辽宁省消费者协会与中国人民银行沈阳分行日前联合发布风险提示，梳理信用卡使用过程中的五大骗术，提醒消费者引起注意。

一是变身银行官方号码发钓鱼网址。利用伪基站群发“假冒银行官方号码＋钓鱼网址”的短信占据很大比重。王女士收到由“95XXX”发来的“积分换礼品”信息，但被要求填写身份证号、信用卡卡号与密码。专家提醒，难以分辨时需致电相关银行信用卡官方热线核实。

二是冒充网店客服发钓鱼网址。利用消费者真实购物信息，冒充网店客服，致电称商品断货，需要提供信用卡卡号、有效期、CVV2码等信息“退款”，随后引诱消费者进入钓鱼网站填写。一旦泄露信息，信用卡很可能被盗刷。

三是在微信互动界面和“红包”嵌入钓鱼网站。不法分子在微信群中分发嵌入钓鱼网站的红包，或者在微信互动界面中嵌入钓鱼网址。例如，吴女士曾随手转发微信群里一条祝福页面并填写个人信息，后来频频收到信用卡消费短信。专家提醒，不能因为是熟人就点击不明来路的链接与“红包”。

四是“山寨”微信公众号推钓鱼网址。赵先生是某手机游戏的热心玩家，他在微信上搜索到某游戏的公众号添加关注，之后在界面购买了游戏套餐，输入了信用卡信息，结果发生了盗刷事件。

五是免费WIFI存陷阱。专家提示，尽量不要在公共场合连接来源不明的无密wifi，连接也不要有涉及支付类的操作。一旦中了木马病毒，应第一时间修改用户账户密码，立即解除所有网上支付绑定，联系信用卡发卡行。