关于加强信息保护和支付安全、防范电信网络欺诈的风险提示（四）

大华银行（中国）有限公司（下称“我行”）非常重视客户的财产安全及合法权益，应中国人民银行办公厅要求，为进一步加强落实《中国人民银行关于加强支付结算管理 防范电信网络新型违法犯罪有关事项的通知》、《中国人民银行关于开展整治非法买卖银行卡信息专项行动的通知》及《中国人民银行关于进一步加强银行卡风险管理的通知》的要求，现就相关风险提示提请您认真阅读并引起重视。

1. 何为网络电信诈骗

网络电信诈骗指不法分子通过网络、电话、短信等方式，编造虚假信息、设置骗局、对受害人实施远程、非接触式诈骗，诱使受害人给不法分子转账的违法行为

2. 网络电信诈骗的形式（包括但不仅限于下列形式）

1）虚构子女绑架，利用电话录音（如孩子的哭声）造成家人恐慌，要求家人汇款赎人
2）冒充亲友，以车祸、生病、违法需交纳款项等为由实施诈骗
3）冒充电信局人员，以电话欠费等名义实施诈骗
4）冒充公、检、法、司等国家机关人员以事主涉嫌洗钱、诈骗等犯罪活动为由实施诈骗
5）冒充税务局人员，以退税为由要求事主到银行 ATM 上操作，并诱骗事主使用英文模式操作，实施诈骗
6）谎称事主中奖，要求事主交纳个人所得税、服务费和手续费等实施诈骗
7）发送短信称事主的银行卡在异地刷卡消费，待事主回电时，不法分子假冒银行工作人员实施诈骗
8）通过短信发送银行账号及“速汇款”等信息，行骗碰巧要汇款的事主
9）在互联网上发布帮助挑选或购买股票等信息，骗事主汇款
10） 发布虚假中奖信息，事主上网时会发现 QQ 或邮件中奖信息，但必须先交纳手续费、个人所得税等，不法分子以此骗取事主汇款

3. 网上支付安全隐患

1）确保进行网上支付的电脑安全可靠。不在网吧等公共场所的公用电脑和公用有线 /无线网络上进行网上支付，以免个人信息及账户信息被盗用
2）选择安全、合法、真实的商户网站，不在来历不明的网站上交易和支付
3）在网上支付时，确认连接的是银行真实网上支付页面，以免在虚假连接上支付造成资金损失

4. 消费者安全支付习惯的培养与普及

1）牢记银行门户网站的网址，选择安全登录方式。登录银行网上银行时，应采取直接在浏览器地址栏输入网址登录或通过银行安全证书等银行提供的安全渠道登录，严禁通过其他网站或邮件提供的链接方式间接登录，防止不法分子伪造银行网站骗取消费者卡号、密码等账户信息

2）确保登录网上银行的电脑安全可靠。消费者应定期更新杀毒软件，及时下载补丁程序；不打开来历不明的程序、链接、邮件；不在网吧等公共场所使用网络支付

3）以“不易被猜中”的原则设置相关网银密码、支付密码。避免使用生日、电话号码等于个人信息相关联、容易被猜中的密码，应为电子银行设置区别于其他场合的专属密码，以免因其他密码失窃而造成网银密码泄露，特别是不能与电子邮箱、QQ、网络会员用户等使用相同密码

4）不向任何人透露网银证书保护密码、登录密码及账户支付密码等消费者自设密码，并注意以下几点：

a) 银行不会也不能向消费者索要密码，不会也不得通过任何形式要求消费者转出账户资金
b) 不轻信不明电子邮件、电话和短信，不亲信任何通过电子邮件、电话、短信、微信等方式索要账户和密码或要求转账汇款的行为，若有疑问可拨打相关银行客户电话或到银行柜台咨询
c) 不在不明网站输入银行账号、密码等个人资料，以免被钓鱼网站或网络木马等软件窃取
d) 妥善保管和正确使用银行提供的 USBKey、动态口令卡、动态口令牌等安全工具，切勿交给他人保管。各家银行赋予 USBKey 的名称可能不同，如 K 宝、U 盾、E 令、网银盾等，但实质是相同的

5）在使用网上银行或进行网上支付时养成以下良好习惯：

a) 访问银行网站时直接输入网址登录（通过原已加入“收藏夹”的方式登录时，需再留意一下显示的网址正确与否）
b) 登录网银后，应首先查看欢迎界面上的“上次登录时间”、“已登录次数”、“预留验证信息”、“头像”等信息（具体信息数量各银行有所不同）和实际情况是否相符，发现异常情况的应立即停止交易并及时与银行联系
c) 结束交易后，应通过点击网银页面设有的专用“安全退出”按钮退出网银系统，然后关闭浏览器（即关闭所有已打开的网页），并及时拔出 USBKey 或关闭相关安全工具