关于开展整治非法买卖银行卡信息专项行动的宣传系列三

随着我国银行卡业务交易数量和金额的不断增长，银行卡信息也成为不法分子窥窃的目标。不法分子窃取银行卡信息进而盗取卡内资金的违法犯罪活动日益猖厥，对社会公众利益和金融体系安全造成了严重威胁。不法分子非法窃取银行卡信息主要途径很多，提醒我行客户注意。这些手法包括：通过电信网络手段窃取银行卡信息。主要是搭建免费 wifi“陷阱”，散播隐藏木马的图片、链接或恶意应用程序（APP），或者冒充亲朋好友、公检法、通讯运营商、银行和商户发送诈骗短信，诱使受害人点击短信中的诈骗链接登录钓鱼网站，输入银行卡信息等。

特此为大家介绍一些完全攻略，来保证我行客户的用卡安全。

（一） 保管好账号，密码。

1. 不要相信任何套取账号和密码的行为，也不要轻易向他人透露你的证件号码，账号，密码等。
2. 密码应尽量设置为数字，英文大小写字母的组合，不要用生日，姓名等容易被猜测的内容做密码。
3. 如果泄露了密码，应尽快办理补发或更换业务。

（二） 认清网站网址

网上购物时请到正规，知名的网上商户进行网上支付，交易时请确认地址栏里的网址是否正确。

（三） 确保计算机系统安全

1. 从银行官方网站下载安装网上银行，手机银行安全控件和客户端软件。
2. 设置 Windows 登录密码，Windows XP 以上系统请打开系统自带的防火墙，关闭远程登录功能。
3. 定期下载并安装最新的操作系统和浏览器安全补丁。
4. 安装防病毒软件和防火墙软件，并及时升级更新。

（四） 提升安全意识

1. 使用经国家权威机构认证的网银证书。
2. 开通短信口令时，务必确认接收短信的手机号码为本人手机号码。
3. 不要轻信手机接收到的中奖，贷款等短信，电话和非银行官方网站上的任何信息。
4. 不要轻信假公安,假警官，假法官，假检察官等以“安全账户”名义要求转账的电话欺诈。
5. 避免在公共场所或他人计算机上登录和使用网上银行。
6. 操作网银时建议不要浏览别的网站，有些网站的恶意代码可能会获取您电脑上的信息。
7. 建议对不同的电子支付方式分别设置合理的交易限额，每次交易都请仔细核对交易内容，确认无误后再进行操作。在交易未完成时不要中途离开交易终端，交易完成后应点击退出。
8. 定期检查核对网上银行交易记录。可以通过定制银行短信提醒服务和对账邮件，及时获得银行登录，余额变动，账户设置变更等信息提醒。