网上银行安全防护指南

网上银行安全防护指南

网上银行又称网络银行、在线银行，是指银行利用 Internet 技术，通过 Internet 向客户提供开户、销户、查询、对帐、行内转帐、跨行转帐、信贷、网上证券、投资理财等传统服务项目，使客户可以足不出户就能够安全便捷地管理活期和定期存款、支票、信用卡及个人投资等。可以说，网上银行是在 Internet 上的虚拟银行柜台。虽然网上银行为大家提供了便利，但它也存在着许多安全风险，威胁着企业和用户的财产。本技术手册将向大家介绍常见的网上银行风险、网上银行安全评估与认证技巧以及网上银行安全技巧，帮助金融机构、企业和用户更好的了解网上银行安全。

网上银行风险

美国联邦调查局指出，最近网上银行诈骗以及非法自动票据电子转账的数量激增，到去年年底这种犯罪已经导致中小型企业损失近一亿美元，这确实让人吃惊不已。

- 网银欺诈成为银行业务流失的罪魁
- 手机银行风险及其规避措施
- 移动支付的应用风险
- Gartner 公司的 Avivah Litan 分析网上银行诈骗的增长态势

网上银行安全评估与认证

最近，根据公开的报告，五名窃贼被指控从美国加州卡森市的银行账户中偷窃了 45 万美元。 2007 年，他们成功地在该市财政局长的笔记本电脑中植入了变种的 Talex 银行木马，并截获了数字证书和账户信息。遗憾的是，这并不是一起孤立事件。许多小企业和

市政当局的电脑都正在被复杂的以银行账户和银行数字证书为目标的恶意软件感染，如Zeus、Clampi 和 Silon 等木马。

- 网上银行安全的评估工具
- 鉴定网银用户身份的最佳程序
- 确保网上银行安全的多重身份认证方案

网上银行安全技巧

当银行网站用户在登录的时候，会越来越频繁地被问及这样的问题：你在哪个城市出生？为什么会出现用户在输入用户名和密码之后不能查看账户信息的情况呢？这是因为银行使用了设备标识（device identification）来保证账户的安全，如果用户使用一台以前从来没有用过的电脑进行登录，那么银行会确认登录者是不是真正的账户主人。

- 保护网银安全：设备标识的工作原理
- 保护网银安全：设备标识应用的好处及缺陷
- 如何将网上交易的安全控制的价值传达出来
- 银行账户数据应该加入 PCI 安全要求吗？

网银欺诈成为银行业务流失的罪魁

根据调查显示，许多经受过网上银行欺诈或者其他欺诈遭遇的企业银行顾客倾向于更换银行。

根据一项针对美国中小企业的 533 名雇员的调查，40%遭受过欺诈的企业将他们部分或者全部的企业银行账户转移到其他银行。这其中 11%的企业与他们的银行彻底终结关系，29%的企业则将他们的主要账户转移至其他银行。

总部位于加州洛斯阿多斯的防止在线欺诈公司 Guardian Analytics 受 Ponemon Institute 的委托进行了这项调查。该公司的总裁兼 CEO 特里.奥斯丁表示，“当企业遭受欺诈或者未遂欺诈袭击后，他们倾向于以此为转折点，而决定是否继续留在这个银行。”

在《2010 年企业银行信用调查》中指出有超过一半（55%）的受访者在去年经历过欺诈攻击，其中 58%是在线攻击行为。

联邦政府官员们发出警告称去年针对中小企业的在线企业银行账户的攻击激增。FBI 估计针对中小企业的 ACH 欺诈案造成了大约 1 亿美元的损失。

根据调查，在 80%的欺诈案例中，银行未能在交易之前发现欺诈活动，同时有 87%的案例显示银行没能完全恢复被盗资产。57%的被调查者表示他们的损失没有得到完全赔偿。

67%的受访者表示他们的银行应该为保护他们的账户负最终责任，但只有 30%的人表示他们的银行具有很强的安全性。

“银行有很多机会可以做得更好”，奥斯汀说。

他表示，银行可以采取的方式是与他们的企业银行客户就安全策略问题进行更有效地沟通。24%的受访者认为他们的银行没有就保护企业账户免受欺诈的政策进行解释。

Hillary Machinery 公司是一家位于特科萨斯州 Plano、拥有 20 名员工的小企业。在去年下半年该公司遭受了在线银行欺诈，公司销售与市场副总裁特洛伊欧文表示，他们正在将其账户转移至另一家银行。在遭受网络攻击后，Hillary Machinery 公司被他的前银行、总部位于达拉斯的 PlainsCapital 银行起诉。这个极不寻常的案件最初由新闻记者 Brian Krebs 在他的博客中报道出来。

上个月，该公司以遭受网络抢劫为由反诉 PlainsCapital 银行，称犯罪分子从 Hillary Machinery 公司的一个商业户头上窃取了 80 多万美元，而银行方面追回了近 60 万美元。

“我们是一家十分健康的公司，这个事件没有打垮我们”，欧文针对这笔欺诈损失表示，“但是这迫使我们推迟了一些合作计划。”

他表示，安全是寻找下一个新银行的首要考虑因素。“在这一点上，我们深知要问什么问题”，他补充道。

大部分小企业都没有意识到针对消费者的在线银行保护策略并不适用于企业银行客户，欧文表示，“他们以为一旦当你将钱存入银行，它们就安全了”。

原文出处：http://www.searchsecurity.com.cn/showcontent_33239.htm

（作者：Marcia Savage　译者：叶蓬　来源：TechTarget 中国）

手机银行风险及其规避措施

手机银行以及其他金融服务的出现使用户能够联网支付帐单、查询帐户、转帐甚至进行股票交易。大多数手机银行服务都是通过短信、手机网页和下载到智能手机中的应用程序进行的。调查公司 TowerGroup 预测，到 2012 年，通过手机使用各种银行业务的人数将会达到一亿八千万。

众所周知，手机银行服务快速、便捷，而且发展迅速。但问题是：提供金融服务的公司能抵御手机银行带来的风险吗？这些风险很多与传统的网上银行存在的风险相似，比如网络钓鱼和间谍软件攻击，而与网上银行不同的风险则包括用户手机被盗等。

金融服务公司能否保证手机银行的数据安全，这是一个仁者见仁，智者见智的问题。美国 Gartner 咨询公司的副总裁兼知名分析师 Avivah Litan 表示：“银行和金融服务公司的安全部门的发展赶不上安全领域的发展。因为很多安全问题和欺诈检测技术并不适用于手机。”

Litan 还表示：“其中包括一些用于个人电脑浏览器的反欺诈方法，如地理定位、个人电脑指纹系统（通常用于操作系统和浏览器）等等。把这些方法共同应用起来就能使认证用户安全地进行交易。但是，目前手机银行只能通过用户名和密码来进行安全保障。”

不久前发生的花旗银行事件就是手机银行存在风险的一个例子：花旗银行透露，其用于美国地区的免费手机银行应用软件意外地将用户账号和其他一些敏感信息储存在用户手机上，最后花旗银行通过升级该应用软件才解决了这个问题。

谨慎部署以规避手机银行的风险

金融服务公司表示，由于手机平台的开发相对不够成熟，他们将采取适当的措施来保证用户以及帐户数据的安全。多数银行都谨慎地选择其所开通的服务。

Wells Fargo 银行互联网服务部主管网上欺诈防范和授权认证的执行副总裁 Teddy De Rivera 表示：“只有当我们能够很好的应对潜在风险时，银行才会开通这项服务。”这就是为什么人们现在可以在移动设备上支付已有账单，但不能在智能手机上设置新收款人的

原因。Rivera 补充到：“不法分子会伪装成收款人，除非用户举报，否则很难逮捕他们。”

保障的主管 Todd Inskeep 表示：“我们谨慎地选择能够使用手机银行的交互客户。这不仅是一个安全问题，也是一个客户选择的经验性问题。”

美洲银行的客户对 SiteKey 这个手机安全控制应用程序应该很熟悉。Inskeep 表示：“SiteKey 是一个附加的双因素认证，用于确保让用户知道当通过手机获得账户信息时，他们是在与银行打交道。”

欺诈检测和安全应用程序的发展

在手机银行服务中，银行也采用了其他的安全控制方法来区分欺诈交易。Rivera 解释道：“我们通过观察客户的交易记录来检测非正常交易。银行会根据该交易发生的时间与客户通常的消费时间间隔是否相同来给所有的交易评分。”

其他的防范措施还包括：不在手机上储存敏感的财务和账户信息，将储存在手机上的交易消息和数据进行加密，以及加强应用于移动设备的安全软件的开发。

美洲银行高级副总裁兼手机客户主管 Marc Warshawsky 表示：“我们提供的可供手机用户下载的应用程序都经过了大量的测试，当黑客入侵时这些软件可保证客户账户的保密性和安全性。”

即使银行做出了种种努力，不久前的花旗银行应用程序的失误和过去几十年来电子商务的发展历程都告诉我们，任何新的销售模式或者服务通道都会遇到一些问题，但由于手机用户数量众多，互联网接入途径广泛，手机银行面临着更多安全方面的挑战。

Litan 表示：“智能手机的发展带来的挑战是：银行不能期望所有的客户都使用最新、最好的手机操作系统。银行以后需要开发出普遍适用的应用软件，因为目前的手机安全技术不能满足所有的手机用户。”

原文出处：http://www.searchsecurity.com.cn/showcontent_39695.htm

（作者：George V. Hulme 译者：Sean 来源：TechTarget 中国）

移动支付的应用风险

移动付款被吹捧为最简单的、最方便的资金交换方式，通过移动付款几乎在任何地方都能以电子支付的方式进行购物和支付账单。用户只需单击一下移动设备的按钮或者在销售网点系统附近晃动一下移动设备，就可以进行购物或者支付账单。这对于购买者来说，支付和购物方便了很多；但是它却给提供这个服务的金融机构引入了很大的风险。

这不是移动银行业务第一次亮相了。几年前，在向电子货币和数字身份证转变的第二个革命性阶段就出现了移动付款的身影。那时移动付款业务的发展受到技术限制和高成本的困扰，不论是消费者还是服务提供商都面临这些方面的问题。无线应用协议（WAP1.0）的普及遭遇了很大的挫折，因为移动设备和移动业务服务提供商之间存在着巨大安全缺口，这一情况被叫做“WAP 缺口”。

今天，很多过去的技术限制和安全顾虑都已降低了，而移动付款业务利用这些技术上的进步又一次浮出了水面。其中一个重要的变化是 WAP 2.0 的使用，它允许在移动设备和服务提供商之间进行端到端的加密。

但是移动付款业务还是存在风险，金融机构采用移动付款程序之前，他们应该考虑以下几个关键的风险区域：

第三方供应商：移动付款服务提供商建立了一个机制，可以让用户把他们存在银行帐户或其它受监管的金融企业中的货币取出来。这些服务提供商是财务中间人，他们提供的服务被列为货币服务业务（MSBs）。货币服务业务提供商必须遵守与其合作的州内的法律。然而，不是所有的州都有监管 MSB 活动的法律，所以在选择的过程中应该仔细审查。如果你所在的财务公司决定使用 MSB 进行移动付款交易活动，那么请务必检查 MSB 提供商实际的信息安全情况，从而让自己放心。

监管和法律责任：美国现在几乎没有能够防止移动付款业务被滥用的安全措施。安全措施的规划和宣传指导方面几乎没有进步，传统的洗钱对策不能充分地处理因移动付款滥用引发的电子银行和无现金服务系统威胁。到现在为止，几乎没有任何基金会去研究和发展法律，从而执行现有的几个监管规则。金融机构必须让他们的法律团队和规则遵从团队制定使用移动付款系统的“交通规则（rules of the road）”。规则应该包括全面的 MSB

服务提供商实际安全情况审查，全面的支付卡行业数据安全标准(PCI DSS)的遵守情况审查，以及制定一个强有力的涵盖突发事件应对和责任的合同。另外，如果一个金融机构参加了政治活动团体，则一定要教育和告知团体的代表们，让他们清楚为客户开发相关法律和安全措施的必要性。

预防欺诈/损失的措施：金融机构必须能够监视和跟踪可疑的交易活动，这就要求交易活动对金融机构是透明的，以便于其收集情报。这有时候需要得到政府情报机关和政府执法机构的协助。不幸的是，这些组织在移动付款技术方面几乎没有专业的技能。很多国家在通过移动电话进行货币转移领域没有相关的法律和监管政策。移动电话网络有一些安全功能，可以阻止执法部门和情报服务部门检测可疑的非法交易。迅速发展的技术能力正超过政府追踪货币交易的能力，甚至会使金融机构不必再遵守美国爱国者法案（USA Patriot Act）和银行保密法（Bank Secrecy Act）。

由于无线环境中安全威胁的属性和数量的不确定性，金融机构应该对他们的移动付款系统实行独立的、阶段性的安全漏洞评估，评估的重点放在那些能够识别可疑交易活动或者可疑付款活动的检测系统和反馈系统，这项工作非常的关键。另外，金融机构必须命令他们的第三方付款服务提供商也要进行评估，以便于他们进行审查。这些评估应该在每一次大的环境条件改变时进行。移动付款欺诈处理程序应该有利于对检测到的威胁和滥用展开迅速调查以解除威胁。这将帮助执法部门和政府情报机构在必要的情况下对你的企业进行协助。

总体而言，虽然移动付款业务在电子付款的可行性和安全方面已经有了一些显著的改进，但对于金融机构来说，现在采用这个服务还是有几个大的风险。随着培训和安全措施的改进，以及技术在市场上变得司空见惯，一定会浮现出新的风险和威胁来挑战今天的安全改进。移动付款可以更快、更方便、障碍更少，但是这些对于攻击者来说也是如此。金融机构必须权衡风险和利益，然后决定现在时机是否适当，能否出手一搏。

原文出处：http://www.searchsecurity.com.cn/showcontent_28695.htm

（作者：Rick Lawhorn　译者：Sean 来源：TechTarget 中国）

Gartner 公司的 Avivah Litan 分析网上银行诈骗的增长态势

美国联邦调查局指出，最近网上银行诈骗以及非法自动票据电子转账的数量激增，到去年年底这种犯罪已经导致中小型企业损失近一亿美元，这确实让人吃惊不已。SearchFinancialSecurity.com 采访了 Avivah Litan（Gartner 公司的副总裁、著名分析师），听取了她对这种令人担忧的犯罪趋势的一些看法，以及她对银行应该怎样保护客户的账户信息的一些观点。Litan 是金融诈骗、认证、账号偷窃、诈骗检测和防护技术方面的专家。

对于网上银行攻击来说，最令人担忧的是什么，银行是怎么应对的？

Avivah Litan: 首先，这是非常真实的情况。过去几个月中，我所联系的银行都说他们发现过这种诈骗活动。你是从新闻中得知这种情况的，而我是听银行亲口说出来的，当时我便意识到欺诈已经非常普遍了。其次，那些不具有应对方案的银行被诈骗活动弄得措手不及。你不能临时抱佛脚。因此如果是小银行，他们会手动查看几乎所有的电子转账记录。很明显，大型机构不可能手动复查他们所有的电子转账记录，但是他们一般都有应对方案。于是，中小型机构反而更加猝不及防了。有些大型银行也会出现这种情况，但是对他们来说，更换系统对诈骗进行自动监测以及减少手动复查的数量比较容易。这和匪徒抢劫银行账户而银行无法应对不一样。一旦银行发现了诈骗活动，他们无疑会采取行动——有些靠手动，有些能自动进行。诈骗活动数量的增加说明罪犯的创造性永无止境，他们能轻松击败普通的安全控制技术，比如一次性的秘密标识等。这些攻击还告诉我们，任何通过浏览器传输的内容都是可疑的。你不能相信通过用户浏览器输入的任何内容，不管它是一个登陆凭证、强有力的认证密码，还是交易值——任何东西都可能被更换，都可能被别人截获。

在保护客户账户信息方面，有哪些最佳措施呢？

Litan: 银行真的需要进一步增强他们的防护措施，并使用更加高端的、可以监测整个交易活动（从登录到注销）的诈骗监测系统。因此银行监测的不应该仅仅是交易中的数值，还需要检查整个交易活动的过程。如果你正在监视交易的速度——即填写支付页面的时间或者装载网页的时间——那么通过查看交易反应时间和数据输入的次数，你差不多能够分辨出它到底是僵尸网络还是人工在进行操作。这种方法在银行使用的技术中还是比较

有效的，它们通过监视交易的速度来阻止这种类型的攻击。其他诈骗监测的方案是监测数值——即进入支付要求的密码。它们很有效，但是电子转账数据的结构化很差，所以诈骗者一般把犯罪活动放在交易评价字段（comments field）上面，这使得你必须要去分析一个优秀的诈骗监测系统中的文字。虽然没有任何一种诈骗监测系统是完美的，但是如果你采用了其中某些方案的话，就可以阻止大部分的攻击，至少能够标记出可疑的交易，以便手动复查，从而给很多客户省去麻烦——因为他们减少了错误的次数。

带外（out-of-band）认证在其中扮演什么角色？

Litan: 如果电话不被转接的话，它的作用很大。但是，诈骗者已经知道如何把电话转接到他们那里去的方法了。诈骗者会一直给携带手机的人打电话，说“我将离开城市或者我的电话坏在了家里，你能把所有这些电话转接到这个号码吗？”他们会告诉携带手机的人一个手机号码，然而人们也不验证给他们打电话的人的身份是否有问题就进行了转接。很多公司都使用 Authentify 来进行带外认证，它能够阻止在美国的电话转接（呼叫转移）。虽然这给使用电话转接功能（呼叫转移）的人带来了麻烦，但是那些人只需要给银行打电话就行了。

把基于标识（token）的认证作为攻击防御的方案效果如何？

Litan: 这些诈骗活动给我们敲响了警钟，任何通过浏览器的认证都能够被破解，任何通过浏览器进行的交易也能够被破解。诈骗者基本上可以超控（override）用户和银行能够看到的所有交易。比如说，一个用户想把 10000 美元转到账户 A，那么他们（罪犯）能够在这些钱到达银行之前就把这些钱转移到账户 B。他们还能做其他的事情：如果你用一次性密码进行登陆，他们就能够捕获那些密码。当你输入密码之后，他们会告诉你密码无效，然后说银行服务现在不可用并且不让你登陆。接着他们就用刚才捕获的那个一次性密码登陆。或者他们会让你登陆，但是会改变提交给银行的交易值。…我认为银行应该有一个强有力的认证标准，但是你必须意识到它照样能够被破解。

你如何看待金融服务信息共享和分析中心提出的建议：银行客户需要使用一个未接通因特网的、锁定了的 PC？

Litan: 银行最实用的方法是采用合适的防护措施。那些采用了适当防护措施的银行已经击退了这些攻击。这些银行虽然被攻击了，但是罪犯没有得逞。你可以依靠合适的技术、安全过程以及政策来解决这一问题。

九月份的时候，我曾经跟美国联邦存款保险公司（FDIC）讨论过网上银行诈骗数量上升的事情，他们建议银行需要对客户进行安全方面的培训。你认为诸如此类的客户培训在抵御网上银行诈骗中能起到什么作用呢？

Litan: 这种情况有点类似于一个客户进了银行，恰巧碰到有人抢劫，劫匪把客户打晕然后抢了钱，最后错误却在客户身上。既然银行开通了网上银行，那么他们就应该保护自己的渠道。我对客户培训不是很有信心，因为我认为这超出了客户所能做的范围。客户安装了最新版的杀毒软件，使用了最新版的防火墙，他们还能做什么别的吗？我认为这方面的监管规则有缺陷，并不符合 FFIEC 指导意见。FFIEC 说你必须能够控制相应的风险，而监管人员一直没有从这个角度对银行进行检查。过去他们没有发现商业银行会面临这种风险，但即便是现在风险出来后，他们也没有去跟银行说，“你们没有防御这种风险”，这是其一。其二就是他们没有任何的监管规则来保护商业账户。他们用规则 E（Regulation E）来保护消费者账户，但是却没有类似的规则来保护商业账户。我认为大多数小企业可能都不知道如果有人抢劫了他们的账户财产，银行不必进行赔偿。…监管人员正在试着绕过信用危机问题，但这并不意味着他们应该忽略诈骗这个问题。

未来又会出现什么样的威胁呢？

Litan: 由于越来越多的用户使用手机上网，我认为电话系统会遭受威胁。电话系统已经在受到威胁了——电话转接（罪犯进行的呼叫转移）。相对于对银行的攻击，我们将会看见更多对商业以及政府机构的攻击。罪犯另一种弄钱的办法就是进入支付系统的账户，然后改变受益人账户号码，以此制造虚假的支付。这种犯罪具有增长的趋势。

原文出处：http://www.searchsecurity.com.cn/showcontent_31290.htm

（作者：Marcia Savage　　译者：　Sean　　来源：TechTarget 中国）

网上银行安全的评估工具

最近，根据公开的报告，五名窃贼被指控从美国加州卡森市的银行账户中偷窃了 45 万美元。 2007 年，他们成功地在该市财政局长的笔记本电脑中植入了变种的 Talex 银行木马，并截获了数字证书和账户信息。遗憾的是，这并不是一起孤立事件。许多小企业和市政当局的电脑都正在被复杂的以银行账户和银行数字证书为目标的恶意软件感染，如 Zeus、Clampi 和 Silon 等木马。此类银行木马大多数是通过修改网页、插入新的对话框、篡改 Cookie 等手段感染用户的浏览器，比传统的中间人（man-in-the-middle）攻击更有威胁。为了应对这些威胁，许多商业和自由软件应运而生，确保用户能方便安全地连接到网上银行。让我们来探讨一下这些网上银行安全工具以及它们各自的优缺点。

位于纽约的 Trusteer 公司的 Rapport 软件可能是如今最出名的商业网上银行安全产品。金融机构在其网站上安装 Rapport 系统之后，用户可以下载并安装客户端软件，以此来保护浏览器和通过浏览器与金融网站进行的交互。该软件可在 Windows 和 Mac 系统下运行，通过监测应用程序编程接口（API）来确定是否有其他程序正在试图监控或操纵它们。例如，在 Windows 系统中，WinInet API 被用来建立 SSL 通信，它经常会遭到银行类恶意软件的访问和修改。通过防止恶意软件劫持和修改浏览器，Rapport 能防范 Zeus 等木马的最新的浏览器中间人（man-in-the-browser）攻击。此外，Rapport 是经常更新的，像杀毒软件一样，这使其能够帮助用户抵御恶意软件的最新变种。

使用像 Rapport 这样的软件（或者像英国 Prevx 公司提供的类似的网上银行安全方案 SafeOnline）的好处在于它们能够提供针对浏览器和终端的基本保护，最小化针对大多数终端的冲击，以及检测银行网站的负载能力。然而，许多银行并不想让这个软件成为强制性的，因为用户会觉得安全措施是被“强加”给他们的。此外，该软件需要安装代理才能使用，并可能需要本地管理员访问权限和浏览器的特权用户，以网络安全的实际角度来看这两者都是不可取的。攻击者也不会就此而止步——Zeus 木马和其他恶意软件的新版本已能够检测甚至阻止 Rapport 的某些版本以及其他一些保护性软件的运行。最后，某些保护软件还可能与其他程序或解决方案发生冲突，例如流行的共享软件 Sandboxie。

Sandboixe 或其他类似的软件系统，会在系统中创建一个保护性的独立空间（称为“沙箱”，sandbox）供所有指定的程序运行。如果浏览器是一个孤立的程序，那么即使

恶意软件被执行了，沙箱也能够防止其感染系统的其余部分。有一些系统用硬件来实现同样的功能，即运行自带的浏览工具和环境的 USB 设备。以加密便携硬盘而著名的 IronKey 公司，现在推出一款叫做“可信虚拟计算”的产品。该产品提供了直接在 USB 硬盘运行的虚拟操作系统和浏览器。除了独立的操作系统和浏览器外，该设备还具有内置的反恶意软件扫描和多参数 RSA 认证功能，以及在线更新以防范最新的威胁。这个工具的优点在于不必在主机上安装额外的软件，同时又能在访问金融网站期间更加有效的隔离浏览环境和主机系统。

另一种基于硬件的解决方案是 IBM 公司的区域信任信息通道（Zone Trusted Information Channel，ZTIC），它首先会与预配置的银行网站建立一个安全（SSL/TLS）会话，然后允许主机系统通过浏览器以类似于银行代理的方式进行连接。当用户访问银行网站并输入信息时，它将显示在 USB 设备的 LED 屏上，同时只有在用户手动点击设备上的按钮时，该信息才会传递给银行。这可以阻止浏览器中间人（man-in-the-browser）攻击者任意修改数据或站点信息而不被察觉的现象。不幸的是，这些基于硬件的解决方案需要用户在物理键盘上输入信息，而这很容易被按键记录功能所截获。

一个简单且免费的网银安全的选择是使用一个装有相关操作系统的可引导的 CD/DVD 光盘，只需运行一个被加载到内存中的只读操作系统即可。类似的操作系统发行版本有许多（通常包括 Knoppix、SLAX 和 Webconverger），这些光盘有时被称为“Live CD”。利用 Live CD 的好处是浏览环境与主机操作系统完全隔离，因为用户需要手动从 CD/DVD 启动并引导到只读环境。该操作环境在与银行进行会话期间不会被修改，会话完成后也没有任何信息保存，以防止丢失或者泄露机密数据。这种方案的缺点是需要从光盘启动到只读操作环境中，当然也就需要对用户进行培训。

随着越来越多的银行客户遭遇到由恶意软件所造成的金融诈骗，人们对这种网银安全工具的兴趣无疑会继续增加。这些解决方案各自都有明确的优点和缺点——从“软件安装”到“它们是否能真正隔离浏览环境与操作系统”。但不管怎样，成本始终是银行和终端客户在选择时应考虑的因素之一。

原文出处：http://www.searchsecurity.com.cn/showcontent_37433.htm

（作者：Dave Shackleford　　译者：Sean　来源：TechTarget 中国）

鉴定网银用户身份的最佳程序

基于无线传输和互联网的技术（比如移动银行、远程存取以及网上付款等）事实上已经成为21世纪银行关系（banking relationship）平台的标准：你可以在世界上的任何地方进行存/取款活动。传统的客户关系已经被新技术所替代，这让客户关系完全超出了物理银行（physical bank）的范围，而且没有回头路。这些新技术令人激动、更加有效，而且功能更强大，然而要通过跟这些技术相关的客户身份证明程序（CIP）来识别你的客户（KYC）却变得越来越复杂了。

KYC规则遵从以及CIP

KYC规则遵从的本质就是在企业中确立一个有效的客户识别程序，以此遵守反洗钱法规。一个客户可以是一个人、一个公司、合作伙伴、信托机构或者一个实体（estate），所以要使用合适的文档或者通过其他非文档形式的方法来验证或者识别他们。KYC就是要知道那些客户是谁以及他们跟一个金融机构之间的关系中包括哪些业务活动。

新技术跟旧CIP规则遵从过程并不一样

确认任何银行关系所需要的典型客户信息，包括名字、出生日期、地址以及税务识别码。下一步就是验证所提供的信息。根据关系类型不同，需要验证的可能是一系列范围很广的文档，从驾照、护照或者纳税申报单一直到公司文档或者水电费账单，等等。

问题是新技术以及相应的产品难以适用原来的或者传统的遵从程序。不管产品的情况是什么，一个机构都应该牢记客户以及他们的文档仍然是需要核实的。如果他们只是敲击了回车键并发送给你某些信息，这并不意味着真的就是他们本人。

举个例子，一个新客户可能会通过使用互联网的存款单活动（Certificates of Deposits（CD's）campaign）来访问你的机构。互联网有助于你超越地理位置的物理限制来开拓新市场，有助于企业的竞争，但是你怎么来验证这个客户呢？新技术以及新市场需要新方法来做这些事情，因此为了评估和减轻新操作环境带来的风险，人们需要采用新的步骤。

CIP 规则遵从的非文档（Non-documentary）方法

如果你没有原始的识别验证文档，那么你该怎么办呢？如果检查时无法获得原始文档，而客户又不在营业大厅或无法亲自到银行来，企业可以采用几种非文档技术来满足检查人员的需求，对他们而言也是可以接受的。

需要指出的是，企业选择任何一种方法来代替传统的验证方法都应该进行彻头彻尾的记录，还应该对风险评估进行升级，而且在实施之前这些程序都应该由高级管理人员以及董事会批准。非传统的方法依旧需要传统的审批过程。

非文档方法包括：

1. 通过其他的银行关系参考（存款或者贷款业务）对客户进行验证

2. 接收文档的扫描副本，但是随后通过查询公共记录来验证该机构，比如：
    a. 公司章程
    b. 良好的信誉证书
    c. UCC-1 文件

3. 访问信用报告信息并把它跟网上应用程序提供的信用报告信息相比较。建议包括：
    a. 目前的信用关系
    b. 目前以及以前的地址
    c. 现任以及前任的雇主

4. 获得雇主信息以及工资表建议（用收到的文件代替支票，以此当做直接存款的提示）

我的观点是，如果你仔细考虑了各个选项，并制定出一个依靠信用资源的验证方法，那么你仍然可以在网络环境中核实客户、公司或者业务是否存在。关键是确定所需要的信息，然后使用验证步骤来达到接收并检察原始文件相同的效果。

KYC 规则遵从的后续监视

银行环境全面电子化并不是一件坏事。相反，它给一个企业带来了全新的可能性。此外，当考虑或者使用互联网的时候，KYC 规则遵从并不太困难，但是会有很大的不同。当创建一个虚拟关系的时候，你还需要开发监视这个关系的方法。开始设计在线产品时，你

的设计还应该包括一个跟此技术相一致的监视部件。案例证明：在某起事件发生后，月终的批处理报告并不足以应对那些当日实时的业务。如果那时你才意识到出了问题，已为时太晚了。

充分考虑新技术的各种影响是你保护企业所能做的最好的事情，同时这样做还能够创建一个成功的 CIP 规则遵从框架，从而满足反洗钱法的规定。

原文出处：http://www.searchsecurity.com.cn/showcontent_32986.htm

（作者：Dan M. Fisher　译者：Sean　来源：TechTarget 中国）

确保网上银行安全的多重身份认证方案

2009 年夏天，法院首次开庭受理了印第安纳州花旗金融银行的一位客户的案件，该客户控告其网上银行保障措施中缺少足够的多重身份认证。这起案件的法官指出，在 2007 年该客户帐户被盗的时候，银行只提供了单重身份认证保护，这很明显违反了美国联邦金管会 FFIEC 2005 的规定，该规定指出金融机构要采取多重身份认证来确保网上银行的安全。

随着网上金融交易的增长，网上银行欺诈行为也逐渐增多，用户要求银行能够提供更高级别的保护措施，包括 FFIEC 要求的多重身份认证。把这些控制工作做到位，是减少金融数据盗窃以及虚假帐户活动的关键一步，这样做还可以让银行避免因网上欺诈而要担负的潜在赔偿责任。

按照多重身份认证的要求，在进行用户认证时，须同时提交下面的两个身份验证：一是你知道什么（比如密码）；二是你持有什么（比如一个动态的 PIN 码或令牌码），或者你个人独有什么（比如指纹）。让我们来看看几种银行已经实施的、比较常用的多身份认证系统，以及一些比较新的、确保网上银行安全以及符合 FFIEC 规则要求的选择。

其中，最常用的一种方法是使用传统的、带动态 PIN 生成器的硬件令牌（hardware token）。这些硬件令牌效果明显且容易扩展，但是部署困难，价格也很昂贵。对于许多大公司来说，这显然不是一个可行的方案。在某些情况下，金融机构倾向于使用“软件令牌（soft tokens）”，或者使用基于软件的 PIN 生成工具，用户能够进行下载然后安装在手机上。经过一个简单的注册过程以后，用户可以在他们的移动设备上生成 PIN 密码，其实质上把它们变成了个人的硬件令牌。这种方法性价比更高，而作为硬件令牌的替代方案，这种 “软件令牌”也迅速得到了人们的认可。

另外一种传统的办法是使用一次性密码(OTP)，有时也把它叫做交易认证数字（TAN）。在这种系统中，金融机构会发给每个用户一张特别的卡片，上面印有一次性密码或者密码短语列表。用户每次进行身份认证时，需要使用其中的一个密码或者短语（按顺序），然后把使用过的密码从表格中划掉。金融机构建立并维护着一个用户数据库及其相应的密码列表，还能追踪哪个 OTP 正在被使用。这个系统的性能很好，维护费用也不

贵，因为它只需要利用软件就可以使服务器端和用户端的密码列表同步。唯一的缺点是，当用户丢失他们的密码列表或者双方列表不同步的时候，维护成本会增加。

还有一种与此类似的系统是使用特殊的“宾果卡（bingo cards，类似填字图）”。这些卡片由 Entrust Inc. (IdentityGuard)和 TriCipher Inc.这样的公司提供，它们上面有一个网格，网格的一个轴上印有数字，另外一个轴上印有字母，在网格内部还印有一些数据。当用户要登陆银行应用程序时，首先需要输入用户名和密码，然后根据提示输入一系列在网格上的数据（举个例子，D2）进行认证。每个卡片都是独一无二的（像 OTP 一样），如果卡片丢失，进行替换也很方便，而且价格便宜。除了用户丢失卡片时不能提供技术支持外，这种系统几乎没有缺点。其他的系统能够生成 OTP，并且把它们通过带外(OOB)的方法（比如 SMS、电子邮件和电话等）发送给用户。

另外一种传统的、实施多重身份认证的另类方案是利用用户登陆时使用的电脑作为多认证的一个因素。通过在系统中放置一个已经成功注册的 cookie，用户就能通过输入用户名和密码进行登陆，通常还需要回答一些在注册时事先设定好的“个人”问题。当用户试图用不包含这些 cookie 的电脑进行登陆的时候，他们或者会被拒绝登陆，或者需要回答更多的、更严厉的、事先设定好的一系列问题才能通过认证。

基于 cookie 认证方案主要的问题是 cookie 容易损坏或者丢失。另外，如果 cookie 难以获得或者一个系统无法被识别的话，这种方案就会退化成一些安全系数不高的方案，需要用户回答一系列个人问题。大多数情况下，这些 cookie 是加密的，即使被人通过跨站点脚本攻击以及其他的方式获得的话，也没有多大的用处。

一些银行正倾向于使用另外一种技术，在普通多重身份认证方案的基础上添加一个新的认证因素：基于位置的因素。尽管在一定程度上跟“你持有什么”的方案相关，但是这个较新的双因素模型（有时也被称作设备指纹（device fingerprinting））依靠的是把地理位置的 IP 地址、ISP 连接以及其他位置信息跟提前设置好的用户总体信息联系起来。提供这个技术的厂商包括 41st Parameter Inc.、ThreatMetrix Inc.和 Iovation Inc 等公司。尽管这个方法越来越流行，但是因为大家对将它用于实际的多重身份认证方案还缺乏信心，所以它并没有被广泛采用。许多金融结构和用户认为，这个方法与其他的方法相比缺少移动性和灵活性，如果终端机器被恶意软件感染的话，安全还会受到威胁。

最后，我们将介绍另一种方法，尽管被金融机构使用的非常少：生物辨别系统（biometrics）。然而，由于高成本和维护的复杂性（包括需要给用户提供指纹阅读器或者类似的东西），这种方案在大规模部署操作时不太现实。

总而言之，银行和其他金融机构需要采取行动，实现安全的多重身份认证系统，这对保护用户的账户安全是至关重要的。市面上有许多不同的方案可供选择，即使最大的金融机构也能够添加额外的认证因素，从而验证使用网络银行和其他应用的用户是否合法。如果不采取这些措施，银行将面临因不遵守相关规定而被惩罚的风险，并需承担相应的赔偿责任，同时这还会使得消费者对他们的网上银行缺乏信心。

原文出处：http://www.searchsecurity.com.cn/showcontent_29598.htm

（作者：Dave Shackleford　译者：Sean　来源：TechTarget 中国）

保护网银安全：设备标识的工作原理

当银行网站用户在登录的时候，会越来越频繁地被问及这样的问题：你在哪个城市出生？为什么会出现用户在输入用户名和密码之后不能查看账户信息的情况呢？这是因为银行使用了设备标识（device identification）来保证账户的安全，如果用户使用一台以前从来没有用过的电脑进行登录，那么银行会确认登录者是不是真正的账户主人。

使用设备标识作为预防欺诈的策略是近来一种很不错的办法。由于网络罪犯的目标是网上信用卡交易、新账户的注册以及账户登录，金融机构如果想确认试图使用账户的人是否是用户本人，那么需要验证的已不仅仅是用户的 IP 地址和登录/密码了。

设备标识是怎样工作的？

设备标识是通过使用“设备指纹”来减少欺诈风险的：设备指纹即是一个设备标识符，它以用户系统的 IP 位置以及配置的方式为基础。这个指纹随着时间的推移会允许金融机构分配和跟踪“信誉值（reputation）”：即分配给用户系统的一个风险值，它取决于数字指纹数值，以及当这个设备不在终端用户手中时金融机构确定的风险值，这是一个从用户交易历史中提取的数值。

设备标识是按下面这些信息的哈希值（hashed value）为基础创建这个设备指纹的，但是并没有局限于这些数值：

- 地理位置属性——基于 IP 地址的物理位置数值（举个例子： IP 192.xxx.xxx.xxx =东欧）。λ
- 连接属性——连接是通过一个专用的网络连接（比如一个 Citrix 服务器）还是一个普通的因特网连接？λ
- 时间和时区属性——进行了多少次连接尝试，连接尝试之间的时间间隔又是多少？还有，连接尝试是在什么时候发生的（比如，最终用户所在时区的早上 2：00）？λ
- 网络路由属性——网络流量是怎样路由的（例如，通过不受信任的网络如中东——加勒比——美国东海岸）。λ

- 应用程序属性——应用程序如何访问网站（比如使用 SSL 或者没有安全性）。λ
- 操作系统属性——OS，浏览器，其他的系统标识符。λ
- 交易活动属性——正在进行什么类型的交易（比如，转账，购物等等）？λ
- TCP 协议属性——使用什么样的 TCP 协议访问目的系统（例如，HTTP, FTP,等等）？λ
- 信誉属性——先前赋给系统的值λ

当消费者登录到企业的客户端网站或者门户网站一段时间后，设备标识应用程序开始给每个用户生成一个信誉值。然后，设备标识应用程序会把这个信誉值跟预先设定的风险值相比较。举个例子，设备指纹值的有一个加权和，假设是 70，把这个数跟最小风险值进行比较，假设是 65。如果应用程序以它的指纹值为基础识别了用户的系统，用户可以继续操作。然而，如果应用程序不能识别系统，它就会假设系统没有通过认证，用户必须提供一系列有挑战性的问题的答案才能把设备添加到用户的系统上。如果用户不能正确回答这些问题，访问就会被拒绝。

原文出处：http://www.searchsecurity.com.cn/showcontent_30567.htm

（作者：Randall Gamby　译者：Sean　来源：TechTarget 中国）

保护网银安全：设备标识应用的好处及缺陷

设备标识的好处

多重身份认证（multifactor authentication）需要企业为用户分配昂贵的证书，之后用户才能获准使用公司的网络应用程序。与之不同的是，设备标识是一种确定性的、积极的认证技术，主要依靠已知的用户系统属性，同时允许用户可以继续使用相对便宜的用户名/密码认证。另外，把散列的设备属性集中起来比只使用单个属性更加有效，适合高端交易的办理。

设备标识应用程序最适用于有大量用户通过因特网访问敏感信息的企业。如果银行、网络零售商、信用卡发行商以及其他类似的公司可以不使用一系列用户名/密码证书就可以识别他们的用户，那么他们会节省一大笔成本。

在那些可能是欺诈的访问过程中，向用户询问一系列不难回答的问题（假设他或她是合法的用户），而不是禁用用户的账户，这种做法会提高企业的信誉，还会降低因忽视客户利益而带来的风险。另外，有些公司开始在他们的员工门户网站上使用这些应用程序，从而对远程员工的访问进行控制，让他们跟公司的政策和程序相符合。

设备标识潜在的缺陷

如果没有正确的配置，或者有些数值不能唯一识别系统，设备标识会变得效率低下。它可能会返回错误的否定——被检测设备是先前通过识别的设备，这次却没有被正确识别；或者错误的肯定——被检测的设备被认为是先前通过了识别的设备，但是这个设备以前没有登录过。

拿网上投资公司举例，错误的否定可能会导致高成本的欺诈。例如，不能正确辨别一个偷了用户身份信息的网络罪犯会造成严重的损失。罪犯如果能够全权访问用户的账户，他就可以购买股票和基金或者关闭账户并从用户投资中取走现金，把用户资金转移到自己的账户上。类似的，错误的肯定也会带来麻烦，比如把真正的用户当做了网络罪犯，这样的话由于可能的拒绝访问会对企业收入产生直接影响（比如客户想在市场关闭之前购买股

票），但是因为系统没有识别他的设备指纹而无法完成。这种类型的访问拒绝还会破坏企业的名声，尤其是当一个高级客户被拒绝时。

原文出处：http://www.searchsecurity.com.cn/showcontent_30568.htm

（作者：Randall Gamby　译者：Sean　来源：TechTarget 中国）

如何将网上交易的安全控制的价值传达出来

作为金融服务的安全专家，我们有时候会觉得自己像在做二手车的销售。我们除了不是在销售二手车外，和那些销售人员一样，都是在“强迫销售”，我们“销售“的是安全控制方面的金融服务，这些服务可以用来保护那些为公司盈利的交易。这个比喻非常恰当，因为商业人士的预算一般比较紧，他们不会特别想要买我们的产品，就算需要我们的产品，他们也宁愿用辛苦赚来的现金买其它的东西。

我不知道你的喜好，但是我最不喜欢的工作是销售方面的工作。我不喜欢试图说服别人去花钱买他们觉得没有价值的东西。这就是我为什么花了职业生涯的很大部分时间来寻找窍门，以此来使得我们工作少一些销售成分和更多地与商业保持一致。

事实证明，至少在电子交易的安全方面有了一个不错的解决方法。我意识到商业人士已经了解到交易安全的重要性，只是他们一时间很难将这个观念应用到网上交易。从意识到这个开始，我与客户之间的交流从先前的“强迫销售”转变成“自然”的业务。

实体交易安全比较

不相信我？那么想象零售商们在一天快要结束时，他们将现金取出，填写一张存款单，并将现金放在一个信封里。他们会将信封粘在当地银行的分行的前门上吗？不会，对吧？对所有人来说，他们为什么不这样做是显而易见的。因为如果那样的话，钱几乎肯定会在第二天早上不翼而飞。所以说，这个诀窍就在于打破了对所有人来说简单而显而易见的条件。

在上面的例子背后，隐藏着我们的客户和业务经理都能直观地了解的一组安全需求。客户了解这些需求是因为，就算是他们中最天真的，经常赞叹生活的美好的人都知道提着一袋钱到处晃悠是不明智的。业务人员了解这些需求是因为，他们知道鼓励客户承担风险就是在破坏我们在业务销售中的信誉。

所以当说到实体交易，我们的业务伙伴就已经知道安全控制重要的原因了。如果我们试图使用实体交易领域的这些规则来表示电子交易的技术控制中的规则，那么与客户之间的交流更像是对规则的翻译而不是销售。换一句话说，我们通过降低风险和提高可靠控制

的方法来构建电子交易，这种方法与人们进行过的实体交易类似，从而使得电子交易建立在人们理解的基础之上。

区分风险，选择控制

首先，罗列出与实体交易相似的风险并标注我们已经了解的风险，通过这种方式来区分风险。举个例子，如果你正在为一个经纪人业务建立一个订单输入系统，你的业务合作伙伴已经了解到认证在下订单的过程中的重要性。他们会在一个匿名的电话上要求清除某一客户的所有业务内容吗？或者他们会寻求客户端的确认吗？比较两者的相似点，这样可以解释为什么在系统中构建加强的认证系统非常关键。

其次，一旦你区分了风险，根据如何处理相同风险的方法来标注风险控制，再通过与实体交易类比方式来找到出路。举个例子，如果一个公司正在实施一个用于营业时间之后的电子存款系统，你指出一个所有人都能取的地方作为现金存放地点（就像把他们粘在前门上一样），那么你将被别人所嘲笑。所以，电子系统的控制应该以最小的代价来保护它们。而你应该描述一下文件传输系统是怎样如现金存款一样安全地进行电子存款。

如果你想说服一个企业使用你的电子交易保护服务，而他们已经在实体交易领域有了类似的保护服务，那么说服的过程就比较少地涉及到销售，而更多地是解释。

与业务伙伴在这方面进行交流使你变得更灵活。难道他们不能实施加密的通道是由于技术有限？也许他们可以实施其他的安全控制方法，从而达到同样的安全效果。一旦他们理解了安全控制的目的，他们可以将他们的创造力带到要解决的这个问题上。所以到最后，你已经不是在销售，而是在获取他们的帮助了。

原文出处：http://www.searchsecurity.com.cn/showcontent_28483.htm

（作者：Ed Moyle　译者：行久　来源：TechTarget 中国）

银行账户数据应该加入 PCI 安全要求吗？

为什么在银行帐号中不存在 PCI 安全要求呢？Gartner 公司的副总裁兼著名分析师 Avivah Litan 表示，她一直很奇怪，在敏感的银行账户数据中居然缺乏行业安全标准。最近，她就在一篇博文里面提出了这个问题。

Litan 写到，通过执行 PCI 安全要求，信用卡品牌很好地推动了用户的安全意识，那些处理支付卡交易的公司也对自己的系统进行了升级。Litan 补充到，“我经常在想，为什么一个类似的银行联盟没有尽全力去加强对银行账户和相关数据的保护呢？”

一般说来，虽然在 PCI 数据安全标准体系下的信用卡品牌（如 Visa、MasterCard）都严谨组织，但是支付卡的安全缺陷却越来越多。随着网上银行诈骗的增多，安全方面的情况可能会发生改变。她还说，“如果你问银行威胁在哪里，他们肯定会说是 ACH 和电信诈骗，因为这两者都依赖于银行账户的数据。”

由于针对小型企业、市政机构和非盈利机构银行账户的欺骗行为不断增加，联邦政府官员已经对此发出了警告。据联邦存款保险公司（FDIC）估计，因为欺诈性的转账行为，在 2009 年第三季度已经导致了约 1.2 亿美元的损失。

Litan 表示，网上企业银行账户正受到攻击，但是欺诈造成的损失一般都会转嫁到银行客户身上，这也让银行没有多少动力去增强保护措施。

Litan 说，“PCI 的实施是用来保护信用卡公司而不是消费者的。当银行采取措施保护自己免受经济损失时，他们做得很好，但是如果这种损失能转移到客户身上，那么他们就不一定愿意去加强同样的保护了。”

一些企业告诉 Litan，当他们为支付卡数据执行 PCI 安全要求时，他们计划将围绕银行账户和社会保险号码等敏感数据执行一些安全措施。除此之外，像 ProPay 公司这样的外包支付提供商已经开始提供除支付卡数据之外的银行账户标记化（tokenization）服务。

ProPay 最近宣布它将把自动结算所（Automated Clearing House，ACH）数据（包括汇款线路和银行账户号码）加密和标记化功能添加到 ProtectPay 服务中去。该公司的高层表示，这种服务是第一个允许组织在没有存储或处理银行账户数据的 ACH 网络上进行交

易的服务。通过使用在线接口或 API，ProPay 可以捕获 ACH 数据、对其进行加密，并返回一个标记（token）。

ProPay 的产品管理副总裁 Raya Oaks 说，“一旦在自己的环境中拥有了那个标记，他们就可以在公司任何正常的业务流程中使用。如果他们需要提取汇款路线和往来账户号码的最后四位数字，可以调用一些 APS 来使用这个标记获得最后四位数字，这样就可以在客户服务中心进行显示和核对。当真正敏感的数据从他们的系统中移除的时候，也能给予数据安全保障。”

Oakes 表示，这项服务是为需要存储银行帐户信息的组织设计的，比如拥有自动缴费或直接存款业务的公司。一些公共事业公司已经在使用这项服务了。

ProPay 的首席信息官 Mark Johnson 表示，由于 ACH 诈骗不断涌现，用户开始表达他们对 ACH 数据的担忧。Oakes 说，他期望像 PCI 这样的标准最终会出现在 ACH 数据中。

Unisys 系统公司风险智能解决方案管理全球总监 Sid Pearl 表示，FS-ISAC 等组织可以和银行一起为银行账户数据建立一套安全标准，当然这需要在理解了到底是什么应该得到保护之后，例如需要从网络攻击者的角度想问题。

Unisys 公司上个月发布的一项研究显示，身份盗窃、信用卡和借记卡欺诈是美国人最担忧的问题。根据最新的 Unisys 安全指数（调查了超过 1000 名消费者）结果显示：超过 64%的受访者非常关注身份盗窃，而超过 62%的受访者担心信用卡和借记卡欺骗。

咨询公司 R.I.S.C. Associates 的常务董事 David Schneier 表示，银行业已经制定了一套新的制度来管理银行账户信息，即 GLBA。

Schneier 说，“管理帐户数据固有风险的问题在于，各个机构能做的不多，而信息会以‘借记卡购买’和‘ATM 活动’的形式在多个渠道上传播，这也是当前供应商管理背后的主要动力之一。”

原文出处：http://www.searchsecurity.com.cn/showcontent_35644.htm

（作者：Marcia Savage　　译者：Sean　　来源：TechTarget 中国）