**个人网上银行安全指引**

网上银行是近年来随着互联网的蓬勃发展而兴起的银行业务，它能够在任何时间、任何地点为客户提供完善、便捷的金融服务，因而被广大客户迅速接受。但是当您通过互联网享受便捷的金融服务时，若没有妥善的安全保护，就可能将某些薄弱环节暴露在互联网上，给犯罪分子提供了可趁之机。

浦发银行在发展网上银行业务时高度重视网上银行的安全性和可靠性，采用了国际先进的网络安全设备和安全策略来保证网上银行系统的安全性。但是网上银行的安全也需要您提高安全意识，养成良好的安全习惯，不给犯罪分子可趁之机。

为了保护您的账户和网上交易的安全，以下的建议会对您有所帮助：

**一、保管好您的数字证书和手机**

1）如何选择安全认证工具  
    数字证书和手机动态密码是确保您网上交易安全的重要手段，必须妥善保管。**我行建议您使用移动证书或动态密码**，并将查询密码和交易密码设置为不同的密码值。  
　　2）证书保管  
    您若使用移动证书（U-KEY）登录网上银行，**证书须下载到U-KEY中**，并妥善保管，不要随意交给他人使用。请**仅在需要使用时才将U-KEY插于电脑，完成交易后，请及时拔出。**您还可以选择启用动态密码保护。具体设置方法：登录网上银行后，选择“网银安全设置”--“通知手机修改”  
    如果您使用浏览器证书，请务必启用动态密码保护，并设置一个较小的动态密码启用金额（例如100元）。  
    动态密码设置方法：您登录网上银行后，选择“网银安全设置”--“通知手机修改” 。  
　　3）动态密码管理   
    开通网银时预留的接收动态密码的手机及手机号码须由您本人使用，不可转借他人。所收到的动态密码不可转发或告知他人，并在使用后及时删除。**任何泄漏动态密码的行为将对您的账户带来安全隐患。** 同时谨防手机病毒，不要随意访问手机网站、接收彩信或其他手机文件；接收的短信请及时删除；否则可能产生安全隐患。

**二、保护好您的密码**

您的查询密码、交易密码，任何时候不得泄露给他人（包括自称银行工作人员的任何人），否则将给您的账户带来安全隐患。不要使用相同数字、连续数字、生日、电话号码等作为密码，查询密码和各卡/折的交易密码均应设置为不同数值，并定期更改。  
    **如您不慎把密码告知他人，建议尽快办理银行卡挂失或销户重开，并向银行柜面人员了解安全措施。**

**三、提高警惕 谨防欺诈**

1）提防假网站   
    访问我行网站时请直接输入网址登录（http://ebank.spdb.com.cn或http://www.spdb.com.cn），不要在此域名以外的地址输入密码。尽量不要采用超级链接方式间接访问我行网站，并留意地址栏的域名变化。网上购物时需认清我行网站，通过查询密码验证，确认页面显示的客户号后，再行输入动态密码。  
    **严防他人通过钓鱼网站或虚假交易骗取动态密码**，输入动态密码前请检查短信中的收款账号、交易金额等信息，尤其应注意防范他人骗取动态密码，修改网银通知手机号码。强烈建议您将我行网站地址添加到浏览器的“收藏夹”中。  
　　2）认清银行短信通知号码 关注短信通知内容   
    我行的短信的通知号码为95528，请认清上述号码，谨防不法分子借用我行名义进行短信欺诈。  
    网银动态密码用户在进行转账、支付等关键交易时要留意交易过程中收到的动态密码短信，请检查短信中的收款账号、交易金额等提示信息是否与您的实际操作相符。  
　　3）防范欺诈邮件  
    不法分子可能发送电子邮件、聊天工具发送木马病毒到您的电脑上以窃取您的键盘输入，因此，来历不明电子邮件，陌生人通过聊天工具发送的文件、照片不要轻易打开。

**四、定期查看账户资金变动情况并关注约定支付类签约交易**

请注意如果您已设置约定支付（如约定汇款、超级网银主动借记等）规则，汇款或支付时将不再验证密码，已签约的约定交易将在您操作修改密码、换卡后仍签约生效。若您曾不慎将密码等信息泄露给他人致使他人曾经使用过您网上银行，建议您立即通过网上银行或我行柜面查询，是否有您不知晓但仍然生效的约定汇款、超级网银主动借记等签约记录，并尽快取消签约，或尽快办理银行卡挂失或销户重开。  
    **强烈建议您开通及时语短信通知服务，有助于您及时了解帐户变动情况。**

**五、关注您计算机的安全性**

1）定期下载安装最新的操作系统和浏览器安全程序或补丁。  
　　2）建议将您计算机中的hosts文件修改为只读。  
　　3）安装个人防火墙，以防止黑客入侵您的计算机。  
　　4）安装并及时更新杀毒软件。养成定期更新杀毒软件的习惯，防止新型病毒入侵。 此外，“中国金融认证中心（CFCA）”和“国家计算机病毒应急处理中心”联合推出了[**“网银病毒专杀工具”**](http://online1.jiangmin.com/KVOnline/wangyin/Jm_Wy_Kill.aspx%20)，可作为您提升计算机安全性的一个辅助手段。  
　　5）使用网上银行的电脑不作为资料、文件共享等类型的服务器。  
　　6）不要开启不明来历的电子邮件。   
　　7）不要随意点击MSN等实时通讯工具中传送的图片等文件。

**六、养成良好的安全习惯**

1）不要在网吧、图书馆等公用网络上使用网上银行，防止他人安装木马程序窃取您的卡号和密码。   
　　2）每次使用网上银行后，应点击“安全退出”按钮，及时退出网上银行。  
　　3）在其他渠道（如ATM取款、自助终端登录）进行交易时，注意密码输入的保护措施，防止他人通过录像等方式窃取到您的卡号和密码。  
　　4）切勿向他人透露您的账号、客户号、密码、证件号码等个人身份识别资料。  
　　5）不把卡号、密码、证件号码保存在电脑或电子邮箱中。   
　　6）在我行使用的密码，不要与您在其他网站使用的密码相同。   
　　7）不使用自己及亲友的生日、电话号码、身份证号码中的数字作密码。   
　　8）查询密码、交易密码应设置为不同的，这样具有更高的安全性。   
　　9）遇到任何怀疑或问题，请及时拨打我行“95528”客户服务电话。