
国家网络安全
宣传周
China Cybersecurity Week
网络安全
一路随行
2019年金融网络安全宣传手册
CYBER SECURITY
中国人民银行
THE PEOPLE'S BANK OF CHINA

《中华人民共和国网络安全法》保护公民、法人和其他组织的合法权益

国家保护公民、法人和其他组织依法使用网络的权利，促进网络接入普及，提升网络服务水平，为社会提供安全、便利的网络服务，保障网络信息依法有序自由流动。

任何个人和组织使用网络应当遵守宪法法律，遵守公共秩序，尊重社会公德，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。

金融知识课堂

1.普惠金融

普惠金融是指以可负担的成本为有金融服务需求的社会各阶层和群体提供适当、有效的金融服务。小微企业、农民、城镇低收入人群等弱势群体是其重点服务对象。

2.个人银行账户分类

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，不同类别的账户有不同的功能和权限。个人在银行开立账户，每人在同一家银行只能开立一个Ⅰ类账户，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类账户是“钱夹”

个人日常刷卡消费、网络购物、网络缴费通过该账户办理，可购买投资理财产品。

Ⅲ类账户是“钱包”

用于金额较小、频次较高的交易，适用于移动支付。

3.IC卡

IC卡是集成电路卡（Integrated Circuit Card）的英文简称，也称之为智能卡、芯片卡等。银联IC卡是指卡号以62开头的金融IC卡。

按种类分为接触式IC卡和非接触式IC卡，按应用分为借贷记卡（类似磁条卡功能）和电子现金/电子钱包卡（金额不超过1000元，只能消费，不能取现）。

4.银行卡分类

银行卡	按是否可以透支分	信用卡	按是否向发卡机构交存备用金分	贷记卡	指发卡机构给予持卡人一定的信用额度，持卡人可在信用额度内先消费、后还款的信用卡。
				准贷记卡	指持卡人须先按发卡机构要求交存一定金额的备用金，当备用金账户余额不足支付时，可在发卡机构规定的信用额度内透支的信用卡。
		储蓄卡	储蓄卡支付限额为账户存款金额，不允许透支支付。		

5.贷款分类

贷款	按期限长短分	短期贷款	指贷款期限在1年以内(含1年)的贷款。
		中期贷款	指贷款期限在1年以上(不含1年)5年以下(含5年)的贷款。
		长期贷款	指贷款期限在5年以上(不含5年)的贷款。
	按有无担保分	信用贷款	指没有担保、仅依据借款人的信用状况发放的贷款。
		担保贷款	指由借款人或第三方依法提供担保而发放的贷款。担保贷款包括保证贷款、抵押贷款、质押贷款。保证贷款、抵押贷款或质押贷款，系指按《中华人民共和国担保法》规定的保证方式、抵押方式或质押方式发放的贷款。

6.闪付

闪付（Quick Pass）代表银联的非接触式支付产品及应用，具备小额快速支付的特征。用户选购商品或服务，确认相应金额，用具备闪付功能的金融IC卡或银联移动支付产品，在支持银联闪付的非接触式支付终端上，轻松一挥便可快速完成支付。

UnionPay 银联

Quick 闪付Pass

7.手机支付

手机支付也称为移动支付，是指允许移动用户使用其移动终端（通常是指手机）对所消费的商品或服务进行账务支付的一种服务方式。

8.二维码支付

使用手机银行APP、银联云闪付APP、第三方支付APP中的“付款码”在各种交易场景中让商户扫码，或使用以上各类APP中的“扫一扫”，扫描商户的“收款码”完成支付。

该二维码为示例图片

什么是个人金融信息？

依据《中国人民银行金融消费者权益保护实施办法》，个人金融信息是指金融机构通过开展业务或者其他渠道获取、加工和保存的个人信息，包括个人身份信息、财产信息、账户信息、信用信息、金融交易信息及其他反映特定个人某些情况的信息。

个人金融信息包括哪些内容？

个人身份信息，包括个人姓名、性别、国籍、民族、身份证件种类号码及有效期限、职业、联系方式、婚姻状况、家庭状况、住所或工作单位地址及照片等。

个人财产信息，包括个人收入状况、拥有的不动产状况、拥有的车辆状况、纳税额、公积金缴存金额等。

个人账户信息，包括账号、账户开立时间、开户行、账户余额、账户交易情况等。

个人信用信息，包括信用卡还款情况、贷款偿还情况以及个人在经济活动中形成的，能够反映其信用状况的其他信息。

个人金融交易信息，包括银行业金融机构在支付结算、理财、保险箱等中间业务过程中获取、保存、留存的个人信息和客户在通过银行业金融机构与保险公司、证券公司、基金公司、期货公司等第三方机构发生业务关系时产生的个人信息等。

衍生信息，包括个人消费习惯、投资意愿等对原始信息进行处理、分析所形成的反映特定个人某些情况的信息。

在与个人建立业务关系过程中获取、保存的其他个人信息。

个人金融信息泄露渠道

▶ 1.随意填写个人资料。

◀ 2.个人金融信息被倒卖或者盗取。

▶ 3.随手在网上晒个人信息。

◀ 4.贸然连接不明免费Wi-Fi，随便扫码。

个人金融信息泄露的危害

▼ 1.骚扰电话接二连三。

本来只有亲朋好友知道的电话，却经常有陌生人打进来推销。你可能还在纳闷他们怎么知道你的电话之时，你的信息早被卖过多次了。

▼ 2.垃圾短信源源不断，垃圾邮件铺天盖地。

几乎人人都会遇到垃圾短信和邮件的骚扰，这已经是非常普遍的事，个人信息被泄露后，手机和电子邮箱每天都会收到很多这样的垃圾信息，主要是以广告推销为主。

▼ 3.信用卡被盗刷、账户钱款不翼而飞。

不法分子通过获取个人信息非法办理银行账户或信用卡的密码挂失、密码重置等交易，你账户里的钱款可能就不翼而飞了，信用卡也莫名地被盗刷了。

▼ 4.莫名其妙，无端涉案。

不法分子可能利用你的个人信息，去干些坏事，如果犯了什么案或发生什么事故，公安机关或交通管理部门可能会依据身份证的信息找到你，弄得你莫名其妙还要配合调查，以至于把你搞得精疲力竭。

▼ 5.不法分子利用亲朋、个人的信息前来诈骗。

不法分子知道了你的个人信息，编出来一些耸人听闻的消息，甚至对你的哪个朋友、同学或亲戚知根知底，还能报出姓名与单位，在你心神不宁之时，可能做出错误判断，在慌乱中上了骗子的当。

▼ 6.冒充亲朋、同学、公安，坑蒙拐骗趁虚而入。

因为非法获取了你的个人信息，那些躲在暗处的人会费尽心机地想法子坑你、蒙你、拐你、骗你。有道是“明枪易躲，暗箭难防”，稍不留神，可能就会落入坏人的圈套。他们根据手中掌握的你的个人信息，冒充你的亲戚、朋友、同学甚至是公安人员，实现以假乱真。

个人信息被泄露后，个人名誉很可能无端受损。别人冒用你的名义所干的一切坏事都归到你的名下，一时间很难解释清楚。所以我们要提高网络安全防护意识，保护好我们的个人金融信息。

个人金融信息风险防范要点

❶ 切勿把自己的身份证件、银行卡、金融账户等转借他人使用。

❷ 不要因为赠送礼品就注册账户并提供个人身份信息、个人账户信息。

❸ 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。

❹ 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。

❺ 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和期限，例如："仅供XX年XX月办理XX业务使用"，以防身份证复印件被移作他用。

❻ 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。

❼ 不要轻信来历不明的电话、短信和邮件。对方身份未核实前，切勿透露本人银行账号、密码或进行转账操作。

❽ 在电脑和手机上，不要随意点击他人发来的不明链接或网上搜索到的非正规网站链接。

❾ 不要随便扫描二维码。

❿ 在使用二维码支付时，不要提前展示二维码，以免被不法分子扫码扣款。

金融消费者维权

《中华人民共和国消费者权益保护法》第39条规定，消费者和经营者发生消费者权益争议的，可以通过下列途径解决：

（一）与经营者协商和解；

（二）请求消费者协会或者依法成立的其他调解组织调解；

（三）向有关行政部门投诉；

（四）根据与经营者达成的仲裁协议提请仲裁机构仲裁；

（五）向人民法院提起诉讼。

典型案例分析

案例1 网络诈骗被银行及时制止

张某不慎泄露了个人信息，不法分子利用其信息在网上购买基金，使张某收到其银行卡里17000余元被转走的短信，接着打电话自称能帮张某追回被转款项，试图通过取消基金认购操作制造将“被转款项”追回的假象，并诱骗张某将银行卡里的余额转至所谓“安全账户”（不法分子持有）。张某在操作时，A银行工作人员见其神色慌张便询问缘由，确认这是一起诈骗案件。A银行迅速启动应急预案，并协助张某到ATM操作，让对方听到ATM提示音获取信任，成功套取对方的银行卡号，并锁住该账户交易功能。随后，张某收到17000余元已回到账户的短信，被转的款项全部追回。

安全提示：
（1）不明扣款勿慌张，及时求助真银行。
（2）诈骗套路千万项，安全意识要加强。

案例2 “伪基站”诈骗

小丁在睡梦中被持续的手机震动声吵醒，他起床发现手机连续收到了数十条短信验证码和消费通知，并且移动网络从4G下降到了2G。验证码的平台包括途牛网、瓜子二手车、支付宝、京东等。他通过短信消费通知发现，其绑定在APP上的银行卡正在被消费。

不法分子利用手机2G网络（GSM）不加密传输的漏洞，通过伪基站、短信嗅探器，在一定距离内，盗取受害者手机号、短信验证码，之后，再利用各大银行、网站、移动支付APP存在的漏洞和缺陷，窃取信息，修改支付密码，实现资金盗刷。

不法分子还会利用“伪基站”伪装成银行或通信运营商发送诈骗短信或二维码，引诱手机用户点击链接，填写个人身份证、银行卡等信息，从而获取用户的重要隐私和财产信息实施诈骗。

安全提示：
（1）当发现手机网络突然变化，如“停止服务”、“4G变为2G网络”等情况，应尽量避免使用手机进行转账交易等操作。
（2）手机应安装安全防护软件，并启用伪基站防护、垃圾短信拦截等功能。
（3）睡觉时尽量关机或采用飞行模式，尽量关闭免密支付功能。
（4）如果收到银行等金融机构发来的验证码，但不是本人操作，除了关闭手机，还要尽快冻结银行卡，减少损失。

案例3 假冒手机银行APP诈骗

王某收到一则短信，以10开头，内容为••银行网银升级，提醒用户升级手机银行APP，并提供下载链接http://••••••。王某没有丝毫怀疑，点击短信中的链接下载安装。安装到手机上后，该APP操作界面和之前使用的手机银行一模一样，王某按提示登录账户，填写手机号、银行卡、身份证号等信息，没有放在心上。不久之后，王某在银行网点查询卡内余额发现已被洗劫一空，才意识到自己中招了。

不法分子将手机木马伪装成常见银行的手机客户端，放在不安全的软件市场、论坛，引诱用户下载；或是通过伪基站发短信，引诱用户点击短信中的链接，下载安装。

该木马和正版手机银行客户端完全一样，诱导用户填写个人信息，并以短信形式发送到指定的手机号。不法分子获取信息后，此木马将隐藏图标，在后台偷偷拦截并转发短信验证码，这样不法分子就可利用“找回密码”修改中招手机用户银行交易密码，将用户银行卡内的钱财洗劫一空。

安全提示：

(1) 在银行网点或正规渠道下载手机银行客户端。

(2) 切勿轻信未经认证的软件市场，或是论坛、短信里的下载链接，不要随意点击。

(3) 不要将有大额现金的银行卡绑定手机银行，设置银行卡转账限额。

案例4 二维码支付被盗刷

2019年4月21日至5月4日期间，四名消费者手持微信二维码在超市等待付款，在排队的几分钟里，被人从背后通过手机扫码，盗刷500元到900元不等的资金，扣款方都是名为“一站式24小时便利店”的账户，根本不是超市收款。

安全提示：

(1) 关闭免密支付，或调低免密支付的额度。

(2) 不要在排队购物时打开付款码，等到自己要进行支付交易时再打开支付用的二维码。

(3) 仔细辨别付款码和收款码，对外收款时别使用付款码。

(4) 尽量少让别人扫自己的付款码。

(5) 对于网上支付账户，调低支付金额上限，或只存少部分钱。

案例5 网贷连环诈骗

刚毕业的福州网友小兰遭遇电信骗局，短短两天被骗走28万元。

小兰先接到自称“福州通信局”的电话，通知其手机号因群发赌博信息被举报，一号骗子利用威吓成功迷惑住小兰，二号骗子通过伪造公安官方电话的来电显示骗取信任，加了受害者QQ进一步制造行骗语境和场景，小兰完全陷入骗子杜撰的剧情，配合其调查一起涉嫌200多万的洗钱案件，将全部存款转到了所谓“安全账户”。为扩大诈骗“战果”，骗子继续诱导小兰从10家网贷平台借款并要求缴纳9万保证金，当小兰发现已无力缴纳保证金时，才发现自己受骗了。

安全提示：

(1) 但凡收到客服、有关部门或公检法的电话，切勿轻信。

(2) 切勿轻信以任何名义要求转账、借款、缴纳保证金，以免背上负债，造成损失。

(3) 如发现转账账户为个人账户，一定是骗子。

案例6 征信诈骗

山东的小张忽然收到一条短信，手机自动识别是“**银行”发来的，短信号码也是106开头（已认证号段），告知他的信用卡因严重逾期已临时冻结，逾期行为也被录入征信系统。小张准备买房，对自己的信用很是爱惜，他赶紧打短信中的电话询问情况，对方告诉他因为还款逾期要交2万元方可解冻，并告诉他只需关注一个“**银行自助服务中心”的公众号，即可迅速办理，否则影响以后的车贷、房贷。小张担心受影响，就在对方的提示下，在公众号转了2万元。后来小张觉得不对劲，拨打银行电话核实，得知其实根本没有逾期。

安全提示：

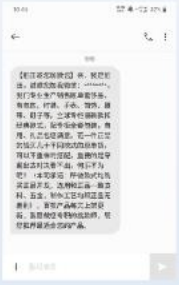
(1) 看到的信息不一定是真的(包括银行发来的短信以及所谓的认证公众号)。

(2) 在接到类似逾期信息后，要及时通过官方客服或者到银行营业网点确认。

(3) 如有征信问题，可到人民银行或指定银行的征信柜台查询、打印。

案例7 网购A货遭骗

刚毕业的银小姐收入一般，但非常喜欢网购，看到同事、同学使用奢侈品，很羡慕。正好收到微商朋友的短信，可以低价购买原单奢侈品。按自己的需求，向对方支付了货款。开始对方还提供“快递”信息，并以海关检查为由，发送链接给银小姐，要求填写个人身份信息和个人账户信息，并录制了银小姐手持身份证的视频。7天后银小姐再次查询发货情况时发现对方已将其拉黑，同时有网贷公司联系银小姐询问还贷情况。



安全提示：

(1) 不占小便宜，通过官方渠道购买商品。

(2) 不随便点击他人发来的链接。

(3) 不要随意提供个人身份信息和个人账户信息。

(4) 不参与刷单、刷信用。

案例8 联手黑客网络敲诈

2019年6月21日，武汉市公安局江汉分局破获一起网络敲诈案。广东一对夫妻在深圳注册两家公司，并联合黑客攻击了国内多家公司的电脑，以解密为由索利，先后获利700余万元。

安全提示：

(1) 电脑连接互联网时一定要做好安全防护措施。

(2) 电脑应安装专业防病毒软件。

(3) 对于个人信息和重要数据，可采取加密等方法保存并做好备份。

案例9 大型企业遭攻击勒索

2019年3月2日，俄罗斯企业遭受大规模网络攻击。攻击者使用物联网设备，伪装成欧尚、马格尼特、斯拉夫尼奥夫等知名公司，向公司内部网站发送钓鱼电子邮件，对公司人员进行勒索攻击。

安全提示：

(1) 企业使用的电脑，连接互联网时一定要做好安全防护措施。

(2) 能够发送电子邮件的设备，如调制解调器、路由器、网络存储、智能家居生态系统和其他小工具，都是入侵者可用于网络钓鱼攻击的途径，对于这些设备的安全隐患要高度防范。

金融安全攻略

7个妙招防范网络金融风险

一 陌生短信不要回，不明链接不要点

大家都接到过陌生号码发来的中奖、兑换、配资等内容的短信，其中绝大多数是假消息。即使是标注为银行官方号码发来的也不要轻信、不要回复，犯罪分子很容易更改短信显示号码。短信中的链接就更不要点击，千万不要按其要求输入个人信息，否则您的信息很有可能会泄露。

二 金融支付要注意，多留心眼防盗刷

使用银行卡、移动支付等进行金融支付时一定要注意，千万不要让银行卡、手机离开自己的视线，移动支付时不要提前打开付款码，不法分子在手机上安装收款软件以后也能扫码收款，盗走您的资金。打开二维码后注意用手遮挡，也可在APP中设置支付时需要密码、指纹等再次确认的方式。

三 手机里千万别存身份证照片

身份证对于我们来说非常重要，在开立证券账户或办理其它网上业务时需要提供身份证照片，一定要记住身份证照片用完之后立即删除。如果您的手机不慎丢失并且存有身份证照片，那风险就大了，通过身份证照片及手机短信验证码，可以将您的各类账户密码重置，然后盗走账户中的资金。

四 有人跟您借钱一定要电话核实

如果有朋友通过微信或QQ跟您借钱，不要直接就把钱打过去，因为朋友的账号有可能被盗。这时候一定要拨打朋友的电话确认，如果朋友说不方便接听，那十有八九就是诈骗了，要及时通知朋友账号被盗，避免让其他人上当受骗。

五 短信验证码不要对任何人透露

千万不要忽视了短信验证码的重要性，实际上它比支付密码更重要。现在犯罪分子手段都很高超，可以用各种方法获取银行卡或网络支付密码，而短信验证码没法直接获取，有验证码就能在网上执行转账、消费等操作。所以，短信验证码不要透露给任何人，即使是您的亲友也要小心。

六 不要所有的账户都用一个密码

我们使用的密码越来越多，除了银行卡、信用卡密码外，还包括电商平台的密码、第三方支付密码等，很多人为了省事都用一个密码，这种做法存在极大的风险。一旦其中一个平台遭受攻击泄露了用户信息，所有账户都将处于危险之中。

七 高收益金融软件不要信，投资选正规途径

投资者在网上时常会看到一些声称包赚不赔的炒股或炒黄金软件，通过所谓的“专业”及虚假夸大宣传来引起投资者注意，并且承诺高额投资收益，还虚构一些“成功案例”现身说法。股票、基金、黄金投资市场都会有风险，不可能包赚不赔。投资者一定要通过正规途径投资。