Information Safety Problems and Prevention of Network Bank

Fang SHAO
Economics and Management School, Zhongyuan Industry University, Zhengzhou, China
Email: shao_fang@126.com

Abstract: With the rapid development and extensive application of the computer technique and the network communication technique, network bank provide clients with more and more complete and fast services at all times. But on the other hand, the information risk brings both bank and clients much security hidden trouble, even draw down financial risk. This article introduces the risks of network bank, and the measures of dealing with the risks.

Keywords: network bank; information safety; protection

网络银行信息安全问题与防范

邵　芳
中原工学院经济管理学院，郑州，中国，450007
Email: shao_fang@126.com

摘　要: 随着计算机及网络通信等新技术在银行业的广泛应用，网上银行为客户提供方便快捷服务的同时，由于信息风险，给银行与客户都带来了众多安全隐患，还由此引发了诸多金融风险。本文介绍了网上银行的几个风险点，并针对风险介绍了防范的措施。

关键词: 网络银行；信息安全；安全防范

1 引言

伴随着计算机技术和通讯技术的发展，电子信息技术日益渗透到社会生活的各个方面，深刻地改变着人们的工作方式与生产方式，银行业也开始步入网络银行时代。面对竞争日趋激烈的金融市场，国内外的多家银行为了扩大业务，在不同地段增设营业网点，这样可以增加用户，进而银行的效益也增加，而且在一定程度上方便了储户，扩大了银行知名度。但它也存在一些不利因素：增设网点的同时，租用楼宇的租金、购置设备和增加工作人员等加大了银行的投入，还要考虑到人们到银行储蓄的便利性和安全性等。因此，以互联网技术为核心的网络银行使银行业务发生了巨大变化[1]。

2 网络银行的产生与发展

网络银行在为金融企业的发展带来前所未有的商机的同时，也为众多用户带来了实实在在的方便。作为一种全新的银行客户服务渠道，客户可以不必亲自去银行办理业务，只要能够上网，无论在家里、办公室，还是旅途中，都能够每天 24 小时安全便捷地管理自己的资产，或者办理查询、转账、缴费等银行业务。据美国的一项调查资料显示，美国网络银行的开办费用一般只有传统银行的 1/12，传统银行的成本占收入的比例一般为 60%，而网络银行的这一比例只为 15--20%。美国商务部的统计结果显示，传统银行在营业点办理每笔业务的单位成本是 1.07 美元，而网络银行只需 0.1 美元，网络银行的巨大成本优势以及信息、时空优势使得网络银行的发展非常迅速，逐渐成为各大银行的重要业务办理渠道。网络银行可以大幅度降低交易成本，因此，发展网络银行业务是大势所趋。

根据国际权威机构对网络银行的表述，网络银行是指利用互联网作为其产品、服务和信息的业务渠道，向其零售和公司客户提供服务的银行（美联储对网络银行的定义)；通过电子信道，提供零售与小额产品服务的银行（巴塞尔银行监管委员会定义）；或指那些利用网络为通过使用计算机、电视、机顶盒及其它一些个人数字设备连接上网的消费者和中小企业提供银行产品服务的银行（欧洲银行标准委员会定义）。综

上所述，网络银行有两个特点，一是为客户提供金融服务，银行与用户通过互联网连接起来，在网上实现诸如查询余额、转帐、利率查询、电子货币、在线购物、订票、缴费等操作，使用户足不出户，也可以完成多种交易；二是其业务主要通过互联网络来完成。银行可以在拥有互联网的任何地方，于任何时间，为客户提供不间断金融服务，网上的交易和资金的划转非常方便、快捷，极大地减少了资金在途时间，提高了资金利用率。网络银行无需像传统银行那样设营业网点，无需柜面营业人员，大大降低了银行的运营成本，提高了工作效率，改善了服务，增强了银行的竞争力。

1995 年 10 月，美国花旗银行率先在因特网上设立站点，形成了网络银行的雏形。1996 年 6 月，美国的“安全第一网络银行”建立了全球第一家无任何分支机构的网络银行，开业短短几个月，就有近千万人次上网浏览，给金融界带来极大的震撼。随后各国都纷纷在网上开设银行。1996 年 2 月，中国银行在国际互联网上建立了主页，首先在 Internet 上发布信息，并于 1998 年 3 月 6 日成功办理了我国大陆第一笔国际互联网间的电子交易，从而拉开了中国大陆网络银行的序幕。我国目前已经有多家银行的多个分支机构拥有网址和主页，其中一些已开展了一定规模的实质性网络银行业务，客户数量也超过了电话银行和手机银行。截止 2006 年 12 月，我国网络银行用户数量达到了 7494.5 万户，网上交易总额达到 95 万亿元，网络银行交易笔数达到了 11.5 亿笔，预计未来五年内个人用户仍将较快增长。然而更重要的是，网络银行正在逐渐摆脱“一种离柜业务形式”的渠道身份，而转变成银行的一项业务，甚至是一个单独的产品。这不仅仅是网络银行本身的进步，也是中国的各大银行向真正的金融企业转变的折射。中国最早的网络银行业务仅为电子商务提供在线网络支付，而现在，包括查询、支付、外汇买卖等在内的传统业务几乎都被“移植”到了网上，业务品种涵盖个人银行业务和企业银行业务两大领域[2]。

网络银行的最终目标在于推出全方位的金融服务，存、取、贷款以及汇兑、代收等服务都在互联网上实现，乃至实现与其他金融机构连接的虚拟银行。它使得客户可以不受银行营业地点的限制，从而形成一个集银行帐户和银行自身于一体的全开放银行体系，促使社会向“无现金、无支票”方向发展。对于“信用重于一切”的银行来说，网络银行的信息安全尤为重要。

3 网络银行存在的信息安全问题

3.1 技术风险

3.1.1 网络自身安全隐患

目前，许多流行的操作系统均存在网络安全漏洞，网络安全协议也存在缺陷。此外，不少网络银行系统在防火墙的配置上不尽合理，无意识地扩大访问权限，从而被外部人员利用，获得作案的有用信息。

3.1.2 网络通讯的安全隐患

具体表现在：①电磁信号辐射容易出现网络信号泄漏现象，为那些技术高超、拥有先进设备的网络作案者提供可乘之机；②作案者采用主动或被动攻击方式，通过联接上网，盗取客户网上登录的信息、数据或密码，窃取资金；③银行网络专线发生故障而启用备份拨号线路时，由于电话号码保密不严，使不法分子伺机登录主网作案，给银行网络安全构成极大威胁。

3.1.3 操作系统、应用系统缺陷

使用了过期及没有“补”好的操作系统，用户自己开发的网上银行系统软件存在缺陷，或者委托公司开发的系统软件被人家留下缺陷或后门，这些都可能对网上银行系统带来不安全因素。

3.2 黑客攻击

黑客利用系统和网络漏洞技术日益提高，黑客工具的泛滥使黑客群体不断扩大，使黑客攻击变得越来越可怕。

3.2.1 地址欺骗

地址欺骗即犯罪分子伪装成合法网上银行网站欺骗用户进行交易，这种欺骗会造成很大的经济损失。犯罪分子冒用一个安全的、可信的银行网址，并发布相似的 Web 页面去欺骗用户输入身份及认证代号，便可获得机密信息。

3.2.2 网络监听

对网上银行最具威胁性的是监听一个客户与一个银行网站站点进行交易的 Internet 会话，黑客借机窃取客户信息。

3.2.3 拒绝服务攻击

拒绝服务攻击的危险性在于攻击者只需要很小的代价就能达到目的。它利用系统和网络之中某些程序的脆弱之处，使系统重要资源迅速饱和，导致网上银

978-1-935068-12-9 © 2010 SciRes.

行系统瘫痪，拒绝服务。

3.2.4 计算机病毒代码的攻击

目前，Internet 上计算机病毒相当泛滥，破坏性越来越大，严重影响网上银行系统安全。

3.3 操作风险

操作风险是指由于系统的可靠性、稳定性和安全性的重大缺陷而导致潜在损失的可能性。网络银行客户疏忽、缺乏网络安全知识可能会给自己和银行都带来损失。比如，客户在没有安全防护措施的场合使用信用卡号、银行账号等私人信息，就很容易被他人窃取而导致账号泄密。网络银行安全系统设计缺陷也会引起操作风险。随着计算机处理能力的增强和通讯手段的增多，网络银行客户地理位置更加分散，网络银行对客户进入其账户的授权管理相应也变得复杂。如果对客户进入账户没有明确授权或进入时授权过于繁琐，都可能导致客户蒙受经济损失，加大网络银行操作风险。对网上支付而言，网络银行安全的缺陷使客户很难辨认交易是否真实，从而产生对网络银行的怀疑，这种不信任往往构成网络银行另一种形式的操作风险[3]。

网络银行员工工作失职或缺乏职业道德，也会导致网络银行严重的操作风险，甚至危及网络银行的总体安全。比如，某些员工利用职务便利，有目的地获取客户私人资料，并使用客户账户进行买卖股票、炒外汇等风险投资，将交易风险直接转嫁到客户身上。

4 针对网上银行信息安全问题的防范措施

针对目前网上银行所存在的风险，银行和客户应积极采取相应的安全防范措施，增加网上银行的安全性，防范化解安全风险，促进网上银行业务的进一步发展。

4.1 银行方面

4.1.1 加强安全管理

网络银行对于客户是虚拟银行，但在网络银行的背后，需要一支管理水平一流，技术手段高超，具有高度责任心和使命感，勇于创新的队伍。搞好网络银行的安全工作，技术和管理要双管齐下。网络银行主管要高度重视安全工作，要认识到安全是网络银行的生命线。首先，必须根据本银行的实际情况，对系统做出风险评估，然后有针对性的制定完整有效的安全策略，根据安全策略，合理分配资金、人员、设备等资源。做好系统及网络的分权限管理，合理配置网络安全资源，最大限度地发挥其效能，建立网络漏洞扫描和入侵检测系统，努力做到事前及时发现问题、事后及时解决问题。对重要数据采取备份措施。要建立健全规章制度，并监督执行。定期对重点业务系统或设备进行安全检查，及时发现问题，堵塞漏洞。做好重要业务系统的安全审计工作，广泛宣传计算机安全的重要性，提高员工的安全意识，使员工充分认识到每个人都是网络银行安全体系里重要的组成部分，要有一荣俱荣、一损俱损的危机感，只有全体员工共同参与，网络银行的安全才有保障。

4.1.2 加固防火墙

Internet 防火墙技术目前已比较成熟，简单的防火墙技术可以在路由器上通过 IP 地址过滤直接实现。专用的 Internet 防火墙除了具有 IP 地址过滤以及克服了 Cp/Ip 协议缺陷的功能外，还具有许多其它功能，显然比路由器上实现防火墙更加可靠。在银行的网络中心或关键之处建立专用的防火墙，可有效地防止非法 IP 地址的计算机进入其业务网络系统。

4.1.3 增强操作系统的安全性

许多银行的操作系统以 ScOUNIX、WindowsNT、window:95/98 等为主，它们均存在一定的安全漏洞，并且越流行的操作系统(如 WindowsNT、Windows95/98)出现的问题越多。操作系统的安全性能对于整个应用系统的安全性至关重要，为增强系统安全性，银行应对现有各种操作系统应进行安全性增强和合理配置。

4.1.4 使用入侵检侧系统

利用防火墙技术，经过仔细的配置，通常能够在内外网之间提供安全的网络保护，降低网络安全风险。但是入侵者会利用防火墙背后可能敞开的后门，入侵者也可能就在防火墙内。入侵检测系统目的是提供实时的入侵检测以及采取相应的防护手段。它包括基于主机的入侵检测系统和基于网络的入侵检测系统两种。

4.1.5 使用安全扫描系统

安全扫描系统是现阶段最先进的系统安全评估技术，它能够测试和评价系统的安全性，并及时发现安全漏洞。安全扫描系统包括基于服务器的安全扫描系统和基于网络的安全扫描系统。

4.1.6 完善安全监控制度

加强网络管理和安全监控，及时记录和发现银行网络系统在运行过程中出现的各种问题，是保证银行网络系统安全运行的最重要的一个方面。目前银行网络系统中均有安全监控系统，能记录各种非正常操作，对这些安全监控记录的及时检查、分析，能使银行及早发现系统中大部分潜在的安全问题[4]。

4.2 用户方面

对于用户方面，为了网上银行的安全性，确保自己的信息不被窃取，账户上的钱款不被窃取，主要应从以下几个方面来进行防范：

4.2.1 妥善设置密码和保管账号及数字证书等

用户领到银行卡后应及时更换密码，并应经常修改密码，不宜用电话号码、生日等易于被破译的数字作密码，建议选用数字、字母混合密码，交易密码与信用卡密码尽量不同，身份证和银行卡也应分开存放。作废的存、取款凭条，银行的利息单，自动柜员机交易流水单等任何含有相关信息的凭证切忌随意丢弃。尽量避免在公用计算机上登陆网络银行，以防遗失账号，以及数字证书等机密资料落入不法分子之手，并定期查看网络银行办理的转账和支付等业务记录，或通过短信定制账户变动通知，随时掌握账户变动情况。

4.2.2 识破假冒银行网站

登陆网络银行的时候，用户应尽量避免使用搜索引擎或网络实名，以免假冒银行网站乘机而入。应从正规银行网点取得网上银行的网址并牢记。应留意核对所登陆的网址与协议书中的法定网址是否相符，以防止一些不法分子假冒银行网站骗取用户信息。另外，银行网站大多由专业部门管理，运行稳定，一般不会出现“系统维护”等提示。若遇重大事件，系统必须暂停服务，并提前公告客户。用户操作时如遇到“系统维护、升级”之类的提示，应立即拨打银行客户服务热线进行确认，以免被假冒网站所欺骗。如若不慎资料被盗，应立即修改相关交易密码或进行银行卡挂失。用户在使用网上银行提供的查询、转账付款、代理业务等自助金融服务时，如发现有异常情况，要随时向警方报警。

4.2.3 安装防病毒软件，堵住软件漏洞

为了防止木马等病毒程序感染电脑，窃取账号和密码等个人信息，用户在使用网上银行过程中，一定要加强防范意识，应在自己电脑上安装有隐私信息保护功能的“防火墙”软件，进行实时监控，安装防病毒软件，并及时加以升级。为防止不法分子利用软件漏洞进入计算机窃取资料，客户还要及时更新相关软件，下载补丁程序。

4.3 建立健全相关法律法规

4.3.1 建立网络银行法律监管体系

目前，我国网络银行许多监管规范仍停留在审批阶段，对于事后与事中的监管力度不够。因而，有关方面应及时修改、修订有关法律法规，将网络银行业务纳入其管理体系，做好网络银行的外部惩罚措施以及涉及网络银行的市场退出机制。

4.3.2 建立网络银行业务运营法律体系

这需要建立《电子银行法》、《电子签名法》、《电子资金划拨法》等法律法规，同时还应对已有法律法规进行充实、修改。

4.3.3 完善网络银行配套法律法规建设

主要有税收征管法、合同法、国际税收法、电子商务法、刑法、诉讼法、票据法、证券法、商业银行法、消费者权益保护法、反不正当竞争法等相关法律法规。

4.3.4 加强与国际立法、司法实践的交流与合作

通过合作与交流，加大打击网上洗钱、网上盗窃等电子犯罪的力度。

网络银行作为金融服务信息化最集中、最突出的表现形式，代表着银行业发展的未来，是大势之所趋。无论国际还是国内，网络银行都面临着不少亟待解决的问题。网络银行发展的关键就在于如何打破信息安全这个最大的瓶颈，在这个方面，需要充分运用先进的管理手段和科学技术，需要社会各界的通力配合，需要全体员工团结一心，共同努力，才能共创中国网络银行美好明天。

References (参考文献)

[1] Liu Hai, Yuan Zheng. Slove Projects of Electric Business and Network Bank, High-Technology & Industrialization. 2003(7):48-50
刘海，袁正. 电子商务与网络银行安全解决方案[J]. 高科技与产业化，2003(7): 48-50.

[2] Wang Hui. Analyse Risk which Our Network Bank face and Search Results. Finance and Accounting Monthly 2003(B1): P43-44.
汪卉. 析我国网络银行面临的风险与对策[J]. 财会月刊，2003(B1): 43-44.

[3] SET secure electronic transaction specification [DB/OL].http://www.setco.org/set-specifications.html.

[4] Schneier B. Applied Crytography Protocola, Algorithma and Surce Code in C. New York: Joho Wiley & Sono. Inc., 2004

978-1-935068-12-9 © 2010 SciRes.