个人网上银行使用指南与安全提示

一、个人网上银行使用指南

感谢您选择开通我行个人网上银行服务。您可通过您的网银用户名、登录密码和动态令牌登录并使用我行个人网上银行。如个人网上银行的功能及服务有任何调整，我行将会通过官方网站发布公告，敬请您关注我行官方网站相关公告信息。

1. 如何完成个人网上银行的首次登录？

如您已开通我行个人网上银行服务并获得动态令牌，请按以下流程完成个人网上银行的首次登录：

1) 建议您使用 Microsoft Edge 浏览器登录我行官方网站（www.ocbc.com.cn），在首页右侧下拉框中选择“个人网上银行”，您可以自由选择线路切换，并点击“登录”；
2) 在个人网上银行登录页，按页面提示依次输入网银用户名、初始密码、页面验证码（如需），并点击“登录”；
3) 请按新弹出的页面提示通过动态令牌获取并输入 6 位数字的动态口令，并点击“确定”；
4) 进入《电子银行服务条款与条件（适用于个人客户）》、《个人信息处理告知及授权书》、《敏感个人信息处理单独同意授权书》和《向境外提供个人信息单独同意授权书》页面，请认真阅读并核对页面最下方的手机号码，确认无误后，请勾选确认，并点击“同意”；进入修改个人网上银行登录密码页面，请按页面提示输入初始密码、新密码、确认新密码，并点击“获取动态口令”；
5) 请按新弹出的页面提示通过动态令牌获取并输入 6 位数字的动态密码，并点击“确定”；
6) 动态密码将自动显示在个人网上银行登录密码修改页面，点击“确定”，页面提示密码修改成功，即完成首次登录。

2. 使用个人网上银行初始密码时要注意什么？

1) 您在我行营业网点成功开通个人网上银行时，可设置您的个人网上银行初始密码。
2) 该密码自签发之日起 15 天内有效。请您及时登录个人网上银行，设置新的网银登录密码。如逾期未使用可通过个人网上银行重置密码或持有效身份证件亲临我行任一个人银行服务网点申请重置密码。

3. 使用个人网上银行动态令牌时要注意什么？

如果您在使用个人网上银行动态令牌过程中有疑问，请您登录我行官方网站（www.ocbc.com.cn），在首页右侧电子银行登录下拉框中点击“个人网上银行”进入个人网上银行登录页，然后通过点击登录页面左下方“动态令牌使用指南”获得帮助。如个人网上银行登录页无法打开，可在首页右侧电子银行登录下拉框中点击“个人网上银行”下方的“线路切换”进入登录页。

4. 个人网上银行提供哪些服务？

您可以：

1) 浏览您的账户信息
2) 进行转账交易
3) 开立定期存款、通知存款
4) 购买结构性存款产品
5) 进行基金交易（代销国内基金产品及自营 QDII 产品）
6) 购买、赎回代销理财产品
7) 购买、赎回结构性票据产品
8) 查询贷款信息、预约领取文件
9) 浏览或更新您的个人信息
10) 获取各类通知
11) 了解我们最新的产品与服务

5. 如您在操作中遇到问题，如何联系我们？

请拨打我行全国统一服务热线进行咨询：40089 40089（中国内地）；+86 755 2583 3688（港澳台地区及海外）。人工服务接听时间为 7:30 至 22:00。

二、个人网上银行安全提示

为了保护您的资金安全，我行致力于为您提供安全的网上银行服务，并不断提升网上银行系统的安全性。我行对所有网上银行交易信息进行终端到终端的加密，也就是说数据将从客户端就会被加密，到银行端才会被解密，其传输过程处于全程加密保护之下。

客户必须保证客户终端和用户信息的安全，才能安全地使用网上银行服务。客户终端如果被植入了恶意程序，仍然存在交易信息被篡改的风险，相应的资金盗划风险将由客户承担。所以请务必注意客户终端和用户信息的安全保护。

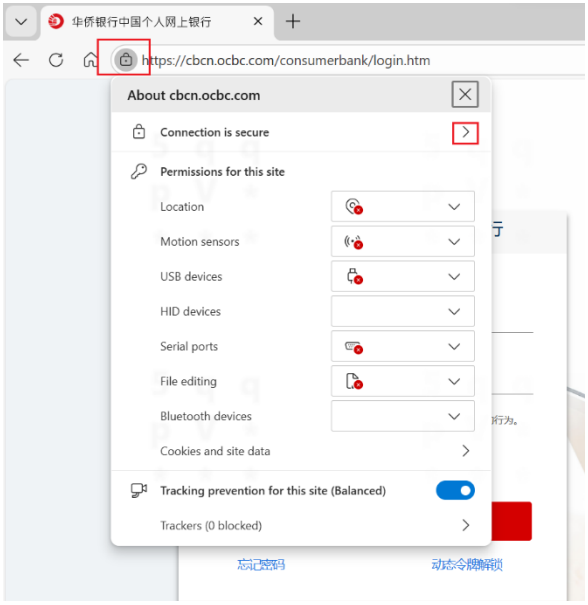
以下安全提示仅作参考之用，我行无法对该等网络安全相关提示的准确性与完整性负责。具体请向信息安全

专家咨询。

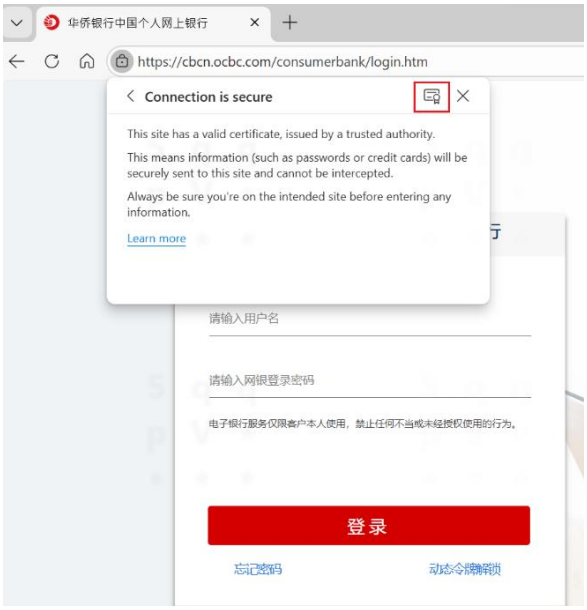
1. 确保您进入的是我行官方网站

图谋网络钓鱼的非法假冒网站常常冒用银行的徽标、图片、设计风格，仅凭网页本身往往难以识别。建议通过以下方法识别：

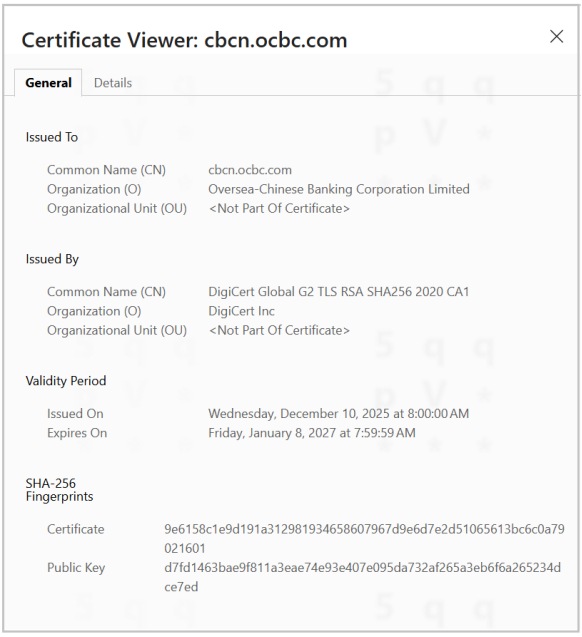
1) 确认网站地址：www.ocbc.com.cn；点击官网首页右侧电子银行登录下拉框中的“个人网上银行”进入个人网上银行登录页
2) 验证网站的 SSL 证书，步骤如下：
   - 单击地址栏旁边的“挂锁”图标，点击“Connection is secure”右侧的“>”



   - 点击“查看证书”图标



   - 验证该证书是颁发给域名“cbcn.ocbc.com”
   - 验证该证书由“DigiCert”颁发



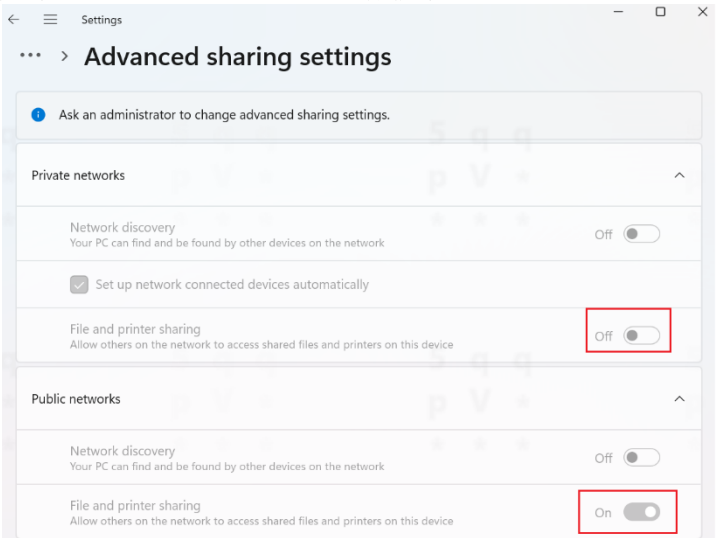
2. 关于网站证书的警告或错误提示

当您遇到网站证书相关警告或错误提示时，应该如何做：

1) SSL（安全套接层）及其升级版 TLS（传输层安全）是为网络通信提供安全及数据完整性的一种安全协议，在网上银行服务中是用于银行服务器和客户浏览器之间安全加密的技术。这种连接能够确保，通过银行网络服务器和浏览器之间所有的数据保持保密和安全。SSL/TLS 是一个行业标准，被银行用于保护我们和我们客户间的网上交易。
2) 这种安全连接以证书的形式分配一个加密密钥。如果您在登录网上银行系统时，遇到任何证书警告或证书错误的相关提示信息，请立刻注销并通知银行。
3) 我行致力于为客户提供最高级别的安全保护，请确保您的电脑支持 TLS1.2 传输层安全协议，否则将无法正常登录网上银行。

3. 保护您的电脑

1) 安装防病毒、反间谍和防火墙软件，保护您的个人电脑，防止黑客攻击、病毒攻击和其他恶意程序如“特洛伊木马”的攻击。当您的电脑是通过宽带、数字用户线或电缆调制解调器连接时，特别容易受到攻击。安装这些安全软件将预防和发现对您电脑未经授权的访问。
2) 禁用操作系统中的“文件和打印机网络共享”功能，可以防止外部对您的计算机进行非法控制和侵入。这个功能可以通过以下操作被禁用：选择控制面板中的“网络和共享中心”，点击左侧“更改高级共享设置”，将所有的“文件和打印机共享”设置为“关闭”，点击“保存修改”。



3) 不要使用公共/共享个人电脑(如网吧的电脑)，登录您的网上银行或执行任何金融交易。
4) 在不清楚网站信誉的情况下不要下载任何程序。
5) 可疑的病毒可能会通过附件的形式连接到邮件中，所以不要打开来自不明发件人的电子邮件中的附件。
6) 定期使用安全补丁或下载最新版本来更新您的防病毒、反间谍和防火墙产品。
7) 删除文件和共享在您的电脑打印机的信息，尤其是当您通过电缆调制解调器、宽带连接或其他类似的设置窗口进入互联网时。
8) 考虑使用数据加密技术保护敏感的数据信息。
9) 不要安装或运行不明来源的任何程序。
10) 不要使用任何不信任的电脑和驱动（例如：拇指驱动、便携式驱动）。
11) 当您登录网上银行之后，如需暂时离开座位，请先安全退出。

4. 保护您的网银用户名及登录密码

1) 不要将您的网银用户名及登录密码透露给任何人。如果您怀疑有人获取了您的网银登录密码，请立即进行更改或通过个人网银登录页“忘记密码”交易进行自助重置。
2) 网银用户名和登录密码避免使用相同的数字或相同顺序的字母。
3) 避免和其他账号使用相同的密码，如：电子邮件密码、QQ 密码、手机密码等。
4) 在设置登录密码的时候请尽量同时使用大小写字母和数字，最好包含符号。
5) 避免使用容易识别的数字作为登录密码，如：电话号码和生日。
6) 经常使用“登录密码修改”功能对登录密码进行更改。
7) 记住您的登录密码，并且不要进行任何形式的物理纪录保留。如您忘记登录密码，请通过个人网银登录页“忘记密码”交易进行自助重置。
8) 检查并确认您的计算机浏览器不会存储您的登录密码。如果您使用的是 Microsoft Edge 浏览器，请确保浏览器的“自动完成”功能被禁止。
9) 银行工作人员绝对不会询问您的网银用户名及登录密码，如接到类似电话、短信或邮件询问您的密码信息，请不要回复。
10) 不要将您的网银账户交由客户经理代为操作购买我行产品。如果您在网银操作购买我行结构性存款、国内基金、QDII 等产品过程中，客户经理介入进行营销推介，需到柜面进行录音录像，然后再进行购买。
11) 经常清除电脑浏览器的缓存，以保证您的账户信息可以从系统记录中被永久地删除。
    - Microsoft Edge 浏览器清除缓存的方法，仅供参考：
      - 点击浏览器右上角三个点“…”图标；
      - 在弹出的菜单中选择并点击“清除浏览数据”选项；
      - 勾选需清除的项目；
      - 点击“立即清除”按钮。
    - Mozilla Firefox 浏览器清除缓存的方法，仅供参考：
      - 点击浏览器右上方的“工具”→“清空最近历史记录”，打开清除历史窗口；
      - “安排清除历史记录的时间”选择“全部”；
      - 点击“详细信息”，勾选“浏览、下载历史”、“表单&搜索历史”、“Cookies”、“高速缓存”和“活动的已登录会话”；
      - 点击“立即清除”即可。

5. 保护您的密码器（包括动态令牌和签约手机）

1) 不要将您的密码器转交任何人代为保管、使用或者篡改您的密码器。
2) 不要将您的密码器放置在不安全的场所。不使用时，应该妥善保管。
3) 不要将您的动态令牌序列号透露给任何人。
4) 不要将您的动态令牌生成的动态密码或手机动态密码（一次性密码）透露给任何人，也不要输入到除我行网上银行以外的其他任何系统。
5) 如果您遗失了您的密码器，请及时持本人有效身份证件亲临我行营业网点更换新的动态令牌，或拨打我行全国统一服务热线申请暂停网上银行服务。

6. 电子邮件和其他保护措施

1) 预防网上诈骗，请您留意以下几点：
    - 任何不明电子邮件地址；
    - 可能误导您进入网站或电子邮件地址的任何不明标识或者图片；
    - 在银行网站上或者其他金融机构的网站上出现的任何伪造的域名；
    - 任何伪造网站的链接；
    - 任何在电子邮件中出现的表格；
    - 或者误导您提供个人详细信息的其他任何方式，例如：您的网上银行用户名及登录密码、账户的取款密码、任何其他敏感信息；
    - 其他网络诈骗。
2) 永远不要通过任何电子邮件中的链接进入我行的网上银行。
3) 登录网上银行时，请通过您的浏览器敲击我行的域名（www.ocbc.com.cn）进入我行网站。请您采取必要的预防诈骗的措施并且不要通过任何其他链接间接进入我行网站。若有任何怀疑，请致电全国统一服务热线与我们取得联系。
4) 建议您定期删除垃圾邮件及任何不明来历的邮件。不要打开陌生人发给您的邮件。
5) 如果您发现或认为有任何针对您、银行其他客户、我行或者我行集团的欺诈性邮件、欺诈网站，请立即通过拨打我行全国统一服务热线与我行取得联系。

7. 如何防止“网络钓鱼”？

用于欺诈的网络钓鱼电子邮件往往使用与银行相似的网络域名、标识和图像，极易引起混淆。如果您收到了借银行之名，以安全升级目的来索取您账户信息的邮件，请千万不要回复。我们特别提醒我们的客户及其他社会人员，我行官方域名为 www.ocbc.com.cn，应该特别警惕与我行域名相近的任何网站。

如果您访问过任何此类网站或者收到任何指示您披露或提交关于您的银行账号、网银用户名、登录密码等敏感信息的电子邮件、短消息（SMS）或者未知发件人的即时消息（IM），不要予以回复，请立即致电我行全国统一服务热线通知我们。

我行不会以电子邮件、短消息（SMS）、即时消息（IM）等任何形式向客户要求提供其个人信息，不会指示客户进行具体的交易操作，不会提示客户进入任何非我行的网页。我行始终将保护您的信息安全作为我们的首要任务。

三、语言

个人网上银行使用指南与安全提示以中英文写就，若两份版本之间有冲突的，以中文版本为准。