2016年的元旦已过，新一波消费高峰也即将到来，随之而来的也会有不法分子的各类信用卡诈骗。对此，银行信用卡专家总结了2015年信用卡的一些诈骗手法，提醒大家在即将到来的年末节庆购物高峰中，一定要提高警惕。

骗术一：变身银行官方号码+伪基站 发送钓鱼网址

专家指出，通过手机和移动互联网实施的诈骗中，利用伪基站群发“假冒银行官方号码＋钓鱼网址”的短信依然占据很大比重。例如王女士曾收到由“95XXX”发来的“积分换礼品”信息，短信的内容大致是登录某网站可激活领取礼品，落款为“某某银行”。但细心的王女士却发现网站要求提供自己的身份证号、信用卡卡号与密码等，疑心这是个钓鱼链接，才没有再继续下去。

交通银行信用卡中心专家提醒，如遇到类似情况难辨真伪，可致电相关银行信用卡官方热线进行核实。

骗术二：冒充网店客服“退款”发送钓鱼网址

诈骗分子通过利用消费者的真实购物信息，充当网店客服致电客户，声称商品断货，需要客户提供信用卡卡号、有效期、CVV2码等信息进行“退款”，随后引诱消费者进入钓鱼网站填入上述信息。一旦消费者上当泄露信息，信用卡就很可能被盗刷。

据交通银行专家介绍，有些不法分子发现常规的诱骗已经不起作用，他们还会冒充老同学、老乡发送假相册，甚至冒充“小三”通过激将法诱骗用户点击链接，其诈骗实质依然是钓鱼网址。

骗术三：微信互动页面、微信“红包”嵌入钓鱼网址

很多不法分子会在微信互动界面中嵌入钓鱼网址，用户在点开链接的同时，其相关个人信息便被盗取。例如，有位吴女士曾随手转发了微信群里一条祝福页面并填写了个人信息，随后却频频收到信用卡消费短信，幸亏其及时联系银行冻结卡片，才避免了更大的损失。

此外，微信红包也被一些不法分子利用，这些人会潜藏在人数较多的微信群中，通过分发嵌入钓鱼网站的红包，来盗取用户的信息。专家提醒，消费者千万不能贪图小利，或因为是熟人就点击不明来路的链接与“红包”。

骗术四：开发“山寨”微信公众号或APP推送钓鱼网址

许多不法分子也采取了更为“高端”的诈骗手段——建立“山寨”的微信公众号或企业APP。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便添加关注，之后在优惠活动界面购买了游戏套餐产品，输入了信用卡信息，结果发生了盗刷事件。

恒丰银行有关人士提醒，在关注公众号的时候，一定要认真核对企业的公众号名称以及是否取得微信认证。在下载APP时，也要去正规网站下载，安装可靠的安全软件，并注意安装时软件是否试图获取敏感度较高的用户授权。

骗术五：免费wifi存陷阱勿扫不明二维码

银行信用卡专家提示，尽量不要在公共场合随意连接来源不明的无密码wifi，如果需要连接，也不要有涉及支付类的操作。若看到不明来源的扫二维码、填信息免费送礼品的活动，也不要贪图小便宜。一旦不慎中了木马病毒，应该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，从而确保信用卡安全。

骗术六：代办大额信用卡广告诱人 财产损失悄无声息

诈骗分子通过冒充银行的客服电话、聊天软件或网页等发布虚假办卡信息，号称可以办理高额度信用卡作饵。不法分子以“管理费”、“保证金”等各种名目不断收取高额费用，或以办卡需要提交“存款证明”做“流水账”，要求对方提供银行借记卡卡号以及该卡预留的手机号，暗中利用到手的信息将对方借记卡中的资产进行转移。

民生银行信用卡人士特别提醒，消费者切勿轻信他人能代办大额信用卡，一定不要听信任何非法渠道办理信用卡的宣传。信用卡应通过正规渠道办理，银行不会收取任何费用，更不会向客户索要密码等支付信息。