网络改变着我们的生活方式，也改变了金融服务的含义。网上银行因其全天候、低成本、功能全面、方便快捷等优点，越来越被广大用户所接受。然而近年来，一些不法分子通过假邮件、假网站、木马病毒，以及蓄意诈骗等欺诈手法，窃取用户个人信息，进而盗取客户账户资金，网上银行的安全性越来越受到用户的关注。在国内最早大力推广网银的招商银行，从“一网通”系统开发设计起，始终将网上银行业务的安全性放在首位，保持着在这一领域的同行业最先进水平。现在办理五彩优KEY，可享受五折优惠。5万元以上金卡客户，免费赠送。“目前在国内相比较而言，招商银行在网银安全方面做得最好，账号被盗案件也最少发生。”谈起招商银行的网银安全，不少业内人士如是说道。

晚报记者 倪子 通讯员 赵磊/文 晚报记者 赵楠/图

招商银行 八重防御打造网银安全

第一重 网上个人银行专业版
——网银安全避风港

据悉，招行的个人网上银行“一网通”分为大众版和专业版。大众版无需数字安全证书，也无需到柜台办理任何手续和缴纳任何费用。只要拥有招行的银行卡，用网页形式就能登录进行在线操作。但是大众版有一定的安全隐患，所以招行只为客户提供限于本人账户内的功能，包括账户信息查询、本人名下账户之间的转账、本人名下的基金和理财产品的购买等。

“与此相比，‘一网通’专业版的功能要强大得多，也拥有更高级别的安全系数。它采用证书+客户端程序的双重保护模式，安全性极高，可以担负现金交付外的绝大部分银行业务，满足客户更高端的需求。”该行的工作人员说，数字证书是专业版的安全性赖以成立的根基。专业版采取的X.509标准数字证书体系运用数字签名技术和基于证书的强加密通讯管道，确保客户身份认证和数据传输安全，已获得国际权威VERISIGN公司CA安全认证。

第二重 免驱动五彩“优KEY”
——网银安全守护神

专业版的数字证书分成文件数字证书和移动数字证书“优KEY”两种。客户申请文件证书时，会从柜台获得一份系统自动生成的授权码，凭此在电脑上登录并注册后，即会有一个“安全证书”保存在这台电脑上。“每次登录专业版，该软件都会对你的证书信息进行在线认证，以确保不是他人冒用。”该工作人员说，移动数字证书是一个外形类似U盘的便携式硬件。它可以使账户认证数据独立于电脑硬盘，降低了被盗风险。

在此基础上，招行又进一步升级推出了最新型的移动证书——五彩优KEY。“这是国内最早推出的免驱动移动数字证书。它可以在任何一台连接互联网的电脑上实现‘即插即用’，为使用专业版的客户免除了硬件驱动的麻烦。”该工作人员说，专业版还为用户提供专用的客户终端。使用专业版的客户必须从招行“一网通”网站上下载专业版软件进行安装。该终端的运行不依赖于web页面，可避免病毒和木马的攻击。登录时，终端软件还会强制客户关闭浏览器的远程终端选项才能启动。客户使用专业版进行理财、转账、缴费等业务操作，不必担心会被黑客远程攻击。

“如果不法分子想要利用‘一网通’专业版盗窃客户存款，必须知道该客户网上银行的登录密码，掌握安有证书的电脑或装载移动证书的优KEY，同时还要知道取款密码，这无疑大大增加了通过网银实施犯罪的难度。”该工作人员说，通过专业版的系统设置，客户可以选择对自己的交易实施基于互联网最高安全级别的保护。同时，使用专业版的客户还可以设置关闭大众版登录功能，以避免账户遭到不法份子通过大众版的互联网渠道的侵袭。

第三重 支付保护期
——新用户的安全岛

想体验招商银行网上支付的轻松方便吗？不必亲自到网点柜台申请，招商银行为客户提供的网上或人工电话就可以成功申请了。针对不熟悉网上银行操作、网络安全意识相对薄弱的新用户，招行在“一网通”大众版专门设置了一处“安全岛”——为大众版用户限定支付限额的保护期。通过大众版申请网上支付的用户，在一定的保护期内，每天可以进行的支付被自动控制在一定的额度之下。这一设置为新用户降低了无心之失带来的资金风险。

第四重 限额控制 ——账户资金防护墙

针对已对“一网通”网上银行有一定了解，开始使用专业版的用户，专业版系统赋予他们手动设置“每日交易限额”的权限。刚开通的专业版并不自动具备网上支付功能，需要客户手工开启。用户可以根据自身需求，设定一个每日允许支付的最高金额并随时自行更改。这项功能也能够在一定程度上保证客户的存款安全。

第五重 密码安全控件 ——账户密码铁将军

为了防止网络黑客通过木马程序窃取账户密码，招行的网上银行在所有密码输入区域都设置了密码安全控件。有了这道“铁将军”把门，数据交换的安全性大大提高，确保客户能够放心借助网络完成交易。

第六重 “一网通网盾”安全软件 ——虚假网站露原形

在当前层出不穷的网络欺诈手段中，钓鱼网站是比较常见的一种。“所谓‘钓鱼网站’，是指诈骗分子伪造一个跟真正银行网站很类似的页面，并使用极易与银行名称相混淆的域名。用户如搜索银行网站，一不小心就会误入上当。”招行的工作人员说，该类网站往往还模拟银行的客户服务邮箱给用户发邮件，声称“您的网上银行出现问题”，诱骗用户提供自己的账号和密码。针对此，招行专门开发出“火眼金睛”的“一网通网盾”软件。它能够自动识别针对招行网银的钓鱼网站和伪冒邮件，并及时进行风险提示或阻止在可疑网站提交账号密码，防止资料泄密。用户可随时登录招行主页下载安装这款软件，为网上银行树立一道反欺诈屏障。

第七重 动态验证码 ——网上冲浪无忧虑

为了及时维护网银用户交易安全，客户申请开通专业版，柜员即会要求客户预留手机号码。客户启用专业版后如进行证书备份和恢复的操作，招行即会实时发送“动态验证码”到该手机号码上，请客户通过网页提交该验证码进行身份验证，有效保证该操作确是由客户本人认可。同样的保护也存在于网上支付的相关操作中。对客户的网上支付，“一网通”大众版和专业版的系统都设置了一套风险评估的后台体系。该体系通过一系列技术策略、风险控制策略、客户保护策略，判断每笔支付的风险程度，并以此为依据，在交易超过一定的风控标准时发送动态验证码，向客户进行身份核查。

第八重 交易短信和邮件通知 ——账户变动及时通

短信邮件通知是另外一项增强网银安全系数的贴心设计。若账户发生大众版的网上支付交易或专业版的大额转账交易，招行都会以短信或邮件形式发送交易信息至客户预留的电话或邮箱上，以便客户及时了解账户变动情况，核对资金进出，反馈可疑交易。

八重安全措施，共同构成了“一网通”保护客户资金安全和交易畅通的铜墙铁壁。其实，在招行网银的安全体系中，这八重防御还只是客户能够直接感受到的一面。在客户接触体验不到的系统背后，招行的业务团队、IT团队为加强“一网通”网银的安全性，一直在付出巨大的努力。“为了准确无误地验证账户信息，招行的网银系统在用户的每次操作背后都要进行瞬时的大规模数据交换。为了在网上交易中保护客户资金不遭遇风险，招行在不断改进强化‘一网通’专业版的功能的同时，还与淘宝、腾讯等第三方支付平台以及公安部门通力合作，组建强大的监测团队，主动发现可疑交易并联系客户，为客户全方位打造资金流动的安全渠道。”该行相关负责人说，通过招行的不懈努力，“一网通”网银越来越体现出把握安全与便捷平衡点的出色性能。

相关链接

用户安全常识小贴士

网上银行作为一个新生事物，必然要经历不断完善的发展过程。鉴于网络环境的复杂，网银用户还是应当保持一定的警觉意识，正确使用网银服务，在尽情享受网上支付带来的便利和乐趣的同时，也要看好自己的钱包。招商银行郑州分行的工作人员提醒广大用户：安全使用网上银行关键是保护好银行账号和密码的信息，妥善保管账号和密码是安全使用网上银行业务的前提条件。

贴士一：严防网络黑手

坚决抵制任何通过电子邮件、短信、电话、弹出网页等方式索要账号、密码或身份证的行为。密码重置、修改电话以及跨行转账和账户冻结要求激活账户这类业务必须由客户自己通过银行柜面、电话或网站办理。

贴士二：勤装杀毒软件

为了防范木马病毒，要下载并安装由银行提供的用于保护客户端安全的控件，保护卡号和密码不被窃取。定期下载安装最新的操作系统和浏览器安全程序或补丁，打开Windows XP自带的防火墙，关闭远程功能。不要使用盗版反病毒软件和防火墙软件，须用正版相关软件，并及时升级更新。

贴士三：警惕上网安全

避免让太多人使用自己的个人电脑，长时间无人操作电脑时，中断网络连接或关机。安装网银软件的电脑不作为资料、文件共享等类型的服务器。网银文件证书不要备份在电脑硬盘或邮箱中，不要在网吧、图书馆等公共场所的电脑上使用网上银行。上网购物时要选择知名度较高的购物网站，如无意购买或只想试用，请不要留下个人资料。

贴士四：及时联系银行

如果手机、固定电话、Email等客户资料变更，应主动通知银行，确保发生紧急情况或安全隐患时银行能够及时联系到您。如果账户信息不小心泄露，要尽快通过银行客服电话、营业网点或网上银行办理修改密码或紧急挂失。为了维护账户安全，最好记住银行的客服信箱和正确网址。

答疑解问

1.“优KEY”会不会感染病毒？

“优KEY”是招商银行采用精尖加密技术，将网上个人银行专业版(下称“专业版”)数字证书信息存放在专用设备上的新型移动数字证书。“优KEY”提供了USB接口，必须插入电脑的USB接口才能使用，但并不是我们日常生活中所使用的U盘，并不会感染病毒。

2.黑客能绕开“优KEY”安全体系吗？

“优KEY”是招商银行采用精尖加密技术，将网上个人银行专业版(下称“专业版”)数字证书信息存放在专用设备上的新型移动数字证书，是招商银行网上个人银行的安全守护神。“优KEY”不会感染病毒，黑客也无法从“优KEY”中获取资料，请您放心使用。