

网上银行日趋流行安全革命悄然来临 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/232/2021_2022__E7_BD_91_E4_B8_8A_E9_93_B6_E8_c40_232986.htm 随着电子商务的迅速发展，网上银行的概念将在很长一段时间内影响金融和消费市场，各大网络支付平台迅速成为消费者追逐的对象。与此同时，一些不法分子也将网上银行作为作案目标，各种危害网上银行用户资金安全的案例频繁发生，让部分消费者对网上银行持有安全疑虑。不过，这种现状正在发生改变，网上银行掀起了安全革命。技术已不是安全障碍 网上银行在很长一段时间内处于不瘟不火的状态，其消费对象主要集中在从事B2C交易的商务人群。因为网上银行业务的高技术性、无纸化和瞬时性特点，决定了其经营风险要高于实体银行业务的风险，成为金融机构和广大客户最为关注的问题，而技术风险又是网上银行风险的核心内容，技术问题不解决就注定了网上银行业务难有大的作为，除了一批对网上交易有迫切要求的国际商务人士，一般的消费者对使用网上银行的概念并不接受。据业内人士解释，网上银行的技术问题主要包括交易主体的身份识别、交易过程的商业秘密、电子通讯的安全、交易和其它记录的保存和管理，特别是未经授权的中途拦截和篡改等，以及一些主观方面造成的安全技术隐患。这些问题如果不能有效的解决好，必然会造成损失、影响信用。随着中国金融认证中心推出了网上银行数字认证书，网上银行的理念开始为更多的人接受。中国金融认证中心作为独立于交易行为的第三方，与10多家银行、16家证券商、13家基金商建立业务联系，推出的CFCA网上银行数字证书，成为

避免网上银行被盗窃事件的一道防线。随后，各大银行为了确保技术安全又相继推出了一系列的保障形式，包括USBKey形式、动态密码等，这些安全保障措施对于防范木马、病毒、黑客以及假网站已足够，除非证书、账号、登录密码以及支付密码被同一个人窃取，可以说，目前各大银行的网上银行在技术上已经过关，记者了解到，相对于假网站，真正高级的欺骗手段是通过病毒程序盗取密码，国外的网上银行安全问题也大多是这类，对于这类事件的防范，使用专业版网上银行的数字证书或USBKey就可以解决。同时据艾瑞市场咨询分析，目前市场上所发生的网上银行安全事故很少是由于网上银行技术不够而带来的，技术问题已经不是网上银行安全的障碍，只要用户能加强安全防范意识，便可以放心使用网上银行。

网上银行反欺诈联动机制 在网上银行技术向好的趋势发展的情况下，各商业银行联合发起的《网上银行反欺诈联动机制》也同样值得关注。这个机制包括建立网上银行黑名单机制，有欺诈记录的不法分子、可疑的网站IP地址将被列入黑名单在银行间共享；建立网上银行案件资料库，对已经发生的案件进行整理并在银行间共享，帮助银行采取积极措施，防患于未然。与之配套的还有，建立银行间的不安全事件联动协查机制，通过建立银行间的联系人网络，第一时间协调各商业银行进行联动调查，减少用户损失，提高网上银行案件的追查效率。发布这个声明的十几家商业银行，其实都有各自的反欺诈应对策略，只是在信息共享上稍有逊色，这次发布联动机制是力图站在促进整个金融业发展的高度，加强对网上银行发展的统一管理，在安全技术、经营管理和数据处理等方面进行总体规划，建立统一的安全保障平

台，共同维护网上银行的资金安全。当然，从消费者的角度看，银行的这招管不管用，还有待时间的检验，但是各大银行能做出行动，还是能够给予消费者不少的期待。近期不断增加的网上银行交易数额正体现了消费者的态度。银行需承担相应责任 网上银行以其便利性和快捷性而受到消费者的欢迎，但由于安全事故的频繁发生，不少用户又对使用网上银行抱着观望态度，对这部分有试水意向的用户来说，网上银行用户资金被盗的案件一直是他们关注的焦点。近日，重庆市一起关于他人持假证件注册网上业务后，盗取一名储户12万元存款的案件经法院二审判决，判决结果是由农行赔偿储户存款12万元及利息。法院认为该行在办理网上银行业务时，未对相关证件进行必要的审查，仅凭虚假身份证及卡号即为他人注册了网上银行业务，违反了注册网上银行须持原始储蓄卡凭证的相关规定，导致他人直接从网上银行进行交易盗取了储蓄存款，为此农行应对被盗取的款项承担赔偿责任。在过去，网上银行的风险大多由用户来埋单，用户承担使用网上银行风险的惯例被再一次打破，业内人士认为，由银行失职造成的用户损失，银行具有不可推卸的责任，随着相关政策法规的完善，网上银行的用户一方和银行一方都会有明确的责限，按照法律，网上银行的安全风险会有公平科学的处理结果。100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com