如何让您的手机银行更安全？

1

请您务必从正规的渠道下载手机银行，并定期更新该类应用软件。

2

确保您的移动设备安全，建议使用手势密码或口令保护移动设备，并将设备设置为一段时间后自动锁定。切勿尝试破解或修改设备，因为这可能会使设备受到恶意软件的攻击。

3

若您使用Wi-Fi联网，请在确保无线网络安全的情况下再连接至您的手机银行站点或应用程序。

4

APP提供保存密码选项时，建议您不要勾选，每次登录要重新输入登录密码，同时建议设置较为复杂的登录密码、支付密码等。

5

若您更换了手机号码，请及时致电银行更改手机号。遇到手机被盗，请及时挂失手机号、冻结银行卡。

6

在使用交易类、银行类APP进行支付或者转账的过程中保证手机在本人手中，不要在操作过程中远离手机，如确有紧急事项，立即结束当前交易并退出APP。在操作完毕后及时结束APP进程，不要在后台继续运行。

扫码观看视频讲解

刷脸支付安全吗？

依据《金融科技（FinTech）发展规划（2019-2021年）》基于实体渠道的人脸识别支付应用使用相对封闭服务环境，通过金融网点、专用终端（具有安全芯片、加密模块等）等实体渠道，结合 3D 结构光 /TOF、近红外活体检测等技术，可有效防范隐私泄露和假体攻击，能够较好地保护用户信息及资金安全，风险基本可控。总的来看，基于个人移动终端的人脸识别支付应用仍存在诸多风险，尚不具备应用条件；基于实体渠道的人脸识别支付应用技术已成熟，具备应用条件。

声纹识别有哪些优势？

《移动金融基于声纹识别的安全应用技术规范》把声纹作为一种独立认证因子进行考量，明确了声纹注册、验证、变更、注销等环节的基本需求；提出了采样、抗噪音、防攻击、抗时变等技术要求；对声纹信息采集、传输、存储、处理、删除等全生命周期的安全进行了规范。

声纹识别优势

声音信号中含有语言信息、副语言信息和非语言信息，还具有“形简意丰”的特点，有利于识别用户真实意图，具有行为可追溯性，这可以让声纹识别技术发挥更多功能。

交易验证要素分为哪几类？

常见的交易验证要素分为以下几类：

1. 用户本人知悉要素，如静态密码等。静态密码由用户自行设置，使用便捷，广泛用于各类金融服务场景。

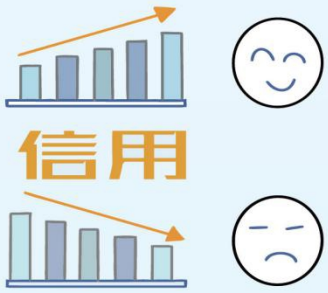
2. 用户本人持有并特有的不可复制或者不可重复利用的要素，如短信验证码、数字证书等。短信验证码具有信道独立、一次性使用、普及容易等特点，广泛用于快捷支付等领域。数字证书具有应用成熟度高、伪造难、安全性高等特点，具备法律效力，广泛用于网上银行、手机银行等场景。

3. 用户本人生物特征要素。生物识别借助于人体生理特征或行为特征进行身份识别，具有唯一性、不易丢失或遗忘等特点，逐步应用于金融领域。

信用报告里记录了什么？

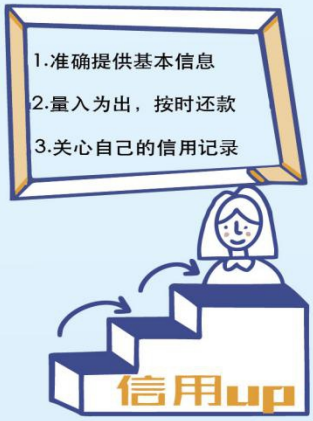
信用报告全面、真实记录您在银行借债还钱、遵守合同和遵纪守法情况，既有您按时还钱的记录，也有您未按时还钱或借钱未还的记录。根据中国人民银行征信中心发布信息，信用记录主要储存在人民银行征信系统中，并以信用报告的形式向本人提供查询。

信用报告有哪些作用？



信用报告广泛应用在商业银行贷款、信用卡审批和贷后管理中，还用于任职资格审查、员工录用等许多活动中。信用报告能够节省银行贷款时间，帮您快速获得贷款。如果信用良好，银行还可能会在贷款金额、利率上给予优惠。但如果您有逾期记录，银行在放贷时会更加慎重，不利于您获得贷款，并可能增加您的贷款成本。

如何维护个人良好的信用记录？



呵护信用要靠自己。日常生活中，主动与银行保持畅通的联系渠道，注意更新手机号码，准确提供自己的基本信息。量入为出，按时还款、避免出现逾期。如果已有逾期记录，应尽快还款，积极采取措施避免类似情况再次发生；如果逾期信息有误，应尽快提出申请，及时纠正。在个人征信报告中显示近五年个人征信情况。

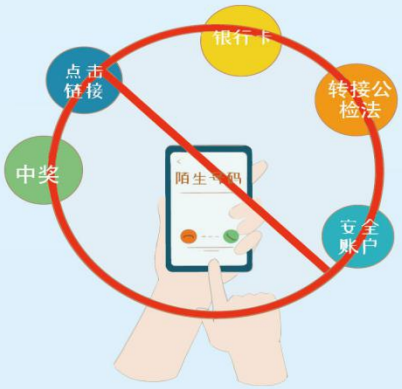
安 全 意 识 普 及

十个“凡是”识别电信诈骗

谨记十个“凡是”：
凡是自称公检法要求汇款的；
凡是叫你汇款到“安全账户”的；
凡是通知中奖、领取补贴要你先交钱的；
凡是通知“家属”出事先要汇款的；
凡是在电话中索要个人和银行卡信息的；
凡是叫你开通网银接受检查的；
凡是叫你宾馆开房接受检查的；
凡是叫你登录网站查看通缉令的；
凡是自称领导（老板）要求汇款的；
凡是陌生网站（链接）要登记银行卡信息的。
以上十个“凡是”，都是诈骗。

六个“一律”防范电信诈骗

只要一谈到银行卡，一律挂掉；
只要一谈到中奖了，一律挂掉；
只要一谈到“电话转接公检法”的，一律挂掉；
所有短信，让点击链接的，一律慎重；
微信不认识的人发来的链接，一律不点；
提到“安全账户”的，一律是诈骗。



保护好个人金融信息要牢记四个“不”

不 外 借

不将身份证、银行卡、网银U盾、手机等重要物件外借给他人。

不 乱 丢

不随意丢弃含有个人金融交易信息的凭条、银行卡和旧手机。

不 乱 晒

不将信用卡卡号、卡面上的3位或4位安全码、有效期等信息晒到朋友圈、微博等社交平台。

不 乱 点

不点击可疑链接，不扫来历不明的二维码，不在银行提供的官方渠道以外输入银行账号、密码，防止钓鱼网站窃取信息。

防范不法分子冒充公检法和银行人员骗取钱财

1. 办理电子银行签约后，应保管好电子银行用户名、密码、动态口令和手机交易码，切勿将上述信息告诉他人，包括银行员工；

2. 请不要轻信以任何名义和理由要求您办理电子银行或通过电子银行划转资金的来电或短信；

3. 不轻信任何陌生电话、短信、邮件等。