INTERNET BANKING: DICAS DE SEGURANÇA

Alexandre Kaspary[1]
Alexandre Ramos[2]
Leo Andre Blatt[3]
William Rohr[4]
Fábio Matias Kerber[5]

Palavras-chave: Segurança da Informação; Internet Banking; Fraudes; Riscos.

Com o crescimento constante de transações financeiras por meio eletrônico, é de suma importância a aplicação das tecnologias de segurança para manter os usuários seguros contra fraudes e roubos eletrônicos.

De acordo com alguns agentes internacionais como FraudAction Intelligence da RSA, o Brasil é campeão mundial na geração de malware sobre temas financeiros e está entre os três países mais atacados por algum desses malwares nos meses de abril e maio de 2014. Os chamados Brazilian Bankers foram responsáveis por 32% das tentativas de fraudes no último ano.

Neste contexto a principal prevenção é a navegação consciente dos usuários. Visando deixar os usuários informados dos cuidados que devem ser tomados para que não tenham seus dados bancários roubados, será criada uma cartilha contendo informações importantes a cerca do assunto.

Para a execução desse trabalho será feita uma cartilha que expõe os riscos e cuidados que os usuários devem ter antes e durante o acesso a sites bancários. Esta cartilha será entregue ao Sicoob Creditapiranga e no dia será realizada uma explanação sobre o assunto aos funcionários da Cooperativa.

Nos dias atuais o assunto segurança da informação é algo muito relevante ainda mais se tratando do Internet Banking. Essa afirmação é válida inclusive para usuários comuns de computadores e tendo em vista que essa classe vem aumentando drasticamente quanto ao número de usuários que usam serviços bancários on-line, vimos a necessidade da criação de uma cartilha com o seguinte tema: Internet Banking: Dicas de Segurança.

[1] Cursando Gestão da Tecnologia da Informação, alexandre.kaspary@hotmail.com;
[2] Bacharel em Ciências Contábeis, cursando Gestão da Tecnologia da Informação, ramos.85ale@gmail.com;
[3] Cursando Gestão da Tecnologia da Informação, leoandreblatt@gmail.com;
[4] Cursando Gestão da Tecnologia da Informação, willirohr2@gmail.com;
[5] Professor do curso de Gestão da Tecnologia da Informação, fabio@seifai.edu.br;

A finalidade desta cartilha é demostrar ao usuário comum como acessar um serviço bancário da forma mais segura possível, evitando que ele tenha perdas financeiras.

O objetivo geral do presente trabalho é identificar as principais medidas de segurança no acesso ao Internet Banking.

Os objetivos específicos buscados nessa pesquisa compreendem:

- Criar uma cartilha de segurança em Internet Banking.

- Palestrar aos colaboradores do Sicoob Creditapiranga abordando a segurança em Internet Banking.

- Demostrar os riscos e cuidados necessários no acesso ao Internet Banking.

- Disponibilizar exemplares da cartilha para associados do Sicoob Creditapiranga.

Com o passar dos anos, a importância do compartilhamento de dados utilizando a internet aumentou gradativamente. Com isso, a preocupação em proteger estes dados aumentou também. Sofremos ataques cibernéticos a todo instante, seja por Invasão, Scan, Web, ou qualquer outra forma que os hackers utilizam para se infiltrar em nosso meio virtual. E é ai que entra a segurança da informação.

Gerando um Plano de segurança, que se baseia no levantamento de dados para que possamos chegar a um resultado final, poderemos ter em mãos informações importantes para a boa segurança dos nossos dados, ou seja, é a listagens de possíveis “brechas” que possam haver em nosso servidor, possibilitando a vulnerabilidade do mesmo, favorecendo os hackers nas possíveis invasões. Todos os itens do plano de segurança da informação deverão conter um documento formal, o qual deverá ser assinado por todos os envolvidos nos processos relacionados.

A segurança da informação esta relacionada com proteção de um conjunto de informações, considerado um bem ativo de valor para as empresas com a sua importância para os negócios, ela protege a informação de variados tipos de ameaças e riscos, garantindo a confidencialidade, integridade e disponibilidade do mesmo.

A rede mundial de computadores traz inúmeras possibilidades de uso, entre essas possibilidades o uso do Internet Banking vem se destacando devido seu crescimento significativo nos últimos anos. Com o aumento do acesso a informações bancarias também vem o aumento as possibilidades de fraudes que podem ser realizadas através da internet.

Quando falamos em internet banking logo nos vem à mente o fato de não precisarmos enfrentar filas e ficar restritos aos horários de atendimento dos bancos. Além disso, esse meio de acesso nos fornece uma gama muito grande de produtos e serviços. Mas toda essa facilidade e praticidade exige que os usuários tomem alguns cuidados. De acordo

com pesquisadores da ESET, empresa de segurança online, a preocupação quanto à insegurança do internet banking não é infundada. Só no último ano, o laboratório da ESET na América Latina identificou mais de 16 ataques específicos a usuários de serviços bancários online no Brasil, boa parte deles voltados a roubar senhas e informações pessoais dos clientes.

"Assim como qualquer outra transação financeira, o uso do internet banking requer cuidados por parte dos usuários. Mas se as pessoas tomarem as medidas necessárias, dificilmente, elas serão vítimas de cibercriminosos", destaca o country manager da ESET Brasil, Camilo Di Jorge.

Para obter acesso às informações pessoas das vítimas ou até mesmo fazer com que elas realizem ações, como por exemplo, executar códigos maliciosos os golpistas procuram engana-las e persuadi-las das mais diversas formas. Uma dessas formas se dá pelo uso de páginas falsas (phishing). Ocorre por meio do envio de mensagens eletrônicas que, tentam se passar pela comunicação oficial do banco atiçam a curiosidade do usuário tentando fazer com que ele passe dados pessoas e financeiros.

Outra forma de ataque é por meio de Spyware, que constitui um tipo de código malicioso capaz de monitorar as atividade de um sistema e enviar as informações para os golpistas. Existem várias formas e ataque por meio de Spyware, sendo os mais comuns, o Keylogger que possui a capacidade de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador. Outra forma de captura de dados é o Screenlogger, usado para capturar as teclas digitadas em teclados virtuais, usados em Internet Banking.

Fica evidente que os usuários devem tomar alguns cuidados ao usar seu computador ou dispositivo móvel, caso contrário poderão sofrer perdas bancárias, como por exemplo, transferências indevidas de dinheiro e pagamentos de contas de outras pessoas. Além disso, os usuários poderão sofrer invasão de privacidade, violação de sigilo bancário e participação em esquemas de fraude.

Alguns dos principais cuidados que devem ser tomados ao acessar informações bancárias:

- Não fornecer senhas e outros dados pessoais a outras pessoas;
- Certificar a procedência do site da instituição e conexão de internet a ser usada;
- Não realizar transações a partir de computador de terceiros e redes públicas;
- Não utilizar sites de buscas para acessar o site da instituição, geralmente os domínios são bem conhecidos;
- Evitar links para acessar o site do banco;

Acima foram relacionados alguns dos principais cuidados a serem tomados ao acessar as informações de sua conta bancaria através da internet, mas os riscos da internet não se limitam a fraudes bancárias, criminosos podem facilmente obter informações de grande valor através de redes sociais e outros meios. Essas informações que obtidos podem variar de um número de celular ou telefone, endereço de trabalho ou domiciliar, documentos pessoais, e outros, podendo assim o criminoso se aproveitar de alguma forma dessas informações obtidas.

Somos alvos de ataques cada vez mais sofisticados, o que é certamente danoso à sensação de segurança que normalmente os serviços de internet banking passam aos usuários. Os serviços de internet banking tem vários mecanismos de segurança e passam por diversos testes para que se tenha segurança nas realizações de transações via internet, o que normalmente ocorre é que os principais culpados ou alvos dos ataques são os computadores das vítimas, que por meio de engenharia social utilizada por fraudadores conseguem extrair das vitimas as senhas necessárias para conseguir realizar transações ilícitas.

Como aponta José Nabuco Filho,

> Uma das que merece destaque é o envio de e-mail em que se simula ser uma mensagem enviada pelo banco, no qual se solicita que os dados da conta (inclusive senha), sejam digitados. Com tais informações, o agente acessa a conta da vítima e realiza transferência em prejuízo do correntista. Em tais situações, está configurado o estelionato, pois o autor usou a fraude (e-mail fictício do banco) que levou a vítima ao erro (fazendo com ela digitasse seus dados), o que permitiu ao agente que ele obtivesse a vantagem (transferência do dinheiro) em prejuízo alheio. Não só estão presentes os elementos, como há o nexo causal entre cada um deles. (FILHO, 2010, p. 1)

Essa problemática requer atenção não apenas das instituições bancárias, mas de todos os que estão envolvidos nesse processo, principalmente os clientes. Naturalmente, as instituições devem sempre se atentar para questões de segurança envolvendo seus serviços, mesmo porque as soluções de contenciosos jurídicos podem não ser favoráveis à eles, embora estes possuam diversos mecanismos de proteção em seus ambientes.

A pesquisa para a elaboração da cartilha será baseada em livros que se referem a segurança da informação, em cartilhas on-line do referido tema principalmente se tratando do Internet Banking. Além de pesquisas bibliográficas e na internet, serão usados os conhecimentos adquiridos ao longo do Curso de Gestão da Tecnologia da Informação, sendo que o curso fornece uma disciplina específica de segurança da Informação e que será determinante para realização da cartilha.

REFERÊNCIAS

CENTRAL DE PROTEÇÃO E SEGURANÇA (Org.). **Privacidade e segurança online**. 2012. Disponível em: <http://www.microsoft.com/ >. Acesso em: 01 set. 2014.

DIGITAL, Redação Olhar. **Dicas de como evitar riscos no uso do internet banking**. 2012. Disponível em: <http://olhardigital.uol.com.br/noticia/dicas-de-como-evitar-riscos-no-uso-do-internet-banking/24184>. Acesso em: 22 set. 2014.

EQUIPE CERT.BR (Org.). **Cartilha de Segurança para Internet.** 2012. Disponível em: <http://cartilha.cert.br/>. Acesso em: 01 set. 2014.

FILHO, José Nabuco Galvão de Barros. **Algumas observações sobre o estelionato**. A questão da pessoa induzida em erro. Jus Navigandi, Teresina, ano 15, n. 2644, 27 set. 2010. Disponível em: <http://jus.com.br/revista/texto/17458>. Acesso em: 01 set. 2014.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2009.