2021年国家网络安全宣传周

“网络安全为人民，网络安全靠人民”

2021年10月11日- 2021年10月17日

本页内容来源于人民银行《2021年金融网络安全宣传手册》

我们这样应对社交网络风险

1.不随意点击不明链接

2.在正规应用商店下载应用程序

3.将社交应用中的个人隐私信息设置为隐藏

4.慎重选择好友，涉及资金或敏感信息时，要当面核实或电话确认

本页内容来源于人民银行《2021年金融网络安全宣传手册》

密码设置安全建议

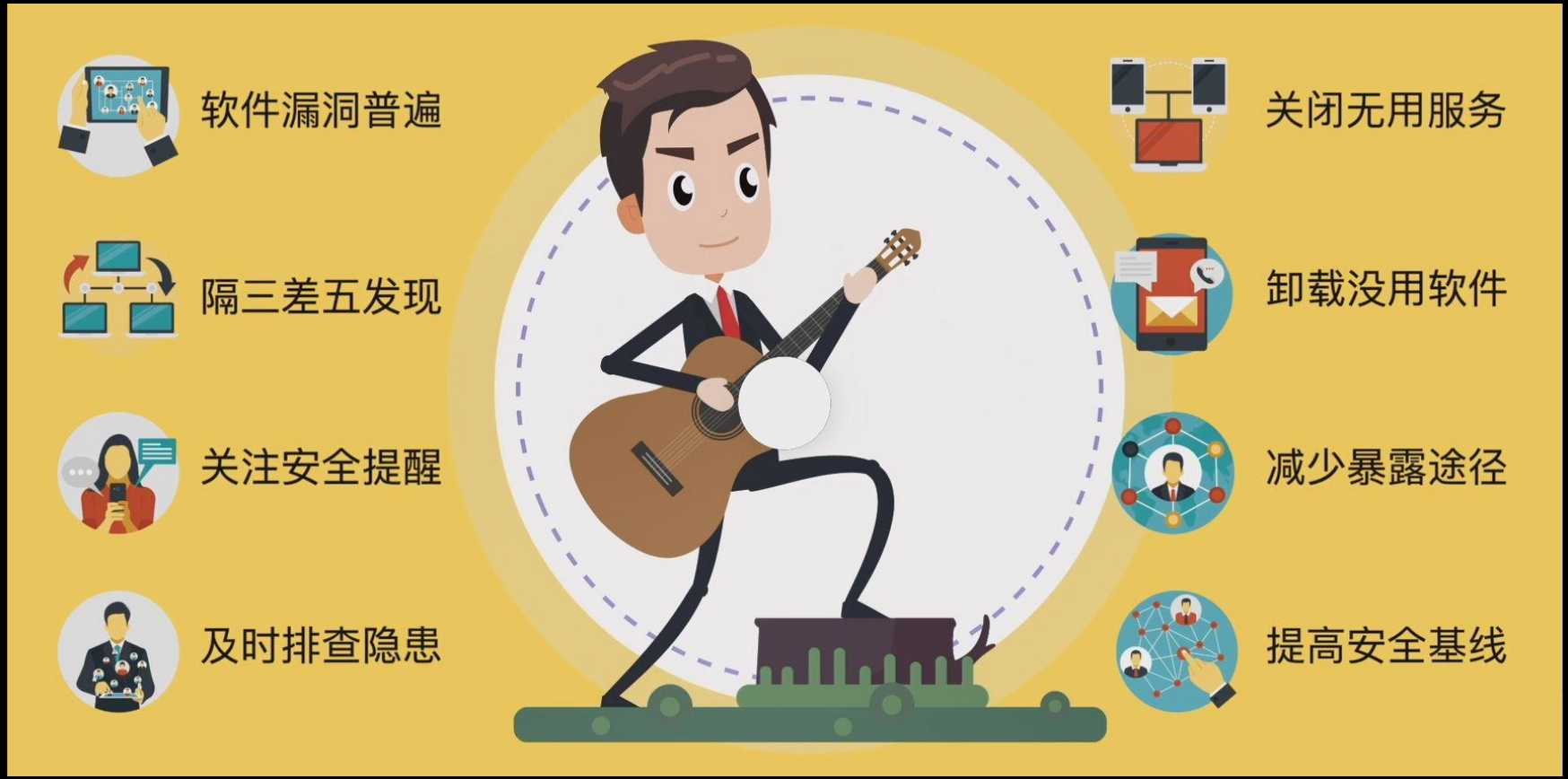
用你近期的目标作为密码，再用字母、数字、特殊字符组合的方式来设置，比如：3个月瘦10斤，可以设置为：3gYs10@j!

密码的长度应大于8位

定期修改你的密码

不要所有的账户都用一样的密码

本页内容来源于人民银行《2021年金融网络安全宣传手册》



本页内容来源于人民银行《2021年金融网络安全宣传手册》

本页内容来源于人民银行《2021年金融网络安全宣传手册》

固若金汤

守护金融网络安全防线

手机银行安全使用Tips

谨慎开通勿出错

开通手机银行时，安装使用银行官方渠道发布的客户端，并确认签约绑定的是本人使用的手机号，同时根据平时转账金额设立合适的额度，如果只是小额支付，可以把转账额度设定小一些。

密码复杂不外泄

为手机银行账户设置单独的、高安全级别的登录密码，尽量在8位以上、包含数字、大小写字母及特殊符号，务必保证与邮箱等其他账号密码有所区别。手机内不要存储密码，以防外泄。

登录退出多留意

尽量不在公共场所WiFi环境下登录或使用手机银行。每次登录要仔细核对欢迎信息、上次登录时间是否正确，发现异常情况立即退出。每次使用完手机银行后，一定要安全退出，避免手机银行在后台运行期间被攻击。

使用期间莫分心

不要在登录使用手机银行期间，随意查看来历不明的短信或邮件、点击不明链接、下载不明文件、扫描不明二维码，谨防木马、钓鱼邮件攻击。安装杀毒软件，定期查杀病毒并升级手机银行客户端。

交易信息要掌握

开通短信通知业务或银行微信服务号通知功能，即时掌握账户资金变动。如有手机银行被盗用的情况，能够第一时间发现异常支付信息，并联系银行客服查询或向公安部门报警。

手机遗失速冻结

一旦发生手机或SIM卡遗失的情况，尽快向提供服务的电信运营商办理挂失或申请停止服务，同时第一时间通过银行网点柜台或致电银行客服热线暂停手机银行服务、冻结网银功能，避免因手机中的账号或密码被盗而造成更大损失。

根据中国人民银行发布的《移动终端支付可信环境技术规范》（JR/T 0156—2017），现在，不少手机银行运用了“手机盾”技术，基于手机芯片的TEE(可信执行环境) 和SE(安全元件)，实现硬件级的安全性，方便大众在手机上实现安全的大额转账、身份认证等功能。手机盾功能可咨询各大银行客服或前往柜台进行开通。

警惕网上购物陷阱

- 核实网站资质及联系方式的真伪，要到知名、权威的网上商城购物，不要轻信不知名网店的低价推销。
- 尽量通过网上第三方支付平台交易，并检查支付网站的真实性，切忌直接与卖家私下交易。
- 购物时要注意商家的信誉、评价和联系方式。
- 交易完成后，完整保存交易订单等信息。
- 直接使用银行账号、密码和证件号码等敏感信息时要慎重。

警惕网上贷款陷阱

- 警惕贷款前需要先行缴费的网贷机构，正规的贷款机构在放款之前是不会收取任何费用的。
- 银行对于无抵押贷款有严格要求，仅凭身份证是无法办理的，因此不要轻信“无抵押贷款”“低息”“免息”“当天放款”等广告标语，也不要相信仅凭身份证就可办理的贷款。
- 一旦发觉网贷机构可能是骗子，马上停止汇款操作并立即进行举报，可以拨打银行官网客服电话、当地派出所电话或110报警电话进行求证或举报。

虚拟货币与数字人民币

虚拟货币 VS **数字人民币**

虚拟货币是指基于区块链等技术，通过复杂数学算法产生的加密数字货币，如比特币、以太币等。虚拟货币不由中国人民银行发行，不具有法偿性和强制性等货币属性，并不是真正意义上的货币，不具有与货币等同的法律地位，不能且不应作为货币在市场上流通使用。从我国现有司法实践看，虚拟货币交易合同不受法律保护，投资交易造成的后果和引发的损失由相关方自行承担。广大消费者要增强风险意识，树立正确的投资理念，不参与虚拟货币交易炒作活动，谨防个人财产及权益受损。

数字人民币由中国人民银行发行，是有国家信用背书、有法偿能力的法定货币。与比特币等虚拟货币相比，数字人民币是法币，与法定货币等值，相当于“电子版人民币现金”，其效力和安全性是最高的。而虚拟货币是一种虚拟资产，没有任何价值基础，也不享受任何主权信用担保，无法保证价值稳定。这是数字人民币与比特币等虚拟货币最根本的区别。

数字人民币具有双层运营、支持银行账户松耦合、双离线支付、点对点交付、高可追溯性等特点。

警钟长鸣

金融网络安全典型案例

网贷陷阱

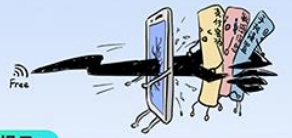
做小本生意的刘先生因为疫情损失订单、缺少流动资金，陷入困境。这时，他接到骗子的短信和电话，骗子冒充银行客服人员，表示可以为刘先生办理无息贷款，需要他缴纳十万元押金。刘先生先后两次打电话咨询银行正规客服，客服均回复没有这类贷款，提醒刘先生小心被骗。病急乱投医的刘先生在骗子的一再诱惑下，决定通过网银给骗子转账。刘先生来到银行网点，银行工作人员发现刘先生曾多次咨询客服，立即核实情况，与刘先生沟通，阻止了刘先生被骗，并为刘先生办理正规贷款，解决燃眉之急。

安全提示：

通过网络借贷平台贷款前需要通过官方渠道查验真伪，切勿相信非法网贷、校园贷等非正规渠道贷款，不要被“无抵押”“到款快”“无息”等广告诱惑。建议尽量通过银行等金融机构的正规渠道贷款。

免费WiFi陷阱

市民张先生使用公共场所的WiFi后，电脑被黑客入侵，在U盾、银行卡均未丢失的情况下，网银被他人在两天内盗刷69次，卡上的6万多元仅剩下500元。更可怕的是，他的手机也被黑客做了手脚，接收消费提醒短信的功能全部被屏蔽，所发生的69次交易他根本没收到任何短信提示，钱在不知不觉中被转走了。



安全提示：

关闭手机和计算机的自动连接WiFi的功能。在公共场所，不要连接未知的WiFi。不要将自己家的WiFi密码共享，定期修改密码。在未知的WiFi信号下不要输入QQ、微信、游戏、银行、支付宝等密码。

新冠疫苗骗局

罗先生收到一条“疾管中心”发来的手机短信，称“新冠疫苗接种预约已在我市开放，名额有限，截止于本周五前暂停报名”，并附带一个预约报名链接。随后，罗先生接到自称社区卫生服务中心打来的电话，声称要统计社区居民新冠疫苗接种情况，如果在月底前仍未接种将限制跨省出行，并督促罗先生尽快按照短信通知预约。罗先生赶紧访问短信链接，在未能识别其为钓鱼网站的情况下，按照提示依次输入了姓名、身份证号、银行卡号、密码等信息。十分钟后，罗先生收到了银行卡消费8000元的短信，才意识到被骗。

安全提示：

对于提及“新冠”“疫苗”等与当下重大疾病、灾害或热点相关的信息，要提高警惕。对可疑的电话或短信不要轻信，更不要直接与短信内给出的电话号码联系，有疑问应及时致电相关单位官方电话核实，银行账户、密码，特别是手机验证码不得外泄，做好个人金融信息保护。

弱密码泄露

某天，李小姐的银行卡发生“隔空被盗”的现象，卡好好地揣在兜里，却莫名收到了钱被跨国刷走的短信提示。经过警方与银行联合调查，发现是专业黑客从银行、商场等地窃取了李小姐的银行卡信息，转卖给国际盗刷组织。由于李小姐银行卡使用了生日这样的弱密码，被黑客轻易破解，盗刷金额上万元，损失惨重。

安全提示：

弱密码也称弱口令，指容易被他人猜测或被破解工具破解的密码。银行卡、手机银行、网银、第三方支付软件等的登录及支付密码应杜绝使用弱密码，密码应同时包含大写字母、小写字母、数字和特殊字符，不包含连续字符（如“123456”“qwertyui”）、重复字符组合（如“AAAAAA”“123123”）、特殊含义字符组合（如“5201314”）、完整英文单词（如“password”“iloveyou”）等，也不包含个人及父母、子女、配偶的姓名、生日、手机号等信息。不与其他社交账号、游戏账号共用相同密码，养成定期更换密码的习惯。

本页内容来源于人民银行《2021年金融网络安全宣传手册》

警钟长鸣

金融网络安全典型案例

网贷陷阱

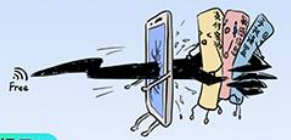
做小本生意的刘先生因为疫情损失订单、缺少流动资金，陷入困境。这时，他接到骗子的短信和电话，骗子冒充银行客服人员，表示可以为刘先生办理无息贷款，需要他缴纳十万元押金。刘先生先后两次打电话咨询银行正规客服，客服均回复没有这类贷款，提醒刘先生小心被骗。病急乱投医的刘先生在骗子的一再诱惑下，决定通过网银给骗子转账。刘先生来到银行网点，银行工作人员发现刘先生曾多次咨询客服，立即核实情况，与刘先生沟通，阻止了刘先生被骗，并为刘先生办理正规贷款，解决燃眉之急。

安全提示：

通过网络借贷平台贷款前需要通过官方渠道查验真伪，切勿相信非法网贷、校园贷等非正规渠道贷款，不要被“无抵押”“到款快”“无息”等广告诱惑。建议尽量通过银行等金融机构的正规渠道贷款。

免费WiFi陷阱

市民张先生使用公共场所的WiFi后，电脑被黑客入侵，在U盾、银行卡均未丢失的情况下，网银被他人在两天内盗刷69次，卡上的6万多元仅剩下500元。更可怕的是，他的手机也被黑客做了手脚，接收消费提醒短信的功能全部被屏蔽，所发生的69次交易他根本没收到任何短信提示，钱在不知不觉中被转走了。



安全提示：

关闭手机和计算机的自动连接WiFi的功能。在公共场所，不要连接未知的WiFi。不要将自己家的WiFi密码共享，定期修改密码。在未知的WiFi信号下不要输入QQ、微信、游戏、银行、支付宝等密码。

新冠疫苗骗局

罗先生收到一条“疾管中心”发来的手机短信，称“新冠疫苗接种预约已在我市开放，名额有限，截止于本周五前暂停报名”，并附带一个预约报名链接。随后，罗先生接到自称社区卫生服务中心打来的电话，声称要统计社区居民新冠疫苗接种情况，如果在月底前仍未接种将限制跨省出行，并督促罗先生尽快按照短信通知预约。罗先生赶紧访问短信链接，在未能识别其为钓鱼网站的情况下，按照提示依次输入了姓名、身份证号、银行卡号、密码等信息。十分钟后，罗先生收到了银行卡消费8000元的短信，才意识到被骗。

安全提示：

对于提及“新冠”“疫苗”等与当下重大疾病、灾害或热点相关的信息，要提高警惕。对可疑的电话或短信不要轻信，更不要直接与短信内给出的电话号码联系，有疑问应及时致电相关单位官方电话核实，银行账户、密码，特别是手机验证码不得外泄，做好个人金融信息保护。

弱密码泄露

某天，李小姐的银行卡发生“隔空被盗”的现象，卡好好地揣在兜里，却莫名收到了钱被跨国刷走的短信提示。经过警方与银行联合调查，发现是专业黑客从银行、商场等地窃取了李小姐的银行卡信息，转卖给国际盗刷组织。由于李小姐银行卡使用了生日这样的弱密码，被黑客轻易破解，盗刷金额上万元，损失惨重。

安全提示：

弱密码也称弱口令，指容易被他人猜测或被破解工具破解的密码。银行卡、手机银行、网银、第三方支付软件等的登录及支付密码应杜绝使用弱密码，密码应同时包含大写字母、小写字母、数字和特殊字符，不包含连续字符（如“123456”“qwertyui”）、重复字符组合（如“AAAAAA”“123123”）、特殊含义字符组合（如“5201314”）、完整英文单词（如“password”“iloveyou”）等，也不包含个人及父母、子女、配偶的姓名、生日、手机号等信息。不与其他社交账号、游戏账号共用相同密码，养成定期更换密码的习惯。

网购退款诈骗

大学生王同学手机收到一条陌生号码发来的短信，称王同学网购的商品订单系统出错，要王同学联系订单中心办理退款。王同学按照短信上提供的号码拨打过去，对方能准确说出王同学的订单号，并声称该订单被冻结了，需要去附近银行解冻。当王同学质疑为何不能直接退回支付账户时，对方称，由于该订单在系统升级时出现了问题，无法通过原账户进行退款，并叮嘱王同学要尽快完成这笔退款，不然会更麻烦。当天下午5点，王同学在校园内的ATM机上按对方的指示操作，向对方账户汇了1888元的“订单解冻金”，直到收到银行卡被消费1888元的信息，王同学才反应过来被骗。

安全提示：

网上购物选择可信度高的电商网站，不要乱晒网购订单、购物凭证，不要随意丢弃含个人信息的快递单、快递盒。收到各类网购异常提示的短信或电话，先直接拨打购物网站的官方客服热线进行查询核实，对于要先汇钱或提供卡号密码等信息再退款的要求一概不予理会。

二维码陷阱

张女士发现自己路边停放的车上被贴了罚单，上面还印有快速缴费二维码，张女士随即扫描该二维码并缴纳罚款。事后，经朋友提醒，张女士打电话咨询交管部门，才发现自己扫描了假的二维码。

安全提示：

不法分子常通过伪造带有二维码的交通罚单、物业费缴纳单、学费单、党费单等，引诱大家扫码支付。一定要通过官方联系渠道与收款方确认二维码真伪，不要随便扫描未知二维码。扫描后若要求填写个人账户信息的，坚决拒绝。警惕商户或出租车费支付、共享单车或共享充电宝租借等张贴在公共区域的二维码，扫描前检查是否有被人替换、覆盖的痕迹，扫描后擦亮眼睛，看好商户信息或应用信息后再支付。使用付款二维码时，不要将付款码暴露给身边的陌生人，防止不法分子利用“小额免密”功能盗刷。

虚拟货币骗局

张先生用手机浏览网页时，无意中弹出的一个“XX云币”虚拟货币投资网站，详细介绍虚拟货币投资情况和收益报表，看到购买后每周都有收益，回报还不低，他就想试一下，随即添加该网站客服的微信号进行咨询。随后，张先生按照对方指引，用手机下载了该虚拟货币平台APP，并转账100元到该APP上提供的银行账户，租用了100元的矿机（用于赚取虚拟货币的计算机）。一个星期以后，他看到之前租用的100元矿机真的有收益进账，觉得可信，就继续租用了一种1000元的矿机试一下。大约一周后，张先生欣喜地发现自己在该网站平台APP的账户上又新增一笔数目可观的收益。这时，客服向他推送了“租用5000元矿机送200元话费”的“优惠活动”，尝到甜头的张先生决定放手一搏，租用了一批5000元的矿机，既能充话费，又能尽早赚够可以提现的收益。可张先生等了一整天，却始终不见赠送的话费到账，联系客服也迟迟没得到回复。张先生心生怀疑，再次用手机登录该网站平台APP，才发现APP已经无法登录，微信客服也已将他拉黑。意识到上当受骗的张先生，立即向公安机关报了案。

安全提示：

随着以比特币为代表的虚拟货币规模不断扩大，各种以“区块链”“虚拟货币”为噱头、打着“金融创新”技术旗号的骗局也层出不穷，如一些注册在境外的ICO项目、虚拟货币交易平台等，实际上只是“借新还旧”的庞氏骗局，其资金运转难以长期维系。对于此类非法集资诈骗，广大消费者要擦亮双眼，保持理性，强化风险防范意识，自觉抵制与代币发行及“虚拟货币”相关的非法金融活动，切勿盲目轻信天花乱坠的承诺，避免自身财产受到损失。

不幸被骗怎么办

- 及时致电发卡银行客服热线或直接前往银行网点向柜台报告欺诈交易，监控银行卡交易或冻结、止付银行卡账户。
- 对已发生损失或情况严重的，应及时向当地公安机关报案，配合公安机关或发卡银行做好调查取证工作。
- 仔细回想此次受骗过程中是否泄露了个人信息或密码、泄露了哪些信息，尽快阻断信息泄露渠道，并更换可能受到牵连的账户密码，避免损失扩大。

本页内容来源于人民银行《2021年金融网络安全宣传手册》

RIGHT BY YOU