国家网络安全宣传周
China Cybersecurity Week

网络安全 你我同行

2022

金融网络安全宣传手册

中国人民银行
THE PEOPLE'S BANK OF CHINA

9个建议助您
防范个人信息泄露

1. 网上购物谨防钓鱼网站，尽量到正规的大型网站，并仔细检查网站域名是否正确，不轻易接收和安装不明软件，不随便点击聊天中对方所发来的链接。

2. 身份证等证件复印时一定要写明用途，在含有身份信息区域注明“本复印件仅供XX用途，他用无效”和日期。

3. 填写个人简历时要注意查看求职平台和企业是否正规，只写必要信息，不要过于详细填写本人具体信息。

4. 妥善保管、处理好包含个人信息的票据，如快递单、火车票等。

5. 谨慎在网上或者街头参加一些需要填写真实身份、手机号码等个人信息的活动。

6. 微信不要添加来路不明的人为好友，不要在朋友圈通过视频、照片、文字等形式暴露自己的真实身份、家庭住处、单位地址、子女情况等信息；在微信“附近的人”设置中，要谨慎开放陌生人查看权限，不晒包含个人信息的照片。

7. 不要随意扔弃或出售未经处理包含个人信息的手机、电脑等电子设备。

8. 大型正规支付平台不会因为系统升级导致支付失败；对于自称是平台客服的人员，需要与官方客服电话进行联系并确认；在网上对任何人都不能透露自己的密码和短信认证信息。

9. 电脑、手机等电子设备应安装安全软件，并定时进行安全扫描，避免因系统漏洞被不法分子利用，导致个人信息泄露。

4 “举”案例说法 这些套路要警惕

01-虚假APP诈骗

李先生神色慌张来到某银行，申请开立银行卡。网点经理上前询问其开卡用途，李先生表示准备向银行申请5万元贷款，支付其在某平台上的贷款保证金。值班经理认为男子的开卡用途可疑，向其进一步了解后得知李先生最近计划开办一家实体店，缺乏启动资金，故下载了一款贷款APP，按操作提示填写个人资料后获批了20万元的贷款。

但贷款在最后放款环节提示放款账号有误，随后自称是该APP客服人员与之联系，要求其缴纳5万元保证金来解冻贷款资金，并出示了“监管部门公函”，强调必须在2小时内缴纳5万元保证金，否则将被控告“恶意套用贷款罪”，接受上门取证调查。被吓懵的李先生赶紧将其卡内的1980元马上转给对方，但因手头资金实在凑不齐5万元，这才想到来银行办理贷款支付该笔保证金。在仔细查看了李先生与对方的聊天记录后，网点经理基本确定这是一起典型的网络安全诈骗案件，随后帮助客户联系公安机关报案。

安全提示

本案例是近年来多地多次发生过的典型网络安全诈骗案例，诈骗分子通过短信、QQ、微信、APP等方式发布可办理高息贷款或信用卡套现等虚假信息，以提前交纳手续费、税款、利息、解冻资金等方式，诱骗受害人汇款，以此骗取钱款。作为普通金融消费者，我们应注意增强防诈警觉意识、提高分辨能力，在正规金融机构的网上、手机渠道办理相关业务，对于来历不明的信息注意拨打官方客服电话和国家反诈中心电话进行确认。

02-“征信修复”骗局

张先生在购买新房办理房贷时，发现自己的征信报告存在多次信用卡逾期记录，导致银行拒贷，陷入困境。此时，两名陌生人士的交谈引起了张先生的注意，其中李某声称在王某的帮助下完成“征信修复”，并成功办理贷款。随即张先生主动加入交谈，并留下王某联系方式。

后经多次联系，王某提出支付2万元即可帮张先生“修复征信”，并要求其先支付40%作为定金。一个月后，王某通知张先生已“征信修复”成功，索要剩余的60%。但当张先生办理房贷再次来到银行时，发现逾期记录并未消除，在银行工作人员的解释下，方知被骗，此时王某已经联系不上。

安全提示

根据《征信业管理条例》有关规定，任何机构和个人都无权擅自修改、删除信用报告上真实、准确的征信信息。每个人作为信息主体，在日常生活中都要注意量入为出、合理借贷、按时还款，避免逾期，保持良好的征信记录。同时，需提高警惕，不要相信“征信修复”广告并远离“征信修复”骗局，避免上当受骗，造成财产损失及个人信息泄漏。

03-虚拟物品骗局

小张是某网络游戏的忠实玩家，在该网络游戏上花费了不少的时间和金钱，游戏账号装备了价值不菲的皮肤。某天小张在游戏论坛中偶然翻到了一条广告，“网络游戏饰品租赁网站，稳定收益无风险，大平台担保…”。

看到很多论坛网友都晒出自己的收益，小张没有多想点开了广告中的网址，并注册了账户。起初，只尝试出租了一套游戏皮肤，很快就有求租的“玩家”主动联系，一周过后小张从网站中成功提现了余额，觉得没有多大风险的他索性把账号中所有皮肤都挂在了网站上，可一连几天过去了却无人问津。

此时，内心焦急的小张询问网站的客服人员，其“建议”卖家的皮肤直接寄存在网站的机器人账号中，交易时间更快，也更容易租出去，并再三以“大平台担保”“保证金制度”“理赔案例”等说辞保证账号安全。被利益冲昏头脑的小张将所有的皮肤转到了网站的机器人账户，两周后小张想要提现自己的收益时，发现网站已经不能使用自己的账号登陆，小张共损失了价值数万元的皮肤，等到小张报警后才发现，这些价值不菲的虚拟资产早已经被转移。

安全提示

游戏交易诈骗属于一种新型的网络诈骗方式，其特点是受害者比较集中，而且每位受害者的损失数额相对较大。诈骗团伙往往在较为封闭的游戏论坛和贴吧发布虚假信息，以游戏账号租赁赚钱、游戏装备兑换现金等作诱饵，引诱受害者将游戏中的虚拟物品转移到他们手中。游戏中的虚拟资产转移比常规资产更加容易，虚拟资产的价值也难以认定，受害者的损失相对难以追讨，因此我们应当把游戏仅仅当作一种消遣方式，在游戏中要保持清醒的头脑，理性消费。

04-围绕“疫情”设骗局

2022年2月，某县公安局网安大队巡查发现，有人利用群众对口罩迫切需求的心理，制作名为“某县防护口罩预约服务”的网页发布至微信朋友圈、微信群，假借预约口罩，非法获取群众的公民个人信息。某县网安部门经过缜密侦查，迅速锁定了犯罪嫌疑人薛某，并于同月将其抓捕归案。经查，薛某共非法获取公民姓名、电话号码、身份证号码、家庭住址等公民个人信息5530条。

安全提示

《中华人民共和国个人信息保护法》规定，任何组织、个人不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息；不得从事危害国家安全、公共利益的个人信息处理活动。

若手机收到关于疫情流调的短信，要求点击链接后自行填报个人信息，一定要谨慎判断，最好通过官方渠道进行求证；如未求证，谨慎点击短信链接，防止受骗。

05-“钓鱼广告”骗局

某天刘先生浏览手机时，无意中看见以某商业银行名义投放的打卡送礼品活动广告（广告内二维码实为钓鱼二维码），刘先生扫二维码跳转到伪造的打卡活动网页，并直接下载安装了一款理财软件，刘先生看见软件中实名注册打卡送礼品的活动后非常心动，便填写了姓名、身份证号、手机号等敏感信息，并按活动要求连续2天参与打卡活动，在领取礼品页面又填写了自己的详细收货地址，之后，刘先生便接到了客服的电话，对方以发放礼品需甄别用户真实性为理由，引诱刘先生购买一定金额的理财产品获取礼品，骗取了刘先生5000元。

安全提示

①银行等金融机构不会在非官方平台发布签到、抽奖兑礼品等活动信息。

②查看网站链接和页面是否为官方渠道。诈骗短信或二维码提供的网页链接可能是假冒手机银行或网上银行网页的钓鱼链接，也可能是病毒木马，不应轻易点击和操作。

③任何含可疑二维码、链接、应用程序的广告、短信等消息，不要轻易点击，若无法辨别真实性，应及时联系官方机构求证。

④涉及提供个人信息、资金转出时请务必三思，一旦发现受骗，请及时拨打110报警，并保留好相关证据。

⑤请下载“国家反诈中心”APP。“国家反诈中心”APP是公安部联合国家互联网应急中心开发的一个可以智能识别诈骗电话、短信和网址的软件。使用“国家反诈中心”APP可有效防范不断更新、真假难辨的诈骗手段。

1 “学”政策法规 这些内容要了解

《中华人民共和国网络安全法》

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通过《中华人民共和国网络安全法》，自2017年6月1日起施行。

1 明确个人、组织禁止的行为

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。

2 明确社会公众对危害网络安全行为有举报权

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。

3 明确网络运营者的责任义务

网络运营者开展经营和服务活动，必须遵守法律、行政法规，尊重社会公德，遵守商业道德，诚实信用，履行网络安全保护义务，接受政府和社会的监督，承担社会责任。

4 明确公众被侵权时的权利

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。

《中华人民共和国数据安全法》

2021年6月10日，第十三届全国人民代表大会常务委员会第二十九次会议通过《中华人民共和国数据安全法》，自2021年9月1日起施行。

1 明确个人、组织禁止的行为

任何组织、个人收集数据，应当采取合法、正当的方式，不得窃取或者以其他非法方式获取数据。

非经中华人民共和国主管机关批准，境内的组织、个人不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据。

2 明确保护个人、组织的合法权益

开展数据处理活动，应当遵守法律、法规，尊重社会公德和伦理，遵守商业道德和职业道德，诚实守信，履行数据安全保护义务，承担社会责任，不得危害国家安全、公共利益，不得损害个人、组织的合法权益。

3 明确公共服务应保障老年人、残疾人的需求

国家支持开发利用数据提升公共服务的智能化水平。提供智能化公共服务，应当充分考虑老年人、残疾人的需求，避免对老年人、残疾人的日常生活造成障碍。

4 明确开展数据处理活动的原则

开展数据处理活动以及研究开发数据新技术，应当有利于促进经济社会发展，增进人民福祉，符合社会公德和伦理。

《中华人民共和国个人信息保护法》

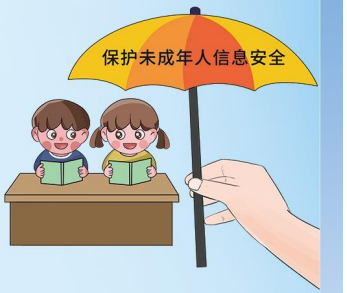
2021年8月20日，第十三届全国人民代表大会常务委员会第三十次会议通过《中华人民共和国个人信息保护法》，自2021年11月1日起施行。

1 明确个人、组织禁止的行为

任何组织、个人不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息；不得从事危害国家安全、公共利益的个人信息处理活动。

2 明确对未成年人个人信息的保护

个人信息处理者处理不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的同意。个人信息处理者处理不满十四周岁未成年人个人信息的，应当制定专门的个人信息处理规则。



3 明确自动化决策规范，禁止“大数据杀熟”

个人信息处理者利用个人信息进行自动化决策，应当保证决策的透明度和结果公平、公正，不得对个人在交易价格等交易条件上实行不合理的差别待遇。

2 “懂”金融科技 这些知识要知道

金融科技伦理 01

金融科技伦理是金融领域开展科学研究、技术开发等科技活动需要遵循的价值理念和行为规范。秉持以人为本，坚持科技向善。

金融科技发展的现状 01

在新一轮科技革命和产业变革的背景下，金融科技蓬勃发展，人工智能、大数据、云计算、物联网等信息技术与金融业务深度融合，为金融发展提供源源不断的创新活力。

金融科技发展面临的伦理挑战 02

- 数据安全不容忽视
- 算法滥用日益严重
- 无序竞争亟须规范
- 数字鸿沟有待弥合

金融科技伦理治理的几点要求 03

——**伦理先行**。加强源头治理，注重预防，将科技伦理要求贯穿科学研究、技术开发等科技活动全过程，促进科技活动与科技伦理协调发展、良性互动，实现负责任的创新。

——**依法依规**。坚持依法依规开展科技伦理治理工作，加快推进科技伦理治理法律制度建设。

——**敏捷治理**。加强科技伦理风险预警与跟踪研判，及时动态调整治理方式和伦理规范，快速、灵活应对科技创新带来的伦理挑战。

——**立足国情**。立足我国科技发展的历史阶段及社会文化特点，遵循科技创新规律，建立健全符合我国国情的科技伦理体系。

——**开放合作**。坚持开放发展理念，加强对外交流，建立多方协同合作机制，凝聚共识，形成合力。积极推进全球科技伦理治理，贡献中国智慧和中国方案。

弥合“数字鸿沟” 04

随着我国互联网、大数据、人工智能等信息技术快速发展，智能化服务得到广泛应用，深刻改变了生产生活方式，提高了社会治理和服务效能。但同时，我国老龄人口数量快速增长，不少老年人不会上网、不会使用智能手机，在出行、就医、消费等日常生活中遇到不便，无法充分享受智能化服务带来的便利，老年人面临的“数字鸿沟”问题日益凸显。如何帮老年人迈过“数字鸿沟”是一个新考题。中国人民银行发布的《中国普惠金融指标分析报告（2019年）》建议，应协调推进“线上+线下”普惠金融业务发展，降低“数字鸿沟”的不利影响。

金融科技是弥合数字鸿沟、解决发展不平衡不充分问题的重要手段，主要途径包括：

1. 纾解城乡间数字化建设鸿沟
2. 破解群体间数字化应用鸿沟
3. 缓解机构间数字化发展鸿沟

金融数据安全级别 02

金融数据安全分级

根据金融业机构数据安全性遭受破坏后的影响对象和所造成的影响程度，将数据安全级别从高到低划分为5级、4级、3级、2级、1级。

个人金融信息类别：根据信息遭到未经授权的查看或未经授权的变更后所产生的影响和危害，将个人金融信息按敏感程度从高到低分为C3、C2、C1三个类别，并对三类信息实施不同级别的保护。

C3 主要为用户鉴别信息，包括银行卡有效期、账户登录密码等信息。

C2 主要为可识别特定个人金融信息主体身份与金融状况的个人金融信息，以及用于金融产品与服务的关键信息，包括支付账号、账户登录名等信息。

C1 主要为机构内部的信息资产，主要指供金融业机构内部使用的个人金融信息，包括账户开立时间、开户机构等信息。

3 “防”网络风险 这些概念要知晓

“防”数字人民币诈骗

数字人民币是人民币的数字化形态，是把人民币放进APP里。它和人民币完全等价。它们都是由中国人民银行发行的法定货币。

（1）数字人民币APP（试点版）已在应用市场公开上架。试点客户可在苹果App Store、安卓手机应用市场和应用宝、360手机助手、豌豆荚等第三方市场下载注册数字人民币APP。请勿通过不明渠道下载伪冒安装程序。

（2）您可拒绝任何个人、机构、组织企图索取您数字人民币APP登录密码、支付密码、短信验证码的要求。谨防不法分子冒充政府机关和银行、电商平台等机构人员骗取您的信息。

（3）任何单位或机构（如公检法、中国人民银行、商业银行）不会直接通过电话或短信的方式要求您向指定数字钱包、银行账户、支付账户等进行转账汇款，请勿相信此类要求。

（4）数字钱包的名称由用户自行设置，不一定代表对方真实身份，请勿仅依据钱包名称判定对方身份。

（5）数字人民币是数字形式的法定货币，与纸钞和硬币等价，不存在交易炒作空间，请勿相信用数字人民币在交易所交易获利等诈骗信息。

（6）如您怀疑自己遭遇假借数字人民币名义开展的电信诈骗，请第一时间拨打当地110电话报警。数字人民币产品用户，也可拨打数字人民币试点咨询热线4001391000咨询。

“防”大数据杀熟

胡女士多次通过某APP预定机票、酒店，消费了10余万元，因此成为8.5折优惠的钻石贵宾客户。2020年胡女士通过该APP订购了某酒店的一间豪华湖景大床房，支付价款2000多元，离开酒店时，胡女士发现酒店的挂牌价仅为自己支付价款的一半左右。胡女士与APP所属公司沟通，该公司以并非订单的合同相对方等为由，仅退还了部分差价。

胡女士认为：一是新下载该APP后，用户必须点击同意其“服务协议”“隐私政策”方能使用，如不同意，将直接退出，APP以不提供服务的方式形成了对用户的强制。二是该APP的“服务协议”“隐私政策”均要求用户特别授权其及其关联公司共享用户的注册信息、交易、支付数据，允许对用户数据进行分析和进一步商业利用，既无必要性，又无限加重用户个人信息使用风险。三是该APP的“隐私政策”要求用户授权其自动收集用户的个人信息，包括订单数据、日志信息、设备信息、软件信息、位置信息等，要求用户许可其使用个人信息进行营销活动、形成个性化推荐。APP收集的上述信息超越了形成订单必需的要素信息，属于非必要信息的采集和使用。

胡女士以APP所属公司采集个人非必要信息，进行“大数据杀熟”等为由诉至法院，要求退一赔三并要求该APP增加不同意“服务协议”和“隐私政策”时仍可继续使用的选项，以避免采集个人信息。

法院判决该APP所属公司赔偿胡女士未完全赔付的差价及订房差价的三倍赔偿金，且在运营的APP中增加不同意现有“服务协议”和“隐私政策”仍可继续使用的选项，或者修订“服务协议”和“隐私政策”，去除对用户非必要信息采集和使用的相关内容。

《中华人民共和国个人信息保护法》第二十四条明确规定：个人信息处理者利用个人信息进行自动化决策，应当保证决策的透明度和结果公平、公正，不得对个人在交易价格等交易条件上实行不合理的差别待遇。由国家网信办等四部门联合发布的《互联网信息服务算法推荐管理规定》将算法推荐纳入监管体系，第二十一条明确规定：算法推荐服务提供者向消费者销售商品或者提供服务的，应当保护消费者公平交易的权利，不得根据消费者的偏好、交易习惯等特征，利用算法在交易价格等交易条件上实施不合理的差别待遇等违法行为。这些法律法规的出台意味着“大数据杀熟”被明令禁止，实施此类行为涉嫌违法。但这种“杀熟”行为往往披着差异化营销的外衣，后续治理还需要制定具有可操作性的统一认定标准和执法尺度，借助有效的技术手段，实现事前事中事后全流程、全链条监管。

对于广大消费者来说，避免被大数据“杀熟”，可以尽量减少对单一软件的依赖，多比较不同账号、软件间同一商品或服务的价格差异，同时给购物、打车等各类APP授予最小权限，避免自己的个人信息被过度收集，陷入大数据“杀熟”陷阱。

“五大反诈利器”
有效防范电信网络诈骗

- 国家反诈中心APP
- 96110预警劝阻专线
- 全国移动电话卡“一证通查”服务
- 12381涉诈预警劝阻短信
- 云闪付APP“一键查卡”

网络安全为人民　网络安全靠人民

加强金融科技伦理建设

促进金融安全健康发展