

TÉCNICAS UTILIZADAS PARA EFETIVAÇÃO E CONTENÇÃO DAS FRAUDES SOBRE INTERNET BANKING NO BRASIL E NO MUNDO

Marcelo Lau
Pedro Luís Próspero Sanchez

Resumo

Este artigo apresenta as técnicas utilizadas para a efetivação da fraude sobre o ambiente Internet Banking no Brasil no passado recente que são hoje utilizadas para a prática deste crime no mundo. Algumas propostas de contenção utilizadas no Brasil e no mundo são apresentadas, permitindo uma avaliação de segurança sobre o cenário atual.

1. INTRODUÇÃO

A fraude é um tema que precede o surgimento da Internet, e que deverá permanecer presente do cotidiano do ser humano, independente dos subsídios tecnológicos existentes ou que ainda estão por vir. É importante salientar que as técnicas utilizadas no passado e presente para a efetivação da fraude, são pontuais podendo nos preparar para a evolução deste processo nos próximos anos, entretanto os processos psicológicos sobre as vítimas são, e devem permanecer os mesmos utilizados no mundo real¹. Neste artigo, a fraude está associada à distorção intencional de um fato que levará a obtenção de lucro ilícito, existindo a necessidade de três elementos principais para a consumação da fraude: a vítima, o fraudador e o canal *Internet Banking*.

O tema fraudes sobre *Internet Banking* existe desde o momento que se disponibilizou este serviço aos clientes de instituições financeiras. No Brasil, os primeiros serviços foram disponibilizados na segunda metade da década de 90, permitindo aos seus clientes comodidade para realização de diversas transações a partir do canal Internet.

Dos incidentes de segurança registrados no Brasil (CERT,2006) , mais de 40% são registros associados à tentativa de fraude² sobre o ambiente Internet. Neste percentual são contempladas fraudes sobre sites de comércio eletrônico, serviços de *Internet Banking*, cartas nigerianas e outras tentativas de efetivação de fraude. Apesar da falta de dados sobre a distribuição dos registros, há percepção que maior destes ataques estão relacionados ao ambiente *Internet Banking*, pois foram divulgadas perdas que superam 300 milhões de reais no ano de 2005 (B2B Magazine, 2006).

Quando comparamos o cenário brasileiro com o mundial, percebe-se que diversas regiões do mundo são afetadas por este tipo de crime³. O Brasil representa apenas 1,55% de todos os ataques incidindo hospedagem de página ou código malicioso⁴ no mundo (APWG, 2006), onde os Estados Unidos são os líderes entre os países mais afetados, superando 40% de todos os ataques⁵, precedido pela China com 8%⁶. Pelos números apresentados pelo APWG, comparados aos dados do CERT.br, o Brasil representa um terço de todos os incidentes registrados no mundo, portanto, considera-se importante a partir dos dados apresentados o envolvimento de diversos segmentos da sociedade e de diversas nacionalidades, visando minimizar impactos sobre a confiabilidade do meio eletrônico junto aos usuários.

¹ As fraudes aplicadas sobre o mundo real, em geral, não contemplam aparatos tecnológicos para a efetivação da fraude. Quando se trata a fraude sobre o ambiente *Internet Banking*, realiza-se uma analogia com o mundo virtual.

² Os incidentes reportados superam 5000 incidentes ao mês nos meses de Outubro a Dezembro de 2005.

³ Os crimes mencionados neste texto estão associados às tentativas de subtração de credenciais que permitem acesso ao serviço de *Internet Banking* através de *scam* e *phishing*. Termos que serão detalhados neste artigo adiante.

⁴ Entende-se que a hospedagem não corresponde diretamente à população alvo do ataque, pois no Brasil, se encontram diversos relatos de hospedagem de *scam* e *phishing* no exterior.

⁵ Os incidentes reportados superam 15000 incidentes ao mês nos meses de Outubro e Novembro de 2005.

⁶ A distribuição apresentada não segmenta as atividades de negócio impactadas. Pelo APWG, o maior foco está sob a fraude em transações eletrônicas, sejam elas associadas à *Internet Banking* ou comércio eletrônico.

2. TÉCNICAS UTILIZADAS

Visando uma maior compreensão sobre o cenário atual e sua evolução com o passar dos anos, é necessário se conhecer as três técnicas utilizadas para efetivação da fraude sobre clientes do serviço de *Internet Banking: scam, phishing e pharming*.

2.1 Scam

É um tipo de mensagem eletrônica⁷ repudiada pelos usuários, pois além de causar desconforto aos usuários de caixas postais, como o *spam*⁸, eles apresentam natureza fraudulenta (Lau). A natureza fraudulenta destas mensagens está associada à tentativa de convencimento do receptor mediante a alguma oferta descrita pelo responsável no envio desta mensagem eletrônica. Nestes casos, a oferta se constitui em um golpe, levando a vítima a perdas financeiras.

Este tipo de mensagem eletrônica pode ser classificado em categorias. Exemplos são os *scams* de compras em tempo real, *scams* de investimento em tempo real e as cartas nigerianas, conhecidas também como "*Nigerian Letters*" (INFOSEC).

As "*Nigerian Letters*" ou cartas nigerianas são mensagens enviadas a caixas postais eletrônicas e disponíveis para envio em outros meios como máquinas de fax, e são entregues por carteiros em todo o mundo, oferecendo oportunidade, aventura, viagens, e muito dinheiro.

Este esquema popular recebe o nome de "nigeriano", pois este é o lugar onde o golpe se originou. Atualmente há evidências que este tipo de *scam* se espalhou no mundo inteiro. Os responsáveis pelo envio destas mensagens hoje estão localizados geralmente na Inglaterra, Canadá, Ásia, Europa e Estados Unidos (FRAUDAID).

Para classificar esta ameaça sob a ótica do ambiente Internet Banking, busca-se descrever as características do *scam* no Brasil são as seguintes:

- O conteúdo da mensagem pode ou não conter uma marca comercial forjada⁹;
- Contém endereços de e-mail e *links* forjados¹⁰;
- Representa uma mensagem que aguça a curiosidade a vítima;
- O golpe busca atingir a vítima, através da instalação acidental de um programa existente no *link* forjado. A partir da instalação deste agente, os dados são coletados no computador infectado por meio de digitação ou ações realizadas a partir do mouse. Estes programas também são conhecidos como cavalos de tróia;
- O processo de captura de credenciais pode ser imperceptível a vítima, ou se apresentar na forma de uma tela sobreposta sobre os aplicativos do computador, induzindo a vítima a colaborar voluntariamente com o fornecimento de dados pessoais;
- Em geral, os dados capturados são enviados ao fraudador por meio de protocolos de transferência de arquivos (*ftp - file transfer protocol*), ou protocolos de envio de mensagens (*smtp - simple mail transfer protocol*)¹¹.

⁷ É necessário mencionar que no início de 2006 são registrados os primeiros incidentes envolvendo oferecimento de SCAM em mensagens enviadas no serviço Orkut (<http://www.orkut.com>)

⁸ O *spam* é definido como uma mensagem eletrônica não solicitada, geralmente enviada indiscriminadamente a múltiplas caixas postais eletrônicas, não permitindo aos usuários destas caixas postais a escolha de recebê-las (INFOSEC).

⁹ Estas mensagens apresentam logomarcas de empresas ou instituições conhecidas no mercado brasileiro.

¹⁰ Os *links* existentes nestas mensagens geram a percepção de acesso a um arquivo que não corresponde à descrição do texto existente no corpo da mensagem.

¹¹ Dentre os dois protocolos mencionados, é importante mencionar que o *smtp* é o processo mais utilizado para envio de dados coletados ao fraudador.

2.2 Phishing

O *phishing scam* ou simplesmente *phishing* é um tipo particular do *scam*, onde mensagens eletrônicas falsas são enviadas aos usuários de caixas postais, convidando-os a acessar páginas fraudulentas na Internet. Têm a intenção de capturar informações pessoais e confidenciais, tais como números de cartões de crédito, contas e senhas de acesso bancário. Estas páginas fraudulentas são criadas por fraudadores que imitam as páginas legítimas de grandes companhias como bancos (INFOSEC).

Assim como foi descrito no *scam*, classificam-se como *phishing*, mensagens eletrônicas que apresentam as seguintes características:

- O conteúdo da mensagem contém uma marca comercial forjada¹²;
- Contém endereços de e-mail e *links* forjados¹³;
- Busca representar uma instituição de comércio eletrônico ou financeiro;
- O golpe busca atingir a vítima, coletando informações digitadas em formulários *HTML*¹⁴, existentes na mensagem eletrônica ou uma página *Web*, resultante do link forjado;
- O processo de captura se apresenta na forma de uma interface *Web*, induzindo a vítima a colaborar voluntariamente com o fornecimento de informações sensíveis;
- Os dados capturados são enviados ao fraudador por meio dos protocolos de hipertexto (*http – hyper text transfer protocol*).

2.3 Pharming

O *pharming* é um conceito recente ao público mundial¹⁵, entretanto foi um meio largamente utilizado para a efetivação da fraude sobre o ambiente *Internet Banking* no Brasil. O mecanismo utilizado por este ataque promove o redirecionamento da vítima a páginas falsas de instituições financeiras, tal como descrito pelo *phishing*, entretanto esta variação de ataque não utiliza uma mensagem eletrônica como vetor de propagação. O atacante busca fragilizar serviços de resolução de nomes na Internet, conhecidos como DNS¹⁶, que resultam no acesso errôneo do usuário à página da instituição financeira, mesmo que o usuário efetive o acesso à página do banco através da digitação da URL no *browser* utilizado na navegação Internet.

3. MÉTODOS PRATICADOS PARA A EFETIVAÇÃO DA FRAUDE NO BRASIL E NO MUNDO

É importante mencionar que este é o *scam* é o método mais utilizado para a efetivação de fraude sobre o ambiente *Internet Banking* no Brasil, em substituição a outros dois métodos amplamente utilizados no passado, que são o *phishing scam* e *pharming*¹⁷.

Em virtude da ameaça de *pharming* se caracterizar como a primeira modalidade de incidente registrado no Brasil, resultando em atuação forte de instituições financeiras e órgãos de regulamentação sobre provedores de acesso. Os principais responsáveis pelo processo de contaminação do serviço DNS, considera-se que este fator foi o principal responsável pela mitigação deste risco, permitindo o surgimento de outra ameaça, o *phishing scam*.

O *phishing scam* afetava diversos provedores de hospedagem de páginas na Internet. Vulnerabilidades que no passado eram explorados por *defacers*¹⁸, foram aplicadas para resultados financeiros através da fraude

¹² Estas mensagens apresentam logomarcas de instituições financeiras e seus órgãos representativos.

¹³ Os *links* neste contexto diferem do *scam*, pois neste processo a vítima é redirecionada a uma página *Web*.

¹⁴ *Hypertext Markup Language*, linguagem utilizada para produção de páginas em ambiente *Web*.

¹⁵ O termo PHARMING é mencionado no site do APWG Anti-Phishing Working Group apenas a partir do ano de 2005

¹⁶ *Domain Name Services*.

¹⁷ *Phishing* foi amplamente difundido no Brasil no ano de 2004 e o *pharming* no ano de 2002 e 2003.

¹⁸ Nome dado aos responsáveis pela alteração de uma página *web* sem prévio consentimento do hospedeiro.

sobre o ambiente *Internet Banking*. Este tipo de golpe teve seu auge em 2004. Devido à publicação deste tema na mídia, seja impressa televisiva ou através de boletins disponíveis na Internet, os usuários do serviço começaram a avaliar com maior critério a URL disponível no acesso de uma página falsa. Em muitos momentos os dados digitados não refletiam as informações desejadas pelo fraudador, resultando em perda de produtividade ao responsável pela ação. Em virtude desta mudança cultural esta técnica foi suplantada pelo scam, onde um cavalo de tróia poderia obter dados capturados da vítima através de técnicas como captura de teclas digitadas (técnica de *keylogging*), captura de imagens ao redor do *click* do *mouse* (técnica de *screenlogging*) e sobreposição de tela no acesso do serviço de *Internet Banking*.

No mundo, a primeira referência publicada sobre ataques foi disponibilizada por um grupo intitulado APWG (Anti-Phishing Working Group). Este grupo foi criado em no ano de 2003, buscando informar ao público os primeiros incidentes de *phishing* registrados nos Estados Unidos.

O primeiro incidente reportado pelo APWG utiliza a técnica de *phishing*, onde mensagens eletrônicas foram disseminadas em setembro de 2003, utilizando o nome de um banco norte americano, sediado em Santa Clara, estado da Califórnia, o Westpac Bank. Atualmente o *phishing* é a técnica mais utilizada no exterior para efetivação da fraude.

Com o passar dos anos de 2004 e 2005 o *phishing* continuou sendo o meio mais utilizado para a prática de fraude no ambiente Internet, entretanto no início de 2005, uma nova ameaça começou a ser utilizada no exterior, a prática de *pharming*. É importante mencionar que o nome *pharming* surgiu apenas no ano de 2005, entretanto é possível evidenciar a partir deste trabalho que o Brasil já foi vítima destes ataques nos anos de 2002 e 2003, não ocorrendo nenhum registro nos anos de 2004 e início de 2005.

Nota-se ataques de *scam* foram detectados apenas no segundo semestre de 2005 no exterior, hoje amplamente utilizado para a realização de fraudes em clientes do sistema financeiro brasileiro. Acredita-se que é possível uma grande disseminação destes ataques ocorra no mundo no ano de 2006. Pelo APWG, os ataques de *scam* são conhecidos como *phishing-based malicious code attacks*, que em português pode ser traduzido como ataques de *phishing* baseados em códigos maliciosos. Entretanto das técnicas mencionadas em *scam*, apenas os ataques baseados em *keyloggers* estão sendo aplicados, portanto são desconhecidos no exterior, ataques baseados na captura de telas, os *screenloggers*, e as sobreposições de telas que ocorrem com frequência no Brasil.

Apesar do volume e qualidade das informações disponíveis pela APWG, é possível perceber o desconhecimento dos riscos que ainda podem afligir os clientes de serviços financeiros no exterior. Neste caso, o Brasil, infelizmente, é o precursor deste tipo de ataque.

4. MEDIDAS DE CONTENÇÃO À FRAUDE

É possível perceber a partir do capítulo anterior que há um processo evolutivo nos mecanismos utilizados para efetivação da fraude junto aos clientes de serviços *Internet Banking*. Esta evolução é uma necessidade adaptativa dos fraudadores em virtude da perda de eficácia dos ataques ou desejo no aumento de produtividade na coleta de credenciais que permitam acesso a serviços financeiros de vítimas, resultando em um volume financeiro que justifique o investimento realizado para o lançamento dos ataques.

Apesar desta evolução, há similaridades no processo utilizado pelos fraudadores, que buscam iludir a vítima. Em todos os incidentes registrados há clara intenção de convencimento da vítima à realização de uma ação que levará o fornecimento voluntário das credenciais de acesso aos serviços de *Internet Banking*. Algumas variações ocorrem no processo de convencimento, seja este associado ao scam, phishing ou pharming.

Percebe-se atualmente no Brasil, que a maior parcela dos ataques o convencimento das vítimas está atrelado ao processo de curiosidade da população sobre o conteúdo existente em uma mensagem. O conteúdo destas mensagens traz temas como suposto recebimento de cartões virtuais, possíveis débitos pendentes junto a órgãos oficiais, oferecimento de fotos que contenham nudez, ou fatos de grande repercussão na imprensa ou mídia televisiva, entre outros argumentos. Levando o usuário a realizar o *download* de um programa, que

resultará a instalação de um executável residente em memória, capaz de capturar dados diversos, realizando a função de um *spyware*. Dentre os dados capturados, incluem-se as credenciais de acesso a serviços de *Internet Banking*.

Nos Estados Unidos, o processo de convencimento das vítimas difere em virtude da cultura da população. Percebe-se que os norte-americanos são mais suscetíveis às marcas ou logomarcas contidas em mensagens eletrônicas. A percepção de legitimidade de uma mensagem eletrônica está diretamente atrelada ao fato da mensagem eletrônica disponibilizar elementos que associem empresas de comércio eletrônico e instituições financeiras. Diferente dos ataques atualmente registrados no Brasil, a maior parcela dos ataques ocorre por meio de mensagens contendo alertas a correntistas, membros de sites de leilão ou serviço de compras na Internet. Estes alertas recomendam acesso a um link, em virtude de temas como recadastramento de contas, confirmação de identidade ou confirmação de operações eletrônicas podendo até se utilizar de argumentos como possível fraude registrada junto à vítima. O resultado deste ataque poderá resultar no roubo de credenciais e dados pessoais inseridos em uma página similar ao outro serviço legítimo disponível na Internet.

Considerando os fatores apresentados acima, é possível afirmar que a orientação dos usuários dos serviços Internet Banking é um passo inicial que pode ser realizado, em busca de conscientização sobre o problema.

Recentemente o Brasil iniciou um processo de conscientização de seus usuários a partir de um órgão representativo de diversas instituições financeiras no país, a FEBERBAN, (Federação Brasileira dos Bancos). Em Janeiro de 2006 ocorreu a primeira coletiva de imprensa levando como objetivo a orientação das fraudes junto à população. Antes deste evento, nenhum pronunciamento oficial das instituições financeiras sobre o assunto havia ocorrido¹⁹. Entretanto notícias e palestras sobre o assunto já são de conhecimento desde 2003. Apesar da mensagem alarmista utilizada em diversos meios de comunicação sobre o assunto fraude, os clientes não se intimidaram no uso do serviço de *Internet Banking*. A iniciativa da FEBERBAN busca mostrar transparência ao assunto fraude, visando esclarecer os clientes, tornando-os menos suscetíveis aos temas utilizados para efetivação da fraude, buscando ao mesmo tempo incentivar os usuários para o aumento no uso da solução, já que o *Internet Banking* resulta no menor custo transacional no processo de intermediação financeira.

Nos Estados Unidos, há ocorrido há alguns anos o processo de conscientização dos usuários em relação aos exemplos de fraude praticados no ambiente *Internet Banking*. Apesar de esta ação preceder o processo de conscientização adotado no Brasil, percebeu-se que esta ação não foi efetiva na mitigação dos ataques aos clientes destes serviços. Partindo deste caso, questiona-se a efetividade de campanhas de conscientização como ferramenta eficaz na mitigação das fraudes.

Além do processo de conscientização, outros meios podem ser adotados para a mitigação das fraudes. A tecnologia é um meio que pode ser adotado visando a melhor proteção do acesso do cliente ao serviço. Há algumas instituições financeiras que não adotam apenas o fornecimento de usuário de acesso e senha. Clientes que as credenciais subtraídas podem levar a efetivação de fraude, dispositivos conhecidos como OTP (*One Time Password*) são adotados em alguns serviços de *Internet Banking*, devido à alteração constante de senha. Em segundos ou minutos a senha é alterada automaticamente pelo dispositivo, oferecendo sempre uma nova senha de acesso ao usuário. Esta é uma das soluções mais robustas visando à proteção dos clientes.

Há outra tecnologia também adotada que aumenta a robustez na autenticação dos usuários, a certificação digital. O certificado digital é composto por uma chave privada²⁰, que pode ser armazenada no

¹⁹ É necessário mencionar que recomendações sobre o uso seguro do *Internet Banking* fazem parte das páginas institucionais de diversos bancos no Brasil

²⁰ Chave privada é uma das chaves utilizadas no processo de criptografia assimétrica. Neste processo são utilizados pares de chaves públicas e privadas. A chave pública é divulgada aos membros que realizam comunicação e são utilizados para a encriptação de dados. A chave privada é gerada e armazenada ao junto com ao dispositivo do usuário que responsável pela guarda do certificado. É necessário lembrar que apenas a chave privada consegue decifrar uma mensagem encriptada pela chave pública.

sistema operacional ou dispositivo que permite apenas a inserção do dado cifrado resultado sua decifração, não permitindo extração ou leitura da chave privada. No Brasil os certificados são classificados pelo Governo Federal em classes de A1 a A3, onde A1 trata da guarda do certificado em sistema operacional e A3, armazenamento de certificado em dispositivos especializados para a guarda de chaves, sensíveis à temperatura, atividades sísmicas e tentativas de violação²¹. Aos clientes dos serviços de Internet Banking, recomenda-se o uso de certificação A2, que trata do armazenamento do certificado em *smart card*, cartão plástico contendo um *chip*, capaz de armazenar certificados digitais, impossibilitando a extração ou leitura da chave privada. Proteções sobre o smart card possibilitam destruição ou inutilização do certificado em caso de tentativas indevidas de acesso sobre o dispositivo.

Outra alternativa adotada à mitigação da fraude é similar ao OTP, visando à adoção de uma solução a baixo custo. Há instituições financeiras no Brasil e no mundo que adotam o uso de um cartão plástico contendo uma matriz de números. A quantidade de números é variável para cada instituição financeira. Este dispositivo visa à solicitação de uma senha ao cliente, em função à posição (linha x coluna), existente no cartão. Como os números estão impressos, considera-se esta uma solução limitada, já que a frequência de utilização do serviço *Internet Banking* indicará a necessidade de substituição do cartão pela instituição financeira responsável pelo produto.

Há instituições financeiras no Brasil que adotaram algumas práticas sistêmicas que visam à redução da fraude sobre o serviço. Dentre as alterações está a limitação de transações em função a volumes financeiros, sendo que algumas instituições solicitam prévio cadastro de favorecidos a crédito antes da realização de créditos bancários. Outra alternativa adotada foi a solicitação de senhas adicionais no processo de validação de transações e estorno de transações realizadas, caso haja suspeita no processo de transações do cliente. É importante lembrar que o estorno de transações ocorre a partir da adoção de redes neurais para análise do comportamento do cliente. Estas decisões de estorno podem ser de origem sistêmica ou de intervenção manual.

Em virtude da deficiência de proteções antivírus junto aos clientes dos serviços de *Internet Banking*, algumas instituições financeiras no Brasil adotaram a instalação de *software anti-trojan* em seus clientes. O *anti-trojan*, é um agente, instalado a partir de *Active X*²², que permite execução do código no computador receptor deste código, mantendo-o residente em memória, visando proteção no cliente no processo de inserção de credenciais no ambiente *Internet Banking*. Estas aplicações buscam identificar ameaças através de uma atualização constante na tabela de assinatura de ameaças e através de comportamentos similares aos adotados por *malwares*²³. Em virtude de sua natureza intrusiva, é questionável o uso desta tecnologia junto aos clientes.

A tecnologia também pode ser uma grande contribuição além do ambiente da instituição financeira. Considera-se importante a proteção do ambiente doméstico para a realização de transações financeiras no ambiente Internet. Ter o hábito de atualizar o sistema operacional com as correções disponibilizadas pelo fabricante do software é imprescindível. Diversos ataques estão baseados em vulnerabilidades do sistema operacional²⁴ ou *browser*²⁵. Além desta medida, a adoção de um *software* antivírus é importante em casos de comprometimento de cavalos de tróia ou injeção de códigos ou *scripts* maliciosos. Por fim, recomenda-se aos usuários mais avançados a adoção de um *software firewall*. Apenas usuários com conhecimento no processo de comunicação de portas são recomendados nesta última recomendação, pois se percebe que o usuário leigo não está atento às mensagens sobrepostas na tela do sistema operacional, ignorando o seu conteúdo, possibilitando o permissionamento de um tráfego malicioso.

²¹ O modelo adotado no Brasil segue o FIPS 140-1 que corresponde ao certificado A1 e FIPS 140-3 que corresponde ao certificado A3

²² *Active X* é um conjunto de controles que permitem a iteração de componentes de software a outro ambiente através de uma rede.

²³ *Malicious Software*. É o termo mais abrangente para ameaças como vírus, vermes e cavalos de tróia.

²⁴ No Brasil os ataques estão baseados na instalação de cavalos de tróia sobre a plataforma Microsoft Windows.

²⁵ Em phishing, há modalidades de ataques que conseguem ocultar o endereço da página falsa, permitindo a visualização de um endereço idêntico ao utilizado pela página legítima.

Por fim, a tecnologia ainda pode ser aplicada em mais um segmento, no processo de contenção do envio de mensagens eletrônicas categorizadas como *scam* e *phishing*. Esta atuação trata da recomendação de bloqueio de mensagens em sistemas *anti-spam*, sistemas de correio eletrônico e em serviços de DNS²⁶. Sistemas anti-spam e sistemas de correio eletrônico devem oferecer um bloqueio para mensagens que contêm características que se assemelham a uma ameaça. Estes elementos podem ser obtidos através de características existentes no cabeçalho da mensagem ou texto disponível no corpo da mensagem. É importante salientar que estas medidas resultarão em adaptação do fraudador, visando à quebra deste bloqueio.

Outra medida importante pode ser realizada através de uma alteração na configuração do serviço de DNS. Esta alteração é denominada SPF, *Sender Policy Framework*. O SPF permite a configuração do serviço de resolução de nomes, informando a outros serviços DNS configurados com SPF a faixa de endereçamento IP utilizado para o envio de mensagens eletrônicas associado a um domínio na Internet. Um exemplo do SPF é a configuração do DNS informando que qualquer mensagem com remetente *@mybank.com*, só será legítima se for encaminhada pelo endereço 125.10.1.4. Neste caso, qualquer mensagem eletrônica com origem de outro endereço IP, que não seja 125.10.1.4, será descartada em um servidor DNS com SPF implementado.

Percebe-se que diversas medidas podem ser adotadas para a mitigação das fraudes. A decisão em adotar um ou mais soluções depende do custo envolvido e o retorno financeiro esperado para cada situação. Nesta decisão deve ser considerado o público alvo destas mudanças, o contexto de adoção de medidas por outras instituições financeiras e os resultados existentes ou esperados para cada solução. Não há fórmula única para solução deste problema, e nem devem ser consideradas as soluções mencionadas acima como as únicas existentes, pois é de conhecimento a constante evolução destas ameaças.

5. CONCLUSÃO

As três técnicas apresentadas para efetivação da fraude sobre o ambiente *Internet Banking* surgiram como um processo evolutivo no Brasil, sendo possível perceber diferenças entre o conjunto de técnicas utilizadas hoje no Brasil e no mundo.

Pelos fatos apresentados, percebe-se uma precedência no uso de todas as técnicas no Brasil, sendo estas utilizadas no exterior em momentos posteriores, não respeitando o mesmo processo evolutivo ocorrido no Brasil. Também é possível afirmar que os processos de captura de credenciais de usuários do serviço *Internet Banking* no exterior contemplam todas as técnicas apresentadas e já são aplicados pelos fraudadores no Brasil.

Considerando que estas técnicas sofreram uma evolução e amadurecimento, e que estas resultaram em transferência de conhecimento para outros países, considera-se bem provável que as técnicas utilizadas no exterior sofrerão evolução ao modelo hoje aplicado no Brasil.

E cientes das medidas de contenção da fraude, adotadas em diversas instituições financeiras no Brasil, recomenda-se a outros países a avaliação de todas as alternativas apresentadas. Mesmo que a mitigação não esteja associada a uma ameaça existente no presente, é importante avaliar estas alternativas em um cenário que certamente provavelmente se concretizará em questão de meses ou anos.

6. REFERÊNCIAS BIBLIOGRÁFICAS

APWG – **Anti - Phishing Working Group**. Disponível em:<
http://www.b2bmagazine.com.br/ler_materia.aspx?numero=15005> Acesso em: 05 fev. 2006.

B2B Magazine – **Febraban admite que informa pouco sobre segurança** Disponível em:<
http://www.b2bmagazine.com.br/ler_materia.aspx?numero=15005> Acesso em: 05 fev. 2006.

²⁶ *Domain Name Services*

CERT.br - **Incidentes Reportados ao CERT.br -- Outubro a Dezembro de 2005**. Disponível em: <<http://www.cert.br/stats/incidentes/2005-jul-sep/tipos-ataque.html>> Acesso em: 05 fev. 2006.

FRAUDAID - **Nigerian Scam Letters** - First Aid for fraud victims. Disponível em: <http://www.fraudaid.com/ScamSpeak/Nigerian/nigerian_scam_letters.htm> Acesso em 25 de mar. 2004.

INFOSEC - **Email Spamming (include scam/phishing). Information Security & Prevention of Computer Related Crime**. Disponível em: <http://www.infosec.gov.hk/english/itpro/sectips/sectips_emailspam.htm> Acesso em 10 de mar. 2004.

LAU, Marcelo – **Fraude via e-mail por meio de Cavalos de Tróia e Clonagem de sites financeiros** – SSI 2004. São José dos Campos. Novembro de 2004.