反洗钱宣传
金融网络安全

中国人民银行
THE PEOPLE'S BANK OF CHINA

中国商务出版社
CHINA COMMERCE AND TRADE PRESS

一、《网络安全法》相关的法律规定

2016年11月7日，第十二届全国人民代表大会常务委员会第二十四次会议审议通过了《中华人民共和国网络安全法》，自2017年6月1日起执行。

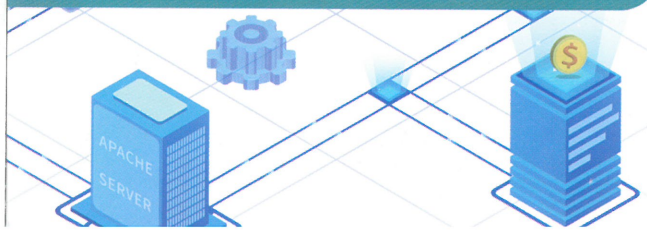
《网络安全法》第四十四条规定：任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

《网络安全法》第四十三条规定：个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。

《网络安全法》第十四条规定：任何个人和组织有权对危害网络安全的行为向网信、电信、公安等部门举报。收到举报的部门应当及时依法作出处理；不属于本部门职责的，应当及时移送有权处理的部门。有关部门应当对举报人的相关信息予以保密，保护举报人的合法权益。

《网络安全法》第四十七条规定：网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。

《网络安全法》第十三条规定：国家支持研究开发有利于未成年人健康成长的网络产品和服务，依法惩治利用网络从事危害未成年人身心健康的活动，为未成年人提供安全、健康的网络环境。



二、金融网络安全知识普及

如何安全使用手机银行?

01

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.

02

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。

03

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。

04

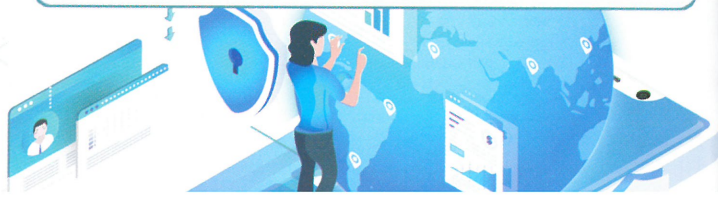
APP提供保存密码选项时，建议您不要勾选，每次登录要重新输入登录密码，同时建议设置较为复杂的登录密码、支付密码等。

05

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。

06

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。



如何保护好个人金融信息？

01 所有涉及资金的平台均设置复杂的登录及交易密码；

02 在使用聊天工具或社交平台时，注意与陌生人保持适当距离，不要轻易向他人透露年收入、财产状况等个人金融信息；

03 切记勿将自己的资金转移到所谓的“安全账户”；

04 提供个人身份证、户口薄等复印件办理业务时，在复印件上注明用途和日期，例如：“仅供办理XX业务使用”；

05 含有个人金融交易信息的凭条、个人信息的快递单、信用卡对账单及作废的金融业务单据等，应撕碎或用碎纸机销毁，不随意丢弃；

06 不要轻易在社交媒体上分享含个人敏感信息的照片，或随意暴露个人定位信息；

07 不要将身份证、银行卡、网银U盾、手机等重要物件外借给他人使用，务必本人办理金融业务，并保管好个人的账户、密码等信息；

08 不要轻信来历不明的电话或消息，在未核实对方身份前，切勿着急进行转账等操作；

09 不要轻易相信你不了解的法律政策，必要时，应咨询专业人员或查询政府机关等网站核实真伪；

10 不要在任何不明网页、公众号等渠道填写个人身份证或银行卡信息。

如何防范银行卡被盗刷

1、把磁条卡换成IC芯片卡。卡储存容量更高，应用拓展性更强，抗磁场干扰更强，数据保存年限更长，安全性也更高，卡片不易被复制。

2、及时确认账户资金变动信息。网上交易尽量捆绑小额度银行卡，并设置交易限额。

3、不要将各类验证码给任何人。包括确认付款、注册、修改信息等短信验证码，以及换卡用的USIM卡验证码。

4、警惕伪基站发送的假冒短信。不要盲目打开短信里的未知来源网址。

5、刷卡时，多留意细节。刷卡时勿让卡离开视线，使用ATM机时，要注意检查有无外接异物。

6、不扫描来历不明的二维码。防范恶意链接。

7、使用可信的Wi-Fi接入点。恶意Wi-Fi可瞬间盗取个人一切隐私，使用公共场所Wi-Fi，不进行账号信息输入交易。

8、安装防病毒软件。防病毒软件可以防御病毒攻击，还可以识别诈骗短信和电话。

9、谨慎使用短信同步功能。一旦关联的账号被窃取，可能存在信息泄露的风险。

10、妥善保管好各类密码。定期修改密码，将交易密码与其他密码区分开来。

遭遇金融诈骗怎么办？

如果还能登录账户：请立即修改支付口令和登录口令，同时转出剩余资金，查询交易明细，如有可疑交易须立即拨打金融机构客服电话。

如果还输入了银行卡信息：请立即致电金融机构申请临时冻结账户或电话挂失。

如果已经无法登录：请立即拨打金融机构的电话，申请对账户进行临时监管。对电脑进行全面杀毒，确认安全后重新修改登录和支付口令。

如何防范电信诈骗？

01 陌生短信不要回，不明链接不要点；

02 金融支付要注意，多留心眼防盗刷；

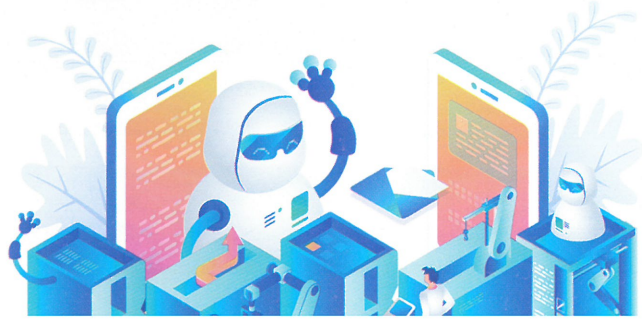
03 手机里千万别存身份证照片；

04 有人跟您借钱一定要电话核实；

05 短信验证码不要对任何人透露；

06 不要所有的账户都用一个密码；

07 高收益金融软件不要信，投资选正规途径。



三、精选案例

APP投资诈骗

案例：2020年10月14日，张某用手机打开浏览器时，看到一条广告上写着关于投资融资的信息，就点击网页进行查看。点进去后发现，手机正自行下载一个叫“融证所”的软件，接着就提示填写相关个人信息进行了注册，注册后“客户经理”就教张先生操作在该平台进行投资，张某先后充值了共20万进行投资购买股票。11月16日9时，张某发现自己投资有了收益就想进行提现，提现后却发现一直未到账。报案后才发现自己被骗。

警方提醒：陌生链接不点击，下载软件时务必选择官网或者正规应用商店等渠道，不听信他人宣传通过扫码或者点击链接随意下载。理财投资必须选择合法正规的平台，切勿在来路不明的APP里进行投资。在不确认对方身份的情况下，不轻易涉及金钱往来，更不要轻易相信高收益、高回报的投资产品。

办理低息无抵押贷款诈骗

案例：2020年9月16日，赵某接到一个电话，对方自称贷款公司工作人员。赵某信以为真后添加对方为好友。当他通过对方办理贷款时，对方却以办理贷款需要保证金、风险金等理由骗走赵某5万元后失联。

诈骗手段：嫌疑人要求借款人预先转账支付保证金、手续费、首月利息等款项，受害者轻信转账后，对方立即会玩“消失”。

警方提醒：贷款请走正规渠道，官方查验真伪，切勿轻信他人，以免上当受骗。

网络刷单、兼职诈骗

案例：2020年7月，大学毕业生黄某看到有人在网上发布消息称，招聘“网购刷单员”，日工资三百至五百元。成功应聘“网购刷单员”后，黄某刷完一单100元的订单，赚了5元佣金。随后，他在客服的指导下连续刷了20单，支付了35000元，结果血本无归，客服也失联了。

诈骗手段：嫌疑人通过短信、网络、链接等渠道招募“网购刷单员”，通过刷首单让受害人尝到甜头。当刷单交易金额变大后，嫌疑人就会以各种理由拒不退款或直接“消失”。

警方提醒：凡招聘“网购刷单员”、短视频点赞员、网游推广员等均是诈骗行为，切勿贪图蝇头小利，避免造成不必要的损失。

冒充公司领导诈骗财务人员

案例：郝某是公司的会计。2020年12月，他的微信接到公司“领导”询问相关工作的信息。短暂“交流”后，“领导”让其看一下公司年底账上还有多少货款。郝某回复后，“领导”以需要给合作伙伴结货款为由，让郝某给其提供的银行账户转账40万元。因为之前曾出现过类似情况，郝某便没有按照公司相关财务管理制度的相关规定执行。直到转账后的第二天，他才发现自己被骗。

诈骗手段：嫌疑人往往利用木马程序添加会计或财务联系方式，然后用伪装成公司领导的聊天工具交流，获取受害人信任。在了解公司有关工作情况后，便会要求财务或会计人员转账，造成受害公司财产损失。

警方提醒：财务人员，要严格遵守财务制度。微信或QQ上，无论多熟悉的亲戚或朋友，如果对方提出借钱、汇款、现金转账等要求时，一定要提高警惕，转账汇款前一定要拨打电话确认；同时要养成良好的上网习惯，不随意添加微信群、QQ群，不随便点击不明网址链接。