

来源：安徽财经网

“规范金融科技创新，营造金融安全环境”，安徽省金融机构共同开展2020年国家网络安全宣传周线上活动，引导百姓关注个人金融信息保护，增强金融安全意识，提高防范网络诈骗能力，自觉抵制网上金融谣言和金融负能量，共建清朗网络空间，让金融发展更好地满足人民日益增长的美好生活需要。

保护个人金融信息

想要保护好个人金融信息，就要牢记四个“不”：个人的身份证、银行卡、网银U盾、手机等重要物件不外借；含有银行卡信息的交易凭条不乱丢；信用卡，特别是卡号、卡面上的3位或4位安全码、有效期等信息不能晒；各种不明链接以及来历不明的二维码不乱点乱扫，不在银行提供的官方渠道以外输入银行账号、密码，以防钓鱼网站窃取信息。

防范不法分子冒充公检法

犯罪分子花样层出不穷，诈骗手段五花八门。一些不法分子冒充公检法、银行人员，利用虚假案情恐吓并骗取公众的信任，诱骗公众汇款至所谓的“安全账户”，从而获取经济利益。对付这类诈骗，防范手段有三：一、办理电子银行卡签约后，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；二、不要轻信以任何名义和理由要求你办理电子银行或通过电子银行划转资金的来电或短信；三、不轻信任何借口的陌生电话、短信、邮件等。

警惕虚拟货币骗局

近日，一些不法分子打着“金融创新”“区块链”的旗号，通过发行所谓的“虚拟货币”“虚拟资产”“数字资产”等方式吸收资金，侵害公众合法权益。他们通过租用境外服务器搭建网站，声称获得了境外优质区块链项目投资额度，可以代为投资。这极有可能是诈骗活动。这些不法分子以空投糖果等为诱惑宣称币值只涨不跌，投资周期收益高风险低，实际是通过幕后操纵所谓的虚拟货币价格走势等手段非法牟取暴利。他们以“静态收益”和“动态收益”为诱惑吸引公众投入资金，并利用投资人发展人员加入，不断扩充资金池。这具有非法集资、传销、诈骗等违法行为特征。广大公众应树立正确的投资理念，切实提高风险意识，对发现的违法犯罪线索，积极向有关部门举报。

金融消费者密码管理

金融消费者密码管理应该注意哪些方面？首先，密码要既复杂又易记，尤其是涉及

资金交易的密码，要尽可能复杂，可以包含数字、字母、符号多个类型，但也要便于记忆。比如，出生地拼音首字母+父母的出生月日数字，或最喜欢的一本书书名首字母+共计章节数字等。密码最安全的保存方式是记在自己的脑海中，还要定期进行更换，如果怀疑有泄密可能，应该立即更换。其次，不要用易破解的密码，不要使用出生日期、门牌号码、手机号码、车牌号码、身份证号码等与个人信息相关度高以及简单数字排列等易被破解的密码。最后，不要与社交工具同密码，涉及资金交易类密码不要与邮箱、微博、微信等社交工具的密码相同。一些安全度较低的中小网站以及各类使用频繁的社交工具都容易成为攻击、盗取对象，犯罪分子通过用户名、密码比对，就有可能破解您的资金交易密码。

个人金融信息保护技术规范

2020年央行正式发布了《个人金融信息保护技术规范》，首次将个人金融信息按照敏感程度由高到低划分为C3、C2、C1三个类别。C3类别信息主要为用户鉴别信息，包括银行卡信息、各类账户登录、交易、查询密码及用户鉴别生物识别信息。C2类别信息主要包括各类账号、交易信息、账户余额、验证码、动态口令等，可以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。C1类别信息主要包括账户开行时间、机构、支付标记信息以及C2、C3类别信息中包含的其他个人金融信息。技术规范要求金融机构遵守：权责一致，目的明确，选择同意，最少够用，公开透明，确保安全，主体参与的原则。

网络安全，守护你我。公众在日常生活中要增强网络安全意识，筑牢网络安全的思想防线，时刻绷紧网络安全这根弦，让网络安全意识内化于心、外化于行。同时，广大网民要积极参与国家网络安全宣传周的各项活动，主动获取有关法律法规知识和网络安全知识，谨慎进行电子交易、网上支付等涉及经济利益的操作，防范个人信息泄露和财产损失。

网络空间成为继陆地、海洋、天空、太空之外的第五空间，虚拟空间和现实世界深度融合。提升网络安全水平，需要我们每个人从身边的点滴小事做起，维护网络安全人人有责。

汪文娟/整理