关于防范短信钓鱼诈骗的风险提示

中国银保监会

近日，一些不法分子通过群发短信，假冒多家银行名义发送服务信息，声称客户手机银行、银行卡、身份证等过期或失效，诱导客户点击短信中网站链接访问虚假手机银行系统,客户一旦受骗提供银行卡号或手机号、账户密码、短信验证码等信息，不法分子将迅速冒用客户身份进行转账，盗取银行卡内资金，使客户资金遭受损失。在此，**中国银保监会消费者权益保护局发布 2021 年第一期风险提示：**提醒消费者注意保护个人账户信息安全，从官方渠道办理手机银行或网上银行业务，谨防短信钓鱼诈骗侵害资金安全。

向消费者发送短信钓鱼链接是电信诈骗的常用手法之一。此次短信钓鱼诈骗在全国范围密集爆发，攻击目标和行为特征相对一致，受骗对象多为风险防范意识较弱、对手机银行或网上银行登录操作不熟悉的人群。此类诈骗一般是有组织的专业诈骗，目的主要是窃取消费者银行账户敏感信息或盗取账户资金。

中国银保监会消费者权益保护局提醒：广大消费者一定要对不明短信、不明网站链接和页面、不明手机 APP 提高警惕，尤其是在被要求提供个人银行账户敏感信息时，要多看多思，防范被诈骗风险。

一看短信是否真实。诈骗短信假冒银行名义会降低消费者警惕性。消费者在收到署名为银行发送的信息时，要注意辨别真假，尤其不能盲目相信异常号码发送的短信。消费者若不确定短信是否真实，可以到银行营业网点或向其官方客服咨询。

二看网站链接和页面是否为官方渠道。诈骗短信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。建议广大消费者登录手机银行或网上银行时从银行官方手机 APP 或网站等正规渠道进入，尽量不要点击第三方提供的网站链接操作，以免被不法分子诱骗。

三看对方索要信息是否为个人重要敏感信息。消费者的身份证号、银行卡号、账户密码、短信验证码、付款码等均为个人重要且敏感信息，当有第三方要求提供或输入上述信息时，需提高警惕。不轻易提供重要敏感信息给他人，不点击来路不明的网站链接，不随意在除银行官方渠道之外的网页填写重要敏感信息。如发现自己上当受骗，请立即联系银行冻结银行账户，保存证据，及时报警。

编辑：冀晓航