、遭遇电信网络诈骗后的应急措施

1. 第一时间自救：看对方账户是哪家银行的，通过该银行网银、电话银行等，对嫌疑人银行卡采取输错多次错误密码（一般为3-5次）、口头挂失等方式阻断嫌疑人取款。时间一般为24小时，这宝贵的24小时将使对方无法将钱转移，避免损失扩大，也为警方破案提供时间。

2. 及时报警：收集被骗过程的汇款凭证、通话记录等相关信息，前往当地派出所或拨打110报警。

3. 拨打中国银联专线95516请求帮助。

四、如何防范电信网络诈骗

骗子都是利用受害人趋利避害和轻信麻痹的心理，诱使受害人上当而实施诈骗犯罪活动的。我们在日常生活和工作中，应从以下几方面提高警惕，加强防范意识，以免上当受骗。

（一）克服“贪利”思想，不要轻信麻痹，谨防上当。世上没有免费的午餐，天上不会掉馅饼。对犯罪份子实施的中奖诈骗、虚假办理高息贷款或信用卡套现诈骗及虚假致富信息转让诈骗，不要轻信中奖和他人能办理高息贷款或信用卡套现及有致富信息转让，一定多了解和分析识别真伪，以免上当受骗。

（二）不要轻易将自己或家人的身份、通讯信息等家庭、个人资料泄露给他人。对于家人意外受伤害需抢救治疗费用、朋友急事求助类的诈骗短信、电话，要仔细核对，不要着急恐慌，轻信上当，更不要上当将“急用款”汇入犯罪份子指定的银行账户。

（三）遇到疑似电信诈骗时，不要盲目轻信，要多作调查印证。对接到培训通知、冒充银行、公检法机构等声称银行卡升级和虚假招工、婚介类的诈骗，要及时向本地的相关单位和行业或亲临其办公地点进行咨询、核对，不要轻信陌生电话和信息，培训类费用一般都是现款交纳或者对公转账，不应汇入过个人账户，不要轻信上当。对于来电声称是公安、检查、法院、银行等的电话号码，务必多方印证，尝试回拨电话核实，防止犯罪分子利用改号软件等手法冒认电话号码。

（四）正确使用银行卡及银行自助机。到银行自动柜员机（ATM、CRS 等）存取遇到银行卡被堵、被吞等以外情况，认真识别自动柜员机的“提示”真伪，千万不要轻信和上当，最好拨打自动柜员机所属银行电话的客服中心了解查问，与真正的银行工作人员联系处理和解决。

（五）日常应多提示家中老人、未成年人注意防范电信诈骗，提高老人、未成年人的安全防范意识。犯罪分子通常喜欢选择相对容易上当受骗的老年人、未成年人作为诈骗目标，作为子女或者父母，除了自己注意防范电信诈骗外，应积极主动向加重老人、未成年人传递防诈骗的知识，为我们

敬爱的长辈和需要呵护的下一代筑起防诈骗的知识围墙。

五、防范电信网络诈骗小技巧

在遭遇电信网络诈骗后，应尽快做到以下三步：一是准确记录骗子的账号、账户姓名；二是尽快拨打 110 或者到最近的公安机关报案；三是及时准确将骗子的账号和账户姓名提供给民警，由公安机关进行紧急止付。

六不：不轻信，不汇款、不透漏、不扫码、不点击链接、不接听转接电话。

三问：遇到情况，主动问本地警察，主动问银行、主动问当事人。

养成七个好习惯：

1. 保护好个人身份证和银行卡信息，保管好不用的复印件、睡眠卡、交易流水信息。

2. 网上银行操作时，最好手工输入银行官方网址，防止登录钓鱼网站。

3. 输入密码时，用手遮挡。

4. 密码要设置得相对复杂、独立，避免过于简单，避免与其他密码相同，定期更换。

5. 开通账户动账通知短信，一旦发现账户资金有异常变动，立刻冻结或挂失。

6. 不随意链接不明公共 wifi 进行网上银行、支付账户操作。

7. 单独设立小额独立银行账户，用于日常网上购物、消费。

六、电信诈骗的常见手段（48种）

1. QQ冒充好友诈骗。利用木马程序盗取对方QQ密码，截取对方聊天视频资料，熟悉对方情况后，冒充该QQ账号主人对其QQ好友以“患重病、出车祸”“急需用钱”等紧急情况为由实施诈骗。

2. QQ冒充公司老总诈骗。犯罪分子通过搜索财务人员QQ群，以“会计资格考试大纲文件”等为诱饵发送木马病毒，盗取财务人员使用的QQ号码，并分析研判出财务人员老板的QQ号码，再冒充公司老板向财务人员发送转账汇款指令。

3. 微信冒充公司老总诈骗财务人员。犯罪分子通过技术手段获取公司内部人员架构情况，复制公司老总微信昵称和头像图片，伪装成公司老总添加财务人员微信实施诈骗。

4. 微信伪装身份诈骗。犯罪分子利用微信“附近的人”查看周围朋友情况，伪装成“高富帅”或“白富美”，加为好友骗取感情和信任后，随即以资金紧张、家人有难等各种理由骗取钱财。

5. 微信假冒代购诈骗。犯罪分子在微信朋友圈假冒正规微商，以优惠、打折、海外代购等为诱饵，待买家付款后，又以“商品被海关扣下，要加缴关税”等为由要求加付款项，一旦获取购货款则失去联系。

6. 微信发布虚假爱心传递诈骗。犯罪分子将虚构的寻人、扶困帖子以“爱心传递”方式发布在朋友圈里，引起善良网民转发，实则帖内所留联系方式绝大多数为外地号码，打过去不是吸费电话就是电信诈骗。

7. 微信点赞诈骗。犯罪分子冒充商家发布“点赞有奖”信息,要求参与者将姓名、电话等个人资料发至微信平台,一旦商家套取完足够的个人信息后,即以“手续费”、“公证费”、“保证金”等形式实施诈骗。

8. 微信盗用公众账号诈骗。犯罪分子盗取商家公众账号后,发布“诚招网络兼职,帮助淘宝卖家刷信誉,可从中赚取佣金”的推送消息。受害人信以为真,遂按照对方要求多次购物刷信誉,后发现上当受骗。

9. 虚构色情服务诈骗。犯罪分子在互联网上留下提供色情服务的电话,待受害人与之联系后,称需先付款才能上门提供服务,受害人将钱打到指定账户后发现被骗。

10. 虚构车祸诈骗。犯罪分子虚构受害人亲属或朋友遭遇车祸,需要紧急处理交通事故为由,要求对方立即转账。当事人因情况紧急便按照嫌疑人指示将钱款打入指定账户。

11. 电子邮件中奖诈骗。通过互联网发送中奖邮件,受害人一旦与犯罪分子联系兑奖,即以“个人所得税”、“公证费”、“转账手续费”等各种理由要求受害人汇钱,达到诈骗目的。

12. 冒充知名企业中奖诈骗。犯罪分子冒充三星、索尼、海尔等知名企业名义,预先大批量印刷精美的虚假中奖刮刮卡,通过信件邮寄或雇人投递发送,后以需交手续费、保证金或个人所得税等各种借口,诱骗受害人向指定银行账号汇款。

13. 娱乐节目中奖诈骗。犯罪分子以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。

14. 冒充公检法电话诈骗。犯罪分子冒充公检法工作人员拨打受害人电话，以事主身份信息被盗用涉嫌洗钱等犯罪为由，要求将其资金转入国家账户配合调查。

15. 冒充房东短信诈骗。犯罪分子冒充房东群发短信，称房东银行卡已换，要求将租金打入其他指定账户内，部分租客信以为真将租金转出方知受骗。

16. 虚构绑架诈骗。犯罪分子虚构事主亲友被绑架，如要解救人质需立即打款到指定账户并不能报警，否则撕票。当事人往往因情况紧急，不知所措，按照嫌疑人指示将钱款打入账户。

17. 虚构手术诈骗。犯罪分子虚构受害人子女或老人突发急病需紧急手术为由，要求事主转账方可治疗。遇此情况，受害人往往心急如焚，按照嫌疑人指示转款。

18. 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。

19. 电视欠费诈骗。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。

20. 退款诈骗。犯罪分子冒充淘宝等公司客服拨打电话或者发送短信谎称受害人拍下的货品缺货，需要退款，要求

购买者提供银行卡号、密码等信息，实施诈骗。

21. 购物退税诈骗。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。

22. 网络购物诈骗。犯罪分子开设虚假购物网站或淘宝店铺，一旦事主下单购买商品，便称系统故障，订单出现问题，需要重新激活。随后，通过 QQ 发送虚假激活网址，受害人填写好淘宝账号、银行卡号、密码及验证码后，卡上金额即被划走。

23. 低价购物诈骗。犯罪分子通过互联网、手机短信发布二手车、二手电脑、海关没收的物品等转让信息，一旦事主与其联系，即以“缴纳定金”、“交易税手续费”等方式骗取钱财。

24. 办理信用卡诈骗。犯罪分子通过报纸、邮件等刊登可办理高额透支信用卡的广告，一旦事主与其联系，犯罪分子则以“手续费”、“中介费”、“保证金”等虚假理由要求事主连续转款。

25. 刷卡消费诈骗。犯罪分子群发短信，以事主银行卡消费，可能个人泄露信息为由，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。

26. 包裹藏毒诈骗。犯罪分子以事主包裹内被查出毒品为由，称其涉嫌洗钱犯罪，要求事主将钱转到国家安全账户以便公正调查，从而实施诈骗。

27. 快递签收诈骗。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。

28. 医保、社保诈骗。犯罪分子冒充社保、医保中心工作人员，谎称受害人医保、社保出现异常，可能被他人冒用、透支，涉嫌洗钱、制贩毒等犯罪，之后冒充司法机关工作人员以公正调查，便于核查为由，诱骗受害人向所谓的“安全账户”汇款实施诈骗。

29. 补助、救助、助学金诈骗。犯罪分子冒充民政、残联等单位工作人员，向残疾人员、困难群众、学生家长打电话、发短信，谎称可以领取补助金、救助金、助学金，要其提供银行卡号，然后以资金到帐查询为由，指令其在自动取款机上进入英文界面操作，将钱转走。

30. 引诱汇款诈骗。犯罪分子以群发短信的方式直接要求对方向某个银行帐户汇入存款，由于事主正准备汇款，因此收到此类汇款诈骗信息后，往往未经仔细核实，即把钱款打入骗子账户。

31. 贷款诈骗。犯罪分子通过群发信息，称其可为资金短缺者提供贷款，月息低，无需担保。一旦事主信以为真，对方即以预付利息、保证金等名义实施诈骗。

32. 收藏诈骗。犯罪分子冒充各类收藏协会的名义，印制邀请函邮寄各地，称将举办拍卖会并留下联络方式。一旦事

主与其联系，则以预先交纳评估费、保证金、场地费等名义，要求受害人将钱转入指定帐户。

33. 机票改签诈骗。犯罪分子冒充航空公司客服以“航班取消、提供退票、改签服务”为由，诱骗购票人员多次进行汇款操作，实施连环诈骗。

34. 重金求子诈骗。犯罪分子谎称愿意出重金求子，引诱受害人上当，之后以诚意金、检查费等各种理由实施诈骗。

35. PS 图片实施诈骗。犯罪分子收集公职人员照片，使用电脑合成淫秽图片，并附上收款卡号邮寄给受害人，勒索钱财。

36. “猜猜我是谁”诈骗。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，一些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。

37. 冒充黑社会敲诈类诈骗。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，然后提供账号要求受害人汇款。

38. 提供考题诈骗。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。

39. 高薪招聘诈骗。犯罪分子通过群发信息，以月工资数

万元的高薪招聘某类专业人士为幌子，要求事主到指定地点面试，随后以培训费、服装费、保证金等名义实施诈骗。

40. 复制手机卡诈骗。犯罪分子群发信息，称可复制手机卡，监听手机通话信息，不少群众因个人需求主动联系嫌疑人，继而被对方以购买复制卡、预付款等名义骗走钱财。

41. 钓鱼网站诈骗。犯罪分子以银行网银升级为由，要求事主登陆假冒银行的钓鱼网站，进而获取事主银行账户、网银密码及手机交易码等信息实施诈骗。

42. 解除分期付款诈骗。犯罪分子通过专门渠道购买购物网站的买家信息，再冒充购物网站的工作人员，声称“由于银行系统错误原因，买家一次性付款变成了分期付款，每个月都得支付相同费用”，之后再冒充银行工作人员诱骗受害人到 ATM 机前办理解除分期付款手续，实则实施资金转账。

43. 订票诈骗。犯罪分子利用门户网站、旅游网站、百度搜索引擎等投放广告，制作虚假的网上订票公司网页，发布订购机票、火车票等虚假信息，以较低票价引诱受害人上当。随后，再以“身份信息不全”、“账号被冻”、“订票不成功”等理由要求事主再次汇款，从而实施诈骗。

44. ATM 机告示诈骗。犯罪分子预先堵塞 ATM 机出卡口，并在 ATM 机上粘贴虚假服务热线告示，诱使银行卡用户在卡“被吞”后与其联系，套取密码，待用户离开后到 ATM 机取出银行卡，盗取用户卡内现金。

45. 伪基站诈骗。犯罪分子利用伪基站向广大群众发送网银升级、10086 移动商城兑换现金的虚假链接，一旦受害

人点击后便在其手机上植入获取银行账号、密码和手机号的木马，从而进一步实施犯罪。

46. 金融交易诈骗。犯罪分子以某某证券公司名义通过互联网、电话、短信等方式散布虚假个股内幕信息及走势，获取事主信任后，又引导其在自身的搭建虚假交易平台上购买期货、现货，从而骗取事主资金。

47. 兑换积分诈骗。犯罪分子拨打电话谎称受害人手机积分可以兑换智能手机，如果受害人同意兑换，对方就以补足差价等理由要求先汇款到指定帐户；或者发短信提醒受害人信用卡积分可以兑换现金等，如果受害人按照提供的网址输入银行卡号、密码等信息后，银行账户的资金即被转走。

48. 二维码诈骗。犯罪分子以降价、奖励为诱饵，要求受害人扫描二维码加入会员，实则附带木马病毒。一旦扫描安装，木马就会盗取受害人的银行账号、密码等个人隐私信息。

理财知识

一、理财的概念

理财就是学会合理地处理和运用钱财，有效地安排个人或家庭支出，在满足正常生活所需的前提下，进行正确的金融投资，购买适合自己的各种金融产品，最大限度地实现资产的保值和增值。

二、常见银行个人理财工具

（一）银行储蓄

银行储蓄包括活期储蓄存款、整存整取定期储蓄存款、零存整取定期储蓄存款、通知存款、教育储蓄存款。

（二）商业银行理财产品

商业银行理财产品是指商业银行将本行开发设计的理财产品向个人消费者和机构消费者宣传推介、销售、办理申购、赎回等行为。商业银行个人理财产品分为保证收益理财计划和非保证收益理财计划两大类。每种理财计划根据收益和风险的不同又可以分为固定收益理财计划、保本浮动收益理财计划和非保本浮动收益理财计划。

（三）国债

国债俗称“金边债券”，由国家财政信誉担保，信誉度非常高，其安全性（信用风险）等级是所有理财工具中最高的，而收益性因其安全性高而有所降低。

（四）基金

基金有广义和狭义之分，从广义上说，基金是指为了某种目的而设立的具有一定数量的资金。例如，信托投资基金、公积金、保险基金、退休基金、各种基金会的基金。狭义的基金一般是指证券投资基金，即通过发行基金份额，集中消费者的资金，由基金托管人托管，由基金管理人管理和运用资金，是一种利益共存、风险共担的集合证券投资方式。

证券投资基金按基金单位是否可增加、赎回，分为开放式基金和封闭式基金；根据组织方式不同，分为契约型基金和公司型基金；根据投资目标不同，分为成长型基金、收入型基金、平衡型基金；根据投资对象的不同，分为股票型基金、债券型基金、货币型基金、指数型基金、黄金基金、衍生证券基金。

开放式基金和封闭式基金共同构成了基金的两种基本运作方式。开放式基金是指基金规模不固定，基金发起人可根据市场供求情况发行新份额，基金持有人也可根据市场状况和自身投资决策增加认购份额或赎回基金份额的投资基金。封闭式基金是指基金规模在发行前已确定，在发行完毕后和规定的期限内，基金规模固定不变的投资基金。

开放式基金是我国比较流行的由专家帮助理财的一种集合投资理财产品。开放式基金也是世界各国基金运作的基本形式之一，已成为国际基金市场的主流品种。

三、家庭理财规划

（一）如何进行家庭理财

家庭理财是关于如何计划家庭收支、如何管理家庭财富的学问。正确的理财，可以避免无谓的浪费，增加家庭财富，储备家庭财力，过上更加富裕的生活。

家庭理财包括开源和节流两个方面。开源指增加收入和让家庭现有资产增值，节流指节省支出与合理调节家庭消费结构，通过长期合理的家庭财政安排，实现家庭成员所希望达到的理想经济目标。

（二）制订家庭理财规划

理财做得好，首先要有全盘规划。家庭理财规划是指在全面考察收支状况、家庭资产财务情况后，根据家庭理财目标和个人的实际情况，灵活制订合理的家庭投资理财方案。

每个家庭或个人都应有自身的资产负债表并定期跟踪（可参考下表），对影响家庭资产负债表扩张（收缩）或内部结构变化的重大事项（如购房、买车）要予以足够的重视。通过与资产负债表相关的三个主要指标即流动性比率、负债收入比和资产负债率可以监测自身的财务健康状况。

（三）养老理财规划

在我国现行养老保障体系下，我国退休人员的养老待遇主要依赖“第一支柱”基本养老保险，由企业自主建立的“第二支柱”企业年金和职业年金，对参保职工的养老保障作用

相对有限；但值得期待的是，“第三支柱”个人养老金¹政策全面推出后，个人客户可享受政府税收优惠，自主选择银行、保险、基金等各类专属养老产品和服务，满足养老保障需求，做好适合生命周期的养老金融储备，改善家庭资产配置。

现阶段，基本养老金替代率处于较低水平，为保障退休生活质量，越来越多人选择银行理财产品作为稳健、可靠的养老投资渠道。

银行发行的养老理财产品主要有以下几个特征：一是投资期限较长，没有流动性设计；二是投资金额总量较大，部分产品为累积型，鼓励客户长期持有；三是追逐长期收益，根据客户的年龄结构设计差异化的风险投资策略；四是针对老年人需求，部分银行推出综合性养老理财业务，提供个性化的增值服务。

四、给消费者的知情提示

（一）给商业银行理财产品消费者的知情提示

消费者应当认真评估自身风险承受能力，理性购买适合自己的产品。消费者要认真阅读理财条款特别是除外责任、费用等信息，认真判断后再确定购买与否，并签名确认。

非保证收益理财计划不等同于一般存款产品，其涉及的主要风险有：

1、认购风险：如出现市场剧烈波动、相关法规政策变化

¹2018年，财政部、银保监会等五部委联合发布《关于开展个人税收递延型商业养老保险试点的通知》（财税〔2018〕22号），“第三支柱”个人养老金启动保险业试点。

或其他可能影响理财产品正常运作的风险。

2、政策风险：如国家政策和相关法律法规发生变化，可能影响理财产品的认购、投资运作、清算等业务的正常进行，导致理财产品理财收益降低，甚至导致本金损失。

3、市场风险：理财产品可能会涉及利率风险等多种市场风险。

4、流动性风险：如出现约定的停止赎回情形或顺延产品期限的情形，可能导致消费者需要资金时不能按需变现。

5、信息传递风险：如消费者在认购产品时登记的有效联系方式发生变更且未及时告知，或因消费者其他原因导致无法及时联系消费者，可能会影响消费者的投资决策。

6、募集失败风险：产品认购结束后，商业银行有权根据市场情况和《协议》约定的情况确定理财产品是否起息。

7、再投资提前终止风险：商业银行可能于提前终止日视市场情况，或在投资期限内根据约定提前终止本理财产品。

8、不可抗力风险：因自然灾害、社会动乱、战争、罢工等不可抗力因素，可能导致理财产品认购失败、交易中断、资金清算延误等。

（二）给基金消费者的知情提示

1、基金是一种长期投资工具，其主要功能是分散投资，降低投资单一证券所带来的个别风险。基金不同于银行储蓄和债券等能够提供固定收益预期的金融工具，投资人购买基

金，既可能按其持有份额分享基金投资所产生的收益，也有可能承担基金投资所带来的损失。

2、基金在投资运作过程中可能面临各种风险，既包括市场风险，也包括基金自身的管理风险、技术风险与合规风险等。巨额赎回风险是开放式基金所特有的一种风险，即当单个交易日基金的净赎回申请超过基金总份额的百分之十时，投资人将可能无法及时赎回其持有的全部基金份额。

3、消费者应当充分了解基金定期投资和零存整取等储蓄存款的区别。定期定额投资是引导消费者进行长期投资、分摊投资成本的一种简单易行的投资方式，但并不能规避基金投资所固有的风险，消费者既可获得收益，也可能遭受损失。购买基金不是替代储蓄的等效理财方式。

4、代销银行和基金管理人承诺基金份额持有人利益优先，以诚实守信、勤勉尽责的原则管理和运用基金资产，但不保证旗下基金一定盈利，也不保证最低收益。旗下基金的过往业绩及其净值高低并不预示其未来业绩表现。基金管理人应提醒消费者基金投资的“买者自负”原则，在作出投资决策后，基金运营状况与基金净值变化引致的投资风险，由消费者自行承担。

5、银行作为基金的代理销售机构，其受理交易委托的处理结果以注册登记机构的确认结果为准，银行不承担确保交易成功的责任，对产品的业绩不承担任何担保或保证责任。

6、银行从业人员应对消费者的风险承受能力进行调查和评价，并根据其风险承受能力推介相应的基金品种，但所做的推介仅供消费者参考。消费者在投资基金前应认真阅读《基金合同》、《招募说明书》等基金法律文件，根据自身风险承受能力选择相适应的基金产品并自行承担投资基金的风险。

（三）给保险消费者的知情提示

1、银行代理销售银保产品是一种基于代理关系的行为，银行不承担由此产生的保险人、投保人、被保险人和受益人等保险合同相关人之间涉及的法律风险。

2、银保产品消费者在购买银保产品时要仔细了解产品属性，特别是投资类保险产品的收益和风险，内容主要包括：保险产品的缴费期限、犹豫期规定、保险责任和除外责任、保单现金价值、保单初始费、账户管理费等相关费用标准及收取方式、犹豫期后退保可能遭受的保险金的损失，满期给付的注意事项等。

3、代理银保产品的从业人员应认真对购买某些银保产品的消费者进行风险承受能力调查和评价，并根据消费者的风险承受能力推荐相应的保险品种，但所做的推荐仅供消费者参考。消费者应根据自身风险承受能力选择保险产品并自行承担相应的投资风险。

4、银保产品消费者购买一年期以上的人身保险产品，保

险公司会在犹豫期内对消费者进行投保回访，进一步了解消费者的购买意愿，消费者应当利用这一时机再次确认产品相关属性是否符合自身要求，防止销售人员误导销售或错误销售。如果在犹豫期内退保，保险公司将全额退还所交保费

5、银保产品不能简单等同于“存款”、“储蓄”等，产品收益率具有不确定性。分红险的历史分红率不代表未来分红率，各年分红率可能波动较大；万能险只能保证结算利率高于保底利率，具体结算利率会定期调整；投连险更是与基金类似，没有所谓的保底收益率。

6、选择期缴产品的消费者，要注意自身收入情况是否与后续缴费时间与金额匹配，否则到时不能按时足额缴费，可能会出现保单失效或者退保损失等情况。一般建议收入持续稳定的消费者购买期缴保险产品。

7、对涉及投保、缴费、保险单变更、保险单迁移、账户变更、退保、保险金额领取等情院，应由保险合同当事人亲自签字的，银保产品销售人员不得代为签字。对按有关规定必须由保应面问当事人亲自抄录有关声明的，银保产品销售人员也不得代为抄录。

8、对于涉及保险合同的有关纠纷，银保产品消费者最好直接与保险公司协商处理，也可以请代理银行代为联系保险公司协商处理。

五、树立理财风险防范意识

（一）了解产品

消费者在购买理财产品时，应仔细阅读理财产品说明书、合同条款等信息，充分理解理财产品的各项要素，重点关注产品期限、投资方向或挂钩标的、流动性、预期收益率、产品风险等。

（二）了解自己及家庭

消费者在选购理财产品前，应综合权衡自己的财务状况、风险偏好、风险承受能力和预期收入、流动性需求等，不盲听、盲信、盲从，不追逐“热门”产品。在购买理财产品前，应配合银行人员认真完成风险评估内容，并综合考虑评估结果，产品特性和个人情况选择产品。

一是做金钱的主人。树立钱是为人服务的观念，积累财富的目的是为了让家庭拥有更加美好的生活。

二是改变“资金少就无法投资”的观念。不管家庭财力的情况如何，都应根据自身资产管理和养老储备需求，选择合适的金融产品。

三是学会对大宗财富支出进行规划。对家庭的大额消费进行合理计划，可以优化家庭支出的结构。

四是学会投资，让钱生钱。财富是有时间价值的，如果我们不会进行有效的金融投资，现金资产就会被通货膨胀所侵蚀，所以家庭生活需要理财，要学会让家庭财富保值增值，发挥专业产品抵御通胀、产品久期、市场化投资保障能力。

五是善于控制投资风险，避免重大的家庭财产损失。

六是要有风险责任意识。投资必定有风险，特别是股票、期货等投资工具，高收益必定有高风险，消费者要有风险自担的意识，对自己的行为负责，善于积累分析投资成功与失败的经验教训。

（三）确定选择

消费者可以从购买行为中获得利益，同时也要为自己的购买行为负责，承担相应的风险。消费者要在充分理解理财产品风险的前提下，在风险揭示书上对风险评估结果签字确认并亲笔抄录：“本人已经阅读风险揭示，愿意承担投资风险”。在确定购买理财产品后，需签署相关协议，一旦签字认可，消费者即须根据合同内容履行买者责任。

（四）跟踪变动

在理财产品存续期内，消费者应持续关注理财产品的投资运作与收益表现，通过致电咨询或向消费者经理了解等多种方式掌握相关的产品信息，以便能够及时了解产品的收益、风险等状况。

（五）关注账户

理财产品到期后，消费者应及时关注投资本金和收益是否按照合同约定返还至理财账户，以便能够及时进行新的投资。

六、资管新规介绍

2018年4月27日，人民银行、银保监会、证监会、外管理联合印发了《关于规范金融机构资产管理业务的指导意见》（以下简称《资管新规》）；2018年9月28日，中国银保监会正式颁布《商业银行理财业务监督管理办法》（以下简称《理财办法》）；2018年12月2日，中国银保监会正式颁布《商业银行理财子公司管理办法》。这些政策对老百姓和企业购买银行理财都产生了重要的影响。

近年来，我国金融机构资管业务快速发展，规模不断攀升，截至2017年末，不考虑交叉持有因素，总规模已达百亿元。资管业务在满足居民财富管理需求、增强金融机构盈利能力、优化社会融资结构、支持实体经济等方面发挥了积极作用。但由于同类资管业务的监管标准不一致，导致了一些隐性的风险和监管真空，一定程度上干扰了宏观调控，提高了社会融资成本，影响了金融服务实体经济的质效，加剧了风险的跨行业、跨市场传递。在党中央、国务院的领导下，中国人民银行会同中国银行保险监督管理委员会、中国证券监督管理委员会、国家外汇管理局等部门，坚持问题导向，从弥补监管短板、提高监管有效性入手、在充分立足各行业金融机构资管业务开展情况和监管实践的基础上，制定了资管新规。并在后期陆续出台配套制度文件。

资管新政的整体思路是：按照资管产品的类型制定统一的监管标准，对同类资管业务作出一致性的规定，实行公平

的市场准入和监管，最大程度地消除监管套利空间，为资管业务健康发展创造良好的制度环境。资管新政的基本原则是：一是坚持严控风险的底线思维，减少存量风险，严防增量风险；二是坚持服务实体经济的根本目标；三是坚持宏观审慎管理与微观审慎监管相结合、机构监管与功能监管相结合的监管理念；四是坚持有的放矢的问题导向；五是坚持积极稳妥审慎推进。

《资管新规》和《理财办法》的适用范围：

《资管新规》主要适用于金融机构的资管业务，即银行、信托、证券、基金、期货、保险资管机构、金融资产投资公司等金融机构接受消费者委托，对受托的消费者财产进行投资和管理的金融服务。私募投资基金产品也应参照执行。

《理财办法》适用业务和产品：《理财办法》与《资管新规》保持一致，定位于规范银行非保本型理财产品。理财办法所称理财业务是指商业银行接受消费者委托，按照与消费者事先约定的投资策略、风险承担和收益分配方式，对受托的消费者财产进行投资和管理的金融服务；理财产品是指商业银行按照约定条件和实际投资收益情况向消费者支付收益、不保证本金支付和收益水平的非保本理财产品。

《理财办法》适用机构：《理财办法》适用于在中华人民共和国境内设立的商业银行，包括中资商业银行、外商独资银行、中外合资银行；其他银行业金融机构开展理财业务，

适用理财办法规定；外国银行分行开展理财业务，参照理财办法执行。

根据资管新规要求，金融机构不得开展表内资产管理业务。保本理财作为表内资产管理业务的一种形式，将在过渡期内逐步退出市场。

追求保本的低风险偏好消费者可以选择存款产品。理财办法规定保本型理财产品按照结构性存款或者其他存款进行规范管理。同时，在附则中承接并进一步明确现行监管制度中关于结构性存款的相关要求，包括：将结构性存款纳入隐含表内核算，按照存款管理，相应纳入存款准备金和存款保险保费的缴纳范围，相关资产应按规定计提资本和拨备；银行销售结构性存款应执行《商业银行理财业务监督管理办法》及附件关于产品销售的相关规定，充分信息披露、揭示风险，保护消费者合法权益；银行开展结构性存款业务，需具备相应的衍生品交易业务资格等。

什么是净值型理财产品？

净值型理财产品是指以份额和每份净值形式展示的非保本浮动收益型理财产品。净值型理财产品不设预期收益率，消费者的实际收益与产品实际投资运作的净值有关，并通过产品净值增长或产品份额增加的方式体现。

净值型理财具备信息透明、定价公允、收益风险匹配的特点。

（一）信息透明：根据监管要求，净值型产品须定期公告及披露信息，消费者可以完整的了解到净值型理财产品的募集信息、资金投向、杠杆水平、估值情况、收益分配方式、托管安排、投资账户信息和主要投资风险等内容。不同净值型产品披露的信息有所不同，有利于消费者做出符合风险偏好的投资决策。

（二）定价公允：除产品说明书中约定的费用外，净值型产品的投资收益均通过净值增长的形式分配给消费者。

（三）收益风险匹配：通过净值化管理，将资产收益、风险、市值的波动传通过产品传导给消费者，真正做到“卖者尽责，买者自负”。

七、购买银行理财产品的注意事项

（一）首次购买理财产品前，需到银行营业机构进行风险承受能力评估，了解自身的风险等级。根据自身的风险等级、投资目的、流动性需求，阅读相关银行理财产品销售文件，了解理财产品的购买流程、产品风险、产品投向等后选择适合的理财产品。

（二）做好销售录音录像。在营业网点购买理财产品时，要对销售过程全程同步录音录像，要完整客观地记录销售人员对产品的营销推介、风险承受能力调查、产品适合度评估、风险揭示、产品收费信息和关键信息提示，以及消费者的确认和反馈等重点销售环节，特别是消费者对

银行销售人员提示内容明确表示“清楚明白或同意”的确认过程。

为什么在银行营业场所购买银行理财产品要进行录音录像？

2017年8月23日，中国银行保险监督管理委员会颁布《银行业金融机构销售专区录音录像管理暂行规定》，要求商业银行在营业场所销售自有理财产品的，要对销售过程进行同步录音录像。完整客观地记录营销推介、相关风险和关键信息提示、消费者确认和反馈等重点销售环节。

支付安全

一、银行卡（账户）安全防范

（一）借记卡种类

现有借记卡从物理结构上来讲，基本上分为三大类：

A. 磁条卡：利用磁性载体记录字符与数字信息，磁条卡容易被消磁无法使用且信息容易被复制，安全性较低，社会上层出不穷的盗刷事件，基本都与磁条卡信息被复制有关。

B. 芯片卡：也称金融 IC 卡，以芯片作为介质的银行卡。芯片卡具有安全性高、存储信息大、智能动态验证多项技术优势，截至目前全球尚未出现 IC 芯片卡被攻破的案例。

C. 磁条芯片复合卡：既有磁条又有芯片。当客户使用芯片进行交易时，它的安全性等同于芯片卡，可以有效保障账户资金安全。

2017 年 5 月 1 日，国内关闭了磁条芯片复合卡的磁条交易功能，综合考虑，为了资金安全，顺应时代趋势，建议及早将磁条卡升级为芯片卡。

（二）银行卡（账户）申请

2016 年，中国人民银行研究制定了《关于加强支付结算管理 防范电信网络新型违法犯罪有关事项的通知》（银发〔2016〕261 号，以下简称《通知》）。《通知》规定：“同一个人同一家银行（以法人为单位）只能开立一个 I 类户，已开

立 I 类户，再新开户的，应当开立 II 类户或 III 类户。”

为降低个人资料被盗用风险，建议尽量亲自到营业网点办理银行卡（账户）开立手续，不要委托他人或非法中介机构代办。银行未委托任何中介机构代理银行卡（账户）申请业务。

提供个人身份证件复印件申办银行卡（账户）时，可在复印件上注明使用用途，例如：“谨供申办银行卡（账户）用”，以防身份证件复印件被移作他用。

申请办理银行卡（账户）时，应如实填写个人真实资料，务必留存您本人的手机号码或常用电话号码。手机号码等个人资料发生变更时，务必及时通知银行修改，避免使用过期手机号或与他人共用手机号作为联系方式。

（三）银行卡（账户）保管

请勿随手放置银行卡（账户），公共场合不要将银行卡（账户）放在易丢失、易失窃的地方。同时，银行卡（账户）作为您接触账户资金的工具，仅限本人使用，请勿将您的银行卡（账户）出租、出售、出借给他人使用。

此外，请将您的银行卡（账户）与身份证件分开存放，以免因无法及时办理挂失、补卡等业务而造成不必要的经济损失。

如果银行卡（账户）遗失、被盗或发现被冒用时，请您及时拨打银行客户服务热线办理银行卡（账户）挂失，并注

意留存相关非本人交易证据。

（四）银行卡（账户）信息保护

银行卡（账户）因破损、到期等原因补发新卡时，请将旧的银行卡（账户）的磁条（或芯片）销毁。同时，建议您将不常用的账户撤并，及时到银行网点办理销户等。

由于消费签购单等纸质单据包含卡号等敏感信息，请您务必妥善保管或及时销毁，切勿随意丢弃。

不要将卡号、证件号、姓名、手机号、短信动态验证码、有效期、交易（查询）密码等敏感信息告知他人、中介或在公共电脑上留存上述敏感信息，也不要回复要求提供上述敏感信息的可疑邮件或短信。在任何情况下，银行工作人员都不会直接索取或发送索取短信动态验证码、交易（查询）密码的邮件或短信。如果您收到此类信息，请拨打银行客户服务热线予以核实。

建议您及时开通交易短信提示，定期关注账户资金变动情况，如果发现不明交易，请立即联系银行客户服务热线或至银行营业网点咨询详情。

不要随意在网络留下包含自己银行卡（账户）号、证件号、姓名、手机号等敏感信息的资料，以防信息泄露。

不要随便在街头扫描二维码、填写问卷留下银行卡（账户）号、证件号、姓名、手机号等重要敏感信息。

不要在公共场合随便连接免费 Wi-Fi，不要在 Wi-Fi 登

录页面中输入关于银行卡（账户）号、证件号、姓名、手机号等信息。

（五）银行卡（账户）使用

一旦银行卡（账户）失窃或有异常情况，请尽快与银行联系。如遇资金盗用，请立即向公安机关报案处理。

建议根据自身需要设置和控制银行卡账户资金使用风险，通过电话、网上银行、及营业网点调低 ATM 或 POS 使用限额，如遇有大额交易需求时，可通过柜台或网上银行调高交易限额。

在银行卡（账户）使用过程中，您可以通过银行营业网点、ATM、网上银行等随时修改密码。

建议您分别持有银行一类户银行卡（账户）和二类户银行卡（账户），并绑定使用。一类户银行卡（账户）作为主要结算账户，用于大额投资理财等用途，尽量少用于 ATM 取款、POS 消费等生活场景。同时，二类户银行卡（账户）则主要作为日常生活中小额消费、取款等用途使用。

POS 机刷卡时，请不要让银行卡（账户）离开您的视线范围，输入密码时请注意遮蔽键盘。

使用 ATM 时，请留意插卡口是否有改装痕迹，键盘上方是否有摄像头等隐蔽设备；ATM 出现吞卡等故障时，不要轻易离开，可在原地拨打 ATM 屏幕上显示的服务电话或直接拨打银行客户服务热线咨询，请勿轻信 ATM 周边粘贴的纸质“通

知”及“通知”上的电话。

操作 ATM 时，避免被他人转移注意力，调换银行卡（账户）或窥探密码。交易结束后应及时取回银行卡（账户）和现金。

如果您在持卡消费或取现时经常出现不正常的情况，建议您及时联系银行检查银行卡（账户）。

（六）银行卡（账户）被盗用

如发现银行卡（账户）被盗用，应第一时间致电银行客户服务热线，紧急挂失，防止资金损失扩大。同时，就近前往银行网点，出示身份证件及银行卡（账户），确认银行卡（账户）仍由本人持有且交易非本人操作。如遇夜间，可就近前往银行 ATM 机具，错误输入密码锁定银行卡（账户）。客户应及时向公安机关报案，并前往银行网点提交公安机关出具的报案回执、身份证件复印件、银行卡（账户）正反面复印件等，并当场填写否认交易声明。银行在获取上述信息后，将协助客户开展调查，尽最大可能挽回资金损失。

（七）合法合规安全用卡

根据监管有关规定及银行卡（账户）章程和领用协议相关条款，银行卡（账户）仅限本人用，不得出租、出售、出借银行卡（账户）。买卖银行卡（账户）属于违规行为。同时，买卖银行卡（账户）行为过程中可能会伴随着非法持有大量银行卡（账户）、买卖居民身份证等违法行为，涉嫌违法犯罪。

非法买卖银行卡（账户）具有极高风险。一方面，非法买卖的银行卡（账户）、身份证等可能被用于洗钱、逃税、诈骗、送礼和开店刷信用等行为，扰乱了正常的社会秩序。另一方面，银行卡（账户）内存储了很多个人信息，如果贪图小利出售自己名下的银行卡（账户），有可能被收卡人用来从事非法活动，给自己带来巨大的法律风险，甚至承担刑事责任。一旦所售银行卡（账户）出现信用问题，还可能导致个人信用受损，甚至承担连带责任。

二、密码安全防范

1、密码设置

设置易于记忆但难以破译的密码。请勿设置简单数字排列的密码或用生日、证件号码、电话号码等作为密码，防止被不法分子试出。

切勿将银行卡（账户）登录密码、取款密码和支付密码与其它网站或网上商户使用的各类注册密码设置相同，避免因其它网站注册密码泄漏而导致银行卡所有密码同时失窃。

若您的银行卡（账户）为单位批量办卡，领用后请及时激活设置密码。

2、密码保管

不要将密码写在或保存在任何可能让他人看到或得到的地方。不要将密码存放在手机里，更不要写在银行卡（账户）背面。请勿将密码与银行卡（账户）放在一起保管。

密码作为身份识别的最终依据，应当确保只有本人知悉。若怀疑密码发生泄漏风险，请及时通过银行营业网点、ATM、网上银行和电话银行等渠道修改密码。

请不要向任何人透露您的密码。银行、公安机关、司法机关都不会索要您的密码。

建议不定期修改银行卡（账户）密码。特别是密码使用时间较长或境外出行归来的，应及时修改交易密码。

三、ATM 交易安全防范

1、ATM 交易前

刷卡进入自助银行的门禁无需输入密码。

首先保证您自身安全。留意周围环境是否安全。如果有人离您太近，并且举止可疑，请改用其他 ATM 或终止操作。进入 ATM 隔间后应及时上锁。

检查 ATM。如果发现 ATM 上有多余的装置或摄像头，或者插卡口或出钞口有异常情况或有被改造的痕迹，请更换其他 ATM 操作或至银行营业网点办理业务。

若您不会使用 ATM 操作，您可联系银行客户服务热线进行咨询，切记不要按照他人提示的步骤完成取款操作，谨防诈骗。

2、ATM 交易时

专心操作，不要接受陌生人的“善意”帮助或其他人的询问。被他人引开注意力时，应用手捂住插卡口和出钞口，

防范欺诈分子将卡、现金等调包。

输入密码时，应尽量快速并用身体遮挡操作手势，以防不法分子窥视。

如果 ATM 出现吞卡或不吐钞故障，不要轻易离开，可在原地拨打 ATM 屏幕上显示的银行服务电话或直接拨打银行客户服务热线，请勿轻信 ATM 周边粘贴的纸质“通知”及“通知”上的电话。

3、ATM 交易后

离开 ATM 前，请确认取走您的银行卡（账户）和现金。

请确认取出的银行卡（账户）是否是您本人的银行卡（账户）。

选择打印 ATM 交易单据后，请勿随手丢弃，应妥善保管或及时销毁单据。

四、POS 交易安全防范

1、POS 交易前

申领到银行卡（账户）时，务必在卡背面签名条上签名，并按上述提示，妥善设置并保管密码。

建议您使用 IC 卡。IC 卡又称之为芯片卡，是通过可运算的芯片和存储在其中的密钥，确保终端与银行卡（账户）的交互过程中安全真实，而且能保证联机交易信息的安全，难以复制，安全性高于磁条卡。

2、POS 交易时

刷卡消费时，切勿让银行卡（账户）离开视线范围，并留意收银员的刷卡次数。

输入密码时，应尽可能用身体或另一只手遮挡操作手势，以防不法分子窥视。

尽量不在不正规场所使用银行卡（账户）。

3、POS 交易后

收银员交回签购单及银行卡（账户）后，您应认真核对签购单上的交易日期、金额等是否正确，银行卡（账户）是否为本人的银行卡（账户），不要在非本人交易或交易信息有误的签购单上签名。

刷卡消费时若发生异常情况，要妥善保管交易单据，如发生卡重复扣款等现象，可凭交易单据及时与银行联系。

及时核对用卡情况，如有疑问，请及时联系银行营业网点或拨打银行客户服务热线进行查询。

签购单因错误需重写时，请您要求收银员将原签购单全部撕毁。

若需当场取消交易，或遇收银员重复操作交易，请您要求收银员当场撤销交易，恢复您的银行卡（账户）账户余额。

五、网络交易安全防范

（一）常见的网络支付方式

1. 网上支付：指单位或个人通过电子终端，直接或间接向银行业金融机构发出支付指令、实现货币支付与资金转移

的行为。根据支付指令发起渠道可分为网上支付、电话支付、手机支付等。网上支付是由客户通过在商户端选购商品确认订单后点击支付，跳转银行支付页面的一种支付类型。支持信用卡首次支付免签约服务，客户可选择任何一种支付方式进行支付。包括：银行卡直接支付、网银专业版支付、手机 PUSH 支付、手机 WAP 支付。

2. 快捷支付：是指用户通过电话或者网站等方式订购商品时，不需开通网银，只需提供卡号、手机号码等信息，银行验证客户信息及手机号码正确后，即可完成支付。商户可以选择是否向验证通过的手机号码中发送手机动态口令。目前很多支付工具中用户可以自行设置小额免密额度，使得多频、小额的支付场景更加方便、快捷。

（二）网络欺诈主要风险

1、网络钓鱼是指不法分子通过大量发送冒用来自于银行或其他知名机构的欺诈性垃圾邮件或短信、即时通讯信息等，引诱收信人给出敏感信息（如银行卡号、密码、证件号、手机号、短信验证码等详细信息）的一种攻击方式，然后利用这些信息假冒受害者进行欺诈交易，从而盗用银行卡（账户）账户资金。如不法分子伪冒与银行官方网站非常相似的钓鱼网站，诱使用户输入个人敏感信息。

2、木马病毒是一种基于远程控制的黑客工具，它通常会伪装成程序包、压缩文件、图片、视频等形式，通过网页、

邮件等渠道引诱用户下载安装，如果用户打开了此类木马程序，用户的电脑或手机等电子设备便会被不法分子控制，从而造成信息文件被修改或窃取、银行卡（账户）资金被盗用等危害。

3、社交陷阱是指不法分子利用传销、招聘等社会工程学手段，获取用户个人信息，并通过获取的重要信息盗用用户银行卡（账户）账户资金的网络诈骗方式。例如骗子公司在网上发布招聘信息，利用各种名义收取报名费、介绍费、押金、中介费等不合理收费的欺诈行为。

4、伪基站一般由主机和笔记本电脑组成，不法分子通过伪基站能搜取设备周围一定范围内的手机卡信息，并通过伪装成运营商的基站，冒充任意的手机号码强行向用户手机发送诈骗、广告推销等短信息，通常保护钓鱼链接，诱使客户点击下载病毒。例如用户收到的冒用银行客服热线以“手机银行升级或提升信用卡额度”等为由的诈骗信息。

5、由于部分中小网站安全防护能力较弱，容易遭到黑客攻击，该网站注册用户的用户名和密码便因此泄露。如网站用户设置了与银行卡账户相同的用户名和密码，则极易发生银行卡（账户）账户资金盗用。

（三）网络交易安全防范提示

保护好密码及其他重要身份信息。重点关注密码，勿设置简单易猜测的密码；勿将银行账户密码与互联网邮箱、购

物平台、游戏账户等密码全部设置为同一密码；切勿转发短信验证码。

保护好手机和电脑等终端设备。安装杀毒软件，不点击不明链接；在安全的网络环境下使用手机银行和网上银行。

开通账户交易通知功能，及时发现异常情况。

六、移动支付风险防范

条码支付是以条码为信息载体，通过移动终端或商户受理终端直接或间接获取支付要素以完成交易的支付方式。常见的条码包括二维码、条形码等类型。在使用过程中要增强安全意识，做到：

不扫描来源不明的二维码

不轻易将个人二维码信息泄露给他人

不通过二维码支付进行大额交易

加强对手机等智能终端的安全管理

核对帐户名称与商家是否一致，与商家确认帐户名称是否正确后，再进行支付操作。如发现异常立刻停止支付。

七、案例集合

场景 1：ATM 取现案例

案例 1. 窥视密码，盗走卡片。客户在 ATM 机取现时，不法分子趁持卡人取款时，窥视密码，然后以询问、故意将钱丢在地上等手法，引开出卡人注意力，并趁机将预先准备好的卡片插入 ATM 机插卡口，造成卡片退出的假象，催促持卡

人取卡离开后，将持卡人的卡片退出盗走。

案例 2. 窃取密码，伪造卡片。不法分子在自助银行门禁系统上安装盗录设备及摄像头，待客户刷卡后，盗取磁条信息及密码后，制作伪卡。或者在 ATM 机上安装吞卡装置，或用望远镜窥视安装假密码键盘或在真密码键盘上贴薄膜等手法盗取密码，用微型摄像机偷窃卡号和密码或从持卡人随手丢弃的 ATM 取款凭条上获取相关信息，制作伪卡冒领存款。

案例 3. 造假信息，趁机盗取。不法分子在 ATM 机上安装吞卡装置，ATM 机旁张贴假的银行告示。引诱持卡人拨打告示上的虚假服务电话，并冒充银行工作人员套出持卡人的银行卡密码后，从 ATM 上盗取存款。或者在 ATM 机旁张贴假的银行公告，以“银行程序调试”等为由，要求持卡人将银行卡存款转账到指定账户，盗取卡上存款。

场景 2. POS 消费盗刷案例

案例 1. 刷 POS 机送礼品，银行卡遭异地盗刷。“刷一次 POS 机，消费 49.99 元，可获赠一袋大米和一桶豆油！”面对这样的促销宣传，一些市民信以为真，纷纷刷卡领取赠品。某客户信以为真，分别用银行卡刷了一次 POS 机，得到一张凭条，上面显示“划卡消费 49.99 元”，客户获赠了大米和豆油。然而，一场精心准备好的骗局正悄悄向他们逼近：手机短信一条条响起，显示他们的银行卡在异地被盗刷。

案例 2. 技术改造 POS 机，客户信息被窃取。客户王先生

收到短信，其银行卡突然被刷了近 30 万元！王先生说：“共收到五条消费短信，第一条 49800 元，第二条 98000 多元，后来三条也都是 4 万多。”银行发来的消费短信显示，王先生的银行卡在一家超市内，在不到五分钟的时间里分五次消费了总计 29 万多元。经警方破案，根据不法分子交代，其通过伪造工商证件等方式从一家网络科技有限公司购买 POS 机，并对这些 POS 机进行技术改装，改装后的 POS 机，不但具有盗取银行卡全部信息的功能，还可以把这些信息同步发送短信到移动设备。改装后的 POS 机，被犯罪嫌疑人以降低手续费等为诱饵，销售给餐饮、足浴店、酒店等商家，在全国布点盗取银行卡信息。

场景 3. 密码失窃案例

案例 1. 短信诈骗新花样。目前，短信欺诈出现了新花样，“商场消费”的假短信可能变为“中奖”、“退税”等假短信，诱骗持卡人在 ATM 机上进行“银行卡升级”或在网上银行设置“联网报警系统”。

案例 2. 钓鱼网站窃信息。不法分子在“网上钓鱼”，设立虚假金融机构网站，储户如果登录该网站操作其银行卡的卡号，密码就会被不法分子窃取。

案例 3. 活动链接频盗刷。居民张大爷的手机收到了一条“10086”发来的短信，当天中午，张大爷收到的“10086”的短信，内容为“尊敬的星级客户，您可享受话费赠送活动，

充值 100 元送 100 元，登录充值 <http://10086.com.co/m> 活动今日截止”。张大爷觉得既然是正规的公司短信不能有假，按照短信内容点击此链接到一网站，再按照网站的要求，依次将电话号码、银行卡号、密码输入网站后，张大爷在家中坐等“充值成功”的短信时，结果却收到了银行卡被刷 3000 元的提示短信。警方已接到此类多次报案，罪犯使用技术手段群发此类信息，只要你一登录对方网站，按照对方要求输入银行卡保密信息，即被犯罪分子乘机盗刷银行卡钱财。

案例 4. 网上购物要谨慎，支付信息勿泄露

骗子们通过网络改号软件冒充商户客服，谎称产品有质量问题并声称可以免费退款，要求添加您好友，诱骗您填写个人支付信息，如：短信验证码、信用卡有效期(四位数字)及 CVV2(安全验证码)等支付信息，然后盗刷您的信用卡。

九、安全小贴士集合

1、保障 ATM 操作安全，四要点

(1) 在 ATM 上查询、取款时，要留意周边环境，谨防密码被偷窥；

(2) 选择打印 ATM 交易单据后，要妥善保管或及时处理、销毁，不要将其随手丢弃；

(3) 操作 ATM 出现机器吞卡或不吐钞时，要原地直接拨打银行客户服务热线进行求助；

(4) 要认真识别银行公告，千万不要相信要求客户将钱

转到指定账户的公告。

2、保证刷卡消费安全，五步走

(1) 要在正规商户进行交易，刷卡消费时请勿让银行卡离开自己视线范围，要留意收银员的刷卡次数，避免误刷多刷；

(2) 在刷卡消费输入密码时，应尽可能用身体或另一只手遮挡操作手势；

(3) 签署签购单时，要仔细核对是否是本人的卡号、日期和金额，如发现有误，应要求收银员当面撕毁凭证并取消交易；

(4) 交易完成时，要确认收银员交还的是不是自己的银行卡，并保存好签购单，以便日后与对账单核对；

(5) 开通短信提醒服务，及时掌握账户动态信息，当账户发生异常变化后，要及时联系发卡银行查询交易，一旦发现被盗刷，应及时申请冻结账户和挂失卡片，避免损失扩大。

3、保证网上支付安全，七应该

(1) 网上交易前应确认网址是否正确，要选择信誉好、运营时间长的网站进行银行卡网上支付业务；

(2) 完成网上交易后，应及时退出，避免发生后续风险交易；

(3) 在进行境外网上交易时，应通过安全途径，开通相关认证服务；

(4) 应避免通过公用 WIFI 进行支付，不在网吧等公共场所进行网上交易，以免泄露账号及密码等信息；

(5) 应注意不要扫描来源不明的二维码、登录不明网站，避免被不法分子植入木马病毒。

(6) 办理网络购物、网络退货、退款时，应认清官方渠道，切勿轻信不明身份的电话、网络聊天工具或其它形式提供的非正规的网络链接；

(7) 收到可疑手机短信时，应谨慎确认，如有疑问应直接拨打银行客户服务热线查询。

4、发现信用卡被盗刷，四应对

(1) 一旦发现的信用卡被盗刷，请立即致电发卡银行官方客服电话报告异常交易，及时冻结账户或挂失卡片。

(2) 立即在就近的 ATM 或 POS 上进行一笔刷卡交易，证明卡片在您身上未丢失，如果卡片已经冻结或挂失，刷卡不会成功，通过 ATM 机交易时卡片可能会被吞卡，此情况为正常现象，请按 ATM 机所属银行的相关规定进行后续处理即可，无需惊慌。

(3) 立即向当地公安部门报案，积极配合公安机关开展调查，联系发卡银行办理异议交易申请及相关手续等。

(4) 如您的网银、电话银行、手机银行等设置的密码与被盗刷卡片密码相同，建议您尽快修改用户名和密码等，以防其它账户被盗。

5、安全用卡 12 条

(1) 芯片卡（金融 IC 卡）的安全性远高于磁条卡，因此首先建议您尽快将手中磁条卡升级为金融 IC 卡。

(2) 开通短信、微信提醒功能，可以第一时间发现账户收支详情。

(3) 使用卡片前，要在卡背面签好姓名，防止错拿与被不法分子调换

(4) 不得出售借记卡，也不要将卡片转借他人或将密码告知他人。

(5) 刷卡消费时，不要让卡片离开视线范围，使用密码交易时防止被他人偷窥。

(6) 不要设置较为简单的密码，如 112233、123456 等，更不要将密码存在手机中或卡背面，也不要将第三方密码作为借记卡密码。

(7) 不要使用公共 wifi 接入手机银行、网上银行等，使用完网银及时退出。

(8) 警惕钓鱼网站，对于有奖链接、不熟悉网友的链接等不明网址不要轻易登录。

(9) 取款存条不要随手丢弃，以防被不法分子获取个人相关信息。

(10) 不贪小便宜，警惕街边以及小摊刷卡。

(11) 刷卡消费后，一定要核实刷卡记录上的刷卡信息

与 POS 单上的商户信息是否相符。

(12) 如发现银行卡被盗刷，应第一时间报警，并与银行或第三方支付平台进行联系，及时冻结资金，最大限度保证资金安全。

内容参考：中国人民银行金融消费者权益保护局《金融知识普及读本》