近期，诈骗盗刷案件有密集暴发之势，且诈骗手段一直在推陈出新。怎样防患于未然？只需“三步”，招行还原拆解诈骗手法，支招防骗技巧。

现象一：手机突然无法接听或拨出电话，查账发现资金丢失

第一步：不法分子通过非法渠道获取了持卡人银行卡信息，信息包括身份证件号码、银行卡卡号、密码和手机号等。

第二步：伪造一张持卡人身份证件后，会试图在移动运营商营业厅挂失补办了持卡人手机sim卡。目的是为了截获银行向持卡人手机发送的信息，包括短信验证码和账务变动通知等。

第三步：通过网上银行或手机银行将持卡人银行卡账户上的资金转出。

现象二：客户点击“银行”发送的短信链接，随后资金被盗

第一步：不法分子通过“伪基站”技术，模仿银行客服电话号码向持卡人发来短信，“提示”持卡人积分兑换现金、手机银行升级或过期等，然后附上“积分兑换”、“升级”的链接。

第二步：持卡人信以为真，点击链接，结果进入了不法分子伪装的钓鱼网站，该网站页面可能会与银行官网极为相似，页面也会引导持卡人一步步输入信息，比如身份证号、卡号、密码、手机号、验证码等信息。或者在短信链接嵌入木马病毒，持卡人一点击手机就中了病毒，该病毒可拦截银行向持卡人发送的各种短信（包括转账时的短信验证码和账务变动通知）。

第三步：通过网上银行或手机银行，将持卡人银行卡上的资金转出。

在这个互联网极其便捷的时代，网络欺诈的手段也是防不胜防，一不小心个人信息就有可能被窃取，手机就可能会中木马。为了安心舒畅地在互联网上消费，招行工作人员建议：

1、收到银行专属客服热线相关短信存在疑问，无法辨别真假，不要做任何操作，请及时拨打银行客服电话进行确认（请注意：显示为银行客服热线发出的短信也有可能是伪基站所发）。

2、任何以“积分兑换、手机银行过期升级等”理由要求持卡人录入“银行卡信息”的短信都是诈骗行为，千万不要随意点击短信链接录入银行卡信息，请妥善保管卡号、密码、验证码等银行卡信息。

3、给自己的手机和电脑安装正规杀毒软件，并定期进行杀毒，勿轻信并点开手机收到的链接或图片。

4、通过正规渠道下载银行手机客户端，不要通过二维码、其他链接等方式下载。

5、资金转出时，银行都会校验银行卡的取款密码，因此特别提醒持卡人，取款密码不能和登录密码一样，也不能和其他银行卡、互联网用户、网上商城的密码一样。

6、如不慎落入骗局，请及时报警处理。

7. 请谨记银行官网和手机银行网址，谨防钓鱼网站以假乱真。

热门文章：

关注微信公众号深卡网卡达人（ ），每日提供信用卡知识、提额技巧、用卡攻略，让你火速晋升信用卡达人！