UNIVERSIDADE DE SÃO PAULO
ESCOLA POLITÉCNICA

MARCELO LAU

Análise das fraudes aplicadas sobre o ambiente *Internet Banking*

SÃO PAULO
2006

MARCELO LAU

Análise das fraudes aplicadas sobre o ambiente *Internet Banking*

Dissertação apresentada à Escola Politécnica da Universidade de São Paulo para obtenção do título de Mestre em Engenharia.

Área de Concentração: Sistemas Eletrônicos
Orientador: Prof. Dr. Pedro Luís Próspero Sanchez

SÃO PAULO
2006

Este exemplar foi revisado e alterado em relação à versão original, sob responsabilidade única do autor e com a anuência de seu orientador.

São Paulo, de agosto de 2006.

Assinatura do autor _____

Assinatura do orientador _____

FICHA CATALOGRÁFICA

Lau, Marcelo
Análise das fraudes aplicadas sobre o ambiente Internet Banking / M. Lau. -- ed.rev. -- São Paulo, 2006.
129 p.

Dissertação (Mestrado) - Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Sistemas Eletrônicos.

1.Fraude bancária 2.INTERNET I.Universidade de São Paulo. Escola Politécnica. Departamento de Engenharia de Sistemas Eletrônicos II.t.

Dedico este trabalho aos meus pais, à minha esposa Sandra e aos meus filhos, pelo apoio, compreensão e incentivo ao longo de minha vida acadêmica.

AGRADECIMENTOS

Ao Prof. Dr. Pedro Luís Próspero Sanchez, pela atenção e apoio durante o processo de orientação.

Aos colegas do Laboratório de Sistemas Integráveis da Escola Politécnica pelo incentivo e apoio à execução do mestrado.

Aos colegas e amigos de diversas instituições financeiras, provedores de tecnologia e serviços que me apóiam em pesquisas destinadas à área acadêmica.

E à Escola Politécnica e à Universidade de São Paulo, pela oportunidade de realização do curso de mestrado.

RESUMO

Este trabalho identifica sob o contexto da tecnologia, negócio, engenharia social e investigação a ocorrência de fraudes sobre o ambiente *Internet Banking*. A pesquisa relata a evolução dos métodos utilizados pelos fraudadores para efetivação da fraude desde seu o início, no ano de 2002 à evolução na sofisticação dos meios utilizados para os ataques até meados de 2005.

Como a análise se baseou em um estudo de caso, coletou-se um número quantitativo de incidentes no período de um ano permitindo entender neste escopo a tendência de ataques aos clientes de serviços *Internet Banking*.

E com pleno domínio do assunto, o trabalho traz recomendações para a contenção destes incidentes, através de três linhas de ação; sobre usuários finais, provedores e sobre o fraudador.

ABSTRACT

This research identifies under the technology, business, social engineering and inquiry context the occurrence of fraud on Internet Banking environment. It covers the evolution of the methods used for deceivers since from the beginning, in the year of 2002, and his evolution in the sophistication in several ways used for attacks until 2005.

The analysis is based on a case study and a quantitative number of incidents in the period of one year were collected making possible to see the point of such purpose the trend of attacks on Internet Banking customers.

With full domain of this one's subject, this research brings suggest for incident containment three lines of action; on final users, suppliers and deceivers.

SUMÁRIO

1 INTRODUÇÃO 1

1.1 CONCEITOS 2
1.1.1 Internet Banking 2
1.1.2 Fraude 5

1.2 OBJETIVO DO TRABALHO 11

1.3 JUSTIFICATIVA 12

1.4 METODOLOGIA DA PESQUISA 12
1.4.1 Estudo de Caso 12
1.4.2 Processo de escolha da bibliografia do trabalho 14
1.4.3 Procedimento de coleta dos dados 15

1.5 ESTRUTURA DO TRABALHO 16

2 CONTEXTO DO TRABALHO 17

2.1 VISÃO DA TECNOLOGIA 18
2.1.1 Segurança da Informação 19
2.1.2 Arquitetura da rede 21
2.1.3 Filtro de pacotes ou firewall 22
2.1.4 Segmentação das redes locais 23
2.1.5 Autenticação 25
2.1.6 Criptografia 26
2.1.7 Detecção de Intrusos 29
2.1.8 Segurança nos Servidores 30
2.1.9 Consolidação da Arquitetura 31

2.2 VISÃO DO NEGÓCIO 33
2.2.1 Riscos relativos aos serviços bancários 33
2.2.2 Riscos Operacionais 35
2.2.3 Controle de riscos no ambiente Internet Banking 37

2.3 VISÃO DA ENGENHARIA SOCIAL 40
2.3.1 Princípios da psicologia social 40
2.3.2 Escolha e determinação das alternativas de persuasão 40
2.3.3 Atitudes das vítimas e seu grau de ingenuidade 42
2.3.4 Técnicas de persuasão e influência 44

2.4 VISÃO DA INVESTIGAÇÃO 48
2.4.1 Modelo Investigativo 54

3 FRAUDE NO AMBIENTE FINANCEIRO 56

3.1 FRAUDES BANCÁRIAS EM MEIOS ELETRÔNICOS 56

3.2 FRAUDES BANCÁRIAS NO AMBIENTE INTERNET BANKING 59

3.3 MECANISMOS UTILIZADOS PELOS FRAUDADORES 60
3.3.1 Spam 60

3.3.2 Considerações sobre a definição de termos Scam e Phishing e Phishing Scam 61
3.3.3 Scam 61
3.3.4 Phishing Scam 66
3.3.5 Pharming 67
3.3.6 Métodos utilizados para a efetivação da fraude no Brasil 67
3.3.7 Métodos utilizados para a efetivação da fraude no exterior 79

3.4 DADOS ESTATÍSTICOS SOBRE A FRAUDE NO BRASIL 84
3.4.1 Incidentes de *PHISHING* no Brasil 85
3.4.2 Incidentes de *SCAM* no Brasil 87
3.4.3 Distribuição de hospedagem de cavalos de tróia em *SCAM* no Brasil 91
3.4.4 Distribuição dos tipos de arquivos em *SCAM* no Brasil 94

4 CONTENÇÃO DA FRAUDE SOBRE O INTERNET BANKING 99

4.1 PROCESSO DE MITIGAÇÃO DA FRAUDE 99
4.1.1 Ações junto aos usuários finais 100
4.1.2 Ações junto aos provedores 105
4.1.3 Ações junto aos fraudadores 108

5 CONSIDERAÇÕES FINAIS 110

5.1 TRABALHOS FUTUROS 110

5.2 CONCLUSÕES 111

6 REFERÊNCIAS BIBLIOGRÁFICAS 113

LISTA DE FIGURAS

FIGURA 1 - INCIDENTES RELATADOS AO CERT.BR – OUTUBRO A DEZEMBRO DE 2004 8
FIGURA 2 - INCIDENTES RELATADOS AO CERT.BR – JANEIRO A MARÇO DE 2005 9
FIGURA 3 - INCIDENTES RELATADOS AO CERT.BR – ABRIL A JUNHO DE 2005 9
FIGURA 4 - INCIDENTES RELATADOS AO CERT.BR – JULHO A SETEMBRO DE 2005 10
FIGURA 5 - REPRESENTAÇÃO DA REDE DESMILITARIZADA 23
FIGURA 6 - REDES DESMILITARIZADAS NO AMBIENTE FINANCEIRO 24
FIGURA 7 - PROCESSO DE COMUNICAÇÃO NO AMBIENTE *INTERNET BANKING* 27
FIGURA 8 - DIAGRAMA DE REDE CONSOLIDADO DO AMBIENTE *INTERNET BANKING* 32
FIGURA 9 - MODELO INVESTIGATIVO DE FRAUDES NO AMBIENTE *INTERNET BANKING* 54
FIGURA 10 - PRIMEIRO REGISTRO DE ATIVIDADE DE *PHISHING* DIVULGADO NO APWG 80
FIGURA 11 - INCIDENTES DE *PHISHING* REGISTRADOS NO BRASIL 85
FIGURA 12 - ANÁLISE GRÁFICA LINEAR DOS INCIDENTES DE *PHISHING* 86
FIGURA 13 - ANÁLISE GRÁFICA POLINOMIAL DOS INCIDENTES DE *PHISHING* 86
FIGURA 14 - INCIDENTES DE *SCAM* REGISTRADOS NO BRASIL 88
FIGURA 15 - ANÁLISE GRÁFICA LINEAR DOS INCIDENTES DE *SCAM* 89
FIGURA 16 - ANÁLISE GRÁFICA POLINOMIAL DOS INCIDENTES DE *SCAM* 89
FIGURA 17 - HOSPEDEIROS DE CAVAIOS DE TRÓIA EM *SCAMS* REGISTRADOS NO BRASIL 92
FIGURA 18 - EXTENSÕES DE ARQUIVOS UTILIZADAS EM *SCAMS* REGISTRADOS NO BRASIL 98
FIGURA 19 - MODELO DE MITIGAÇÃO DAS FRAUDES NO AMBIENTE *INTERNET BANKING* 99

LISTA DE TABELAS

TABELA 1 - CUSTO DE TRANSAÇÕES BANCÁRIAS 4
TABELA 2 - INCIDENTES RELATIVOS À FRAUDE REGISTRADOS NO ANO DE 2004 7
TABELA 3 - EXEMPLOS DE TEMAS UTILIZADOS EM *SCAM* REGISTRADOS NO BRASIL (I) 64
TABELA 4 - EXEMPLOS DE TEMAS UTILIZADOS EM *SCAM* REGISTRADOS NO BRASIL (II) 65
TABELA 5 - INCIDENTES DE *PHISHING* REGISTRADOS NO BRASIL 85
TABELA 6 - INCIDENTES DE *SCAM* REGISTRADOS NO BRASIL 88
TABELA 7 - INCIDENTES E HOSPEDEIROS DE *SCAM* REGISTRADOS NO BRASIL 91
TABELA 8 - EXTENSÕES DE ARQUIVOS UTILIZADAS EM *SCAMS* REGISTRADOS NO BRASIL 97

1 INTRODUÇÃO

Com a popularização da Internet nos últimos anos sobre os diversos segmentos da população mundial, percebeu-se um aumento significativo[1] no acesso aos serviços que este meio de comunicação oferece. Conseqüentemente, percebeu-se o acompanhamento deste aumento na utilização dos serviços de *Internet Banking*[2] no Brasil[3] e no mundo[4].

Infelizmente este cenário favoreceu ocorrência de um novo tipo de golpe[5], o roubo de identidade das vítimas que acessam os serviços bancários disponíveis na Internet (STS, p-10-11). A partir desta informação coletada pelos fraudadores, ocorre a subtração de fundos[6] que podem ser direcionados para pagamento de contas de concessionárias públicas e boletos bancários; ou transferidos para outras contas bancárias que podem permitir a extração do papel moeda em terminais bancários de auto-atendimento.

Com a consolidação e o aumento dos incidentes mencionados acima, percebeu-se que o veículo Internet ampliou a possibilidade para realização de fraudes em ambientes bancários.

Conseqüentemente, os usuários destes serviços, preocupados com a segurança deste ambiente, começaram a externar preocupações sobre a confiabilidade da Internet, como meio de se realizar transações bancárias (BITS, p.29) (RNP). Em muitos destes casos, esta insegurança é

---

[1] E-COMMERCEORG. **Dados estatísticos sobre a Internet e Comércio Eletrônico**. Disponível em: <http://www.e-commerce.org.br/STATS.htm> Acesso em 02 dez. 2004.

[2] Serviço bancário oferecido por instituições financeiras a clientes, utilizando como meio de comunicação o ambiente Internet. Detalhes sobre este conceito podem ser consultados no item a seguir deste capítulo do trabalho.

[3] FEBRABAN. **Número de contas, cartões de débito e clientes com Internet Banking**. Disponível em: <http://www.febraban.org.br/Arquivo/Servicos/Dadosdosetor/tecnologia_2003_dadossetor.asp> Acesso em 02 dez. 2004.

[4] E-COMMERCEORG. **Dados estatísticos sobre a Internet e Comércio Eletrônico**. Disponível em: <http://www.e-commerce.org.br/STATS.htm> Acesso em 02 dez. 2004.

[5] Este termo pode ser compreendido como uma manobra traiçoeira realizada por fraudadores – UOL-MICHAELIS. **Moderno dicionário da língua portuguesa**. Disponível em: < http://www2.uol.com.br/michaelis/> Acesso em: 03 dez. 2004.

[6] O objeto em questão é o capital em dinheiro - UOL-MICHAELIS. **Moderno dicionário da língua portuguesa**. Disponível em: < http://www2.uol.com.br/michaelis/> Acesso em: 03 dez. 2004.

resultado de notícias disponíveis na mídia[7], que descrevem o grande volume de perdas financeiras neste setor como conseqüência dos hábitos e cultura destes usuários.

Esta dissertação esclarece este tema (BITS, p.4), com a apresentação dos fatos que propiciam a concretização da fraude sobre o ambiente *Internet Banking* e sua respectiva análise. Para isto, é definido um contexto que permite visualizar o problema através de diferentes óticas, visando à compreensão da fraude como um sistema complexo que aflige o ambiente financeiro. O resultado deste trabalho traz considerações sobre cada um dos pontos que influenciam a existência da fraude, que culmina na proposta de soluções que visam mitigar o problema.

1.1 CONCEITOS

Visando uma melhor compreensão dos termos que descrevem este trabalho, serão expostas as definições de alguns conceitos relativos à fraude no ambiente *Internet Banking*.

1.1.1 Internet Banking

Este termo se refere a um serviço oferecido a clientes de instituições financeiras. O *Internet Banking* é uma opção adicional aos clientes de bancos que buscam realizar transações bancárias em qualquer localidade, onde se dispõe de um computador e conectividade com a Internet.

Os serviços oferecidos aos clientes através deste canal são também conhecidos pelo sistema financeiro como transações bancárias. É possível exemplificar algumas destas transações bancárias (Fortuna, p.145) como:

- Saldos e movimentação em conta corrente;
- Saldo e movimentação de cobrança / contas a pagar;

[7] Há diversas informações divulgadas sobre o assunto em agências de notícia. Visando manter consistência aos fatos, limitou-se a busca ao CERT.br, em virtude da preocupação do centro em divulgar apenas notícias baseadas em fatos que são comprovados. Recomenda-se a consulta à reportagem de 11 de junho de 2005 intitulada "*Fraude virtual cresce 1.313% em um ano no Brasil*" - CERT.br – **Entrevistas e Reportagens sobre o CERT.br**. Disponível em: <http://www.cert.br/docs/reportagens/> Acesso em: 02 nov. 2005.

- Posição, aplicações e resgates em fundos;
- Operações de empréstimo;
- Cotações de moedas / índices e bolsa de valores e;
- Saldo em cardeneta de poupança.

A diversidade de transações bancárias oferecidas na Internet ao cliente difere entre as instituições financeiras. E cada banco por meio de recursos tecnológicos, busca aumentar o conjunto de serviços oferecidos aos clientes. O objetivo é claro, a atração de um maior número de usuários a este ambiente. Este objetivo também é justificado, pois este meio elimina em muitos momentos a presença do cliente à agência bancária, o que reduz em números expressivos os custos deste cliente ao banco.

O perfil do cliente que efetua serviços bancários realizados pela Internet apresenta acesso presencial ao banco somente no momento de necessidade para realização de saques em papel-moeda, que muitas vezes ocorrem em terminais de auto-atendimento existentes em locais públicos.

Mas esta não é a única maneira utilizada pelos clientes para realização de transações bancárias de maneira remota. Há um conceito que precede o *Internet Banking* e mais amplo, chamado de *Home Banking*.

O *Home Banking* é o serviço disponibilizado a clientes de instituições financeiras permitindo a efetivação transações através da conexão de um equipamento à infra-estrutura da instituição financeira por um canal público ou privado. Entende-se canal público o acesso realizado através de um meio de comunicação onde outros usuários também podem fazer uso deste mesmo canal, seja de maneira dedicada ou compartilhada. O acesso discado à Internet, ou acesso discado à infra-estrutura que atende este serviço em uma instituição financeira são exemplos de canais públicos. Do outro lado, o acesso privado é o acesso a uma conexão

dedicada contratada pelo cliente, ou pela instituição financeira, permitindo acesso exclusivo à infra-estrutura do Banco, e conseqüentemente a realização das transações bancárias.

O *Home Banking* é um conceito mais amplo, que permite o uso de outros equipamentos além do computador, para a realização de transações através do conforto de casa ou escritório. Dentre os exemplos de equipamentos que permitem a realização de *Home Banking* é o telefone. O telefone permite iteração do usuário ao banco, através da digitação de dados em teclas do telefone, permitindo a interpretação de dados através de equipamentos conhecidos como Unidade de Resposta Audível (URA), conhecidos também no mercado internacional como *Talker*. Nesta modalidade de serviço, ainda há possibilidade da iteração do cliente através de equipamentos como o Fax, que permitem o recebimento de informações impressas fornecidas pelo banco.

Deve-se entender que o maior motivador para a implantação do serviço através do meio de comunicação Internet ao cliente foi o custo atrativo para a realização de cada transação bancária. A partir do quadro abaixo (Fortuna, p.148), é possível compreender melhor esta afirmação.

Canal de Distribuição	**Custo por Transação (em US$)**
Agências	1,07
Telefone	0,54
Auto-atendimento	0,27
Home Banking	0,02
Internet Banking	0,01

Tabela 1 - Custo de transações bancárias

Percebe-se que o custo transacional em agência é 107% superior ao custo da transação realizada através do canal *Internet Banking*. O resultado desta comparação levou as Instituições Financeiras a direcionar e intensificar a divulgação do canal Internet, buscando-se reduzir o número de clientes em agências bancárias. No período de criação dos primeiros

serviços baseados no canal Internet, na segunda metade década de 80, um projeto foi concebido com a intenção de permitir atendimento remoto a todos os serviços oferecidos ao cliente. Deste projeto surgiu uma nova Instituição Financeira, o Banco Um, parte integrante do Unibanco. Esta proposta permitiu a realização de todas as transações bancárias de maneira remota, além da possibilidade de recebimento de numerário, quando este fosse solicitado através do telefone. Este modelo, entretanto não foi bem sucedido, pois em 2004 os clientes do Banco Um foram remanejados ao Unibanco, cessando desta forma os serviços de um banco inteiramente virtual.

1.1.2 **Fraude**

A definição de fraude está relacionada à distorção intencional da verdade ou de um fato, que busca em geral a obtenção de lucro ilícito (Uol-Michaelis). Entretanto aos propósitos deste trabalho, estamos definindo fraude no contexto no meio de comunicação Internet, onde alguns especialistas definem este termo como “Fraude Internet”.

A Fraude Internet é definido pelo Departamento de Justiça Norte-americano (U.S. Department of Justice), como a aplicação de qualquer golpe relativo à fraude, utilizando os serviços disponíveis na Internet, tais como salas de bate-papo, mensagens eletrônicas e sites disponíveis na Internet. É compreendido como fraude, o aliciamento de vítimas através do fraudador e realização de transações fraudulentas beneficiando um indivíduo ou grupo de pessoas envolvidas no esquema.

Em geral, os mesmos esquemas de fraude praticados antes da criação da Internet, estão surgindo no mundo virtual. Entretanto a velocidade a abrangência de comunicação que este meio proporciona, possibilita ao fraudador a realização mais eficiente e mais ampla de golpes sobre as vítimas.

Os golpes praticados sobre as vítimas podem ser classificados em (U.S. Department of Justice):

- **Venda de produtos, serviços e leilões.** Onde são oferecidos pelo fraudador bens ou serviços de alto valor. As vítimas deste golpe efetuam pagamentos antecipados ao fraudador, que deixa de enviar o produto prometido, ou repassam aos compradores um item de menor valor, ou ainda deixam de executar o serviço solicitado;
- **Oportunidade de trabalho.** Neste golpe, a vítima acredita em uma oportunidade de trabalho que pode ser exercido em casa. O fraudador solicita o envio de uma quantia em dinheiro para que sejam fornecidos o material e as instruções para a efetivação deste trabalho. Entretanto a vítima não recebe qualquer resposta depois do depósito do dinheiro;
- **Roubo de identidade e credenciais.** Alguns esquemas de fraude envolvem o roubo de identidade e credenciais. Este método busca a obtenção de dados pessoais da vítima como número de documentos pessoais, dados do cartão de crédito e senhas para acesso. O objetivo deste mecanismo, em geral, é o ganho financeiro. Neste trabalho, a fraude está baseada no roubo de credenciais, que permitem ao fraudador, acesso aos serviços bancários através da Internet;
- **Esquemas de investimento em tempo real.** Este método de fraude utiliza a disseminação de falsas mensagens que contém dados falsos sobre o mercado financeiro, em geral, do mercado de ações. As vítimas deste golpe acreditando no conteúdo da mensagem realizam transações que beneficiam diretamente o fraudador, que aproveita a oportunidade para realizar lucro sobre ações adquiridas. Entretanto as vítimas, não sabendo desta informação, aguardam a valorização do papel até certo

patamar, o que em geral não acontece. E desta maneira as vítimas perdem a valorização de seus investimentos.

Vale lembrar que as fraudes aplicadas sobre o ambiente *Internet Banking* estão relacionadas ao roubo de credenciais, que permitem ao fraudador a efetivação da fraude através da subtração de denheiro da conta da vítima.

E apesar da classificação dos golpes terem sido definidos pelo departamento de justiça norte-americano, e se aplicarem ao público norte-americano, é possível perceber no Brasil a aplicação dos mesmos ardis, o que nos permite validar este mesmo modelo de classificação para os usuários, vítimas de fraude internet no Brasil.

No Brasil, há um órgão público federal[8] que analisa e contabiliza as tentativas de fraude, utilizando o meio Internet. Estes números são pouco significativos em comparação ao número de outros incidentes de segurança registrados, pois representaram no ano de 2004 apenas 5% dos eventos. A seguir há uma tabela detalhada (CERT.br), informando estes dados.

Mês	Total de Incidentes	Fraude (%)	
Janeiro	**5886**	283	4
Fevereiro	**6110**	170	2
Março	**6002**	343	5
Abril	**4763**	188	3
Maio	**5471**	181	3
Junho	**6502**	193	2
Julho	**6773**	270	3
Agosto	**5910**	371	6
Setembro	**5167**	341	6
Outubro	**11253**	379	3
Novembro	**7149**	572	8
Dezembro	**4736**	724	15
Total	**75722**	4015	5

Tabela 2 - Incidentes relativos à fraude registrados no ano de 2004

[8] CERT.br - **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil.** Disponível em: <http://www.cert.br/> Acesso em: 07 set. 2005.

Apesar da quantidade de incidentes registrados, estes números não nos permitem identificar as perdas financeiras relacionadas a estes golpes praticados. Estes números também não detalham a distribuição do número da fraude sob a ótica do roubo de credenciais sobre o sistema financeiro, aspecto importante para este trabalho que busca um número aproximado das tentativas de fraude aplicadas sob o ambiente Internet Banking.

Outro aspecto importante, relativo às estatísticas do CERT.br é a possibilidade de avaliar a tendência de crescimento de incidentes de fraude relatados. Nas figuras a seguir pode-se visualizar a relação de incidentes relatados de quatro trimestres.

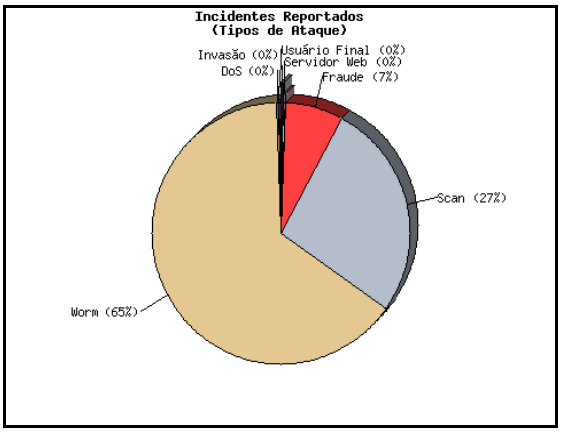

Figura 1 - Incidentes Relatados ao CERT.br – Outubro a Dezembro de 2004[9]

Percebe-se neste primeiro gráfico que a maior parte dos incidentes trata de *Worm* e *Scan*, onde o *Worm* é o resultado de registros de tentativas ou infecções em computadores por códigos que podem comprometer o ambiente do usuário, e que não está relacionada à fraude; e o *Scan*, o registro de varredura em portas de comunicação[10] de elementos conectados à Internet, incluindo computadores que oferecem acesso a serviços e estações de trabalho.

[9] CERT.br - **Incidentes Reportados ao CERT.br -- Outubro a Dezembro de 2004**. Disponível em: <http://www.cert.br/stats/incidentes/2004-oct-dec/tipos-ataque.html> Acesso em: 07 set. 2005.

[10] Em geral as portas de comunicação objeto da varredura estão baseadas em protocolos TCP (*Transport Control Protocol*), UDP (*User Datagram Protocol*) e ICMP (*Internet Control Message Protocol*). E a estatística de *Scam* não contempla varredura de portas por *Worms*.

Percebe-se que nos meses de Outubro a Dezembro de 2004 os incidentes relatados de fraude representam apenas 7% do total.

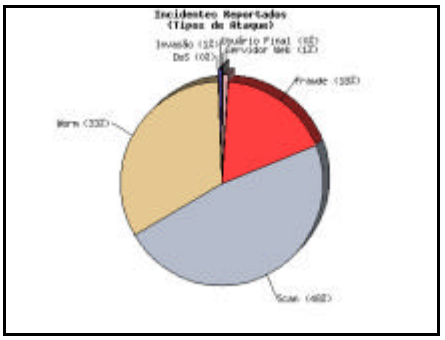

Figura 2 - Incidentes Relatados ao CERT.br – Janeiro a Março de 2005[11]

Percebe-se que neste segundo gráfico ocorre um aumento expressivo na proporção de incidentes *Scan*, e uma diminuição de *Worm*, entretanto os números relevantes a este trabalho estão relacionados aos incidentes relatados de fraude que sofrem um aumento de 7% para 18% do total.

É importante mencionar que os dados disponíveis ao longo deste trabalho se baseiam em dados coletados no ano de 2004 e 2005. Dados de 2006 não foram disponibilizados pelas instituições financeiras para realização desta pesquisa, portanto tendências atuais das tentativas de efetivação da fraude podem se basear nos gráficos disponibilizados pelo CERT.br.

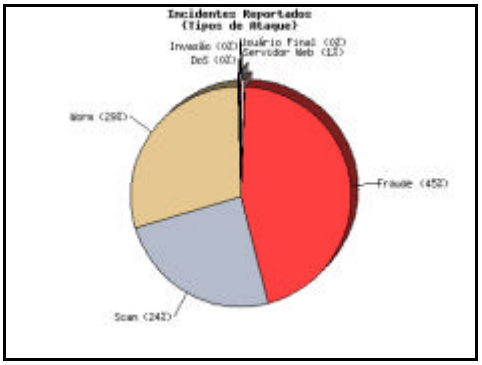

Figura 3 - Incidentes Relatados ao CERT.br – Abril a Junho de 2005[12]

[11] CERT.br - **Incidentes Reportados ao CERT.br -- Janeiro a Março de 2005.** Disponível em: <http://www.cert.br/stats/incidentes/2005-jan-mar/tipos-ataque.html> Acesso em: 07 set. 2005.

Percebe-se neste terceiro gráfico que ocorre uma diminuição expressiva na proporção de incidentes *Scan*, voltando a uma proporção similar existente no primeiro gráfico apresentado e uma manutenção na proporção de *Worm*. Os números relevantes neste trabalho que estão relacionados aos incidentes relatados de fraude que sofrem um aumento ainda maior passando de 18% para 45% do total.

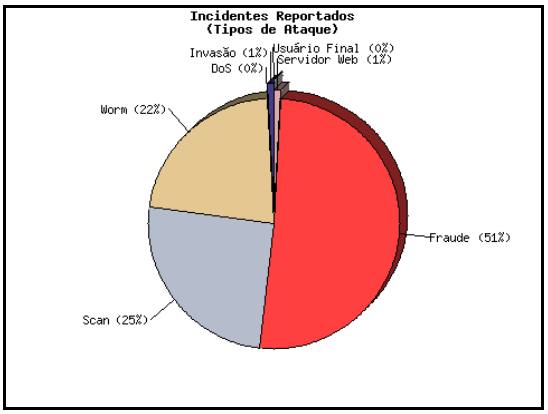

Figura 4 - Incidentes Relatados ao CERT.br – Julho a Setembro de 2005[13]

Por fim, percebe-se neste quarto gráfico o acompanhamento da tendência de crescimento na proporção de ataques relatados, agora representando mais da metade de todos os incidentes registrados pelo CERT.br. Vale lembrar que o crescimento não é tão acentuado, comparado aos últimos meses, mas é importante mostrar consistência no crescimento da proporção dos incidentes registrados.

Portanto, a análise destes quatro gráficos permite avaliar o forte crescimento de denúncia deste tipo de ameaça, refletindo conscientização de parcela de usuários da Internet no Brasil em manter informado o CERT.br na questão de ameaças associadas à fraude.

Através de consultas aos dados acumulados de reportes ao CERT.br nos períodos foi possível perceber que todos os incidentes estão aumentando em números absolutos, entretanto deve-se

---

[12] CERT.br - **Incidentes Reportados ao CERT.br -- Abril a Junho de 2005.** Disponível em: < http://www.cert.br/stats/incidentes/2005-apr-jun/tipos-ataque.html> Acesso em: 07 set. 2005.

[13] CERT.br - **Incidentes Reportados ao CERT.br -- Julho a Setembro de 2005.** Disponível em: < http://www.cert.br/stats/incidentes/2005-jul-sep/tipos-ataque.html> Acesso em: 02 nov. 2005.

levantar a hipótese de que parte dos usuários não estão mais informando incidentes de *scan*, com a mesma intensidade que os incidentes de fraude em virtude deste tipo de ataque (*scan*) ter se tornado comum no ambiente Internet. O mesmo comportamento poder ocorrer sobre os números de fraude do CERT.br no futuro.

Buscando enriquecer este trabalho, buscou-se um volume financeiro estimado da fraude. Em uma recente divulgação[14], foram mencionadas cifras aproximadas da fraude em torno de R$ 250 milhões anuais, onde deste montante, R$ 170 milhões são recuperados e apenas R$ 80 milhões é o efetivo prejuízo das instituições financeiras. Apesar da divulgação destes números relacionarem a Febraban e a Polícia Federal como responsáveis por esta informação, não são possíveis confirmações destes números por nenhuma das duas instituições mencionadas.

1.2 **OBJETIVO DO TRABALHO**

O trabalho apresenta uma abordagem investigativa de um problema que atinge diversos segmentos da sociedade[15]. Este trabalho é destinado a profissionais da área de segurança da informação, analistas de sistemas e negócios envolvidos no processo de idealização, criação, validação e manutenção de funcionalidades existentes em serviços de *Internet Banking*, peritos judiciais ou arbitrais e assistentes técnicos.

Esta pesquisa se propõe aos seguintes objetivos:

---

[14] Esta divulgação ocorreu em reportagem televisiva, e o texto correspondente disponibilizado na Internet. GLOBO.COM - **Capital dos Hackers. Fantástico**, 24 out. 2004. Disponível em:<http://fantastico.globo.com/Fantastico/0,19125,TFA0-2142-5650-192470,00.html> Acesso em 10 mar.2005

[15] A fraude realizada através da subtração de credenciais que permitem acesso ao serviço de Internet Banking atinge usuários de diversas camadas da população que possuem um computador e conexão à Internet. Privilegiam-se nesta análise os segmentos da população que possuem renda superior a cinco salários mínimos, pois este segmento abrange 80% das residências com microcomputador e acesso à Internet. Baseado em: IBGE - **Pesquisa Nacional Por Amostra de Domicílios – PNAD 2002**. Disponível em: < http://www.ibge.gov.br/home/presidencia/noticias/10102003pnad2002html.shtm> Acesso em 07 set. 2005.

- Apresentar dados sobre o número quantitativo de incidentes obtidos pelas instituições financeiras com a análise de tendências aos métodos utilizados para a prática da fraude internet e;
- Propor soluções que visam à minimização de incidência de fraude e conseqüente perda financeira sobre instituições financeiras e usuários do serviço *Internet Banking*.

1.3 JUSTIFICATIVA

O propósito desta análise é identificar os diferentes problemas de segurança existentes no ambiente Internet que atingem clientes e instituições financeiras, através das aplicações *Internet Banking* disponibilizadas pelo sistema financeiro.

Reconhecendo as ameaças, é possível determinar os riscos e propor soluções que minimizam os impactos aos negócios, ao cliente que se utiliza deste serviço, conferindo uma maior confiabilidade ao canal Internet para realização de transações contábeis.

1.4 METODOLOGIA DA PESQUISA

Conforme mencionado no início deste capítulo, o trabalho traz os elementos que apóiam o estudo da fraude sobre o ambiente *Internet Banking* e propõe meios de contenção a este problema. Utilizando esta abordagem, é necessária a adoção de uma metodologia que apóia a pesquisa e a reflexão sobre as informações coletadas, trazendo possíveis soluções a este problema. A metodologia mais adequada é o estudo de caso.

1.4.1 Estudo de Caso

O estudo de caso é um método empírico, baseado em pesquisa, coleta, análise de dados e apresentação dos resultados[16]. Este método é utilizado para propósitos exploratórios, descritivos e explanatórios, onde se busca descrever as causas associadas aos dados coletados.

---

[16] ROBERT K. YIN, **Case Study Research: Design and Methods**, 3.edição. Thousand Oaks, CA: Sage Publications, 2002.

A adoção desta metodologia está relacionada à questão da falta de controle sobre os eventos descritos neste trabalho associado ao foco temporal, que busca resgatar eventos recentes, iniciados em 2002 e que podem ser observados no momento atual.

Em virtude da ausência de trabalhos que abordam o tema fraude no ambiente *Internet Banking*, busca-se na pesquisa teórica[17] a satisfação da primeira parte requerida pelo método científico adotado. Em apoio à pesquisa, selecionou-se uma base bibliográfica[18] enriquece o assunto abordado nesta dissertação, permitindo uma melhor compreensão do problema[19] e conseqüentemente a formulação de soluções propostas ao longo deste trabalho.

A estratégia da adoção do estudo de caso, também está relacionada a esta dissertação, por ser considerado um fenômeno social, pois a fraude é o resultado do fator humano, relacionado à distorção de um fato, buscando o convencimento de outros participantes na efetivação do golpe. Diversos fatores influenciam na ocorrência deste fenômeno, em busca de uma compreensão deste assunto, diversos temas de pesquisa são adotados neste trabalho, alguns abordando aspectos técnicos, outros mostram fatores humanos que influenciam no quadro da fraude à qual a população mundial se encontra exposto.

Há alguns pontos críticos considerados na adoção desta metodologia:

- Possível falta de rigor;
- Possível influência do investigador;
- Oferece pouca base para generalizações e;
- A investigação extensa demanda tempo para coleta dos dados.

---

[17] A pesquisa teórica é delimitada através do contexto adotado para a realização deste trabalho, disponível no capítulo dois desta dissertação.

[18] A base bibliográfica privilegia informações disponíveis na Internet. Este método pode e deve ser questionado, mas apresenta como justificativas a necessidade na obtenção de informações recentes sobre o tema focados à realidade brasileira e que não está disponível em outras publicações. Onde foram privilegiadas as fontes de pesquisa respaldadas pela representatividade junto à sociedade civil, além de isenção na disseminação de informações.

[19] Esta questão é apresentada no capítulo quatro, onde é realizada a coleta, análise dos dados e apresentação dos resultados, que são complementados na conclusão deste trabalho.

Respondendo as duas primeiras questões, buscou-se obter conteúdo quantitativo a partir de instituições financeiras, a partir das áreas que realizam esta atividade diariamente. Os dados disponíveis neste trabalho é o resultado numérico dos eventos coletados nestas instituições. Garante-se que o aspecto quantitativo reflete a soma de eventos distintos, não ocorrendo distorção no processo de agregação de eventos. O pesquisador no papel de uso de divulgação destes números se responsabiliza pelos dados e conclusões apresentados neste trabalho. No entanto, sabe-se que é provável que o número absoluto não reflita a realidade, pois o método utilizado para a coleta de eventos não abrange todo o universo de eventos que podem ocorrer, tornando-se mais um indicativo qualitativo do que quantitativo, pois baseado na mesma amostra, os indicativos delineiam a tendência dos eventos através de uma linha de tempo.

A terceira questão é tratada neste trabalho através de proposições teóricas. Este trabalho não realiza generalizações sobre populações, pois a amostra utilizada neste trabalho, trata de uma população em estudo. Portanto uma generalização para a fraude em outros continentes ou países não é aplicável neste trabalho.

Por fim, em relação a ultima questão, a obtenção dos dados pelas Instituições Financeiras auxiliou na delimitação desta coleta e período adotado para esta análise. Delimitou-se o escopo de coleta para o período de um ano[20], pois o objetivo do trabalho é mostrar um cenário atual, possibilitando avaliação de tendências para o cenário de fraudes sobre o produto Internet Banking no Brasil.

1.4.2 **Processo de escolha da bibliografia do trabalho**

Diversas fontes bibliográficas foram utilizadas para a realização deste trabalho. Algumas delas detalham aspectos técnicos do problema e outras justificam a existência deste trabalho,

[20] De Abril de 2004 a Março de 2005.

pois apresentam fatos disponíveis na mídia que descrevem a ameaça da fraude sobre a sociedade.

Ao longo de toda esta pesquisa, se escolheram fontes que contém informações recentes sobre o assunto, permitindo a disseminação de um conhecimento atual do problema. Justificando esta necessidade, é necessário citar que a maior parte das referências bibliográficas se baseia em consultas de material disponível na Internet, especializados no tema fraude ou relacionados às instituições financeiras e seus órgãos reguladores.

É importante ressaltar a grande importância do material disponível no CERT.br, na contribuição de diversos assuntos apresentados neste trabalho.

1.4.3 **Procedimento de coleta dos dados**

Instituições financeiras foram consultadas no processo de elaboração deste trabalho, buscando-se informações de indicativos numéricos relativos à fraude no ambiente *Internet Banking*. Informações, como a divulgação de perdas financeiras são informações restritas e não são divulgados ao público e não serão abordados neste trabalho. Os únicos dados repassados à pesquisa estão relacionados às informações coletadas pelo pesquisador e agregando o volume de dados quantitativos que podem não representar o todo cenário de fraudes aplicadas sobre os usuários dos serviços de *Internet Banking*, mas permite delinear a tendência do problema ao longo do período de coleta dos dados. Vale lembrar que a maioria dos incidentes apresentados neste trabalho é o resultado da coleta de mensagens disponíveis em diversas caixas de correio eletrônico[21] que foram fornecidas para a elaboração de exemplos descritos no capítulo três.

[21] As contas de correio eletrônicas utilizadas para o recebimento dos exemplos mencionados no capítulo quatro deste trabalho, não serão detalhadas, pois visam proteção à identidade dos usuários e instituições responsáveis pelo recebimento destas mensagens eletrônicas. O pesquisador assume responsabilidade e assume o papel de fonte dos dados aqui informados e analisados.

É necessário lembrar que os dados expostos neste trabalho não estão disponíveis para consulta pública por qualquer um das instituições financeiras consultadas[22] e que as conclusões sobre estes dados é o resultado à análise realizada exclusivamente pelo autor deste trabalho.

1.5 ESTRUTURA DO TRABALHO

Permitindo a compreensão do problema e apoiando o alcance deste objetivo, o trabalho foi estruturado da seguinte forma:

O capítulo dois contextualiza a pesquisa e esclarecendo os pontos relevantes que devem ser apresentados para melhor compreensão das diversas áreas do conhecimento envolvidas no processo de fraude sobre o sistema *Internet Banking*. A contextualização do trabalho está segmentada na visão de tecnologia, negócio, engenharia social e investigação.

O capítulo três contém um foco técnico-descritivo dos problemas que vitimam clientes do ambiente Internet e instituições financeiras. Em virtude da participação do pesquisador nos eventos ocorridos e registrados desde 2002 é possível descrever, com detalhes, a reconstituição de eventos e sua evolução aos dias atuais. Dados sobre incidentes são apresentados e analisados, permitindo caracterizar tendências aos golpes praticados pelos fraudadores.

O capítulo quatro contém a formulação de propostas que buscam mitigar a fraude no ambiente *Internet Banking* com atuação em três pilares principais; o usuário final, provedores e fraudadores.

No final deste trabalho, no capítulo cinco, são apresentadas algumas propostas de temas que podem ser abordados em trabalhos acadêmicos futuros, permitindo a extensão do estudo sobre o tema "fraude sobre o ambiente financeiro", e a conclusão deste trabalho.

---

[22] Em virtude do sigilo requerido no processo de divulgação destes dados, algumas informações foram descaracterizadas, mantendo o teor quantitativo necessário para a realização das análises realizadas neste trabalho. A qualidade das informações apresentadas tem a responsabilidade assumida pelo pesquisador.

2 CONTEXTO DO TRABALHO

A fraude sobre o ambiente *Internet Banking* é um assunto amplo, portanto, deve ter sua análise delimitada através de alguns temas auxiliam a compreensão deste trabalho. O conjunto de itens mostrados a seguir será o contexto deste estudo, permitindo as seguintes visões do problema:

- **Tecnologia.** Esta visão permite identificar os itens de segurança lógica e equipamentos de tecnologia utilizados na criação e manutenção do serviço *Internet Banking*. Serão utilizados elementos pertencentes à segurança da informação para justificar as tecnologias adotadas;
- **Negócio.** Os motivadores para a criação do serviço *Internet Banking* foram introduzidos neste trabalho a partir dos conceitos apresentados no capítulo anterior, complementando estas informações, o contexto de negócio deverá abordar a perspectiva da instituição financeira sobre os riscos existentes ao disponibilizar o serviço *Internet Banking* aos clientes de instituições financeiras;
- **Engenharia Social.** Este tema permite reconhecer os aspectos psicológicos que identificam os métodos de persuasão de usuários do ambiente Internet, possibilitando a subtração de informações confidenciais e permitindo que estes dados sejam utilizados para a efetivação da fraude no ambiente *Internet Banking*;
- **Investigação.** Esta abordagem permite reconhecer os procedimentos necessários para a reconstrução dos fatos relativos a ocorrências de crimes informáticos, e conseqüentemente a coleta de informações necessárias relacionadas à perícia, visando apresentação destes dados coletados sob validade jurídica;

2.1 VISÃO DA TECNOLOGIA

Neste trabalho a tecnologia é interpretada como uma ferramenta necessária para se conceber e realizar um projeto de conectividade entre equipamentos e sistemas, em nosso contexto, um projeto de *Internet Banking*.

Entretanto, cuidados dever ser tomados na utilização de qualquer tecnologia, pois quando se trata de ambientes como a Internet, os riscos de exposição dos sistemas aumentam, devido à disponibilidade dos serviços a um ambiente hostil, permitindo a efetivação de diversos ataques sobre esta infra-estrutura. Tratando o assunto sob esta ótica, é necessário construir esta visão partindo dos princípios básicos da segurança da informação, evoluindo à identificação dos elementos que compõem um sistema de *Internet Banking* e suas conexões. Os elementos escolhidos para o auxílio desta descrição são os seguintes:

- Segurança da Informação;
- Arquitetura da rede;
- Filtro de pacotes ou firewall;
- Segmentação das redes locais;
- Autenticação;
- Criptografia;
- Detecção de Intrusos e;
- Segurança nos Servidores;

Os primeiro item conceitua a segurança no contexto de tecnologia da informação. O segundo item identifica dos elementos físicos e lógicos necessários para a criação de um sistema *Internet Banking* seguro, e os seis itens adiante descrevem detalhes das necessidades identificadas na arquitetura de rede.

Em adição aos tópicos, há um item que consolida os elementos descritos, permitindo a proposta de uma estrutura recomendada na implantação de serviços bancários utilizando a Internet[23].

2.1.1 **Segurança da Informação**

No momento que o problema das fraudes sobre o ambiente *Internet Banking* é tratado sob o aspecto tecnológico, é necessário se recorrer aos princípios básicos da segurança da informação para melhor compreensão deste trabalho. Dentre as diversas terminologias que cercam este assunto, há um que abrange este tema, a Segurança da Tecnologia da Informação. Esta nomenclatura é descrita em (IEEE, p.41) de aceitação internacional, criado pela Comunidade Européia, e inclui os seguintes termos:

- **Confidencialidade.** Mecanismo de prevenção contra o uso não autorizado da informação e busca evitar a quebra de sigilo de dados;
- **Integridade.** Mecanismo preventivo às alterações da informação e busca evitar a modificação não autorizada de dados;
- **Disponibilidade.** Mecanismo que previne a suspensão ou lentidão no acesso a informações ou recursos; busca evitar a subtração de recursos computacionais e comprometimento da qualidade de serviços computacionais.

Dos três termos citados anteriormente, a confidencialidade é o item de imediata correlação ao tema fraude sobre o ambiente *Internet Banking*. Esta correlação se faz presente, pois se interpreta a efetivação do uso inadequado de credenciais de identificação sobre o ambiente *Internet Banking* como resultado direto da quebra do sigilo de dados do portador da informação, ou seja, o cliente da instituição financeira.

[23] É importante salientar que as instituições financeiras podem apresentar diferenças na concepção da arquitetura de rede e segurança, entretanto é importante observar que os elementos apresentados neste tópico estão presentes, em pelo menos, nas maiores instituições financeiras brasileiras.

Entretanto os outros termos apresentam papel complementar, e estão relacionados à fraude. A integridade, neste contexto, é o resultado do uso inadequado de credenciais, visando à realização de transações financeiras através do ambiente *Internet Banking*. Portanto a efetivação de alterações não autorizadas pelo usuário legítimo do sistema, ou seja, o cliente da instituição financeira é uma quebra de integridade aos dados que representam real a situação financeira do cliente.

A disponibilidade também tem seu papel importante quando associamos ao problema de fraudes. Será detalhado, neste trabalho, a existência de programas denominados cavalos de tróia, que induzem a infecção do computador, buscando a subtração de credenciais do usuário deste equipamento. Estes programas, pois mais simples que sejam, comprometem o desempenho do equipamento vitimado por este ataque. Portanto, compromete a qualidade de serviço que este computador pode oferecer. Além disto, há golpes relacionados à fraude que apresentam a capacidade de redirecionar o acesso da vítima a outros ambientes na Internet que simulam o acesso ao sistema legítimo de *Internet Banking* de instituições financeiras. Neste exemplo é clara a quebra de disponibilidade causada por este mecanismo, pois a vítima deixa de acessar o serviço legítimo em busca do acesso acidental a um sistema que se faz passar pelos produtos que a instituição financeira oferece na Internet.

Apesar de muitos dos problemas relativos à segurança da informação apontar fragilidade na infra-estrutura existente no computador dos usuários do ambiente Internet, é necessário aplicar os conceitos de confidencialidade, integridade e disponibilidade sobre os equipamentos e tecnologias relativos à disponibilidade dos serviços de *Internet Banking*, ou seja, na estrutura suportada e disponibilizada pela instituição financeira.

O item a seguir detalhará a disposição lógica dos equipamentos de rede sobre o ambiente dos bancos na Internet.

2.1.2 **Arquitetura da rede**

Para que possamos obter compreensão clara da arquitetura utilizada nestes serviços, precisamos compreender os princípios básicos para a interconexão de equipamentos no ambiente Internet. A abordagem tecnologia partirá do princípio que componentes de rede como *hub*[24], *switch*[25], roteador[26], DNS[27] e servidor *Web*[28] são tecnologias de prévio conhecimento do leitor deste trabalho.

Além dos componentes de rede citados anteriormente, recomenda-se (ISS, p.26-30) (ITSECURITY) o uso dos seguintes itens para concepção da arquitetura de aplicações bancárias no ambiente Internet:

- Filtro de Pacotes ou *Firewall*;
- Segmentação das redes locais;
- Autenticação;
- Criptografia;
- Detecção de Intrusos e;
- Segurança nos Servidores.

---

[24] *Hub* é um dispositivo que tem a função de interligar computadores em uma rede local. A transmissão enviada a partir de um equipamento conectado à hub é propagada aos outros equipamentos conectados a ela – INFOTESTER. **Diferenças entre Hub, Switch e Roteador**. Disponível em: <http://www.infowester.com/hubswitchrouter.php> Acesso em 17 mar. 2005.

[25] *Switch* apresenta a mesma função do hub, a diferença entre os equipamentos está associada à propagação da transmissão de dados, onde a informação só é enviada ao computador destino – INFOTESTER. **Diferenças entre Hub, Switch e Roteador**. Disponível em: <http://www.infowester.com/hubswitchrouter.php> Acesso em 17 mar. 2005.

[26] O roteador apresenta capacidade de interconectar redes, permitindo, o redirecionamento de pacotes, através da melhor rota, em direção a um computador destino. – INFOTESTER. **Diferenças entre Hub, Switch e Roteador**. Disponível em: <http://www.infowester.com/hubswitchrouter.php> Acesso em 17 mar. 2005.

[27] DNS é a abreviação de *Domain Name System*. Este serviço ou sistema é composto por uma base hierárquica, distribuída que permite a resolução de domínios em endereços IP e vice-versa. REGISTRO.BR. **FAQ (Perguntas Freqüentes)**. Disponível em: <http://registro.br/faq/faq5.html> Acesso em 17 mar. 2005.

[28] Servidor Web é um equipamento que agrega um software que permite a disponibilização de serviços de conexão entre página Web existentes no servidor e um visualizador denominado Browser. BOUTELL.COM. **WWW FAQs: What is a web Server?** Disponível em: <http://www.boutell.com/newfaq/definitions/server.html>. Acesso em 17 mar. 2005.

2.1.3 **Filtro de pacotes ou firewall**

A presença de filtro de pacotes ou *firewall* tem o objetivo de estabelecer de regras no tráfego entre redes conectadas (Zwicky, p.165-223). Estas regras, em muitos casos, são as linhas de defesa de uma rede contra ameaças externas.

O Filtro de pacotes é um filtro baseado em protocolo, endereços IP de origem e destino e porta de conexão. Em muitas vezes esta linha de defesa é realizada em roteadores que delimitam o acesso da rede interna à Internet;

O *firewall* além de conter funcionalidades de filtro de pacotes, é um sistema mais complexo composto de um equipamento que contém duas ou mais placas de rede, possuindo capacidade de processamento de informações através de um hardware e um software especializado com a funcionalidade descrita anteriormente.

As topologias de rede contendo *firewalls* são as mais diversas. As configurações mais simples podem ser encontradas em computadores com sistemas operacionais conhecidos (Windows, Unix e Linux), e até em sistemas que são compostos por hardware e software projetados visando melhor desempenho do equipamento.

Em relação ao contexto deste trabalho, o *firewall* tem um papel muito importante no processo de concepção e criação do serviço *Internet Banking*, pois os filtros de pacotes permitem que computadores conectados na rede Internet acessem apenas o serviço Web oferecido pelo sistema da instituição financeira, evitando exposição desnecessária do ambiente, minimizando os riscos de ataques externos ao sistema bancário[29].

[29] No sistema financeiro nacional, algumas instituições financeiras empregam o uso de filtro de pacotes em roteadores de borda, ou seja, nos equipamentos conectados ao link disponível pelo provedor de acesso à Internet, complementado ou outro filtro de pacote existente em um *firewall*. Atualmente são duas as opções de *firewall* utilizado pelos bancos, uma delas se baseia na instalação de um software firewall em um computador contendo sistema operacional de mercado (Plataforma *Microsoft*, *Unix* ou *Linux*), e outra opção que trata da aquisição de equipamentos com sistema operacional e *software firewall* especializados para esta função, conhecidos também como *appliance*. Em virtude da robustez e especialização e desempenho do produto, a versão em *appliance*, em geral, apresenta um custo de aquisição mais elevado comparado à outra opção.

2.1.4 **Segmentação das redes locais**

O conceito de segmentação das redes locais tem como objetivo a restrição do tráfego entre as redes internas e a as redes externas. Neste trabalho a rede externa será representada pelo ambiente Internet. Entre estas redes, recomenda-se a criação de uma área intermediária conhecida como DMZ, ou rede desmilitarizada. A seguir ilustra-se a conexão entre a rede interna, rede externa e a rede desmilitarizada.

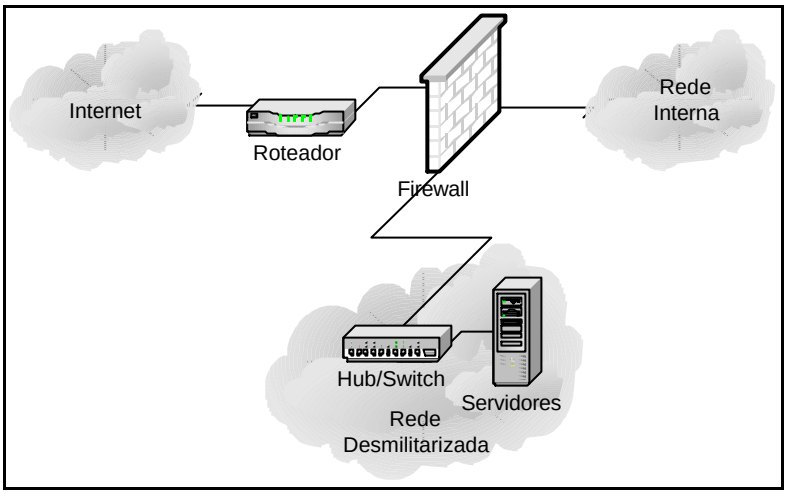

Figura 5 - Representação da Rede Desmilitarizada

É possível perceber na rede desmilitarizada a presença de servidores. Dentre estes equipamentos, encontra-se em instituições financeiras a presença do sistema de *Internet Banking*.

Entretanto, sabe-se que o *Internet Banking* é um dos diversos serviços Web oferecidos à Internet, composto de informações que são disponibilizadas ao cliente, dados que em geral estão armazenados em bancos de dados[30]. Visando uma maior proteção a estes dados, é possível adotar a arquitetura de rede com diversas redes desmilitarizadas, com regras de acesso restritas, permitindo neste contexto, o acesso exclusivo do sistema de dados através do

[30] A arquitetura apresentada em entrevistas a técnicos de algumas instituições financeiras brasileiras. Buscando a preservação destas estruturas, adotou-se também a consulta a duas arquiteturas de rede publicadas FRANKLING SAVINGS BANK - **Internet Banking System Security**. Disponível em: <http://www.franklinsavingsbank.com/site/security.html> Acesso em 18 mar. 2005 e; QUALISOFT - **Case Banco Santos**. Disponível em: < http://www.qualisoft.com.br/casos/bancosantosSG2.asp > Acesso em 18 mar. 2005.

servidor Web. Para melhor ilustrar esta configuração, será mostrado um exemplo de segmentação em um ambiente financeiro.

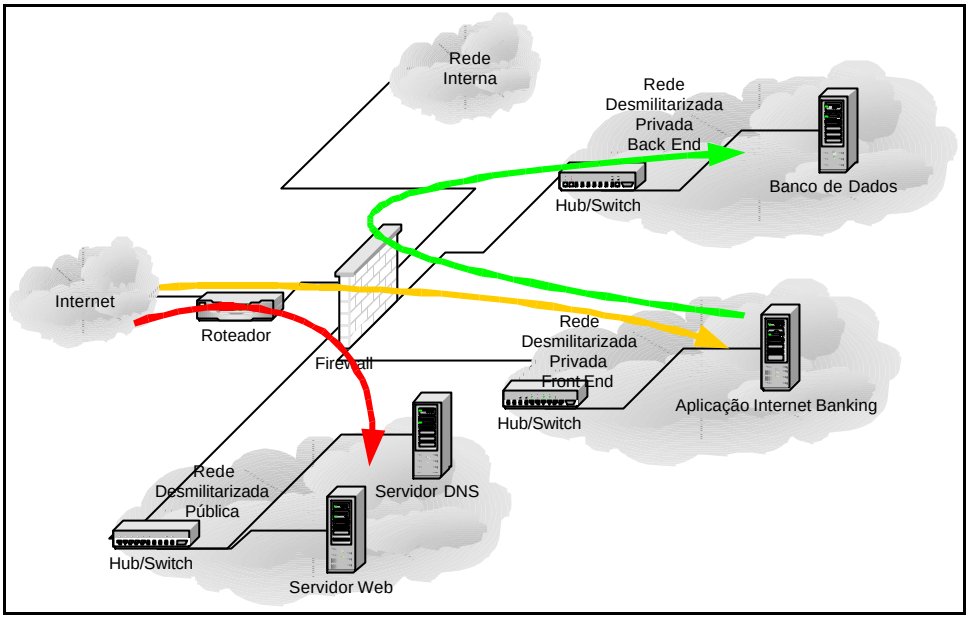

Figura 6 - Redes desmilitarizadas no ambiente financeiro

Pode-se perceber que há três redes desmilitarizadas na figura anterior e três setas que indicam a utilização de filtros para acesso a estas redes.

A rede descrita como desmilitarizada pública permite acesso ao servidor DNS, e Web, através da rede Internet. Percebe-se que este acesso está sendo indicado pela seta vermelha, o que pressupõe uma configuração menos restrita aos usuários conectados no ambiente Internet.

Adiante, percebe-se que a rede Internet também possui acesso à outra rede desmilitarizada denominada rede privada *front-end*[31]. Esta denominação tem caráter mais restritivo comparado à rede mencionada anteriormente, e busca-se neste ambiente a proteção do servidor de aplicação que contém o serviço de *Internet Banking*, disponível aos clientes das instituições financeiras. A seta alaranjada existente na figura acima ilustra o filtro aplicado para acesso a esta rede.

[31] *Front-end* neste contexto está definido como um provedor de serviço que não possui nenhuma informação ou dado armazenado. Neste caso servidor *Web* é não armazena qualquer dado do cliente no equipamento.

Por último, ilustrado pela seta verde, temos o acesso da rede desmilitarizada privada *front-end* à rede desmilitarizada *back-end*[32]. Esta última rede representa o local mais protegido da rede, onde se podem encontrar dados transacionais relativos aos serviços bancários[33]. Portanto, estes dados são acessados apenas pelo servidor de aplicação *Internet Banking*, visando contenção do acesso a este recurso[34].

Apesar da existência de equipamentos de conexão descritos como *Hub* / *Switch* na figura anterior, recomenda-se o uso apenas do *switch*, pois este dispositivo minimiza o risco referente à captura de informações que podem trafegar dentro das redes desmilitarizadas e diminui o tráfego de dados, pois o fluxo é segregado nas portas de conexão do equipamento.

2.1.5 **Autenticação**

A autenticação permite a identificação positiva de um usuário dentro de um sistema. Dentro do contexto deste trabalho, a autenticação está relacionada às credenciais que permitem o reconhecimento do cliente no sistema de *Internet Banking*.

Há três fatores de autenticação utilizados em sistemas, a combinação de dois destes três fatores é considerada uma autenticação forte. Estes três fatores são os seguintes[35]:

- **Algo que o usuário conhece.** São dados que identificam o usuário no sistema e sua respectiva senha;

---

[32] *Back-end* neste contexto, trata do sistema de armazenamento de informações que é acessível por um sistema *Front-end*. Neste caso, um servidor com um banco de dados.

[33] Recomenda-se na existência de bancos de dados a segmentação do acesso ao banco de dados através de um novo conjunto de filtros impedindo que redes menos seguras como a Internet acessem diretamente o serviço do banco de dados (Zwiky, p.664-678).

[34] É necessário lembrar que a topologia apresenta apenas caráter ilustrativo. Recomenda-se para a segregação de ambientes como este a utilização de mais *firewalls*, visando à integridade no acesso às redes caso o equipamento seja comprometido por qualquer tipo de ataque. Caso esta preocupação seja ainda maior, recomenda-se o uso de *firewalls* de diversos fabricantes, nos diferentes segmentos, pois neste caso, a vulnerabilidade de um fabricante pode não comprometer a exposição dos dados de outro segmento da rede, pois a exploração de um dos firewalls pode não ser aplicável ao outro equipamento.

[35] Definição disponível no documento RSA Security - **The Cryptographic Smart Card: A Portable, Integrated Security Platform** Disponível em: < http://www.rsasecurity.com/products/securid/whitepapers/smart/CSC_WP_0301.pdf > Acesso em 06 out. 2005.

- **Algo que o usuário possui.** São objetos que pertencem ao usuário e o auxiliam na identificação. O cartão magnético de um banco, certificados digitais e dispositivos geradores de senhas dinâmicas estão baseados neste fator de autenticação e;
- **Algo que constitui o usuário.** Características pessoais como a íris, voz e impressão digital; podem ser utilizadas para autenticação em sistemas. Hoje a biometria é técnica utilizada para identificação destas características mencionadas.

Hoje em sistemas *Internet Banking*, são utilizados os dois primeiros fatores de autenticação citados anteriormente. Portanto isto representa uma autenticação forte, segundo princípios da segurança da informação[36]. Entretanto a fraude sobre o ambiente é possível em certas condições, onde são subtraídas tanto as informações que o usuário conhece quanto algo que ele possui. Serão detalhadas em um capítulo adiante as técnicas utilizadas para a subtração destes recursos.

2.1.6 **Criptografia**

A criptografia é uma tecnologia que garante a confidencialidade e privacidade dos dados[37]. Há duas utilizações possíveis para a criptografia no ambiente *Internet Banking*, a proteção dos dados armazenados em bancos de dados e o sigilo das informações que trafegam em meios promíscuos como a Internet.

A primeira utilização citada no parágrafo anterior não é obrigatória, entretanto em caso de exposição intencional ou acidental do servidor responsável pelo armazenamento de dados de clientes, as informações sem proteção criptográfica estarão legíveis. Há registro (ISS, p.29) de

[36] É necessário mencionar a existência de um artigo que contesta a afirmação da robustez de dois fatores de autenticação em condições de ataque relativo ao roubo de credenciais utilizados para aplicação de fraude sobre o Internet Banking. Bruce Schneier - **The Failure of Two-Factor Authentication** Disponível em: <http://www.schneier.com/crypto-gram-0503.html#2> Acesso em 06 out. 2005.

[37] É importante lembrar que algumas instituições financeiras também utilizam a criptografia para identificação em alguns segmentos de clientes em Internet Banking, entretanto este assunto não será explorado, pois se busca mencionar neste segmento o papel da criptografia no sigilo das informações trafegadas.

exposição de dados de clientes, em função da ausência desta utilização em servidores de banco de dados, e, portanto a exploração desta vulnerabilidade não é apenas um fato teórico.

A segunda forma citada do uso da criptografia é adotada pelas instituições financeiras[38], pois a comunicação entre o cliente do serviço e o banco pode ser monitorada, permitindo a exposição de dados confidenciais como os dados de autenticação no sistema. A ausência de utilização de criptografia em sistemas bancários permite a subtração dos dados de autenticação do cliente por terceiros, alteração das transações realizadas pelos clientes e permite a aplicação de um golpe, onde fraudadores podem disponibilizar serviços de *Internet Banking* em equipamento externo à instituição financeira, ludibriando clientes que acessam inadvertidamente este servidor.

A criptografia adotada no processo de comunicação utiliza um protocolo conhecido como SSL (*Security Socket Layer*) e o processo de cifragem dos dados ocorrem a partir do uso de estrutura de chave pública e privada (CALLAO). Para melhor compreensão deste processo, será ilustrado a seguir um diagrama utilizado na comunicação SSL:

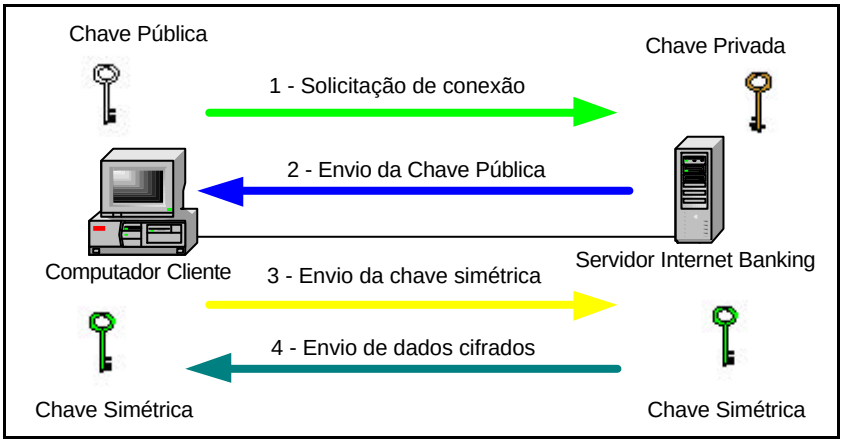

Figura 7 - Processo de comunicação no ambiente *Internet Banking*

A figura ilustra o processo de comunicação ocorre na ordem vertical das setas, seguindo a numeração de um a quatro. Em um primeiro momento, o cliente solicita conexão ao servidor

[38] FEBRABAN. **Segurança no uso da Internet** Disponível em: <http://www.febraban.org.br/Arquivo/Servicos/Dicasclientes/dicas7.asp> Acesso em 18 mar. 2005.

Internet Banking. Em resposta a esta solicitação, o servidor envia ao cliente uma chave pública[39]. Esta chave pública é utilizada pelo cliente para o envio cifrado de uma chave secreta randômica, também conhecida como chave simétrica. O servidor interpreta a informação cifrada enviada através da chave privada do servidor *Internet Banking*. De posse da chave simétrica, a cifragem e a interpretação dos dados protegidos ocorrem apenas com a utilização da chave simétrica.

Justifica-se o uso de chaves simétricas, devido ao menor consumo de recursos computacionais. Além disto, as chaves simétricas, também conhecidas como chaves de sessão, são validas somente durante um intervalo de tempo, devendo ser renegociada uma nova chave após este período.

Tanto a estrutura de chaves públicas e privadas quanto às chaves simétricas trabalham com algoritmos e tamanhos de chaves distintos que podem ser descritos da seguinte forma (MAIA; PAGLIUSI):

- Chave pública e privada;
    - **Algoritmos:** RSA, ElGamal, Diffie-Helman e Curvas Elípticas.
    - **Tamanhos de chaves comuns:** 512, 1024 e 2048 bits.
- Chave simétrica;
    - **Algoritmos:** RC2, RC4, DES, Triple DES, IDEA e Blowfish.
    - **Tamanho de chaves comuns:** 40, 56 e 128 bits.

[39] Há situações onde o cliente possui uma chave privada, padrão RSA. Nestes casos, o cliente é submetido por passos adicionais, onde o cliente envia a chave pública, ocorrendo à validação desta junto ao banco de dados da instituição financeira ou em órgãos certificadores que mantêm serviços de verificação de consistência do certificado no ambiente Internet.

Os serviços baseados em *Internet Banking* utilizam em geral, chaves públicas e privadas, com utilização do algoritmo RSA de 1024 bits e chaves simétricas utilizando algoritmo RC2 ou RC4 com chaves de 128 bits[40].

2.1.7 **Detecção de Intrusos**

A implementação de sistemas capazes em detectar intrusos, em tempo real[41], nas redes das instituições financeiras é uma medida essencial na busca de invasores, sejam eles de origem externa ou interna à empresa (WIKIPÉDIA).

Esta detecção ocorre a partir de equipamentos conectados à rede, chamados de sensores, que podem ser classififcados em:

- ***Network* IDS.** Estes sensores, configurados em equipamentos da rede, buscam características de tráfego na rede que se assemelham a ataques registrados no sistema de IDS e;
- ***Host* IDS.** São agentes instalados em servidores contendo aplicações que buscam por atividades inesperadas ao perfil normal de um usuário ou da aplicação.

Os IDS surgiram na versão de *Network* IDS, protegendo redes e equipamentos contidos no segmento protegido por este serviço. Esta é a modalidade mais utilizada para detecção de intrusos, pois a instalação de um *Host* IDS, por mais simples que seja a sua implementação, consome recursos no equipamento escolhido para a proteção; o que pode comprometer a performance do equipamento e sua respectiva aplicação; resultando em uma possível queda na qualidade de serviço fornecido aos clientes.

---

[40] CERT.br. **Cartilha de Segurança para Internet.** Versão 3.0**.** Disponível em: < http://cartilha.cert.br> Acesso em 08 set. 2005.

[41] Todos os sistemas de IDS são capazes de efetuar identificação de ataques em tempo real, entretanto esta informação nem sempre é mencionada. Em uma das bibliografias consultadas, é possível ler explicitamente esta característica. SYMANTEC. **Symantec Host IDS**. Disponível em: <http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=48&EID=0>. Acesso em 18 mar. 2005.

Entretanto, IDSs utilizados para a proteção do tráfego da rede não são suficientes para a garantia da proteção dos serviços, pois há questões que os IDSs não são capazes de tratar com eficiência. Estas questões são as seguintes (WIKIPÉDIA):

- **Protocolos cifrados.** Implementação de SSL e IPSec, são protocolos que protegem a área de dados do pacote IP, dificultando em muitas vezes a detecção de ataques. Nestas implementações, o IDS apenas pode efetuar a análise sobre o cabeçalho do pacote IP;
- ***Switches.*** Este equipamento que nem sempre permite a utilização de um IDS, pois o tráfego é comutado à porta de destino do switch. Entretanto há implementações de swiches que contém funções de IDS, ou até características de espelhamento de portas, que permitem a análise de tráfego, caso seja necessário; e
- **Redes de alta velocidade.** Há diversas discussões (WIKIPÉDIA) que tratam da capacidade dos IDSs em analisar todos os pacotes trafegados em redes de alta velocidade, buscando resolver este problema há implementações que visam a segregação de funções de IDSs em redes, diminuindo os riscos de perder pacotes IP intrusivos à rede.

No âmbito do serviço de *Internet Banking*, pertecebe-se que o problema mais crítico é a utilização de criptografia SSL no tráfego estabelecido entre o cliente e a instituição financeira. Pois nestes casos os *Network* IDSs não são eficazes; e apenas os *Host* IDSs podem auxiliar na detecção de ameaças, mas devido a criticidade do serviço e o grande volume de acesso efetivado pelos clientes aos servidores responsáveis pela disponibilidade do serviço de *Internet Banking*, a adoção de *Host* IDS é pouco praticada.

2.1.8 **Segurança nos Servidores**

A instalação do sistema operacional e configuração da aplicação *Web* requerem cuidados especiais, pois as vulnerabilidades dos sistemas, quando expostos, podem permitir o acesso a recursos ou informações existentes no servidor que disponibiliza aplicações na Internet. Neste caso, a preocupação está centrada na possível exposição de informações de clientes através do serviço de *Internet Banking*.

Visando a adoção de uma arquitetura segura para servidores, recomenda-se (ISS, p.29) cumprir os itens a seguir:

- Configuração contemplando nível máximo de segurança sobre o sistema operacional;
- Aplicação de recomendações dos fabricantes de equipamentos de rede e servidores;
- Criação de políticas aplicáveis ao gerenciamento de senhas e registros do sistema;
- Análise e auditagem dos códigos utilizados no desenvolvimento do produto *Internet Banking*[42] e;
- Aplicação de testes de vulnerabilidade periódicos.

A aplicação e reavaliação dos itens mencionados acima são essenciais à manutenção dos níveis mínimos de segurança exigidos à preservação do serviço de *Internet Banking* e dados trafegados. Vale lembrar que a própria instituição financeira deve especificar o seu padrão, devido à diversidade de sistemas operacionais existentes no mercado e sistemas utilizados na instalação do servidor no ambiente *Web*[43].

2.1.9 **Consolidação da Arquitetura**

Integrando os itens descritos na visão da tecnologia sobre o ambiente *Internet Banking*, pode-se obter o diagrama a seguir:

---

[42] Recomenda-se que a programação em linguagens como Java, JavaScript, VBScript, Active X, contemple condições de segurança que não fragilize o ambiente, incluindo a Instituição Financeira e o cliente que se utiliza do serviço (Zwiky, p.403-412).

[43] O W3C disponibiliza diversas recomendações de segurança em servidores *Web* de diversas tecnologias e plataformas. STEIN, Lincoln D.; STEWART, Jowh N. **The World Wide Web Security FAQ.** W3C. Disponível em: < http://www.w3.org/Security/Faq/www-security-faq.html> Acesso em 21 mar. 2005.

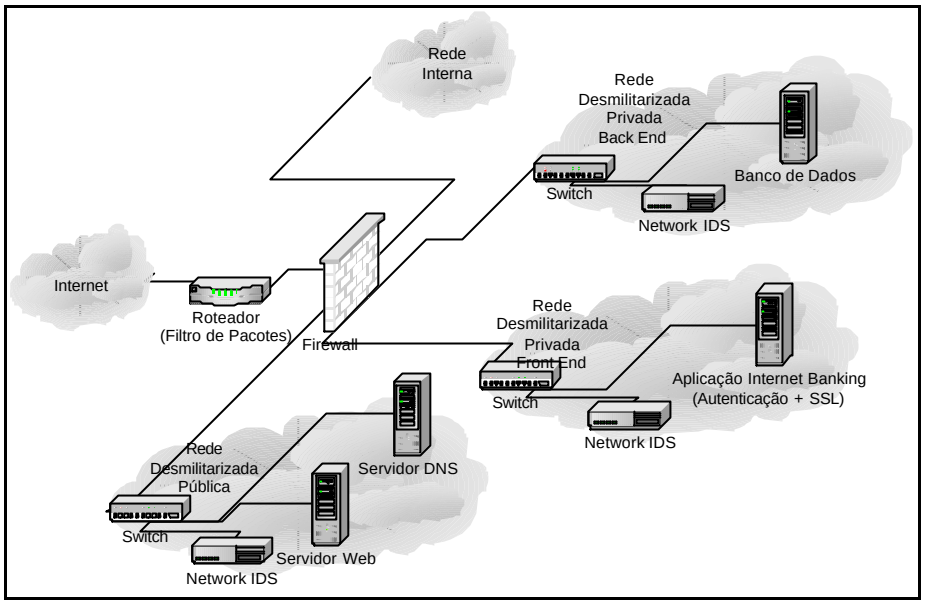

Figura 8 - Diagrama de rede consolidado do ambiente *Internet Banking*

Diferente do diagrama apresentado no item 3.1.2, esta figura ilustra a presença de *Network* IDSs nos diversos segmentos da rede, protegendo seus respectivos sistemas; os equipamentos de interconexão dos segmentos são *switches*, o que melhora o tráfego entre os servidores disponíveis na estrutura apresentada; evidencia-se a necessidade da utilização de filtro no roteador de conexão das redes à Internet, o que indica a primeira linha de defesa da instituição financeira ao ambiente de rede menos seguro; é descrito ainda no servidor de aplicação *Internet Banking* a necessidade de autenticação e criptografia, representado pela sigla SSL; e por fim, não mencionado, mas explícito, há necessidade da configuração segura de todos os equipamentos conectados às diversas redes existentes no diagrama e revisão periódica da inviolabilidade do ambiente.

Vale lembrar que este é apenas um diagrama apenas ilustrativo, que pode e deve ser complementado, considerando o dimensionamento do número de servidores necessários para atendimento dos serviços de *Internet Banking*, além da adoção de redundância do ambiente, garantindo a alta disponibilidade dos serviços aos clientes.

2.2 VISÃO DO NEGÓCIO

Na visão de negócio, o *Internet Banking* é mais um meio utilizado para a efetivação de pagamentos e transações eletrônicas que impulsionam o comércio eletrônico, criando oportunidades maiores às instituições financeiras[44].

Alguns detalhes sobre a concepção e motivação da criação deste tipo de serviço no Brasil foram descritos no primeiro capítulo deste trabalho. Pretende-se concentrar neste item uma avaliação sobre os riscos que estão expostos os serviços bancários, hoje bem descritos e disseminados através do Comitê da Basiléia[45].

2.2.1 Riscos relativos aos serviços bancários

As instituições financeiras, como qualquer empresa, apresentam riscos que podem levar a interrupção de seus serviços. Em geral este aspecto está relacionado a eventos improváveis que levam a perda de capital.

Em virtude da existência destes riscos, é necessária a alocação de capital[46] capaz de suprir adversidades ao longo da existência de um banco. E de acordo com o Comitê da Basiléia, 20% da receita das Instituições Financeiras devem ser reservadas para a cobertura de eventuais perdas. Esta reserva é efetivada através de duas formas (NETO E CRESTO, p.48):

- **Regulatória:** O capital alocado é suficiente para enfrentar as adversidades, preservando a integridade da instituição, capital de acionistas e de terceiros;

---

[44] BASEL - **Risk Management Principles for Electronic Banking and Electronic Money Activities**. Basel Commitee on Banking Supervision. Disponível em: <http://www.bis.org/publ/bcbs35.pdf> Acesso em: 02 mar. 2005.

[45] http://www.bis.org/

[46] A alocação de capital considera diversos fatores dinâmicos, que requer ajustes periódicos na reserva de capital (Jane, p.193-216).

- **Econômica:** O capital reservado é igual ao excesso de ativos sobre passivos, garantindo aos acionistas retornos futuros, mesmo diante de incertezas associadas à atividade.

Este capital alocado deve cobrir os seguintes tipos de riscos[47]:

- **Risco Operacional:** É definido como a estimativa de perdas resultantes de processos internos, falhas pessoais, sistemas inadequados e eventos externos;
- **Risco de Imagem:** São os riscos referentes à reputação da instituição em situações onde a opinião pública negativa resulta na perda crítica de fundos e clientes. Este processo envolve a exposição do banco junto aos seus clientes e parceiros comerciais;
- **Risco Legal:** Este item busca minimizar ou eliminar questões de violações e não conformidades das partes envolvidas em uma transação bancária, perante a lei, órgãos regulatórios e práticas adotadas no mercado e;
- **Outros riscos:** Há outros riscos relativos às instituições financeiras como risco de crédito, risco de liquidez, risco de mercado entre outros, que influenciam a operação e a continuidade de negócio do banco perante o sistema financeiro e à sociedade.

Avaliando a fraude no ambiente Internet como resultado de um risco previamente assumido pelas instituições financeiras, percebe-se que este é o resultado de perdas causadas por agentes externos e, portanto classificado como uma particularidade do risco operacional, conforme a breve descrição dos riscos mencionados anteriormente.

---

[47] BASEL - **Risk Management Principles for Electronic Banking and Electronic Money Activities**. Basel Commitee on Banking Supervision. Disponível em: <http://www.bis.org/publ/bcbs35.pdf> Acesso em: 02 mar. 2005.

Evitando se estender na descrição dos outros riscos, que não são relevantes para a produção deste trabalho, buscaremos mencionar apenas informações sobre os riscos operacionais.

2.2.2 **Riscos Operacionais**

Os riscos operacionais estão relacionados às deficiências ou falta de integridade nos sistemas que oferecem apoio aos serviços bancários[48]. Para identificar os pontos vulneráveis destes sistemas, é necessário mapear os fluxos dos processos, uma vez que estas informações permitirão obter dados sobre causas e efeitos resultantes à ocorrência destes riscos. Com estas informações é possível propor controles rígidos, visando à redução de prejuízos financeiros, podendo chegar à eliminação dos mesmos.

Vale lembrar que risco operacional não está relacionado apenas às transações eletrônicas realizadas através do ambiente *Internet Banking*. Esta categoria de risco também se aplica em outros canais utilizados pelas instituições financeiras para o oferecimento de serviços ao cliente[49].

As instituições financeiras de posse destas informações buscam adotar mecanismos visando à eliminação de riscos e conseqüentemente às perdas relacionadas aos riscos operacionais; entretanto a eliminação dos riscos pode implicar em investimentos que representam custos maiores comparados às perdas. Portanto a instituição financeira precisa decidir neste caso, a aceitação ou não das perdas financeiras. E caso este prejuízo seja aceito pelo banco, este assume implicitamente o risco operacional.

Buscando facilitar a análise sobre os riscos operacionais, o Comitê da Basiléia divide os riscos operacionais em duas categorias:

---

[48] BASEL - Risk Management Principles for Electronic Banking and Electronic Money Activities. Basel Commitee on Banking Supervision. Disponível em: <http://www.bis.org/publ/bcbs35.pdf> Acesso em: 02 mar. 2005.

[49] Estes outros serviços são descritos no primeiro capítulo deste trabalho.

- Riscos de segurança e;
- Projeto, criação e manutenção de sistemas.

Os riscos de segurança estão relacionados aos controles de acesso aos sistemas, informações disseminadas pela instituição financeira e parceiros comerciais, e no caso de dinheiro eletrônico, a adoção de processos contra a falsificação. O controle de acesso aos sistemas é um processo complexo devido à capacidade dos clientes em efetuar acessos aos sistemas bancários utilizando computadores localizados em diversos pontos de acesso distribuídos geograficamente. Estes computadores podem ser desde terminais de auto-atendimento a computadores pessoais com acesso a estes serviços através da Internet.

Os riscos de segurança se traduzem em perdas financeiras no ambiente *Internet Banking*, quando ocorre a captura de informações por terceiros, demonstrando a falta de controles adequados para a proteção destes dados. Vale lembrar que estes controles podem ser adotados tanto no ambiente provedor dos serviços bancários, quanto no equipamento de acesso ao serviço utilizado pelo cliente[50].

Entretanto riscos de segurança não são os únicos responsáveis pelas perdas operacionais. O outro risco existente, relativo ao projeto, criação e manutenção de sistemas nos leva a compreender o quanto é importante proteger sistemas contra ataques ou excesso de utilização do serviço por terceiros que levem à interrupção ou aumento do tempo de resposta do acesso ao ambiente pelos clientes.

A prevenção contra estes problemas se baseia na adoção adequada da arquitetura de rede, e freqüente atualização da tecnologia empregada para a criação e manutenção destes serviços. Portanto percebe-se que o risco dos sistemas se baseia principalmente na velocidade de obsolescência da estrutura que suporta os serviços bancários. Apesar do crescente aumento de

[50] No ambiente *Internet Banking* é possível identificar que o ambiente mais frágil é o equipamento do cliente. 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

acesso de clientes aos serviços de *Internet Banking*[51], e do grande número de vulnerabilidades divulgadas sobre sistemas; as instituições financeiras atualizam freqüentemente o parque tecnológico, minimizando os riscos sobre os sistemas, e conseqüentemente, sobre o serviço *Internet Banking*.

Através da descrição anterior, percebe-se que a fraude sobre o ambiente *Internet Banking* é o resultado da ocorrência de perdas relacionadas aos riscos de segurança, inseridos dentro de riscos operacionais, previsto pelo Comitê da Basiléia.

2.2.3 **Controle de riscos no ambiente Internet Banking**

Em complemento a descrição dos riscos, busca-se identificar os controles sobre os riscos de segurança, mencionados anteriormente, obrigatórios às instituições financeiras, através das recomendações do Comitê da Basiléia, que visam à minimização do risco de operações bancárias realizadas no ambiente Internet. Os controles recomendados são os seguintes[52]:

- **Autenticação de clientes:** As instituições financeiras devem adotar meios para permitir a autenticação de uma identidade e prover autorização aos clientes[53], permitindo a realização de transações através da Internet;
- **Não repudio e contabilidade das transações:** As instituições devem utilizar métodos transacionais de autenticação que possibilitem confirmar a veracidade das operações e o rastreamento da seqüência de transações efetuadas pelo cliente no ambiente *Internet Banking*;

[51] Mencionado no primeiro capítulo deste trabalho.
[52] BASEL - **Risk Management Principles for Electronic Banking**. Basel Commitee on Banking Supervision. Disponível em: <http://www.bis.org/publ/bcbs98.pdf> Acesso em: 30 nov. 2004.
[53] No subitem anterior deste capítulo está disponível a avaliação do processo de autenticação sob a ótica tecnológica.

- **Medidas que asseguram segregação de funções:** As instituições financeiras devem possuir normas que obriguem a segregação de funções de seus funcionários envolvidos em sistemas, bancos de dados e aplicações do ambiente *Internet Banking*;
- **Controles apropriados de autorização em sistemas, banco de dados e aplicações:** As instituições financeiras devem assegurar que os controles de autorização e privilégios de acesso estão definidos de acordo com a função de seus funcionários, de acordo com os perfis de acesso a sistemas, banco de dados e aplicações;
- **Integridade dos registros, informações transacionais:** As instituições financeiras devem adotar medidas que garantam a proteção da integridade dos dados do ambiente *Internet Banking*, tais como registros, informações e transações;
- **Estabelecimento do rastreamento transparente em transações:** As instituições financeiras devem se assegurar da existência de processos transparentes que permitam o rastreio de todas as transações efetuadas sobre o sistema *Internet Banking*;
- **Confidencialidade em informações bancárias essenciais:** As instituições financeiras devem prover mecanismos que garantam a confidencialidade de informações sigilosas, sejam eles dados transmitidos através de meios eletrônicos, ou armazenados em mídias magnéticas.

Quando se realiza uma análise sobre os controles recomendados, percebe-se que alguns destes itens são burlados pelo fraudador[54], tal como o mecanismo de autenticação do cliente, onde através de dados capturados o fraudador adquire a capacidade de se identificar através de um cliente da instituição financeira; e o mecanismo de não repúdio, onde a efetivação da fraude

[54] Recomenda-se para estes casos a avaliação constante dos controles mencionados acima através das áreas de risco, *compliance* e auditoria existentes nas instituições financeiras brasileiras e validadas periodicamente por meio de consultoria externa contratada para a realização desta avaliação.

representa a falta de capacidade do banco em detectar uma transação não legítima, dentre tantas outras legítimas dentro do sistema.

Do outro lado, percebe-se que o mecanismo de estabelecimento de rastreio transparente das transações[55] é um meio que pode ser utilizado pelos bancos, para a detecção dos responsáveis a uma transação não legítima. Conclui-se na visão de negócio, que apesar da previsão dos riscos existentes no ambiente, não é possível neste momento eliminar perdas financeiras, principalmente àquelas que estão relacionadas às fraudes realizadas através do ambiente *Internet Banking*. Entretanto, é dever das instituições a criação e manutenção de indicadores[56] incluindo dados como a freqüência de incidentes registrados e o valor médio de perdas (Voit, p.286-299), permitindo a reserva adequada de recursos.

[55] A atividade de análise destas informações, em geral se encontra em áreas de segurança da informação, inspetoria ou auditoria existentes nas instituições financeiras brasileiras.

[56] Apesar da necessidade de se incluir as perdas em fraude no cálculo de perdas do risco operacional, existem percepções de instituições financeiras que a reserva financeira deve ser realizada empiricamente em detrimento às medições realizadas, pois se considera que diversas variáveis no cálculo são desconhecidos pelos bancos. (Wahlström, p. 493-522)

2.3 VISÃO DA ENGENHARIA SOCIAL

O termo “Engenharia Social” descreve o uso de técnicas sugestivas que permite a influência de indivíduos em busca de determinadas informações. Este método é utilizado por fraudadores tanto no mundo real, quando no universo virtual. Para a realização de um estudo sobre este tema, é necessário se recorrer à psicologia social, para melhor compreensão deste assunto.

Esta visão foi incluída neste trabalho, pois contribui à compreensão dos aspectos psicológicos que auxiliam no processo de iteração e manipulação das vítimas de fraudes com o objetivo de obtenção das credenciais de acesso ao ambiente *Internet Banking*.

2.3.1 Princípios da psicologia social

Três os aspectos da psicologia social, relativos à persuasão (HUSCH) relacionados à realização de fraudes precisam ser compreendidos[57]:

- Escolha e determinação das alternativas de persuasão;
- Atitudes das vítimas e seu grau de ingenuidade e;
- Técnicas de persuasão e influência.

2.3.2 Escolha e determinação das alternativas de persuasão

Na escolha e determinação das alternativas de persuasão, são duas as maneiras utilizadas na abordagem de vítimas, a rota central e a rota periférica de persuasão. A rota central utiliza uma abordagem sistêmica composta de argumentos lógicos que buscam a estimulação de uma resposta favorável[58]. Este processo requer o estímulo auditivo ou visual, que resulta na

[57] Os aspectos mencionados são detalhados nos itens a seguir onde é realizada a contextualização da técnica sobre os riscos de ocorrência de fraude no ambiente Internet Banking.
[58] A resposta favorável mencionada no texto é resultado do convencimento da vítima sobre o golpe aplicado pelo fraudador.

aceitação do estímulo pela vítima. Esta modalidade de estímulo pode ser exemplificada na tentativa de fraude representada pela seguinte seqüência:

- **Passo 1:** Envio de mensagens eletrônicas a possíveis vítimas em nome de instituições financeiras;
- **Passo 2:** O fraudador aguarda o retorno à aceitação do estímulo através do:
    - Acesso ao link existente na mensagem;
    - Acesso à página falsa da instituição financeira e;
    - Inserção voluntária dos dados solicitados à vítima.

O sucesso na execução de todos os passos, demonstra neste cenário uma resposta favorável de uma vítima perante o golpe aplicado por um fraudador. É necessário lembrar que há diversas outras técnicas utilizadas na persuasão de rota central, e o exemplo acima é apenas a descrição de um destes cenários[59].

O outro método utilizado na abordagem é a rota periférica de persuasão, utiliza meios que transpõem a argumentação lógica, provocando o estímulo através do impulso, e não pelo raciocínio profundo. Nestes casos, é oferecido algo à vítima que não representa o objeto da fraude. Exemplo desta abordagem é representado pelo:

- **Passo 1:** Envio de mensagens eletrônicas utilizando temas como cartões virtuais, promoções, comunicados, entre outros[60];
- **Passo 2:** O fraudador aguarda o retorno à aceitação do estímulo através do:
    - Acesso de um link existente na mensagem;
    - Realização de "*download*[61]";

[59] Qualquer golpe aplicado em clientes do serviço de *Internet Banking*, utilizando nome, logomarca ou elementos que criem a falsa percepção do cliente do recebimento de uma comunicação de instituições financeiras utiliza técnica de rota central.

[60] Oposto a técnica de rota central, a rota periférica não contém elementos de identificação de instituições financeiras.

- Instalação de um arquivo executável[62] e;
- Permissão involuntária da vítima à captura de informações e dados inseridos no computador[63].

A escolha da rota de persuasão depende da suscetibilidade da vítima aos estímulos realizados pelo fraudador, que podem estar relacionado a emoções fortes como alegrias e medos; ou baseados na necessidade de iteração pessoal, como o recebimento de um e-mail contendo uma suposta informação relacionada à vítima; e até utilizando a sensação de surpresa e alegria, através de promessas de prêmios ou quantias em dinheiro. Os detalhes dos ardis utilizados pelos fraudadores no Brasil poderão ser vistos com mais detalhes no capítulo quatro deste trabalho.

2.3.3 **Atitudes das vítimas e seu grau de ingenuidade**

Outra dimensão explorada na aplicação da fraude sobre o ambiente *Internet Banking* que está relacionada à psicologia social, são as ações dos clientes que levam à efetivação do golpe. Estas ações são geralmente bem sucedidas em virtude da ingenuidade do usuário, em acreditar na veracidade do oferecimento de prêmios, dinheiro ou qualquer outro bem de consumo em troca de uma ação ou informações pessoais fornecidas pela vítima. As ações são traduzidas pela instalação inconsciente de um cavalo de tróia, relacionado ao *link* de uma mensagem eletrônica; e as ações são exemplificadas pelo fornecimento voluntário de dados pessoais que

---

[61] Neste contexto, o *download* é a gravação do arquivo disponibilizado pelo fraudador em algum equipamento existente na Internet;

[62] A instalação do executável, na maioria dos casos depende da iteração da vítima em solicitar a execução do arquivo, entretanto há técnicas utilizadas pelos fraudadores que efetuam a cópia do software e realizam a instalação sem intervenção da vítima.

[63] No momento que o arquivo se encontre instalado, pronto para realizar a captura de dados de uma vítima, o sistema operacional responsável pelo controle de processos pressupõe permissionamento para captura e envio de dados capturados ao fraudador, conseqüentemente uma liberação de informações pessoais da vítima são enviadas de forma involuntária ao fraudador.

permitem ao fraudador a autenticação e realização de transações no ambiente financeiro a partir da Internet em nome do cliente legítimo do banco.

Deve-se lembrar que a exploração de atitudes e crenças não está limitada apenas sobre clientes de *Internet Banking*. Há situações onde são oferecidos produtos no mundo virtual, onde o interessado pelo produto remete o pagamento pelo bem ou serviço, resultando na frustração do comprador, pois o resultado da aquisição não atende as expectativas do cliente[64]. Estes outros tipos de golpes podem ser praticados através de mensagens eletrônicas, realizando ofertas que aguçam a susceptibilidade das vítimas, ou podem estar disponíveis em sites de comércio eletrônico na Internet, tais como os especializados em leilões de produtos.

Outra forma ainda utilizada na exploração destas crenças a atitudes está relacionada à aplicação de golpes contendo esquemas de investimento. Nesta abordagem, a vítima recebe uma mensagem eletrônica oferecendo uma proposta de investimento acionário em uma ou mais companhias de capital aberto. Este tipo de golpe utiliza a mobilização de diversas vítimas que acreditam no conteúdo da mensagem, resultando no investimento destas pessoas sobre a empresa de capital aberto. O efeito de manipulação destas pessoas sobre o mercado acionário desta companhia leva à valorização da ação no mercado, o que garante lucros ao fraudador, que possui ações desta empresa, antes da efetivação da compra destes papéis pelas vítimas. Uma vez concretizado o golpe, e valorizado o papel, o fraudador vende as ações que ele possui, resultando em lucro à ação fraudulenta e em conseqüência desta venda o papel da companhia se desvaloriza, resultando na perda de dinheiro dos investidores enganados pelo golpe[65]. Vale lembrar que a efetivação da fraude depende de um grande número de vítimas

[64] A frustração ocorre, pois há casos onde o produto oferecido não é entregue ao comprador e em outras situações o produto está aquém às expectativas oferecidas pelo vendedor.

[65] As vítimas se estendem além do universo dos negociantes de papéis convencidos pelo golpe. Neste caso outros investidores do mercado acionário também são afetados, assim como a credibilidade da empresa que disponibiliza os papéis, agência corretoras de valores, e dependendo da extensão do golpe, ocorrem impactos ao sistema financeiro em uma região ou país.

que realizam o investimento e um grande montante de dinheiro investido previamente pelo fraudador.

2.3.4 **Técnicas de persuasão e influência**

São seis os fatores e técnicas de persuasão que são relativos à efetivação da fraude sobre o ambiente Internet (HUSCH). Entretanto apenas quatro deles estão relacionados ao ambiente *Internet Banking*. Vale lembrar que todas as técnicas se utilizam à rota de abordagem periférica.

Os itens relacionados ao *Internet Banking* são os seguintes:

- **Autoridade:** A representação hierárquica superior é um fator importante que leva ao convencimento de grupos que se encontra em níveis inferiores. Esta técnica é utilizada e casos onde vítimas recebem mensagens eletrônicas em nomes de instituições conhecidas, como órgãos públicos, sejam eles privados ou públicos, informando possíveis pendências existentes entre a vítima e o órgão. A partir desta afirmação, a vítima se sente compelida a resolver tal pendência, resultando no acesso a um *link*, e instalação de cavalos de tróia dentro do computador pessoal.
- **Similaridades e preferências:** É uma tendência nos seres humanos a busca por pessoas similares a nós. Esta identificação encurta o caminho utilizado no relacionamento de duas ou mais pessoas. Partindo desta premissa, se consegue compreender que vítimas de golpe são suscetíveis a mensagens eletrônicas que mencionam a suposta traição de alguém que se relaciona com a vítima. Neste caso, se a vítima estiver previamente desconfiada, a mensagem será apenas uma confirmação de seus temores, portanto o acesso conteúdo do *link* existente na mensagem é uma

ação inevitável[66]. Este aspecto mostra o processo de similaridade entre o conteúdo da mensagem e o raciocínio desenvolvido pela vítima do golpe. Em casos de preferências pessoais[67], pode-se mencionar conteúdo de mensagens eletrônicas que contém a descrição de alguém que seja de consciente ou inconsciente de desejo da vítima. Ao passo que o leitor da mensagem eletrônica se identifica ao conteúdo descrito, a vítima pode se sentir compelida a acessar o link do existente na mensagem.

- **Reciprocidade:** Este é o resultado da iteração social em sociedades civilizadas[68]. Reciprocidade é nada mais que a reação do indivíduo a um estímulo. Este estímulo é explorado muitas vezes por meio do recebimento de cartões virtuais através de correios eletrônicos. A vítima que utiliza constantemente[69] o serviço de cartões virtuais, pode interpretar o recebimento de uma mensagem eletrônica contendo um cartão como resposta a um cartão enviado recentemente pela vítima. Vítima desta técnica, o leitor busca acessar o conteúdo e prosseguir com o processo de reciprocidade[70]. Nestes casos, o acesso voluntário ao link existente na mensagem resulta na instalação de um cavalo de tróia.
- **Prova social:** São fenômenos sociais levam populações a realizarem ações sem prévio reflexo mental[71]. Estas ações realizadas através do impulso podem levar vítimas a realizarem ações sem avaliar as conseqüências. Fatos que são abordados na mídia

[66] Este cenário ocorre através da disponibilidade de acesso do *link* e disponibilidade do arquivo para *download*.
[67] As preferências mencionadas no texto refletem desejo da vítima em criar um relacionamento afetivo com outro indivíduo.
[68] A retribuição é um processo de resposta do indivíduo estimulado por alguma ação de origem externa. Na reciprocidade relacionada aos golpes praticados no ambiente *Internet Banking* sempre ocorre um estímulo que resulta no bem estar do receptor. O golpe é concretizado quando a vítima busca obter mais informações do responsável pelo envio deste estímulo.
[69] O uso de serviço de cartões virtuais, mesmo em datas comemorativas caracteriza constância e resulta familiaridade aos usuários deste serviço.
[70] A continuação do processo visa à retribuição ao remetente do cartão virtual.
[71] Eventos de grande repercussão disponível em mídias como jornais, revistas, TV e outros meios atingem a população que busca por mais informações independente da fonte informante, portanto o leitor que se encontra nestas situações está suscetível a uma mensagem eletrônica que supostamente leva em seu conteúdo detalhes destes eventos de grande impacto emocional.

como tragédias, podem ser classificados neste tipo de abordagem, pois além da curiosidade explorada, o conteúdo de uma mensagem eletrônica contêm supostas informações de algum fato, seduzindo a vítima neste golpe. Esta técnica ainda pode resultar em propagação da mensagem forjada, pois a vítima que recebe este *e-mail*, em busca de auto-afirmação repassa a suposta notícia a colegas ou amigos.

E as técnicas que persuasão e influência que não estão relacionados à abordagem deste trabalho são os seguintes:

- **Oferta:** A limitação da oferta de um produto ou serviço pode criar ou aumentar o desejo em adquiri-lo. Partindo desta situação, diversos produtos são oferecidos na Internet, sob o pretexto da limitação da oferta, obrigando os interessados a decidir pela aquisição de um produto ou serviço sem a realização do reflexo sobre a necessidade ou mesmo a veracidade ou qualidade do item ofertado. Ainda não se encontrou nenhum caso de oferta aplicado à efetivação da fraude no ambiente *Internet Banking*.
- **Integridade e reputação:** A reputação e integridade de um indivíduo são constituídas por fatos divulgados ao público[72]. Em muitos destes casos esta reputação é resultado do poder de argumentação de indivíduo, não consistindo de qualquer embasamento em fatos sobre a integridade ou a reputação do mesmo. Usando esta técnica, é possível convencer indivíduos à realização de ações que são recomendadas por alguém "aparentemente confiável[73]". Não se encontrou em qualquer momento a utilização deste método para abordagem de clientes do ambiente de *Internet Banking*.

Apesar a menção dos seis fatores, há ainda mais um ponto que se deve considerar importante como técnica de persuasão.

[72] Nem sempre todos os fatos de um indivíduo se tornam públicos. Portanto é possível que um indivíduo só torne aparente os fatos que refletem idoneidade, havendo ainda a possibilidade da apresentação de fatos que não possam ser comprovados ao público.

[73] A técnica consiste no ganho de confiança da vítima, buscando a realização de ação específica. Neste caso, a realização de uma atividade que leve à fraude.

Este item não é mencionado (HUSCH), talvez pelo trabalho abordar características norte-americanas. No Brasil, devido a traços culturais, há um aspecto muito explorado como técnica de persuasão, a curiosidade.

A curiosidade[74] é o item que complementa todos os fatores anteriores, pois o responsável pelo envio de mensagens eletrônicas relativas à fraude busca o maior número de vítimas através da leitura e acesso do conteúdo da mensagem. Em muitos dos casos, a vítima não se identificará com o conteúdo do e-mail, entretanto a curiosidade do leitor pode levar ao acesso do conteúdo do link da mensagem, resultando na infecção do equipamento através de um cavalo de tróia.

Percebeu-se que todos os exemplos anteriores mencionaram a efetivação da fraude através da instalação de cavalos de tróia. Lembra-se que esta não é a única forma utilizada para a subtração de dados pessoais das vítimas. No capítulo quatro deste trabalho será possível observar as outras técnicas utilizadas pelos fraudadores.

[74] Constata-se que a curiosidade está presente em quase todos os artifícios utilizados para aplicação de golpes em clientes do serviço de *Internet Banking*. Supõe-se que este artifício é mais expressivo no Brasil em virtude da composição cultural da população, pois em golpes aplicados a clientes de Internet Banking em outros países, este tipo de artifício não é utilizado nos dias atuais.

2.4 VISÃO DA INVESTIGAÇÃO

A reconstituição de fatos relativos à efetivação de fraude sobre o ambiente *Internet Banking* é um passo importante no processo de mitigação dos riscos, assunto que será tratado no final deste trabalho.

Esta atividade, em geral realizada através de um perito[75], nomeado judicialmente com o possível auxílio de um assistente técnico, que deve executar alguns procedimentos, permitindo integridade e confiabilidade das evidências coletadas. Os passos apresentados a seguir representam modelo detalhado[76] dos eventos relativos a crimes cibernéticos, que são aplicáveis a incidentes mencionados neste trabalho:

- **Ocorrência de um evento.** Para que uma investigação seja realizada, é necessária à existência de um fato[77] que promova a ação de investigação, esta ação é realizada pela instituição financeira afetada pela fraude, responsável também pela confirmação de uma ocorrência. No contexto deste trabalho, este evento dispara todo o processo investigativo; em geral materializado por meio de uma mensagem eletrônica, emitido pelo fraudador em nome de terceiros ou em nome de uma instituição financeira;

[75] A atividade de perícia e produção de prova pericial é regulamentada pela lei 8455 de 24 de Agosto de 1992, e pode ser consultada em L8455. **Alteração dos dispositivos da Lei 5869, de 11 de janeiro de 1973 – Código do Processo Civil, referentes à prova pericial**. Presidência da República. Disponível em: < https://www.planalto.gov.br/ccivil_03/Leis/1989_1994/L8455.htm > Acesso em: 15 nov. 2005

[76] O trabalho de CIARDHUÀN efetua a compilação de diversos modelos. O modelo proposto se assemelha às necessidades deste trabalho, pois contempla os passos relativos ao tratamento de incidentes em instituições financeiras. CIARDHUÁIN, SÉAMUS Ó. **An Extended Model of Cybercrime Investigations.** International Journal of Digital Evidence. Summer 2004, Volume 3, Issue 1. Disponível em: <http://www.ijde.org/docs/ociardhuain.pdf> Acesso em: 18 mar. 2005.

[77] O fato mencionado é a detecção de operações fraudulentas a um cliente do serviço de *Internet Banking*, seja este um processo sistêmico ou informado por um cliente que percebe subtração de seus recursos.

- **Autorização.** Existindo a confirmação de uma ocorrência, o próximo passo necessário é a realização de procedimentos investigativos. Entretanto tais ações só podem ser realizadas mediante autorização. Este processo ocorre dentro da estrutura da instituição financeira, através da avaliação de relevância do evento[78] e eventual a alocação de recursos do banco à investigação[79]; e também ocorre no âmbito judicial, através de coletas de evidências, segundo autorização da justiça[80];

- **Planejamento.** Esta fase requer iteração das instituições financeiras e órgãos policiais, pois esta fase determina o tipo da informação que necessita ser coletada e a ação de cada um dos envolvidos. Uma destas ações pode ser exemplificada quando é detectada a propagação de mensagens eletrônicas suspeitas[81] a partir de um provedor de acesso[82]. Planeja-se a coleta dos registros[83] no provedor de acesso, e a partir das evidências encontradas, busca-se planejar ações para identificação, incluindo o cadastro do usuário do provedor de acesso, localização do suspeito e registros de identificação telefônica;

- **Notificação.** Este é o processo está relacionado à notificação do proprietário do objeto investigado. Deve-se também considerar que certas investigações requerem a uma

[78] Todas as perdas com fraudes são analisadas, objetivando o ressarcimento ou não de clientes afetados. Neste processo, é necessário lembrar que certas perdas financeiras ocorrem através da autofraude, que é uma ocorrência onde há transferência de recursos com a anuência do cliente, e posterior informe de uma suposta fraude visando ganhos financeiros ao próprio cliente.
[79] A investigação é realizada em virtude da relevância do evento e avaliação de custos dos recursos alocados comparado ao montante financeiro extraviado.
[80] Os processos investigativos ocorrem pela polícia civil e polícia federal. Apenas envolve-se a polícia federal na confirmação de perdas financeiras da CEF, em virtude deste banco se classificar como empresa pública federal. Quando o CEF e outros bancos estão envolvidos em perdas financeiras, a polícia federal trata também estas perdas no âmbito federal. Em todos as outras situações a polícia civil possui alçada para a tomada de ações.
[81] As mensagens citadas no documento se referem a SCAM, termo detalhado no capítulo quatro deste trabalho.
[82] O provedor de acesso é responsável pela infra-estrutura de acesso de um usuário e seu computador à Internet.
[83] Os registros buscam em geral, informações dos endereços de conexão do suspeito em função a horários de conexão. Esta ação não corre sem a prévia notificação do provedor de acesso.

ação de notificação e apreensão o objeto investigado, pois há cenários onde as provas de uma investigação sofrem riscos de eliminação[84] antes da realização da análise das evidências pelo perito. Em geral, os procedimentos adotados para investigações em ambiente *Internet Banking* é a notificação dos provedores detentores dos registros que apóiam todo o trabalho dos assistentes técnicos nomeados pela instituição financeira interessada no processo. Em outro momento esta notificação não acontece; ocorrendo em geral sobre os suspeitos da efetivação da fraude em ações de busca e apreensão dos artefatos[85] relativos à fraude, em geral mídias magnéticas, computadores e anotações;

- **Identificação da evidência.** Este processo requer o preparo para o reconhecimento de evidências. Esta atividade é realizada por peritos da justiça que estão autorizados para efetuar a busca e apreensão de provas, visando à preservação do ambiente que são encontradas estas informações[86];

- **Coleta da evidência.** Ocorrendo a confirmação da existência de uma evidência, este é coletado, ou seja, os órgãos policiais e os responsáveis pela investigação removem do local investigado mídias magnéticas, computadores, anotações entre outras evidências e tomam medidas para preservação e análise deste material. Os procedimentos realizados na coleta[87] definem a validade deste artefato em âmbito jurídico;

[84] Caso o objeto de investigação sofra influências do fraudador.
[85] O contexto de artefato neste trabalho trata da existência de qualquer prova material que permita associar o suspeito a um crime no ambiente *Internet Banking*.
[86] A importância da identificação pode permitir em certos cenários a reconstituição de eventos em uma linha de tempo contínua.
[87] Neste trabalho a coleta está limitada à captura de provas; duplicação de dados e tratamento das evidências.

- **Transporte da evidência.** O transporte da evidência não é apenas uma questão de cuidados no manuseio de transporte do artefato físico, como uma mídia magnética. Caso ocorra necessidade de se realizar o transporte de evidências através da transferência de dados, sejam eles entre mídias magnéticas ou em ambiente de rede, é necessário se observar à necessidade de cuidados para que o dado transportado apresente a mesma integridade que a evidência original[88]. A questão do transporte de evidência no cenário de confirmação de fraude no ambiente *Internet Banking* se baseia em parte no processo de transmissão de registros encontrados em um computador apreendido[89]. Caso a informação transmitida não apresente as mesmas características da prova original, como a data modificação do arquivo de registro original, haverá perda da integridade da prova, e, portanto a perda da evidência[90], ainda é necessária mencionar que a transmissão de arquivos sem o devido cuidado pode expor as informações, se caracterizando uma quebra de sigilo;

- **Armazenamento da evidência.** Este processo é uma etapa importante em uma investigação, pois a análise de artefatos não ocorre geralmente após a apreensão das evidências[91]. É importante lembrar que as análises devem ser realizadas em cópias íntegras dos dados coletados a partir da evidência original, portanto o armazenamento deve prover guarda às provas[92] originais, processo de duplicação das informações e guarda das cópias das provas originais;

---

[88] A integridade é realizada em geral através da comparação de características da prova original e sua respectiva cópia.
[89] O computador é somente apreendido quando este objeto é tratado no processo de coleta da evidência.
[90] É importante lembrar que este cenário trata apenas de evidências que não permitem obtenção posterior do registro original.
[91] Em geral aspectos legais e disponibilidade de profissionais habilitados para o tratamento destas evidências são os responsáveis pelo tempo de armazenamento da evidência.
[92] As provas neste contexto são dados armazenados podendo conter imagens de mídias magnéticas e arquivos diversos como mensagens eletrônicas e arquivos com registro de atividades suspeitas.

- **Análise da evidência.** Este processo requer a busca e identificação de um dado que indique a existência de uma prova. É necessária a utilização de ferramentas que permitam a análise de um grande volume de dados, e capaz de recuperar informações danificadas. Este processo é desempenhado pelos peritos nomeados pela justiça e que estão autorizados para efetuar o manuseio dos artefatos armazenados. É importante salientar que instituições financeiras envolvidas neste processo têm papel de alimentar órgãos policiais e os responsáveis pela investigação, informando segmentos de dados que determinam à existência de transações bancárias, ou dados de clientes existentes em evidências;

- **Definição da hipótese.** Baseado nas informações encontradas torna-se necessária à formulação de uma hipótese que permite reconstituir os fatos em uma linha contínua de tempo. Quando se formula uma hipótese de um incidente envolvendo fraude em instituições financeiras, as hipóteses são formuladas a partir de indícios coletados e experiência dos envolvidos em fraudes registradas no passado. Caso do indício esteja baseado na existência de mensagens eletrônicas, a hipótese buscará correlacionar responsabilidade da fraude ao responsável pelo envio destas mensagens. Através de evidências adicionais como registro de atividades em provedores de acesso, números de identificação telefônicos e endereços são possíveis à formulação de hipóteses incluindo um ou mais suspeitos a partir das informações existentes, podendo permitir em um passo seguinte, a busca e apreensão de equipamentos para realização de perícias adicionais[93];

[93] O exemplo apenas menciona um cenário e uma hipótese para este cenário. Deve-se lembrar que diversas hipóteses devem ser formuladas para o mesmo cenário.

- **Apresentação da hipótese.** A hipótese é a defesa de um raciocínio que está integrado desde o primeiro passo do processo investigativo, ou seja, na avaliação da necessidade de investigação, que será defendida pela instituição financeira. As apresentações de hipóteses são essenciais em outras fases. Tal como no processo de decisão da ação de apreensão, onde investigadores de órgãos de repressão públicos devem apresentá-la, devendo se estender até a apresentação destas hipóteses ao juiz;

- **Defesa da hipótese.** Este processo busca a validação das hipóteses em cada uma das apresentações mencionadas no item anterior. Caso a hipótese apresente alguma falha, é possível que haja a necessidade da reformulação da hipótese, ou recomenda-se o reforço da hipótese através da coleta de evidências adicionais. A necessidade mais forte desta defesa ocorre em âmbito judicial, pois é neste momento que é decidida à culpa ou inocência de um suspeito[94];

- **Disseminação da informação.** Este procedimento busca divulgar os resultados de uma investigação, divulgando os procedimentos adotados visando à formação de uma base de conhecimento que pode ser utilizado em futuras investigações. Este processo pode ser feito na área acadêmica, através de artigos ou outras produções; pode ser o resultado através da divulgação de veredictos, envolvendo acusados e instituições financeiras; e realizado através da mídia, influenciando usuários e provedores de serviços no ambiente Internet.

[94] No contexto deste trabalho, este é um suspeito de praticar fraude sobre clientes do sistema de *Internet Banking* em uma ou mais instituições financeiras;

Consolidando todo o descritivo apresentando, será apresentado um modelo seqüencial que permite a visualização da iteração dos processos e a responsabilidade de atuação.

2.4.1 **Modelo Investigativo**

Os treze processos mencionados anteriormente fazem parte de um fluxo que descreve todo o processo investigativo relativo à fraude do ambiente *Internet Banking*. Estes processos são retro alimentados, de acordo com o resultado da iteração entre os envolvidos e os responsáveis pelas ações. Toda esta dinâmica é descrita a partir do diagrama abaixo, onde visualizamos a seguinte seqüência de ações:

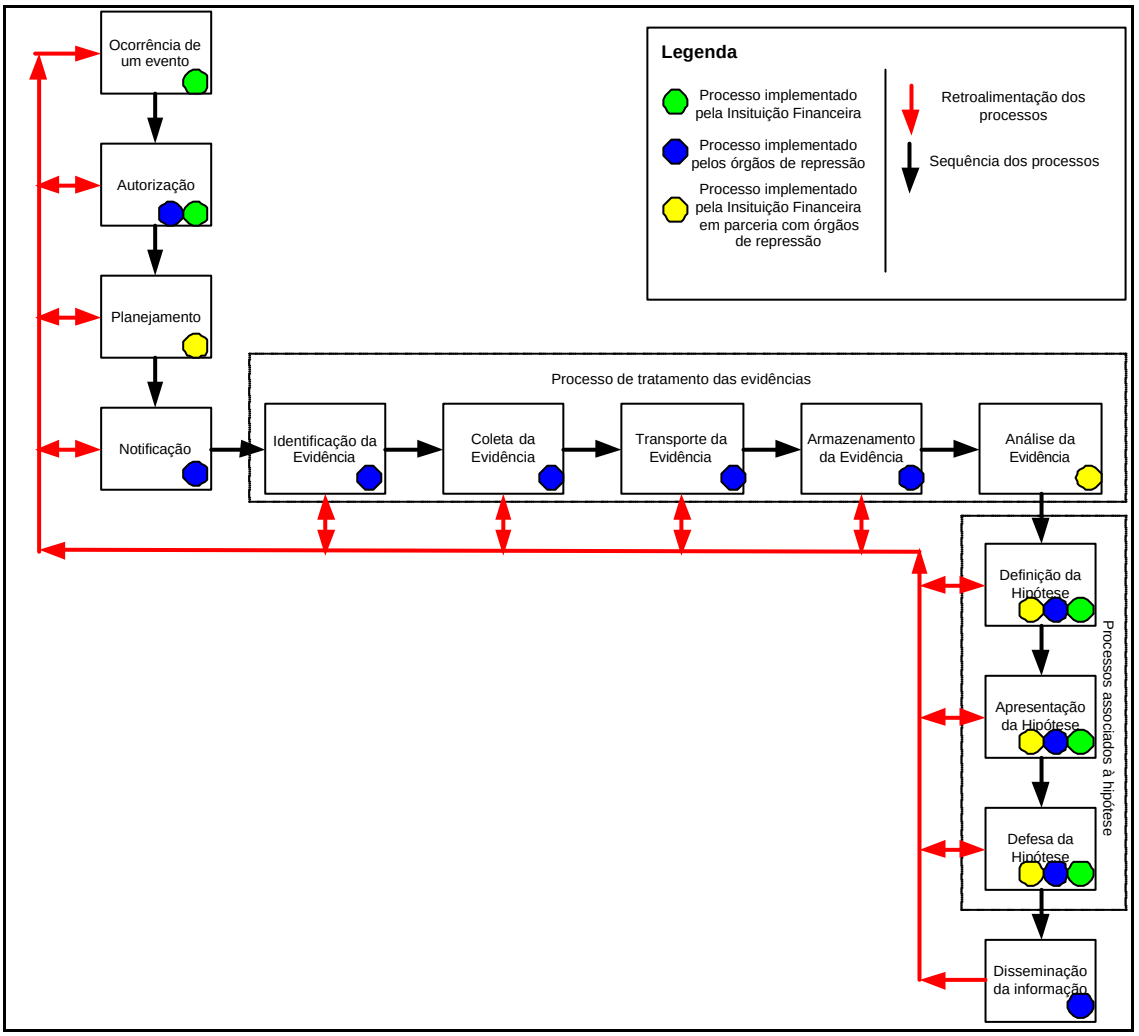

Figura 9 - Modelo investigativo de fraudes no ambiente *Internet Banking*

É possível constatar que há processos que são adotados somente pelas instituições financeiras, representadas pela cor verde; outros que são exclusivamente adotados pelos dos órgãos públicos de repressão, representada pela cor azul; e outros realizados em parceria entre instituições financeiras e órgãos públicos de repressão, representada pela cor verde.

A existência de diversos círculos em um único processo indica que este evento é executado pelos parceiros isoladamente, ocorrendo apenas troca de informações entre os participantes.

Toma-se como exemplo, o processo autorização, onde tanto a instituição financeira quanto os órgãos públicos de repressão necessitam buscar autorizações dentro de seus órgãos para a realização de investigação.

Outro exemplo é o processo de definição da hipótese, onde, tanto a instituição financeira, quanto os órgãos públicos de repressão necessitam elaborar hipóteses junto às respectivas equipes internas. A validação final destas hipóteses ocorre apenas em reuniões compostas por representantes das instituições financeiras e órgãos públicos de repressão.

Em qualquer processo descrito no diagrama anterior é possível realimentação de processos anteriores, permitindo resultados mais confiáveis que serão expostos no processo de disseminação da informação[95].

[95] É possível realizar o processo investigativo em um menor número de fases (Mann, p.125-126), entretanto estas fases subtraídas do modelo demonstrado neste capítulo estarão implícitos em um ou mais fases de qualquer outro modelo proposto.

3 FRAUDE NO AMBIENTE FINANCEIRO

A fraude realizada sobre o ambiente financeiro busca a subtração de recursos financeiros, existentes em bancos ou outras instituições financeiras. O risco da ocorrência da fraude é reconhecido pelos bancos e previsto através do risco operacional, já abordado no capítulo anterior[96], demonstrando as fragilidades que podem ser exploradas por fraudadores. Em complemento ao capítulo anterior, serão detalhados neste capítulo os mecanismos utilizados na efetivação de fraudes, privilegiando uma análise sobre o ambiente *Internet Banking*, objeto deste trabalho.

3.1 FRAUDES BANCÁRIAS EM MEIOS ELETRÔNICOS

As fraudes bancárias em meios eletrônicos ocorrem em como resultado da obtenção e uso de credenciais de um cliente pelo fraudador. Estes dados são capturados da seguinte forma[97]:

- No momento que o cliente utiliza a máquina de auto-atendimento;
- Quando o cliente informa os dados a partir do aparelho telefônico e;
- No fornecimento de credenciais quando há acesso ao serviço de *Internet Banking*.

A captura de credenciais em máquinas de auto-atendimento ocorre através de duas formas. Em um primeiro momento quando, há necessidade do fraudador em obter os dados existentes no cartão magnético da vítima. Isto pode ocorrer através da substituição do cartão bancário do cliente por algum outro cartão sem que a vítima perceba o que está ocorrendo. Outra forma utilizada para a captura destes dados é a utilização de equipamentos sobrepostos[98] à máquina de auto-atendimento, que permitem a obtenção dos dados da tarja magnética existente no cartão bancário. A partir deste dado é possível gerar uma cópia do cartão bancário da vítima.

---

[96] Disponível no capítulo dois, subitem dois deste trabalho.

[97] FEBRABAN – **Você e seu banco – Um guia que vai facilitar seu relacionamento com os bancos.** Edição 2 – 2004. . Febraban. Disponível em: <http://www.febraban.org.br/Arquivo/Cartilha/Manual Febraban 2004 Y.pdf> Acesso em: 22 mar. 2005 (p.47-50)

[98] Os equipamentos sobrepostos mencionados neste trabalho são dispositivos que possuem aparência semelhante ao equipamento de auto-atendimento, contendo mecanismos de captura das credenciais dos usuários.

Observa-se que este procedimento não é bem sucedido em cartões baseados em tecnologia *smart-card*, onde o ponto de contato do cartão ao equipamento de auto-atendimento é composto por contatos metálicos que não permite a obtenção[99] dos dados existentes no cartão do cliente do banco.

Outra forma utilizada para a captura de informações em máquinas de auto-atendimento é a coleta da senha inserida pelo cliente do banco. Isto pode ocorrer através da observação visual direta do fraudador sobre o teclado ou a tela que o cliente utiliza no processo de inserção de suas credenciais, ou através da observação da digitação dos dados da vítima através de captura de imagens da operação do cliente que são transmitidas ao fraudador, em geral, com dispositivo eletrônico localizado junto ao caixa eletrônico alterado previamente pelo criminoso[100].

No processo de captura de credenciais através de aparelho telefônico, podem surgir duas abordagens. Em primeiro lugar, a vítima é contatada pelo fraudador, que busca convencer o cliente de uma instituição financeira a inserir suas credenciais através da digitação dos números no aparelho telefônico. Com esta ação o criminoso obtém os números inseridos pela vítima, traduzindo o tom ou pulsos inseridos no telefone através de equipamentos utilizados por técnicos em telefonia em números que podem ser utilizados posteriormente pelo fraudador. A segunda forma existente, mas pouco utilizada está atrelada ao processo de escuta telefônica passiva, onde o criminoso instala um equipamento que captura a comunicação realizada através a linha telefônica do assinante de uma operadora de telefonia pública. Caso a

[99] O smart card se baseia no armazenamento de informações protegidas por uma chave criptográfica, acessível por terminal autorizado e senhas de acesso. A não possibilidade de obtenção de dados mencionado neste trabalho se baseia em não se possibilitar réplica do conteúdo do smart-card através dos dispositivos hoje utilizados pelos fraudadores.

[100] A obtenção apenas de credenciais inseridas no auto-atendimento permite em certos casos a efetivação de algumas operações bancárias, caso o fraudador não tenha posse do cartão magnético. Neste caso, as transações se limitam à consulta de dados do cliente.

vítima efetue um acesso aos serviços bancários através do telefone, o fraudador utilizará estes dados para acessos aos serviços do banco em nome da vítima[101].

Os detalhes sobre o processo de captura de credenciais no ambiente *Internet Banking* estão mencionados no subitem seguinte[102] deste trabalho.

Visando disseminar estas informações aos clientes de instituições financeiras, a Federação Brasileira de Bancos (Febraban), concebeu uma cartilha[103] disponibilizada no ambiente Internet para que clientes do sistema financeiro possam compreender melhor as medidas de segurança adotadas pelas instituições financeiras e tomar ciência dos cuidados no uso dos serviços bancários. Subentende-se que através desta cartilha o cliente também está a par dos riscos referentes ao uso deste serviço.

Em virtude dos riscos existentes, os bancos também introduziram itens de identificação adicionais, além da senha, confirmando a origem do acesso bancário, esta informação é conhecida no sistema financeiro como identificação positiva do cliente, onde as instituições solicitam algum dado pessoal do cliente que provavelmente seja apenas de conhecimento do usuário legítimo do sistema. Além destes itens, proteções sobre as senhas se tornaram necessárias, dificultando a adivinhação de senhas por parte dos fraudadores. Fazem também parte destas recomendações[104] os seguintes itens:

- Não aceitar a gravação de senhas óbvias (como datas de aniversário, número de telefones e outras informações pessoais);

---

[101] Este método não é viável, pois o custo de investimento em equipamento, profissionais habilitados neste tipo de tecnologia e tempo de espera para realização de transações em geral é mais alto que o benefício esperado pelo fraudador.

[102] Capítulo três subitem três deste trabalho.

[103] FEBRABAN – **Você e seu banco – Um guia que vai facilitar seu relacionamento com os bancos.** Edição 2 – 2004. . Febraban. Disponível em: <http://www.febraban.org.br/Arquivo/Cartilha/Manual Febraban 2004 Y.pdf> Acesso em: 22 mar. 2005

[104] FEBRABAN – **Você e seu banco – Um guia que vai facilitar seu relacionamento com os bancos.** Edição 2 – 2004. . Febraban. Disponível em: <http://www.febraban.org.br/Arquivo/Cartilha/Manual Febraban 2004 Y.pdf> Acesso em: 22 mar. 2005 (p.48)

- Determinar um número mínimo no tamanho da senha[105], possibilitando o uso de senhas alfanuméricas[106];
- Criação de senhas distintas para o acesso do cliente em terminais de auto-atendimento e acesso no ambiente Internet[107];
- Solicitar a cada nova transação a senha e;
- E utilização de teclado virtual no ambiente de *Internet Banking*[108].

A Febraban ainda informa que os bancos são responsáveis pela preservação da integridade, da legitimidade, da confiabilidade, da segurança e do sigilo das transações realizadas nos serviços que são oferecidos, ressaltando que outros fatores dependem do cliente.

3.2 FRAUDES BANCÁRIAS NO AMBIENTE INTERNET BANKING

A fraude no ambiente *Internet Banking* é analisada e contida pelas instituições financeiras que já tratam de fraudes em meios eletrônicos. Entretanto devido à importância que este assunto foi levado mídia nos últimos tempos[109], a população usuária dos serviços bancários percebeu que as instituições mobilizaram esforços para a educação e conscientização de seus clientes sobre os riscos existentes na efetivação de transações neste canal. Vale lembrar que este assunto é tratado desde o ano de 2002 (Lau), período onde são registrados os primeiras tentativas de fraude sobre o serviço *Internet Banking*. O subitem adiante, neste trabalho, descreve a evolução tecnológica utilizada nos golpes aplicados sobre este sistema.

---

[105] As instituições financeiras adotam diferentes limitações para o tamanho de senhas, não sendo esta uma recomendação apenas aos usuários do sistema *Internet Banking*.
[106] Há instituições financeiras que permitem utilizar senhas alfanuméricas para a definição da senha, neste caso recomenda-se ao cliente a adoção de caracteres alfabéticos em conjunto com números para a composição da senha.
[107] Algumas instituições financeiras obrigam através de sistemas a utilização de senhas distintas, com o objetivo de dificultar o roubo de credenciais.
[108] Poderá ser observado no capítulo três subitem três deste trabalho, que os teclados virtuais permitem captura de credenciais, caso o teclado virtual não conte com dispositivos adicionais de proteção.
[109] Informação já mencionada na introdução deste trabalho.

3.3 MECANISMOS UTILIZADOS PELOS FRAUDADORES

No Brasil as tentativas de fraude realizadas sobre clientes do sistema financeiro, usuários do ambiente Internet se basearam ou estão baseadas em ataques conhecidos como *SCAM*, *PHISHING SCAM* e *PHARMING*. Nos dois primeiros tipos de incidentes, o principal vetor de propagação da ameaça é realizado através do envio de mensagens eletrônicas pelo criminoso, que são recebidas pelas vítimas sem solicitação ou consentimento delas, o que podemos definir genericamente *SPAM,* com características que buscam ganho financeiro através da efetivação de fraude. No terceiro tipo de incidente, *PHARMING*[110], outros ambientes podem ser utilizados para o comprometimento do usuário no ambiente Internet, sendo este um golpe bem disseminado em outros países. Visando uma melhor compreensão dos termos mencionados acima, os próximos subitens deste trabalho auxiliarão na descrição destes mecanismos.

3.3.1 Spam

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), quando o conteúdo é exclusivamente comercial, esta mensagem também é conhecida como UCE (*Unsolicicited Commercial E-mail*[111])(CERT.br[112]). O *SPAM* se tornou um grande desconforto aos usuários de Internet, principalmente àqueles que são dependentes do serviço de correio eletrônico para realização de atividades diárias, sejam elas pessoais ou profissionais. Este incômodo está relacionado ao recebimento de mensagens eletrônicas que em muitos momentos resultam na

[110] Este tipo de ameaça já foi amplamente utilizado na aplicação de golpes no Brasil, os detalhes destes incidentes são mencionados no capítulo quatro subitem três deste trabalho.
[111] Mensagem Eletrônica não solicitada.
[112] CERT.br – **Cartilha de Segurança para Internet**. Versão 3.0 – Setembro de 2005. Disponível em: <http://cartilha.cert.br> Acesso em: 08 set. 2005.

eliminação desta mensagem, entretanto algumas destas correspondências, podem se destinar à natureza fraudulenta, como será descrito a seguir:

3.3.2 **Considerações sobre a definição de termos Scam e Phishing e Phishing Scam**

Há diversas interpretações sobre a definição de *SCAM, Phishing* e *Phishing SCAM.* O significado adotado para as terminologias neste documento é a interpretação de profissionais do sistema financeiro e que podem ser corroborados em diversas descrições de definições (INFOSEC), entretanto as definições existentes neste trabalho apresentam outra descrição em uma cartilha[113] recém publicada (CERT.br)[114], o que não indica que quaisquer uns dos dois trabalhos estejam equivocados. Conhecendo estas discrepâncias, recomenda-se um cuidado na interpretação dos termos em outros trabalhos, caso não haja uma prévia identificação de seus significados.

3.3.3 **Scam**

O *SCAM* é um tipo de mensagem eletrônica repudiada pelos usuários, pois além de causar desconforto aos usuários de caixas postais, como o *SPAM*, eles apresentam natureza fraudulenta (Lau). A natureza fraudulenta destas mensagens está relacionada à tentativa de convencimento do receptor mediante a alguma oferta descrita pelo responsável[115] no envio desta mensagem eletrônica. Nestes casos, a oferta se constitui em um golpe, levando a vitima a perdas financeiras.

---

[113] CERT.br – Cartilha de Segurança para Internet. Versão 3.0 – Setembro de 2005. Disponível em: <http://cartilha.cert.br> Acesso em: 08 set. 2005.

[114] O CERT.br define *Phishing* e *Phishing Scam* como a definição genérica dos golpes praticados em busca de credenciais, incluindo o golpe praticado em instituições financeiras. Neste trabalho, três são os elementos necessários para se definir o vetor da fraude, *SCAM*, *Phishing* e *Pharming*.

[115] O responsável por esta ação é o fraudador, seja pelo uso de equipamento próprio ou infra-estrutura de um equipamento comprometido disponível na Internet.

Esta mensagem eletrônica pode ser classificada em categorias. Exemplos são os *SCAMs* de compras em tempo real, *SCAMs* de investimento em tempo real[116] 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[117] 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). Entretanto é válido lembrar que este tipo de golpe não é objeto de estudo neste trabalho.

Para classificar esta ameaça sob a ótica do ambiente *Internet Banking*, busca-se descrever as características do *SCAM*, que são as seguintes:

- O conteúdo da mensagem pode ou não conter uma marca comercial forjada[118];
- Contém endereços de e-mail e *links* forjados[119];
- 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, dados são coletados no

[116] As modalidades de SCAM de compras em tempo real e SCAM de investimento em tempo real não serão detalhados neste trabalho. Entretanto durante a coleta de mensagens eletrônicas pelo pesquisador, percebeu-se a existência de diversas mensagens contendo oferecimento de oportunidades de negócio em aplicações financeiras privilegiando o oferecimento de ações e a promessa de ganhos de dinheiro através de trabalhos que podem ser realizados a partir da Internet, através da compra de um material disponível pelo fraudador.

[117] Foi possível receber diversas mensagens eletrônicas no período da pesquisa com o oferecimento de diversas oportunidades como o recebimento de herança em nome de herdeiros inelegíveis de diversas partes do mundo.

[118] Estas mensagens apresentam logomarcas de empresas ou instituições publicas e privadas conhecidas no mercado brasileiro detalhadas no decorrer deste trabalho.

[119] 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.

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 vitima, ou se apresentar na forma de uma tela sobreposta sobre os aplicativos do computador, induzindo a vítima a colaborar voluntariamente seus 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*)[120].

Recomenda-se que os usuários de sistemas de correio eletrônico se mantenham atualizados com proteção contra os mecanismos utilizados pelos fraudadores, estas informações estão disponíveis em canais de comunicação como jornais, revistas, telejornais e sites especializados na Internet (CERT.br)[121].

É importante mencionar que este 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*[122].

Recentemente foi divulgada uma lista contendo os temas de SCAM mais comuns utilizados nas mensagens eletrônicas, em virtude da falta de conhecimento destes temas pela maioria dos pesquisadores, é importante transcrever o conteúdo deste material, disponível na tabela a seguir (CERT.br)[123]:

---

[120] Dentre os dois protocolos mencionados, é importante mencionar que o SMTP é o processo mais utilizado para envio de dados coletados ao fraudador.

[121] Solicita-se em caso de recebimento de uma mensagem eletrônica de origem fraudulenta o encaminhamento da mensagem à cert@cert.br, caso haja desconfiança de envolvimento de sites brasileiros no envio ou hospedagem de mensagens, arquivos ou páginas contendo material que relativo à efetivação de fraude.

[122] Esta constatação é tratada no capítulo três subitem três deste trabalho, onde é realizada a descrição da evolução dos mecanismos de fraude utilizados no Brasil.

[123] O CERT.br alerta que os temas mencionados na tabela podem não se estender a todos os tipos de mensagens disseminados pelos fraudadores. Além deste alerta, pode-se realizar uma inferência, mencionando que a criatividade dos fraudadores deve produzir outros tipos de mensagens que buscarão um convencimento maior

Tema	Texto da mensagem
Cartões virtuais	UOL, *Voxcards*, Humor Tadela, O Carteiro, *Emotioncard*, Criança Esperança e AACD / Teleton.
SERASA e SPC	Débitos, restrições ou pendências financeiras.
Serviços do governo eletrônico	CPF / CNPJ pendente ou cancelado, Imposto de Renda (nova versão ou correção para o programa de declaração, consulta da restituição, dados incorretos ou incompletos na declaração), eleições (título eleitoral cancelado, simulação de urna eletrônica).
Álbuns de fotos	Pessoa supostamente conhecida, celebridades, relação a algum fato noticiado (em jornais, revistas e televisão), traição, nudez ou pornografia e serviço de acompanhantes.
Serviço de telefonia	Pendências de débito, aviso de bloqueio de serviços, detalhamento de fatura e créditos gratuitos para celular.
Antivírus	Nova versão, melhor opção do mercado, atualização de vacinas, novas funcionalidades e eliminação de vírus do seu computador.
Notícia / boatos	Fatos amplamente noticiados (ataques terroristas, *tsunami*, terremotos, etc.), boatos envolvendo pessoas conhecidas (morte, acidentes ou outras situações chocantes).
Reality shows	*BigBrother*, Casa dos Artistas, etc. – Fotos ou vídeos envolvendo cenas de nudez ou eróticas e discadores.

Tabela 3 - Exemplos de temas utilizados em *SCAM* registrados no Brasil (I)

dos receptores mediante a mensagem eletrônica, podendo incluir remetentes eletrônicos de pessoas conhecidas entre outros conteúdos que resultem na percepção de familiaridade da mensagem pela vítima.

Tema	Texto da mensagem
Programas ou arquivos diversos	Novas versões de *softwares*, correções para o sistema operacional *Windows*, músicas, vídeos, jogos, acesso gratuito a canais de TV a cabo no computador, cadastro ou atualização de currículos e recorra das multas de trânsito.
Pedidos	Orçamento, cotação de preços e lista de produtos.
Discadores	Para conexão gratuita na Internet e acessar imagens ou vídeos restritos.
Sites de comércio eletrônico	Atualização de cadastro, devolução de produtos, cobrança de débitos e confirmação de compra.
Convites	Convites para participação em sites de relacionamento (como *Orkut*) e outros serviços gratuitos.
Dinheiro fácil	Descubra como ganhar dinheiro na Internet.
Promoções	Diversos
Prêmios	Loterias e Instituições Financeiras
Propaganda	Produtos, cursos, treinamentos e concursos.
FEBRABAN	Cartilha de segurança e avisos de fraude.
IBGE	Censo.

Tabela 4 - Exemplos de temas utilizados em *SCAM* registrados no Brasil (II)

Vale lembrar que os temas e textos de mensagens descritos nas tabelas anteriores não são os únicos casos de *SCAM*, registrados pelo CERT.br. A tabela é apenas uma referência dos incidentes mais freqüentes, portanto infere-se que novos temas e textos de mensagens surgirão de acordo à curiosidade das vítimas, e acontecimentos de grande relevância na atualidade brasileira.

3.3.4 **Phishing Scam**

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 pessoas que usam seus conhecimentos técnicos em informática, imitando as páginas legítimas de grandes companhias como bancos (INFOSEC)[124].

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 forjada[125];
- Contém endereços de e-mail e *links* forjados[126];
- Busca representar uma instituição de comercio eletrônico ou financeiro;
- O golpe busca atingir a vítima, coletando informações digitadas em formulários HTML, existentes na mensagem eletrônica ou uma página *Web*, resultante do *link* forjado na mensagem eletrônica;
- O processo de captura se apresenta através do serviço *Web*, induzindo a vítima a colaborar voluntariamente com o fornecimento de informações sensíveis;
- Os dados capturados são enviados ao fraudador por meio do protocolo de hipertexto (HTTP – *hyper text transfer protocol*).

---

[124] O termo Phishing é também conceituado pelo CERT.br como meio utilizado para disseminação de cavalos de tróia. No conceito deste trabalho Phishing está delimitado à disseminação de e-mails que trazem em seu conteúdo *links* que levam as vítimas a páginas que apresentam o mesmo formato de sites de instituições financeiras ou comércio eletrônico.

[125] Estas mensagens apresentam logomarcas de instituições financeiras e seus órgãos representativos.

[126] Os *links* neste contexto diferem do *SCAM*, pois neste caso a vítima é redirecionada a uma página *Web*.

3.3.5 **Pharming**

O *PHARMING* é um conceito recente ao público mundial[127], 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 DNS[128], que resultam no acesso errôneo do usuário à página replicada pelo fraudador, similar a página da instituição financeira, mesmo que o usuário efetive a inserção do endereço da página do banco através da digitação da URL no *browser* utilizado na navegação Internet.

3.3.6 **Métodos utilizados para a efetivação da fraude no Brasil**

Para compreendermos melhor os métodos hoje utilizados para a efetivação da fraude, é necessário reconstituir eventos do passado recente, onde é possível avaliar os mecanismos utilizados pelo fraudador naquele período. Para isto, inicia-se o processo de descrição nos eventos registrados em 2002 (Lau):

- Surgimento dos primeiros *SCAMs*. E-mails contendo cavalos de tróia anexados a mensagens eletrônicas em nome de instituições financeiras;
- Cavalos de tróia com capacidade de captura de teclado (*Keyloggers*[129]);
- Com o passar dos meses os *Keyloggers* permitem associação da identificação de tela da aplicação com o dado capturado;
- Criação das primeiras páginas falsas de instituições financeiras;

---

[127] O terno *PHARMING* é mencionado no site do APWG Anti-Phishing Working Group (http://www.antiphishing.org) apenas a partir do ano de 2005.
[128] *Domain Name Services*
[129] Termo utilizado para descrever a funcionalidade de captura de informações a partir das teclas digitadas.

- Comprometimento do serviço de DNS de diversos provedores de acesso;
- Redirecionamento da vítima através de falhas no DNS e alterações do arquivo *hosts*[130] pelo cavalo de tróia.

Os primeiros *SCAMs*, e-mails que apresentavam natureza fraudulenta, surgiram como mensagens aparentemente inofensivas em 2002, utilizando indevidamente o nome de instituições financeiras, buscando o convencimento das vítimas através de conteúdos que alertavam sobre a necessidade de atualização do sistema *Home Banking*, supostamente utilizado pelo cliente para efetivar transações no ambiente bancário. Inadvertido do risco, as vítimas executavam um arquivo anexado à mensagem resultando, em geral, em uma tela que contendo uma mensagem de erro supostamente emitida pela instituição financeira.

No momento da instalação do executável, ocorria a gravação de arquivos em uma ou mais pastas no sistema operacional[131], adicionando registros ou linhas de comando, permitindo a execução automática dos arquivos após a carga do sistema operacional. Esta ação permitia ao executável assumir o papel de um cavalo de tróia, pois era um software preparado para deixar exposta a segurança do computador infectado[132]. O método desta exposição era efetivado através da captura das teclas digitadas pela vítima, onde todos os dados eram coletados e enviados ao responsável pelo cavalo de tróia através dos mecanismos já mencionados no subitem 3.2 deste capítulo.

Ainda no ano de 2002, os fraudadores perceberam que a análise de todas as teclas digitadas pelos usuários infectados resultava em um grande investimento de tempo, resultando em poucos dados que poderiam ser aproveitados para a efetivação da fraude. Partindo deste problema detectado, o método de ataque se tornou mais sofisticado ainda no ano de 2002.

---

[130] Arquivo existente no sistema operacional Microsoft Windows, responsável pela resolução de nomes locais na máquina do usuário.
[131] Ataque baseado em clientes que utilizam à plataforma Microsoft Windows.
[132] Considera-se exposta a segurança do usuário em virtude da abertura de um canal para envio de dados coletados nas máquinas das vítimas ao fraudador.

Informações sobre a aplicação acessada pela vítima foram inseridas nos registros capturados pelo fraudador, permitindo uma análise mais rápida sobre os dados coletados, pois o início da coleta era realizado somente através do acesso a um *browser*[133], como o *Internet Explorer*[134].

Em paralelo ao desenvolvimento de *SCAMs*, surgem as ameaças de *PHARMING*, que trouxeram em 2002 a primeira reprodução de uma página falsa de uma instituição financeira. O processo de comprometimento do usuário ocorria através de duas formas:

Em primeiro lugar, onde alguns dos arquivos executáveis anexados nas mensagens *SCAMs* possuíam características de alteração em um arquivo existente no sistema operacional Windows, responsável pela resolução de nomes de computadores. Este arquivo, localizado na pasta do sistema operacional, é conhecido como *HOSTS*[135]. Em geral este arquivo não é alterado pelo usuário, pois o sistema de resolução de nomes é provido pela infra-estrutura de rede local onde o usuário se conecta provendo toda a resolução de nomes necessária para acesso aos serviços disponíveis na Internet. Como o processo de resolução de nomes prioriza a existência de registros existentes no arquivo *HOSTS*, esta se torna uma vantagem ao atacante com a promoção de alterações neste arquivo, que permite o acesso a páginas do ambiente Internet de acordo com a alteração realizada pelo cavalo de tróia, disseminado pelo fraudador. Em geral estas alterações contêm a inserção de linhas com as *URLs* de diversas instituições financeiras. Nestes casos, o usuário dificilmente percebe a diferença entre o acesso de uma página legítima e uma página reproduzida com detalhes similares à página da

---

[133] No ano de 2002, os cavalos de tróia se prepararam apenas para a captura de dados no *Browser Internet Explorer*.

[134] O *Browser* é o software utilizado para a navegação dos usuários Internet por meio de páginas disponíveis no ambiente WWW (*World Wide Web*). Percebe-se que apenas o *Internet Explorer* é o *Browser* referenciado nos cavalos de tróia, infere-se que a utilização de apenas esta referência se deve ao fato das contaminações buscarem alvos em usuários do sistema operacional *Windows*, que representa a maior parcela de usuários com acesso ao serviço *Internet Banking* em instituições financeiras.

[135] O arquivo *HOSTS* é responsável pelo processo de resolução de nomes em diversos sistemas operacionais, incluindo o sistema operacional Windows. Este arquivo no sistema de resolução de nomes é o primeiro recurso consultado, antecedendo a validação no serviço de DNS. Portanto uma alteração no arquivo poderia resultar no direcionamento da navegação do usuário do sistema operacional a uma página falsa, apesar da digitação correta da *URL* no navegador utilizado.

instituição financeira, sendo levado a inserir as credenciais de autenticação ao *Internet Banking* em uma página falsa criada apenas com o propósito de capturar estas informações.

Neste período, a vítima poderia apenas identificar diferenças entre a página verdadeira e a página falsa através da visualização de um identificador que diferencia a existência de certificado digital na página legítima da instituição financeira[136] e ausência na página falsa.

Em segundo lugar, o outro meio utilizado para o comprometimento de vítimas através de *PHARMING*, que é a alteração dos serviços de *DNS*, existentes em diversos provedores de acesso. Estes provedores de acesso, onde alguns são conhecidos pelos usuários do serviço Internet no Brasil[137], se utilizavam equipamentos e configuração de *DNS* contendo vulnerabilidades de segurança, e que permitiam a exploração do sistema operacional através de um atacante[138]. No momento que houvesse a possibilidade do acesso do sistema comprometido pelo atacante, as alterações sobre arquivos ou configurações ocorriam, resultando na alteração da resolução de nomes de diversas páginas de instituições financeiras no Brasil.

Visando a contenção destas ameaças, diversos provedores de acesso foram notificados através das instituições financeiras afetadas. Além disto, foram promovidas campanhas de

---

[136] A cartilha de segurança do CERT.br contém na parte IV do documento um dos seus capítulos, item 2.4, voltado à identificação de conexão segura. CERT.br – **Cartilha de Segurança para Internet**. Versão 3.0 – Setembro de 2005. Disponível em: <http://cartilha.cert.br> Acesso em: 08 set. 2005. Entretanto, nos dias atuais, não há garantias neste processo de validação, pois há mecanismos de sobreposição de telas, onde a vítima tem a percepção do acesso à página legítima da instituição financeira, pois os identificadores utilizados para a consulta de certificados digitais são os mesmos utilizados para identificação das páginas legítimas dos bancos.

[137] Não é mencionada a relação dos provedores comprometidos visando proteção das marcas perante seus usuários, e considera-se que esta informação não é relevante ao objetivo deste trabalho.

[138] O comprometimento do serviço de *DNS* buscava a realização de dois tipos de ataques. O primeiro, comprometendo o roteador, responsável pela configuração do *DNS*. Nestes casos, a alteração do endereço *IP* configurado no equipamento permitia o redirecionamento do serviço para outro servidor *DNS* instalado fora do provedor de acesso. O segundo caso buscava o ataque ao serviço de *DNS*, em geral baseado em versões do *BIND*, uma distribuição gratuita de serviço de *DNS* disponível na *URL* (www.isc.org), possibilitando a inserção de arquivos contendo resoluções de nomes de diversos domínios na Internet, em geral, os relativos a instituições financeiras.

conscientização aos clientes disseminados em agências bancárias, em correspondências enviadas pelo banco através do correio[139] e através de mensagens eletrônicas[140].

Outro ponto importante adotado para a contenção de ameaças como o *SCAM*, se baseou na análise de anexos existentes em mensagens eletrônicas. Através da busca por palavras chaves no conteúdo das mensagens eletrônicas e análise da existência de conteúdos, onde foi possível eliminar grande parte destas mensagens eletrônicas nos provedores de correio eletrônico. É necessário mencionar que tanto os provedores, quando as empresas que fornecem soluções de antivírus tiveram importante papel para a eliminação deste tipo de ameaça.

Buscando minimizar os impactos sobre a fraude através da alteração na resolução de nomes em serviços DNS, monitoramentos foram criados em segmentos de endereços IP alocados no Brasil[141], permitindo controle de atividades suspeitas que possam comprometer a segurança dos usuários do sistema financeiro a partir da Internet.

Depois do impacto destes incidentes, algumas instituições financeiras evoluíram com o processo de autenticação inserindo uma tela contendo uma imagem de um teclado sobreposto ao ambiente de *Internet Banking*. Este teclado tornou-se conhecido pelos usuários como teclado virtual. O teclado virtual visa à proteção dos dados de autenticação inseridos em teclados de computadores, desta forma, as instituições financeiras adotaram ou adotam imagens semelhantes à seqüência numérica ou alfa-numérica correspondente ao teclado do computador. Esta tecnologia permite a inserção de senhas através da ação do usuário por meio

---

[139] As campanhas baseadas em envio de cartas ou extratos impressos enviados pelo correio em muitos momentos são ignorados pelos correntistas de instituições financeiras, pois estes leitores negligenciam informações que requerem um estímulo de interesse prévio.

[140] A utilização de mensagens eletrônicas contendo este tipo de alerta, permite ao fraudador a criação de mensagens similares, resultando em mais vítimas no golpe de *SCAM*.

[141] O bloco de alocação de endereços no Brasil está compreendido a partir de 200.100.0.0 a 200.255.255.255. O responsável pelo cadastramento e manutenção das informações de registro é a FAPESP, onde consultas podem ser realizadas a partir da URL http://www.registro.br.

do mouse, o objetivo deste mecanismo era evitar a captura de senhas através dos mecanismos de *keyloggers* existentes nos *SCAMs*.

Prosseguindo com a evolução dos mecanismos de comprometimento de clientes, no ano de 2003 os eventos registrados foram os seguintes (Lau):

- Os *SCAMs* se tornam mensagens que contém *links* a cavalos de tróia hospedados em provedores de conteúdo. As mensagens não estão mais relacionadas a instituições financeiras;
- Surgem os *Keyloggers* associados à *Screenloggers*[142];
- Com o passar dos meses *Keyloggers* e *Screenloggers* são preparados para capturar dados de páginas específicas em *browsers*;
- Surgem dos teclados virtuais falsos sobrepostos à sites de instituições financeiras;
- Cresce o comprometimento do serviço de DNS de diversos provedores de acesso;
- Aumentam as páginas falsas de instituições financeiras. Nasce o *PHISHING*.

Percebeu-se que a utilização de mecanismos de robustez sobre a solução *Internet Banking* pelas instituições financeiras no ano de 2002 obrigou aos atacantes a adotar soluções mais robustas às defesas criadas. Percebeu-se também que esta evolução alterou profundamente o processo de concepção de mensagens *SCAMs*.

A utilização de mensagens não mais relativas a instituições financeiras[143] permitiu que as vítimas fossem induzidas aos diversos tipos de mensagens eletrônicas recebidas, dentre eles falsas promoções que ofereciam supostos formulários ou o *download* de uma aplicação, com pretextos para uso em entretenimento ou proteção no sistema do usuário. É válido lembrar que no ano de 2003 surgiram as primeiras ocorrências de mensagens eletrônicas que se utilizavam

[142] Termo utilizado para descrever a funcionalidade de captura de informações a partir da imagem coletada em eventos acionados pelo mouse ou dispositivo que apresente funcionalidade similar.

[143] No ano de 2002 as mensagens classificadas como SCAM utilizavam exclusivamente logomarcas de instituições financeiras;

nomes e logomarcas de empresas para a disseminação dos cavalos de tróia. A ausência de anexos facilitou a disseminação destas mensagens, pois não trazia mais em seu conteúdo algo que permitia a detecção de uma ameaça através dos serviços de análise de anexos. Do outro lado a existência de *links* nestas mensagens eletrônicas, mascarados pelo código HTML, permitiram uma maior disseminação dos cavalos de tróia, convencendo da vítima a realizar uma ação consciente em busca da falsa promessa[144] existente na mensagem eletrônica.

Outra importante evolução adotada pelos fraudadores no ano de 2003 foi uma resposta à evolução tecnológica dos bancos. A criação dos *screenloggers* foi uma resposta à criação dos teclados virtuais, pois o *screenlogger* era mais um mecanismo que permitia a captura dados, agora através de imagens após o evento de acionamento do botão que permite seleção de regiões da tela do computador através do mouse. Esta captura fragilizou os teclados virtuais concebidos em 2002, criados pelas instituições financeiras em resposta aos ataques de *keyloggers* registrados. As imagens capturadas apresentavam características de compactação que facilitava o processo de transmissão destes arquivos através da Internet. Considerando que a maioria dos usuários utilizava acessos discados, o fraudador também precisou aperfeiçoar o processo de captura e envio dos dados coletados. É necessário mencionar que em nenhum momento ações isoladas[145] de captura de imagens foram detectadas no ano de 2003, pois as imagens complementavam dado capturado através da digitação do teclado realizado pela vítima.

As primeiras versões de cavalos de tróia que utilizavam características de *keylogging* e *screenlogging* e permitiam a captura de qualquer ação realizada no computador, portanto uma grande quantidade de dados era armazenada e posteriormente enviados à Internet quando o usuário se conectava a rede. Este grande volume de informações se tornou inviável ao

[144] No subitem 3.3 há duas tabelas que permitem avaliar os exemplos utilizados atualmente. É necessário mencionar que os incidentes registrados em 2003 não utilizavam todos os temas mencionados.
[145] Isto significa que não surgiu nenhum cavalo de tróia com funcionalidades exclusivas de *Screenlogging*.

fraudador em virtude da necessidade de obtenção das credenciais das vítimas em tempo hábil[146]. A partir desta dificuldade, ocorreu mais um avanço tecnológico desenvolvido pelos fraudadores; a obtenção de dados somente relacionados à credenciais de acesso. Neste caso, o foco da ação de captura se concentrou em iterações do cliente em seus *browsers*, softwares existentes na maioria dos sistemas operacionais que permitem a navegação do usuário na Internet, conseqüentemente, permitindo acesso de clientes bancários ao serviço de *Internet Banking*. A realização de coleta seletiva diminuiu o volume de dados coletados e uma melhora na análise destas informações pelo fraudador.

No ano de 2003 ainda surgiu mais uma evolução tecnológica em resposta à concepção dos teclados virtuais. O fraudador com foco ao roubo de credenciais iniciou o desenvolvimento de teclados virtuais falsificados que apresentavam características similares aos teclados virtuais criados pelas instituições financeiras. Entretanto estes teclados apresentavam propriedades que os diferenciava dos teclados virtuais legítimos; é possível mencionar como exemplo, a existência de múltiplos campos de preenchimento no teclado falsificado que solicita diversas informações permitindo ao fraudador a realização de transações financeiras em nome da vítima apenas com o preenchimento das informações solicitadas pelo fraudador. Estes teclados virtuais falsificados foram desenvolvidos no formato de telas, concebidas em diversas linguagens de programação visual como Visual C, Visual Basic e Delphi, onde não podiam ser removidas da tela da vítima sem a inserção dos dados solicitados. Facilitando em muitos momentos a captura das credenciais de acesso ao serviço de *Internet Banking*.

A existência deste cenário não eliminava as ameaças de alteração do serviço de DNS já detectadas no ano de 2002, ao contrário disto, de percebeu um aumento substancial nas ocorrências desta natureza em um número ainda maior de provedores de acesso. Buscando

[146] Percebe-se que as credenciais coletadas das vítimas não são imediatamente utilizadas. É necessário se realizar triagem destes dados e planejamento por parte do fraudador sobre a utilização deste recurso.

uma contenção a estes incidentes, provedores de acesso foram contatados pelas instituições financeiras e por órgãos de regulamentação, visando uma contenção a este tipo de ataque.

A conseqüência deste aumento levou também a proliferação de páginas reproduzidas pelos fraudadores com características das páginas legítimas de instituições financeiras. Parcela destas páginas era acessada através de alterações realizadas no serviço de DNS, uma característica dos ataques de *PHARMING*; e o restante dos acessos a estas páginas era realizado através de *links* existentes em mensagens eletrônicas que utilizavam nomes e logomarcas de instituições financeiras. Esta modalidade de mensagem é o que se conhece hoje por *PHISHING*.

Instituições financeiras buscaram levar ao público mensagens informando estes problemas, solicitando aos seus usuários cautela no acesso aos serviços de *Internet Banking*. A resposta dos bancos em relação às mensagens eletrônicas em nomes destas instituições foi a recomendação ao serviço de *Internet Banking* apenas através da digitação do endereço por meio do *browser* ou navegador, evitando desta maneira o acesso acidental de uma página falsa em nome de uma instituição financeira através de *links* existentes em mensagens eletrônicas.

Como adaptações[147] são necessárias para a evolução de qualquer processo tecnológico, no ano de 2004, os eventos registrados mostram um aprimoramento aos ataques descritos em 2003. O cenário neste período retratou os seguintes eventos (Lau):

- Os *SCAMs* se aprimoram, utilizando uma diversidade maior de temas que atraem a curiosidade das vítimas. Alguns *SCAMs* contêm *links* a páginas que hospedam o cavalo de tróia;
- Surgem os cavalos de tróia que codificam os dados capturados;

[147] Deve-se interpretar as adaptações como processo contínuo de descoberta de vulnerabilidades de sistemas e suas respectivas correções.

- Com o passar dos meses, alguns cavalos de tróia desenvolvem a capacidade de análise do ambiente instalado com características de atualização automática do dispositivo utilizado para o ataque;
- Surgem casos de comprometimento de computadores através de *scripts Active X* e;
- Surgem os cavalos de tróia que sobrepõem telas ao *browser*, imitando as telas o ambiente *Web* de instituições financeiras.

Em 2004, percebeu-se ausência aos ataques aos serviços de DNS, que atingiram diversas instituições financeiras nos anos de 2002 e 2003. Não há informações sobre todas as causas da eliminação destas ameaças, mas acredita-se que ações realizadas pelos provedores de tecnologia nos provedores de acesso permitiram a extinção desta ameaça.

Em resposta a ausência desta ameaça cresceram os ataques utilizando mensagens eletrônicas associados aos cavalos de tróia. Em busca do maior convencimento de vítimas, diversos temas foram utilizados, incluindo notícias e fatos atuais que geram curiosidade aos leitores. Esta evolução permitiu observar a capacidade de rápida adaptação que os fraudadores possuíam em relação às demandas de novos temas, utilizando assuntos recentes visando o convencimento da vítima em realizar acesso ao conteúdo malicioso[148] referenciado na mensagem eletrônica. Em algumas destas mensagens foi possível detectar a ausência do *link* ao cavalo de tróia, pois a referência existente na mensagem eletrônica aponta para o acesso a uma página disponível na Internet, sendo que esta página contém o *link* ao cavalo de tróia[149]. Neste período também são descobertos incidentes que envolveram um ou mais cavalos de tróia[150] existentes em uma única mensagem eletrônica, dificultando ações de contenção, pois

[148] O conteúdo malicioso mencionado no texto são os cavalos de tróia.
[149] O método utilizado é o mesmo aplicado em 2003, entretanto a vítima necessita passar por um passo intermediário, que é o acesso a uma página disponível na Internet.
[150] Os diferentes *links* existentes em uma única mensagem apontavam acesso a um mesmo provedor relacionando diferentes arquivos. Alguns incidentes detectados foram continham em uma única mensagem *links* a cavalos de tróia hospedados em diferentes provedores.

caso ocorresse um erro no processo de detecção de algum link referenciando um cavalo de tróia, era possível que o ataque ainda se mantivesse efetivo em virtude da negligência da análise do *SCAM.*

No ano de 2004, percebeu-se que parte dos dados capturados pelo fraudador se apresentavam codificados. Esta evolução no processo de envio de credenciais foi uma resposta às diversas ações de investigação realizadas pelos órgãos públicos de repressão sobre estes dados coletados pelo fraudador.

Vale citar que todos os dados capturados por cavalos de tróia eram enviados ao fraudador através de mecanismos de transferência de arquivos, por meio do serviço de FTP (*File Transfer Protocol*) e através do serviço de envio de mensagens eletrônicas, por meio do protocolo SMTP (*Simple Mail Transfer Protocol*). Estes protocolos quando analisados através de um capturador de tráfego de rede, conhecido também como *sniffer*, permite a coleta de todo o processo de comunicação, incluindo neste caso a análise de credenciais utilizadas no envio de dados através destes dois protocolos.

Caso as credenciais de acesso SMTP ou FTP fossem descobertas, tornava-se possível uma investigação sobre os dados armazenados nestes repositórios. Este processo de análise, iniciado em 2003 através de órgãos públicos de repressão ao crime, permitiu a prisão de diversos responsáveis por estas ações fraudulentas. Do outro lado, dados capturados de clientes de instituições financeiras foram repassados aos respectivos bancos afetados, permitindo a proteção destas vítimas antes da efetivação de uma fraude.

O fraudador, vislumbrando um cenário de perdas financeiras através destas ações se viu obrigado a aperfeiçoar mecanismos de fortalecimento a estes dados coletados. A tecnologia adotada neste caso foi a adoção de mecanismos de codificação mencionados acima. A

codificação pode ser uma simples alteração de *bits* que torne o conteúdo ilegível, até a iteração do dado com algoritmos para a proteção dos dados[151].

Mais outra evolução ocorreu no desenvolvimento de cavalos de tróia. Surgiram em 2004 arquivos maliciosos com tamanhos reduzidos (menores de 100 Kb), que continham apenas um módulo inicial do cavalo de tróia. Este método é uma resposta à detecção das ameaças através de diversos antivírus. O funcionamento deste arquivo dependia do *download* de arquivos adicionais, disponíveis na Internet através de extensões ".JPG". Em geral ".JPG" são extensões relacionadas às imagens, neste caso, o arquivo ".JPG" contém um conjunto de comandos e configurações que permite a complementação do cavalo de tróia com dados que introduzem funcionalidades ao cavalo de tróia.

Caso o cavalo de tróia detecte a contenção de algumas variáveis configuradas no executável, o programa busca, através de uma conexão à Internet, a atualização de seu módulo de configuração, permitindo o envio dos dados a um outro provedor de serviços FTP e SMTP existentes no novo arquivo de configuração.

Visando a disseminação de ataques mais sofisticados através do mecanismo de *SCAM*, foram utilizadas em algumas mensagens eletrônicas contendo códigos de programação interpretados por alguns programas existentes no sistema operacional Windows. Estes códigos contêm uma seqüência de ações que efetivam o *download*, instalação e infecção automática do usuário em virtude da abertura e visualização da mensagem eletrônica enviada pelo fraudador. O código utilizado era o *Active X*, mas neste período também foram detectadas as mesmas vulnerabilidades utilizando *Active Scripting*.

Ainda em relação ao *SCAM*, percebeu-se que alguns teclados virtuais sobrepostos ganharam novas funcionalidades e novos mecanismos que buscam ludibriar as vítimas. Os teclados

[151] Não foi fornecido pelas instituições financeiras para esta pesquisa o processo utilizado para a codificação dos dados.

virtuais detectados em 2003 não são mais efetivos à captura de informações, pois as vítimas potenciais já possuíam discernimento à detecção desta ameaça. Em resposta à evolução no processo de detecção dos usuários, os fraudadores utilizaram técnicas de sobreposição de telas que se assemelham às páginas de navegação de instituições financeiras. Este processo não imita apenas um teclado virtual, pois traz uma tela visível à vítima, com a semelhança de um ambiente de navegação do *Internet Banking*. Vale lembrar que estas sobreposições ainda eram detectáveis, devido às pequenas diferenças entre as telas criadas pelo fraudador e as telas legítimas de instituições financeiras. Entretanto vale lembrar que usuários desatentos podiam inserir credenciais de acesso permitindo a posterior efetivação de transações financeiras por fraudadores.

Apesar de não ter sido mencionado nos eventos de 2004, é necessário citar que ataques baseados em *PHISHING* apresentaram crescimento até a metade do ano de 2004. Decrescendo a partir do segundo semestre daquele ano. Percebeu-se que houve uma diminuição substancial do comprometimento de clientes de bancos através de páginas reproduzidas por fraudadores, e um aumento linear de tentativas de comprometimento de equipamentos através da instalação de cavalos de tróia (*SCAM*).

O ano de 2005 não foi objeto da pesquisa contida neste trabalho. Algumas informações sobre este período poderão ser avaliadas através dos dados estatísticos, disponíveis no subitem quatro deste capítulo. Entretanto percebeu-se que a tendência do uso das técnicas apresentadas em 2004 se manteve no início de 2005, onde ocorreu um forte aumento na atividade de *SCAM* e uma quase extinção de incidentes envolvendo a técnica de *PHISHING*.

3.3.7 **Métodos utilizados para a efetivação da fraude no exterior**

Relatórios emitidos no exterior, que mencionam ameaças aos clientes de instituições financeiras são escassos e raramente mencionam o Brasil como uma ameaça. Acredita-se que

esta postura é resultante do desconhecimento das atividades existentes no Brasil e a evolução das ameaças conforme o detalhamento do subitem anterior deste trabalho.

A primeira referência publicada sobre ataques foi disponibilizada por um grupo intitulado APWG (*Anti-Phishing Working Group*)[152]. Este grupo foi criado em 2003[153], informando ao público os primeiros incidentes de *PHISHING* registrados nos Estados Unidos.

O primeiro incidente relatado 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.

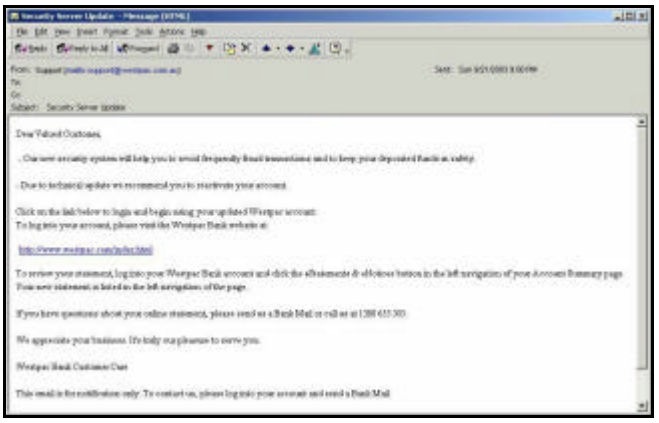

Figura 10 - Primeiro registro de atividade de *PHISHING* divulgado no APWG

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 aplicada 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[154].

---

[152] http://www.antiphishing.org

[153] É possível calcular o surgimento do APWG através da consulta de informações de registro do domínio antiphishing.org. Segundo informações do site Whois.ws (http://www.whois.ws/whois-org/antiphishing.org/), o domínio foi registrado em 21/10/2003 às 19h53min.

[154] A ausência de registros de *PHARMING* no Brasil é um fato comprovado até Abril de 2005.

Nota-se a ausência na menção de ataques de *SCAM* em relatórios oficiais emitidos no exterior, hoje amplamente utilizado para a aplicação de fraudes em clientes do sistema financeiro brasileiro. Acredita-se que é possível uma disseminação destes ataques no exterior a partir do ano de 2006[155].

Em um dos relatórios[156] divulgados pela APWG é possível obter algumas informações sobre o cenário da fraude no exterior (APWG):

- Número de URLs contendo páginas reproduzidas por fraudadores (*PHISHING*) em Março / 2005: 2870;
- Aumento de incidentes (*PHISHING*) entre o período de Julho / 2004 e Março 2005: 28 %;
- Número de marcas utilizadas em incidentes (*PHISHING*) em Março / 2005: 78 e;
- País com maior hospedagem de URLs (*PHISHING*) em Março / 2005: Estados Unidos.

A partir do número de incidentes registrados é possível realizar o cálculo da média de incidentes no período, que se encontra em um número pouco superior a 90 incidentes para cada dia de Março de 2005. A partir do subitem quatro deste capítulo será possível comparar estes números de incidentes no exterior, com os números coletados no Brasil[157].

---

[155] Segundo informado pelas instituições financeiras brasileiras no período da pesquisa deste trabalho, há indícios ainda não comprovados do uso de cavalos de tróia em incidentes isolados no Leste Europeu e América do Norte. E a ausência de artigos ou publicações internacionais sobre o tema comprova o desconhecimento do assunto pelo público estrangeiro. As referências que melhor descrevem o cenário atual de ameaça nos exterior (RUSCH, p 4-5) (HALLAM-BAKER, p12-15) tratam de técnicas de ataque que não são mais utilizados sobre clientes de instituições financeiras no Brasil.

[156] O relatório utilizado para a apresentação dos dados está baseado no documento APWG – **Phishing Activity Trends Report – March, 2005**. Anti-Phishing Working Group. Disponível em: < http://antiphishing.org/APWG_Phishing_Activity_Report_March_2005.pdf> Acesso em: 16 mai. 2005

[157] Os incidentes registrados no Brasil superam 10 vezes o número de incidentes registrados no mesmo período (Março / 2005).

Neste mesmo relatório é possível observar uma menção ao crescimento dos incidentes *SCAM* em língua portuguesa; como os casos mencionados são similares aos registrados no Brasil, acredita-se que este relatório esteja citando os incidentes registrados no Brasil. Entretanto a nomenclatura utilizada no relatório para a denominação destes ataques é *phishing-based malicious code attacks*, que em português pode ser traduzido como ataques de *PHISHING* baseados em códigos maliciosos. Aparentemente o relatório apenas leva ao público informações de ataques baseados em *keyloggers*, portanto são desconhecidos no exterior, ataques baseados na captura de telas, os *screenloggers*, e as sobreposições de telas que ocorrem com freqüência no Brasil.

Apesar do volume e qualidade das informações disponíveis pela APWG, é possível perceber o desconhecimento do público norte-americano sobre os riscos que ainda podem afligir os clientes de serviços financeiros no exterior. Neste caso, o Brasil, infelizmente, é o precursor deste tipo de ataque[158].

Comprovando a afirmação do parágrafo anterior e consolidando informações sobre ataques ocorridos no Brasil e os informados pela AWPG como representante de incidentes ocorridos no exterior, pode-se assumir a aplicação das técnicas pelo fraudador no ambiente *Internet Banking* com a seguinte cronologia:

- Brasil:
    - Pharming (2002 e 2003);
    - Scam (2002-2005)[159] e;
    - Phishing (2003-2005[160]).

[158] A ausência de artigos ou publicações internacionais sobre o tema comprova o desconhecimento do assunto pelo público estrangeiro. As referências que melhor descrevem o cenário atual de ameaça nos exterior (RUSCH, p 4-5) (HALLAM-BAKER, p12-15) tratam de técnicas de ataque que não são mais utilizados sobre clientes de instituições financeiras no Brasil.

[159] Deve-se considerar que os ataques utilizando as técnicas de *SCAM*, são os mais significativos em virtude do tempo de existência e volume de tentativas de ataque mencionados no subitem quatro deste trabalho.

- Exterior[161]:
    - Phishing (2003-2005)[162];
    - Pharming (2005-2005) e;
    - Scam (2005)[163].

Para cada uma das técnicas utilizadas para efetivação da fraude no ambiente *Internet Banking*, É possível afirmar que todas apresentam precedência na ocorrência de incidentes registrados no Brasil.

As técnicas utilizadas no Brasil desde 2002 (*PHARMING* e *SCAM*) surgem em relatórios registrados pelo APWG em 2005 (*PHARMING*) enquanto que o *SCAM* é mencionado em relatórios e artigos que citam o risco de comprometimento do serviço *Internet Banking* por cavalos de tróia mas não comprovam a concreta existência desta ameaça.

O *PHISHING*, que surge no ano de 2005 no Brasil e APWG, apresenta precedentes de sua existência no Brasil, em virtude de dados coletados pelas instituições financeiras deste ataque método de ataque antes do surgimento do APWG.

Com estas afirmações é possível comprovar que todas as técnicas conhecidas para aplicação de golpes sobre o ambiente *Internet Banking* têm como origem o Brasil.

Em virtude do trabalho se limitar à análise do cenário de fraudes sobre o ambiente *Internet Banking* até meados de 2005, não é possível descrever a tendência das ameaças nos anos seguintes.

---

[160] Limitado ao o período da pesquisa, realizado até meados de 2005.

[161] O APWG concentra na notificação de incidentes eventos ocorridos dos bancos Norte Americanos, portanto considera-se que a linha de evolução disponível reflete apenas o que foi relatado nos Estados Unidos.

[162] Os incidentes com Phishing, segundo a APWG são os mais significativos segundo dados absolutos. APWG – **Phishing Activity Trends Report – March, 2005**. Anti-Phishing Working Group. Disponível em: < http://antiphishing.org/APWG_Phishing_Activity_Report_March_2005.pdf> Acesso em: 16 mai. 2005.

[163] Há referências do possível uso de códigos maliciosos no relatório de atividade de Phishing, disponível pela APWG, entretanto não há evidências que comprovam a sua aplicação no ano de 2005.

3.4 DADOS ESTATÍSTICOS SOBRE A FRAUDE NO BRASIL

Os dados apresentados neste subitem é o resultado de diversas coletas, abrangendo incidentes de *SCAM* e *PHISHING*, obtidos através e-mails coletados em caixas postais eletrônicas criadas apenas com o propósito de obtenção de exemplares de mensagens eletrônicas maliciosas. Foram obtidos URLs de incidentes *SCAM* através do CERT.br e algumas instituições financeiras auxiliaram na consolidação deste resultado apresentado neste trabalho[164].

As informações disponíveis compreendem a coleta de dados no período de Abril de 2004 a Março de 2005, portanto são 12 meses de coleta, permitindo obter tendência sobre a evolução do cenário de fraudes no Brasil.

E devido à escolha do contexto mencionado no parágrafo anterior, não serão mencionados neste trabalho, dados estatísticos de *PHARMING*, pois estes não apresentam registros no ano de 2004 e 2005.

É importante mencionar que os números a seguir podem não representar todo o universo de incidentes ocorridos no Brasil, entretanto, devido à busca de informações nas diversas fontes informadas no primeiro parágrafo deste item, infere-se que os resultados apresentados cobrem uma parcela significativa dos incidentes.

É importante mencionar que os incidentes de *SCAM* e *PHISHING* apresentam características[165] distintas de abordagem sobre a vítima de fraude e diferente processo evolutivo. Desta forma, será considerada a apresentação de cada um destes incidentes em tabelas distintas nos próximos itens deste trabalho.

---

[164] Não serão mencionados os nomes das instituições financeiras em virtude da ausência de relevância ao objetivo proposto neste trabalho. O autor deste trabalho se responsabiliza pelas informações apresentadas e conclusões da análise destes dados.

[165] Descrito no subitem três deste capítulo.

3.4.1 **Incidentes de *PHISHING* no Brasil**

Em primeiro lugar são apresentados dados que representam incidentes registrados de *PHISHING* no Brasil.

Período (Mês / Ano)	Incidentes registrados
Abril / 2004	37
Maio / 2004	24
Junho / 2004	48
Julho / 2004	58
Agosto / 2004	74
Setembro / 2004	54
Outubro / 2004	63
Novembro / 2004	58
Dezembro / 2004	55
Janeiro / 2005	23
Fevereiro / 2005	19
Março / 2005	17

Tabela 5 - Incidentes de *PHISHING* registrados no Brasil

A partir dos dados informados na tabela acima, é possível representar o gráfico a seguir:

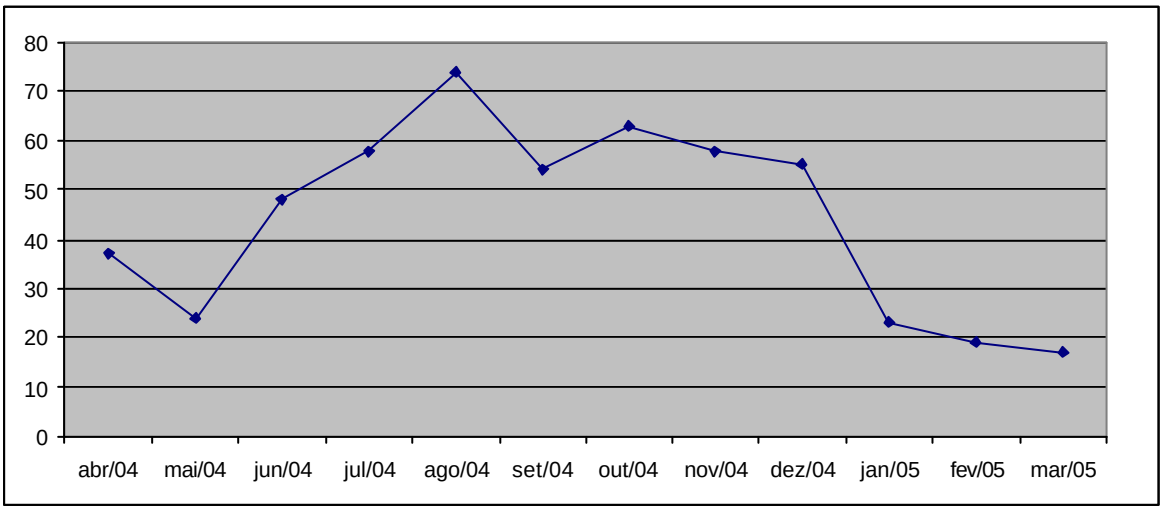

Figura 11 - Incidentes de *PHISHING* registrados no Brasil

A partir do gráfico anterior é possível apresentar uma linha de tendência linear, permitindo obter indícios de decréscimo dos incidentes registrados:

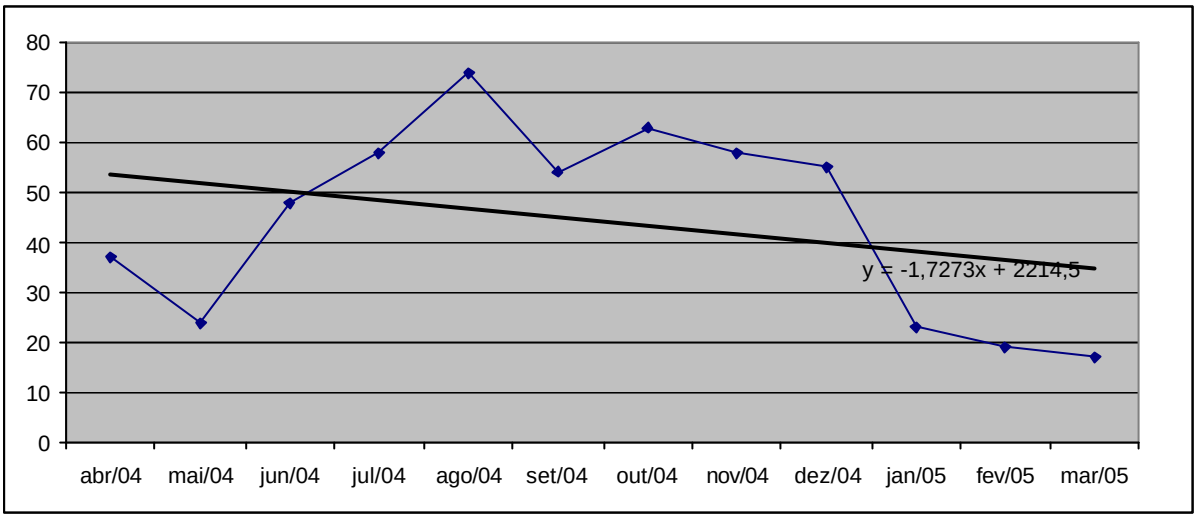

Figura 12 - Análise gráfica linear dos Incidentes de *PHISHING*

E também partir do mesmo gráfico é possível apresentar uma linha de tendência polinomial[166] de ordem dois, apontando os períodos com incidentes expressivos:

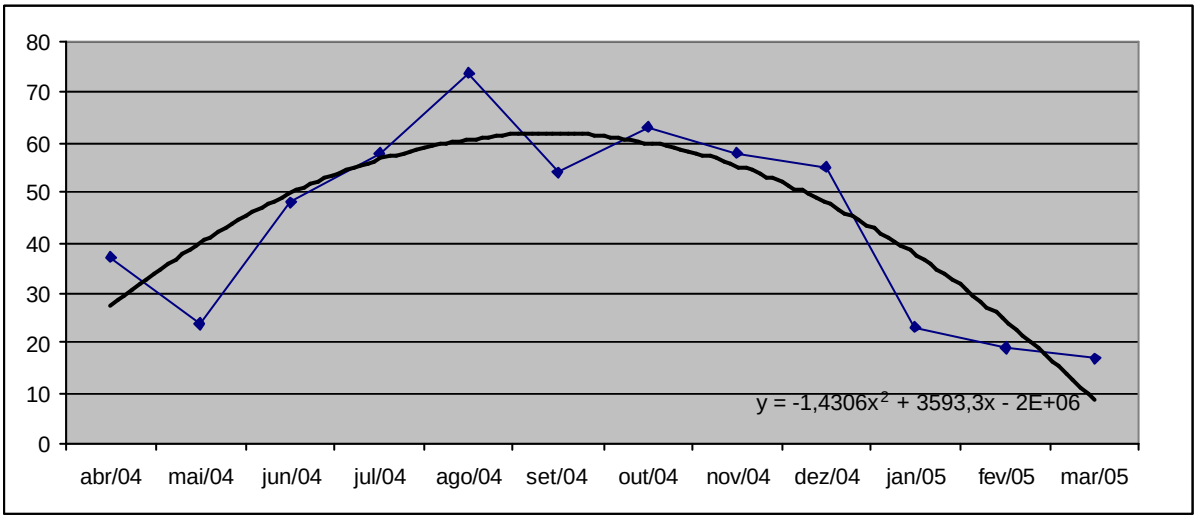

Figura 13 - Análise gráfica polinomial dos Incidentes de *PHISHING*

[166] Todas as linhas de tendência existentes neste trabalho, sejam elas lineares ou polinomiais, estão baseadas em padrões utilizados pelo produto Microsoft Excel, tendo como premissas a necessidade de avaliação linear e polinomial de ordem dois.

Percebe-se que no período delimitado na coleta há um aumento expressivo de incidentes a partir de junho de 2004, permanecendo significativo[167] até o mês de dezembro de 2004. O maior número de incidentes registrados se encontra no mês de agosto de 2004[168], mas deve-se considerar que os incidentes registrados podem estar apenas mostrando parte do cenário real. Os fatos indicam que os ataques baseados em *PHISHING* apresentaram períodos de grande volume, mas com incidentes pouco significativos, se comparados à quantidade de registros de incidentes divulgados pelo APWG[169], apresentados no subitem três deste capítulo.

Em virtude dos números mais significativos dos incidentes de *SCAM*[170], busca-se neste trabalho dar maior ênfase à análise de incidentes que atualmente envolvem um maior comprometimento de clientes do serviço *Internet Banking* através de cavalos de tróia.

Na conclusão deste capítulo, será possível comprovar através de uma análise quantitativa de eventos a constatação do menor impacto de ataques de *PHISHING*, face às ameaças de *SCAM* junto aos usuários do serviço de *Internet Banking* em instituições financeiras[171].

3.4.2 **Incidentes de *SCAM* no Brasil**

É importante lembrar que os números a seguir descrevem o volume de incidentes *SCAM* que podem não representar todo o universo de incidentes ocorridos no Brasil. Mais uma vez infere-se que os resultados apresentados cobrem uma parcela significativa dos incidentes.

---

[167] Considerou-se significativo nesta análise o valor quantitativo superior à primeira coleta realizada. Os dados obtidos neste trabalho são representados continuamente ao longo dos meses, permitindo descrever uma tendência para o período em análise. Esta análise é corroborada pela análise polinomial disponível na figura 13.

[168] Maior valor quantitativo encontrado no período da coleta, e também corroborado pela análise polinomial.

[169] Em uma comparação entre a quantidade de incidentes registrados em Março de 2005 pelo APWG, é possível verificar que os incidentes de Phishing registrados no Brasil não alcançam 1% dos incidentes registrados nos Estados Unidos.

[170] Os incidentes de *SCAM* registrados no Brasil em março de 2005 superam em 50 vezes o número de incidentes registrados de *PHISHING* no mesmo período.

[171] O impacto mencionado no texto deste trabalho reflete o número de incidentes registrados. Não é possível a partir das informações coletadas determinar as perdas financeiras relacionadas a cada um dos mecanismos utilizados pelo fraudador (*SCAM* ou *PHISHING*)

Período (Mês / Ano)	Incidentes registrados
Abril / 2004	101
Maio / 2004	112
Junho / 2004	143
Julho / 2004	265
Agosto / 2004	444
Setembro / 2004	371
Outubro / 2004	353
Novembro / 2004	542
Dezembro / 2004	646
Janeiro / 2005	503
Fevereiro / 2005	771
Março / 2005	904

Tabela 6 - Incidentes de *SCAM* registrados no Brasil

Percebe-se através de uma comparação numérica dos incidentes de *SCAM* e *PHISHING* a superioridade quantitativa dos incidentes registrados em *SCAMs*. Lembre-se mais uma vez que esta técnica envolve a utilização de cavalos de tróia pelo fraudador, e que podem resultar no comprometimento do equipamento de usuários do ambiente *Internet Banking*.

Visando facilitar a visualização dos dados informados na tabela anterior, é possível transcrever os dados da tabela no gráfico abaixo:

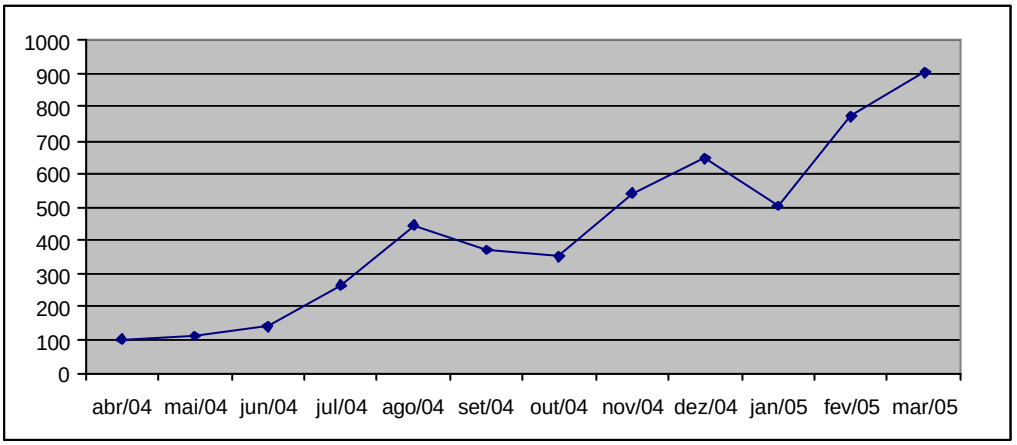

Figura 14 - Incidentes de *SCAM* registrados no Brasil

A partir do gráfico anterior é possível traçar uma linha de tendência linear, obtendo indícios de acréscimo consistente dos incidentes registrados:

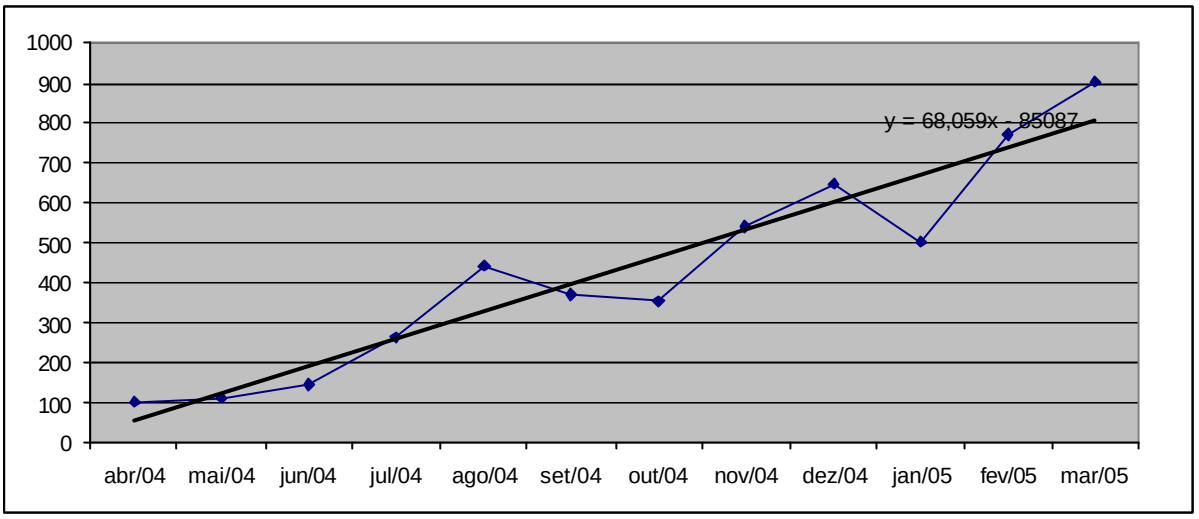

Figura 15 - Análise gráfica linear dos Incidentes de *SCAM*

E também partir do mesmo gráfico é possível apresentar uma linha de tendência polinomial de ordem dois, determinar períodos contendo incidentes expressivos:

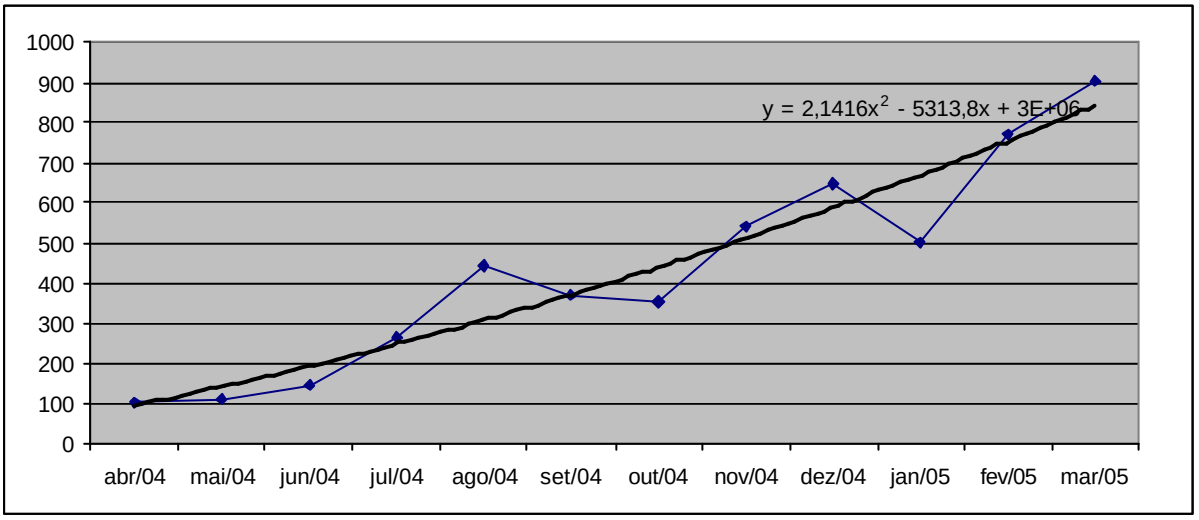

Figura 16 - Análise gráfica polinomial dos Incidentes de *SCAM*

Diferente do gráfico de *PHISHING*, o *SCAM* apresenta uma tendência de crescimento linear constante e consistente perante os dados coletados[172]. Conforme menção anterior neste trabalho, a partir da superioridade numérica dos incidentes de *SCAM* sobre incidentes de

[172] Este fato é constatado através da similaridade dos gráficos lineares e polinomiais obtidos pela análise. Através destes resultados, é possível estimar um aumento significativo no número de incidentes registrados para os outros meses de 2005.

PHISHING é possível afirmar que esta técnica é mais disseminada entre os fraudadores e mais utilizada que a técnica de *PHISHING*. Também é válido afirmar que ao contrário da tendência de diminuição no registro de incidentes (*PHISHING*) envolvendo páginas reproduzidas por fraudadores contendo semelhança a páginas legítimas de instituições financeiras, o *SCAM* apresenta um aumento constante no número de ameaças, acompanhado de saltos significativos no aumento de incidentes desde o início da coleta. Há três incrementos significativos existentes nos diagramas anteriores que precisam ser mencionados, o primeiro deles ocorre em julho e agosto de 2004, outro em novembro e dezembro de 2004, por fim, final do período de coleta ocorre o último incremento, nos meses de fevereiro e março de 2005. Percebe-se que a distância dos meses que separam estes períodos de aumento é menor com o passar do tempo. Extrapolando este gráfico, é possível supor um crescimento significativo de incidentes para os meses e anos seguintes.

Demonstrada a superioridade numérica dos incidentes classificados como *SCAM,* e sua tendência de crescimento em face aos incidentes classificados como *PHISHING*, considera-se importante neste trabalho exploração de características adicionais, que permitem uma maior identificação no perfil deste tipo de ataque. Além da análise apresentada, o pesquisador sugere no subitem de trabalhos futuros existente no penúltimo capítulo deste trabalho a evolução e continuidade desta análise.

Outro fator que reforça esta conclusão considera o fato dos dados apresentarem padrões que permitem determinar características nos ataques de *SCAM,* diferente das ameaças de *PHISHING*, que não permitem a obtenção de conclusões relevantes para este trabalho[173]; como exemplo, é possível mencionar que as páginas reproduzidas por fraudadores apresentam como característica a existência de registros de hospedagem em diferentes localidades o que

[173] O baixo número de eventos registrados para incidentes de *PHISHING* registrados no período não apresentaram detalhes e padrões de hospedagem comparados aos incidentes de *SCAM*.

não permite determinar um padrão de escolha do hospedeiro[174], diferente do *SCAM*, que apresenta segundo os dados coletados uma concentração na hospedagem dos cavalos de tróia. Em virtude destas características, o próximo item deste trabalho apresenta apenas a distribuição de hospedagem de cavalos de tróia resultantes da técnica de *SCAM*.

3.4.3 **Distribuição de hospedagem de cavalos de tróia em *SCAM* no Brasil**

O primeiro dado adicional coletado nos incidentes de *SCAM* está relacionado às características de hospedagem de cavalos de tróia e sua distribuição quantitativa de acordo com a reincidência de eventos envolvendo os cinco maiores responsáveis pela hospedagem destes arquivos maliciosos. Visando a preservação dos provedores, estes são denominados através de letras (A, B, C, D e E). Os dados coletados permitem a criação da seguinte tabela:

Período (Mês / Ano)	**Incidentes Provedor A**	**Incidentes Provedor B**	**Incidentes Provedor C**	**Incidentes Provedor D**	**Incidentes Provedor E**
Abril / 2004	33	32	0	0	0
Maio / 2004	29	24	0	1	1
Junho / 2004	44	20	0	4	2
Julho / 2004	70	62	0	4	23
Agosto / 2004	94	22	0	30	89
Setembro / 2004	71	17	0	60	31
Outubro / 2004	75	26	5	28	26
Novembro / 2004	130	31	14	10	18
Dezembro / 2004	176	25	15	10	24
Janeiro / 2005	188	18	9	7	51
Fevereiro / 2005	383	9	21	29	21
Março / 2005	339	33	38	35	21

Tabela 7 - Incidentes e hospedeiros de *SCAM* registrados no Brasil

[174] O hospedeiro é o local utilizado pelo fraudador para publicação da página clonada. Foram informados pelas instituições financeiras que a escolha do hospedeiro depende da disponibilidade de equipamentos vulneráveis disponíveis na Internet, permitindo a invasão do sistema a partir de brechas de segurança.

Em primeiro momento, é possível perceber uma maior concentração numérica de incidentes em uma das colunas, representando o provedor A, entretanto é pouco visível a tendência entre as outras colunas devido à dificuldade na busca de padrões nos outros provedores. Visando o auxílio desta análise, é possível transcrever estas informações da tabela através do gráfico a seguir:

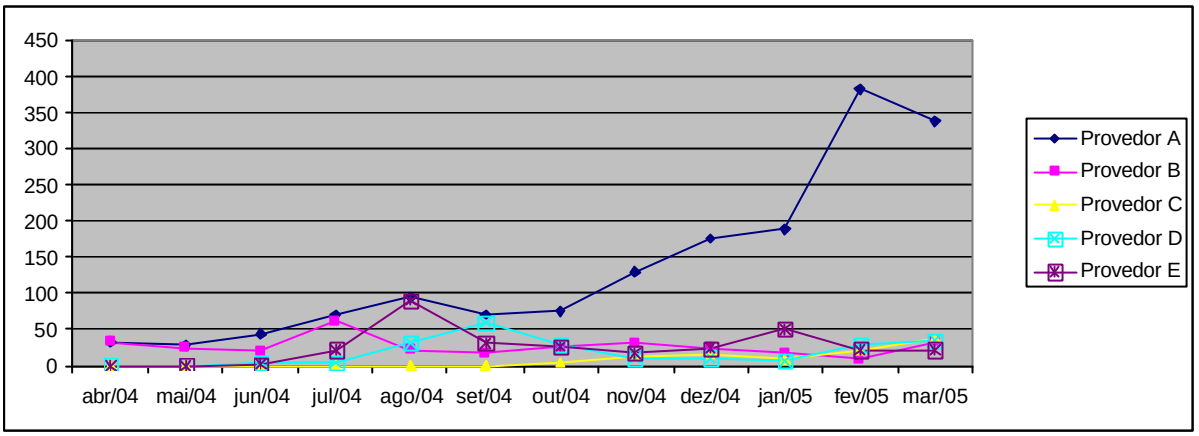

Figura 17 - Hospedeiros de cavalos de tróia em *SCAMs* registrados no Brasil

Mais uma vez, percebe-se que o provedor A apresenta superioridade quantitativa na hospedagem de cavalos de tróia em todo o período delimitado na coleta. A superioridade torna-se mais visível quando são analisados os dados coletados após o mês de outubro de 2004. Não se pode determinar apenas com estes dados os motivos da concentração de incidentes em apenas um único provedor, mas é possível mencionar os indícios que resultam a este comportamento. Foram constatados por meio das instituições financeiras responsáveis pelo fornecimento dos dados da Tabela 7, indícios que permitiam maior facilidade aos fraudadores no processo de hospedagem de arquivos no provedor A. Do outro lado, foram

comprovados que os provedores B, C, D e E se utilizaram de mecanismos mais robustos[175] que dificultam a hospedagem de arquivos a partir do mês de outubro de 2004.

A hipótese da adoção de mecanismos que dificultam a hospedagem nos demais provedores é corroborada a partir de observações na hospedagem de arquivos nos provedores B, D e E respectivamente, onde são observados súbitos aumentos nos meses de julho, setembro e agosto de 2004. O súbito aumento pode estar relacionado à utilização de novos provedores pelo fraudador em virtude da busca de alternativas no processo de hospedagem de cavalos de tróia. Observa-se nestes mesmos provedores o decréscimo de incidentes registrados nos meses posteriores, o que pode demonstrar uma dificuldade na hospedagem de arquivos maliciosos nestes provedores após a adoção de algum mecanismo de contenção.

A partir destas hipóteses, os provedores B, D e E foram consultados em busca da confirmação da hipótese mencionada acima. Todos os provedores informaram que ações foram tomadas para a contenção destes incidentes, tanto na criação de mecanismos de dificultam a abertura de contas que permitem a hospedagem de arquivos, quanto na análise de arquivos hospedados nestes ambientes.

Da mesma forma, o provedor A foi consultado em busca da confirmação das hipóteses mencionadas anteriormente. Foi confirmado que ações foram tomadas, mas não houve eficácia no processo de contenção a estes incidentes.

Ainda resta mencionar a análise do provedor C no gráfico anterior. Percebe-se que este provedor apresentou um significativo crescimento. Devido ao seu rápido aumento quantitativo em hospedagem de cavalos de tróia, estima-se que este poderá se tornar o segundo maior provedor responsável pela hospedagem destes arquivos. Entretanto este provedor não foi contatado durante a pesquisa devido a dificuldades na obtenção de respostas sobre as questões

[175] A robustez mencionada trata da verificação de dados dos responsáveis pela hospedagem e avaliação de características do arquivo.

realizadas aos outros provedores A, B, D e E, já que o provedor C não tem representação no território nacional.

Em complemento às características dos incidentes de *SCAM*, considera-se importante a apresentação de uma análise baseada no tipo de extensão do arquivo, adotado pelos provedores B, D e E, como processo de contenção de incidentes. Entendendo que esta característica é uma importante contribuição para este trabalho, o próximo subitem deste trabalho apresenta os dados e sua respectiva análise.

3.4.4 **Distribuição dos tipos de arquivos em *SCAM* no Brasil**

O processo de contenção do *SCAM* tanto em provedores de hospedagem de arquivos quanto em hospedeiros de mensagens eletrônicas podem se apoiar em filtros baseados na identificação do tipo de arquivo malicioso. É importante mencionar que as extensões de arquivos utilizados na aplicação de fraudes sobre o ambiente *Internet Banking* e existentes nos *links* nas mensagens eletrônicas do tipo *SCAM* são visíveis através da análise do código HTML existente no corpo da mensagem recebidos pelas vítimas. Em geral o fraudador suprime a exposição do tipo do arquivo no momento da visualização da mensagem (*SCAM*) pela vítima em busca de um maior convencimento ao *download* e execução do cavalo de tróia.

Os tipos arquivos mais utilizados no processo de disseminação do *SCAM* estão baseados nas seguintes categorias e extensões[176]:

[176] Esta informação está baseada nos dados fornecidos por instituições financeiras através dos incidentes registrados entre Abril de 2004 e Março de 2005.

Arquivos executáveis[177]:

- .exe[178];
- .scr[179];
- .zip[180] e;
- .rar[181].

Páginas utilizadas na hospedagem de arquivos:

- .htm[182];
- .asp[183];
- .jsp[184];
- .php[185] e;
- .dll[186].

Arquivos complementares utilizados na instalação do cavalo de tróia:

- .jpg[187].

---

[177] Os arquivos classificados como executáveis são interpretados pelo sistema operacional e aplicativos com interpretação de arquivos compactados existentes no computador, não necessitando de outro interpretador para execução.

[178] O arquivo .EXE é o mais utilizado no processo de infecção por cavalo de tróia apresentando como característica principal a execução através da interpretação do código pelo sistema operacional.

[179] A extensão .SCR é conhecida como um arquivo de proteção de tela do sistema operacional Windows, entretanto é necessário lembrar que SCR é também o início da palavra script, que indica uma seqüência de códigos utilizados por diversos programas maliciosos, incluindo cavalos de tróia.

[180] Arquivo compactado pela aplicação Winzip (http://www.winzip.com).

[181] Arquivo compactado pela aplicação Winrar (http://www.rarlab.com/).

[182] A extensão HTM representa uma das extensões mais comuns utilizadas na hospedagem de páginas que se utilizam da linguagem de Hipertexto (*Hyper Text Mackup Language*). O arquivo malicioso é um elemento referenciado no código da página *Web* que requer intervenção do usuário para execução do *download* e execução do arquivo.

[183] *Active Server Pages*, é um formato de página *Web* que permite a geração de conteúdo de forma dinâmica. Para o cenário atual, este tipo de página é utilizado para referenciar arquivos executáveis como a extensão HTM.

[184] *JavaScript Program* é um programa interpretado pelo *browser*, permitindo a execução de programas. Nos incidentes envolvendo cavalos de tróia o programa apenas disponibiliza o arquivo executável para download.

[185] A extensão PHP contém características de dinamismo de páginas similares à extensão ASP, entretanto há características na linguagem que permite realizar referências a banco de dados.

[186] A extensão DLL é utilizado como biblioteca do sistema operacional, permitindo comunicação entre aplicações, sistema operacional e dispositivos do sistema. Para o cenário atual, a DLL foi utilizada apenas como referência para o *download* do cavalo de tróia.

Os arquivos executáveis, mencionados na primeira categoria, são interpretados pelo sistema operacional existentes no computador da vítima, permitindo a imediata instalação do cavalo de tróia após o *download* e execução do arquivo disponível em um provedor hospedeiro previamente configurado pelo fraudador no corpo da mensagem (*SCAM*).

Entretanto este não é o único artifício utilizado pelo fraudador para a disseminação destas ameaças. Uma contramedida adotada pelos fraudadores em relação à proteção de filtragem de mensagens contendo em seu código *HTML* uma ou mais referências a extensões executáveis, é a utilização de mensagens eletrônicas que contém *links* a páginas *Web*. Dentro destas páginas há outras referências para arquivos executáveis em seus *links*. É importante mencionar que nenhumas destas extensões referentes à hospedagem de cavalos de tróia em páginas utilizam códigos *Active X* ou *Active Scripting* para a instalação destas ameaças nos computadores de eventuais vítimas.

E os tipos de arquivos complementares utilizados na instalação do cavalo de tróia são utilizados em versões mais recentes de ataques baseados em *SCAM*. As extensões de arquivo do tipo ".JPG", em geral, relativos a arquivos de imagens, apresentam em seu conteúdo um complemento do mecanismo de captura de dados da vítima e envio destas informações capturadas ao fraudador. Este método permite que o *download* do complemento do cavalo de tróia não desperte sua detecção através de antivírus existentes nos computadores de usuários do ambiente Internet. Em geral verificações de arquivos que buscam por cavalos de tróia são acionadas apenas na presença de arquivos executáveis, excluindo os demais arquivos existentes no sistema, nesta categoria também se excluem as extensões do tipo ".JPG" à análise.

---

[187] A extensão JPG representa uma imagem em formato comprimido, entretanto para o cenário em estudo, a extensão contém dados complementares a um arquivo executável previamente instalado. Neste processo o JPG contém configurações que definem as ações do cavalo de tróia instalado.

Na seleção do dados contendo os tipos de arquivos se mencionam os três tipos de extensões de arquivos mais freqüentes na análise de *SCAM*, disponíveis na tabela a seguir:

Período (Mês / Ano)	**Incidentes Ext. EXE**	**Incidentes Ext. SCR**	**Incidentes Ext. ZIP**
Abril / 2004	71	13	9
Maio / 2004	82	12	7
Junho / 2004	96	25	18
Julho / 2004	160	88	12
Agosto / 2004	285	92	47
Setembro / 2004	184	106	63
Outubro / 2004	159	92	73
Novembro / 2004	283	162	40
Dezembro / 2004	316	213	52
Janeiro / 2005	331	115	46
Fevereiro / 2005	466	200	66
Março / 2005	527	245	81

Tabela 8 - Extensões de arquivos utilizadas em *SCAMs* registrados no Brasil

É possível perceber na tabela 8 que os arquivos mais freqüentes estão relacionados a arquivos executáveis. Entretanto, é necessária a transcrição destes dados em um gráfico tornando possível a visualização da distribuição e concentração destes executáveis ao longo do tempo, permitindo uma melhor análise destas informações, conforme a figura a seguir:

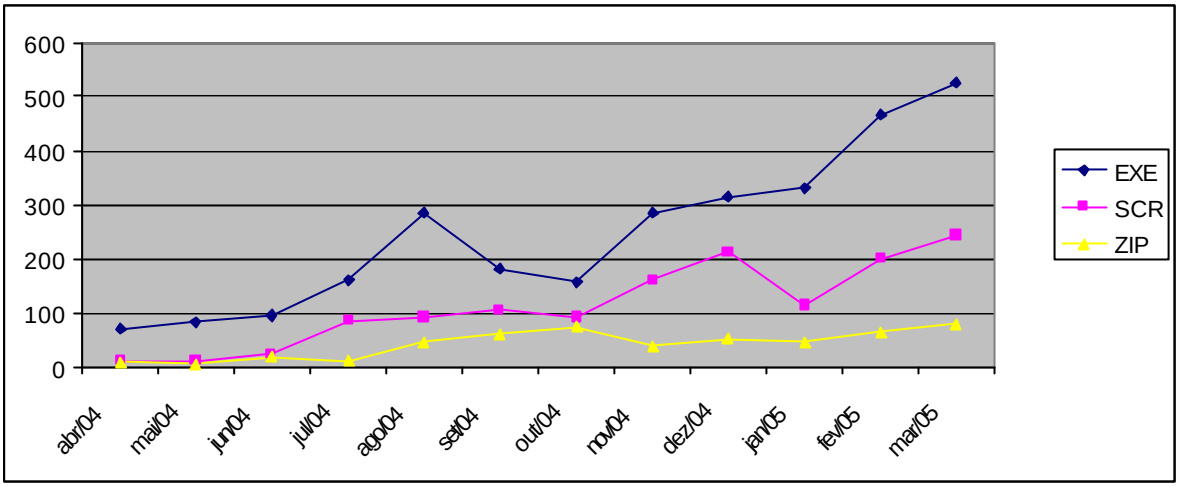

Figura 18 - Extensões de arquivos utilizadas em *SCAMs* registrados no Brasil

Percebe-se que a extensão mais utilizada para a criação de cavalos de tróia está relacionada a arquivos do tipo ".EXE". Não foi possível encontrar evidências que determinem a maior adoção deste tipo de extensão, entretanto é necessário lembrar que a maioria das aplicações utilizadas para a geração de cavalos de tróia geram arquivos do tipo ".EXE". É possível propor a hipótese[188] que diversos grupos responsáveis pela geração de arquivos maliciosos utilizam ferramentas e extensões distintas de disseminação. Se esta hipótese for verdadeira, isto poderá justificar o crescimento desproporcional do aumento de utilização destas extensões, pois este seria um indicativo que grupos de fraudadores responsáveis por estas ações também estão crescendo de maneira desproporcional, e eventuais quedas na utilização destas extensões podem significar o resultado de ações de contenção de órgãos públicos de repressão federais ou civis sobre fraudadores.

[188] Esta hipótese não pode ser provada, pois o estudo de caso não contemplou a avaliação de tecnologias utilizadas para a construção dos cavalos de tróia, assim como a investigação sobre os grupos responsáveis por estas ações.

4 CONTENÇÃO DA FRAUDE SOBRE O INTERNET BANKING

A contenção da fraude no ambiente *Internet Banking* é um processo que está em constante evolução, parte deste processo foi descrito no capítulo anterior, através da descrição de contramedidas tomadas pelas instituições financeiras desde o surgimento dos primeiros golpes ainda em meados de 2002.

Tendo em vista a constante evolução dos golpes mencionados até o momento da conclusão deste trabalho, acredita-se que os métodos utilizados hoje[189] não são suficientes para a mitigação de novas modalidades de fraude que serão aplicadas contra clientes do sistema financeiro na Internet.

Buscando a soluções sobre este problema, este capítulo identifica e descreve os elementos de apoio para a mitigação da fraude.

4.1 PROCESSO DE MITIGAÇÃO DA FRAUDE

Há diversas linhas utilizadas hoje no caminho da mitigação das fraudes no canal *Internet Banking*. Para melhor compreensão deste tema, buscaremos seguir o modelo proposto abaixo (LAU):

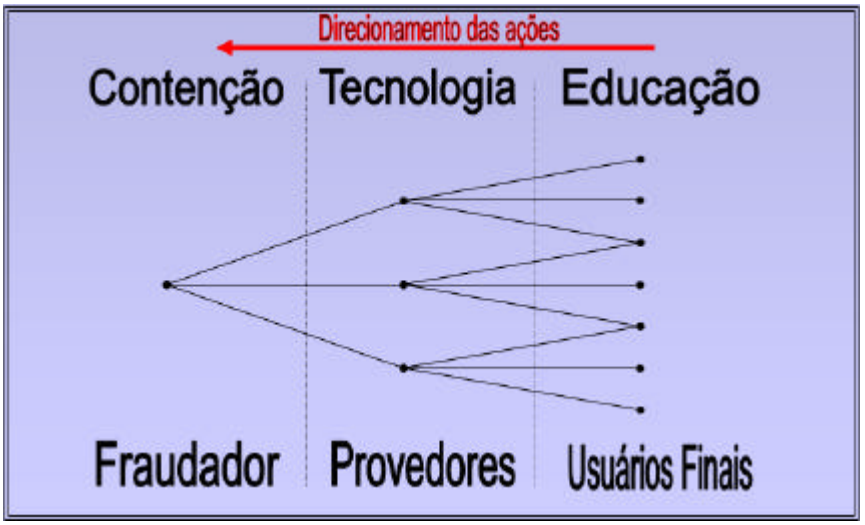

Figura 19 - Modelo de mitigação das fraudes no ambiente *Internet Banking*

[189] Percepção e opinião pessoal do pesquisador no momento da publicação deste trabalho.

O modelo descrito atua em três segmentos distintos:

- Usuários Finais;
- Provedores;
- Fraudador.

4.1.1 **Ações junto aos usuários finais**

Em um primeiro momento, recomenda-se uma ação sobre os usuários finais, que em maior número, necessitam de esclarecimentos sobre este tipo de ameaça[190]. Infelizmente as informações existentes sobre a efetivação da fraude e recomendações hoje oferecidas a clientes de instituições financeiras são escassas[191]. As informações disponíveis sobre este tema se encontram disponíveis em sites especializados de segurança da informação, entre outros meios de comunicação que nem sempre está acessível aos clientes do serviço *Internet Banking*.

Dentre as diversas iniciativas, há uma iniciativa em publicada em 2005[192], liderada pela Câmara Brasileira de Comércio Eletrônico (câmara-e.net), visando conscientização de segurança junto aos usuários de Internet, principalmente aqueles expostos aos riscos existentes no acesso de serviços em sites de comercio eletrônico e instituições financeiras[193].

---

[190] Nem todos os pesquisadores concordam com esta linha de ação, pois consideram que alguns grupos de usuários, mesmo conscientizados sempre estarão propensos aos golpes baseados em ataques de *phishing* ou *scam*. (Potter, p.15-16)

[191] As instituições financeiras que disponibilizam informações sobre o assunto oferecem recomendações aos seus clientes, mas poucos contêm exemplos das ameaças dos golpes praticados pelos fraudadores, o que dificulta a identificação de uma tentativa de fraude em comparação ao acesso legítimo aos serviços bancários.

[192] É possível estimar a publicação do Movimento Internet Segura através da consulta das informações de registro do domínio internetsegura.org. Segundo informações do site Whois.ws (http://www.whois.ws/whois-org/ip-address/internetsegura.org/), o domínio foi registrado em 19/01/2005 às 14h12min.

[193] O Movimento Internet Segura mobilizou alguns órgãos de imprensa, no momento da publicação em Abril de 2005 uma página (http://www.internetsegura.org) contendo algumas recomendações de segurança. INTERNET SEGURA – Movimento Internet Segura. Disponível em: <http://www.internetsegura.org/> Acesso em: 02 nov. 2005.

Entretanto, foi possível perceber que o conteúdo disponibilizado pela câmara-e.net no momento da consulta do pesquisador ao glossário[194] leva seus usuários a dúvidas ainda maiores sobre o tema. Toma-se como exemplo para este trabalho, a transcrição de um termo "Cavalo de Tróia" disponível no momento da pesquisa realizado em 02/11/2005 através da página http://www.internetsegura.org/glossario/glossario.asp:

> *"Cavalo de Tróia*
>
> *Um programa incorporado em um programa que, de outra forma, seria inofensivo, usado para atacar um local."*

Ao avaliar o conteúdo da descrição, percebem-se as seguintes inconsistências:

- *"...programa incorporado em um programa..."* – Não se define o que é um programa para o usuário, o que provoca ao leitor as mais diversas interpretações. Além disto, entende-se que qualquer incorporação de programa por outro programa se caracteriza a criação de um cavalo de tróia, afirmação que não é verdadeira;
- "*...de outra forma, seria inofensivo...*" – Não se explica nesta frase qual é a possibilidade do cavalo de tróia se tornar inofensivo, considerando-se esta uma afirmação verdadeira;
- "*...usado para atacar um local.*" – O ataque não visa um local, visa obter um recurso existente em um local. A vítima de um cavalo de tróia está relacionada à busca de privilégios dentro de um sistema, visando o acesso de recursos sem o prévio consentimento da vítima. O leitor deste termo no glossário pode entender

[194] Realizado em 02/11/2005.

> que a descrição que o cavalo de tróia busca direcionar o ataque a alguma instalação, um local físico, que não é o conceito de segurança aplicado em ameaças sobre o ambiente de comércio eletrônico ou instituição financeira.

Em diversos momentos, membros deste movimento foram alertados sobre os riscos da divulgação prolixa. No momento da entrega deste trabalho, o glossário e outros conteúdos foram readequados parcialmente[195].

Recomenda-se a partir deste trabalho cuidados na elaboração de recomendações de segurança aos usuários de páginas e serviços de instituições financeiras existentes na Internet, permitindo um maior esclarecimento aos usuários. No exterior, diversas instituições financeiras disponibilizam informações de conscientização aos usuários[196], e no Brasil, das diversas instituições Brasileiras que dispõem de serviços na Internet, o Banco Santander[197] é o único que disponibiliza um curso de segurança à distância (*E-learning*[198]) gratuito aos seus clientes[199].

A Febraban ainda informa aos clientes que os bancos mantêm fortes sistemas de segurança em seus computadores e nos programas de acesso via Internet, mencionando que a instituição não pode garantir a segurança no computador que o cliente utiliza no acesso a este serviço. Desta forma, algumas recomendações são feitas aos clientes recomendando prevenção à ocorrência de fraudes (FEBRABAN) nos itens a seguir:

---

[195] No momento da revisão deste trabalho em 04/08/2006 foi possível encontrar um termo no glossário denominado “ataque”, com a seguinte descrição ”Uma “agressão” eletrônica (normalmente não provocada) cujo objetivo é, de alguma forma, prejudicar os computadores, as redes e os mecanismos de segurança que constituem os alvos.”, que também se apresenta inadequada ao usuário.

[196] Recomenda-se como exemplo, o acesso à página do Citibank http://www.citibank.com, onde é possível visualizar na página principal o item “*Consumer Alert. Beware of fraudulent e-mails*”. CITIBANK.COM – **Wellcome to Citibank**. Disponível em: <http://www.citibank.com> Acesso em: 02 nov. 2005.

[197] O acesso a este recurso está disponível na página principal do Banco Santander, através o item “segurança”. BANCO SANTANDER – **Banco Santander**. Disponível em: <http://www.santander.com.br> Acesso em: 02 nov. 2005.

[198] *E-learning* é a grafia existente na página do Santander Banespa e é o nome dado na língua inglesa para curso à distância através de meios eletrônicos, neste caso, através da Internet.

[199] Este fato se limita ao momento da publicação deste trabalho.

- Manter programas antivírus atualizados instalados nos computadores utilizados para o acesso aos serviços bancários;
- No caso de Internet de alta velocidade, com conexão direta à rede, utilizar um programa de segurança;
- Trocar a sua senha de acesso ao *Internet Banking* periodicamente;
- Não execute aplicações, nem abra arquivos de origem desconhecida. Eles podem conter vírus e outros procedimentos prejudiciais, que ficam ocultos para o usuário e permitem a ação de fraudadores sobre sua conta, a partir de informações capturadas após a digitação no teclado;
- Use somente provedores confiáveis. A escolha de um provedor deve levar em conta também seus mecanismos, políticas de segurança e a confiabilidade da empresa;
- Tenha cuidado com e-mails não solicitados ou de procedência desconhecida, especialmente se tiverem arquivos anexados. Correspondências eletrônicas também podem trazer programas desconhecidos que oferecem diversos tipos de riscos à segurança do usuário. É mais seguro excluir (deletar) os e-mails não solicitados e sobre os quais não se tenha absoluta certeza de sua procedência. Tomar cuidado especialmente com arquivos e endereços obtidos em salas de bate-papo (*chats*). Alguns desses *chats* são freqüentados por *hackers*;
- Evitar sites arriscados. Só faça transferência de arquivos (*download*) para o seu computador de sites que você conheça e saiba que são confiáveis;
- Utilizar sempre as versões mais atualizadas dos programas de navegação (*browser*), pois geralmente incorporam melhores mecanismos de segurança;
- Quando for efetuar pagamentos ou realizar outras operações financeiras, você pode certificar-se de que está no site desejado, seja do banco ou outro qualquer, clicando

sobre o cadeado e / ou a chave de segurança que aparece quando se entra na área de segurança do site. O certificado de habilitação do site, concedido por uma certificadora autorizada que aparecerá na tela, confirmando sua autenticidade, juntamente com informações sobre o nível de criptografia utilizada naquela área pelo responsável pelo site (SSL). Não inserir novos certificadores no programa de navegação (*browser*), a menos que conheça todas as implicações decorrentes desse procedimento;

- Acompanhar os lançamentos em sua conta corrente. Caso constate qualquer crédito ou débito irregular, entre imediatamente em contato com o banco e;
- Se estiver em dúvida sobre a segurança de algum procedimento que executou, entre em contato com o banco. Prevenção é a melhor forma de segurança;

E como recomendação final, solicita-se que o cliente consulte o gerente da agência bancária a qual ele mantém relacionamento, entretanto este contato nem sempre é o mais indicado, pois estes funcionários nem sempre estão cientes das recomendações que devem ser feitas, ou mesmo apresentam conhecimentos técnicos que permitem sanar dúvidas do ambiente Internet.

É importante comentar que nem todas estas recomendações mencionadas neste trabalho, disponíveis pela Febraban são compreendidas pelo cliente, pois algumas recomendações não detalham os procedimentos de verificação dos itens mencionados anteriormente. Recomenda-se além destes itens a leitura da Cartilha de Segurança para Internet (Parte IV – Fraudes na Internet)[200].

É também necessário lembrar que um esforço visando conscientização dos usuários na Internet deve buscar atingir o público mais suscetível a estes golpes. Com o propósito de se

[200] CERT.br – **Cartilha de Segurança para Internet**. Versão 3.0 – Setembro de 2005. Disponível em: <http://cartilha.cert.br> Acesso em: 08 set. 2005.

definir este perfil, considerou-se importante mencionar neste trabalho uma pesquisa[201] disponibilizada recentemente contendo indicadores de problemas de segurança encontrados no uso da Internet. Percebeu-se na população pesquisada[202], 0,23% da população foi vítima de fraude com cartão de crédito ou instituição financeira na Internet, o que indica obtenção ilícita dos dados do cartão de crédito ou credenciais de acesso ao serviço de *Internet Banking*. Através dos resultados, percebeu-se que a população mais afetada apresenta as seguintes características:

- Moram na região metropolitana de São Paulo, Curitiba e Rio de Janeiro respectivamente;
- Em sua maioria apresentam renda familiar superior à R$ 1801,00;
- Em geral, as vítimas completaram o curso universitário;
- O sexo masculino concentra um número maior de vítimas;
- As vítimas se concentram em classes sociais B e A respectivamente e;
- A faixa etária que concentra um número maior de vítimas está compreendida entre 16 e 34 anos.

Estes resultados não indicam que o restante da população brasileira não necessite de orientações, entretanto é necessário lembrar que os custos financeiros necessários em campanhas de marketing são elevados em virtude do volume de clientes do ambiente *Internet Banking*. Portanto considera-se importante selecionar a parcela da população que pode gerar um retorno mais efetivo dos investimentos de uma campanha de conscientização.

4.1.2 **Ações junto aos provedores**

[201] NIC.br - **Pesquisa Tecnologias da Informação e da Comunicação (TIC) Domicílios – IPSOS.** Agosto / Setembro de 2005. Disponível em: <http://www.nic.br/indicadores/usuarios/index.htm> Acesso em: 27 nov. 2005.

[202] Foram 8540 domicílios entrevistados, abrangendo 10 capitais e outras cidades nas cinco regiões no Brasil. Abrangeu-se nesta pesquisa a segregação dos resultados em renda familiar, grau de instrução, gênero, classe social e faixa etária.

Os provedores devem ser considerados neste contexto, toda empresa fornecedora de serviços aos usuários, seja este um fornecedor direto, que presta serviço ao usuário, como provedores de acesso e provedores de serviços financeiros através da Internet; ou fornecedor indireto, que são aqueles responsáveis pela infra-estrutura existente nos meios acessados pelos clientes, tais como fornecedores de equipamentos e empresas que realizam monitoramento de tráfego na Internet.

É possível categorizar estas empresas nos itens descritos a seguir:

- **Fornecedores diretos:**
  - **Fabricante de Sistema Operacional**: Empresa responsável pelo fornecimento e atualização do sistema operacional aos seus usuários;
  - **Fabricante de Antivírus**: Empresa responsável pelo fornecimento e atualização de programa antivírus aos seus usuários. Entende-se que os antivírus também são responsáveis pela detecção e eliminação de cavalos de tróia;
  - **Fabricante de Anti-spyware**: Empresa responsável pelo fornecimento e atualização de programas especializados na contenção de ameaças que capturam dados confidenciais. Entende-se que os antivírus devem cumprir esta função, mas em virtude da deficiência dos antivírus, recorre-se à instalação deste tipo de aplicação;
  - **Fabricante de Firewall**: Empresa responsável pelo fornecimento e atualização de programas especializados no bloqueio de comunicação entre o computador e Internet, no contexto deste trabalho, a comunicação que se busca bloquear está relacionada ao envio de dados capturados por cavalos de tróia aos fraudadores. Alguns antivírus cumprem esta função através de características adicionais no produto;

- **Provedor de Acesso**: Empresa responsável pelo oferecimento do acesso Internet aos seus clientes, garantindo segurança e disponibilidade de acesso;
- **Provedor Financeiro**: Instituição Financeira responsável pela disponibilidade de serviços transacionais no ambiente Internet;

- **Fornecedores indiretos:**
  - **Fabricante de Sistema Operacional:** Empresa responsável pelo fornecimento e atualização do sistema operacional aos fornecedores diretos que oferecem serviço junto aos seus clientes;
  - **Fabricante de Antivírus**: Empresa responsável pelo fornecimento e atualização de programa antivírus aos fornecedores diretos e seus respectivos sistemas, garantindo a entrega dos serviços junto aos seus clientes;
  - **Fabricante de Firewall**: Empresa responsável pelo fornecimento e atualização de programas e / ou equipamentos especializados no bloqueio de comunicação entre os equipamentos dos fornecedores diretos e a Internet. Neste contexto, o firewall é um produto especializado para o cumprimento desta função;
  - **Provedor de Acesso**: Empresa responsável pelo oferecimento do acesso Internet aos fornecedores diretos que oferecem serviço aos seus clientes, garantindo segurança e disponibilidade de acesso;
  - **Provedor de Aplicações**: Empresa responsável pelo fornecimento e manutenção de programas utilizados pelos provedores diretos no oferecimento dos serviços aos seus clientes;
  - **Provedor de equipamentos de Rede**: Empresa responsável pelo fornecimento e manutenção de equipamentos que permite conectividade e comunicação entre os provedores diretos e junto aos seus clientes;

Entende-se que todos os provedores mencionados anteriormente são responsáveis pelo oferecimento de serviços seguros junto aos seus clientes. É importante salientar que na ocorrência de fraude, em geral, apenas o provedor financeiro é acionado para o reparo do dano causado ao cliente. Recomenda-se nestes casos avaliar a extensão do dano e envolver todos os fornecedores diretos através da argumentação de co-responsabilidade. Como exemplo, pode-se mencionar a co-responsabilidade do provedor de acesso ao serviço *Internet Banking* comprometido em ataques de *PHARMING*, pois o serviço de resolução de nomes (*DNS*), neste caso, se foi comprometido em virtude de uma imprudência da equipe técnica do provedor ou pela ausência de correções aos equipamentos utilizados no provedor, o que acarreta nesta hipótese a co-responsabilidade do fornecedor indireto.

Atuando na linha de co-responsabilidade a Microsoft incorporou recentemente em um de seus produtos um filtro de bloqueio a ataques de *phishing* e *scam* (Hunter, p.15-16), resultado da parceria com diversos provedores diretos e indiretos, incluindo provedores de serviços financeiros do Brasil e exterior. O filtro foi concebido a partir de necessidades apontadas pelos diversos provedores, utilizando dados de incidentes de *phishing* e *scam* repassados à Microsoft.

4.1.3 **Ações junto aos fraudadores**

Diversas ações bem sucedidas estão ocorrendo na esfera da repressão aos crimes de informática, incluindo a localização e captura de responsáveis por fraudes aplicadas sobre o ambiente Internet Banking (SILVIA GIURLANI). A polícia federal, até o ano de 2005 efetivou duas operações de busca e apreensão sobre responsáveis e usuários de equipamentos informáticos utilizados para efetivação de fraude. As operações que apresentam o nome de "Cavalo de Tróia" e resultou em sua segunda versão[203], a prisão de 63 fraudadores, sendo que

[203] A operação Cavalo de Tróia 2 foi realizada em Outubro de 2004.

18 haviam sido condenados na versão anterior da operação. Partindo desta informação, reforça-se a hipótese que os fraudadores mesmo cientes das punições jurídicas, buscam cometer crimes, acreditando na possibilidade da impunidade destes atos.

O criminoso em geral, apresenta uma faixa etária de 20 anos, originário de famílias de classe média, que através dos golpes no ambiente Internet, não utilizam força física para lesar suas vítimas[204]. Os responsáveis por este tipo de crime são enquadrados em estelionato, formação de quadrilha, furto qualificado, quebra de sigilo bancário e lavagem de dinheiro que somados levam a uma pena máxima de dezoito anos de prisão, mas que na prática se limitam de quatro a seis anos de reclusão.

É importante lembrar que diversos acusados nas operações policiais sejam estas atividades da polícia federal ou polícia civil não se encontram em detenção, pois respondem ao crime em liberdade, aguardando julgamento. Neste caso, alguns destes acusados podem se utilizar da liberdade para a efetivação de outros crimes.

Defende-se para este caso uma ampla divulgação na imprensa de sanções aos criminosos pela efetivação ou participação em fraude Internet. Percebe-se que esta ação é necessária, pois visa desestimular o envolvimento indivíduos suscetíveis ao ingresso neste tipo de atividade ilegal. Em adição a esta recomendação, é necessário mencionar a necessidade de aprovação de leis[205] que tipifiquem estas ações, pois o magistrado brasileiro sem sempre associa o crime de fraude Internet nos códigos civis ou criminais vigentes.

---

[204] Esta afirmação está baseada na entrevista de Paulo Quintiliano, chefe de Perícia de Informática da Polícia Federal, disponível na publicação de SILVIA GIURLANI – Crime virtual, castigo real. **Security Review**, n. 1, p.32, mar./abr. 2005

[205] Uma das leis específicas que podem ser mencionadas é o projeto de lei PL 84/1999 de autoria do deputado Luiz Piauhylino do PDT/PE.

5 CONSIDERAÇÕES FINAIS

5.1 TRABALHOS FUTUROS

Apesar da abrangência deste trabalho diversos assuntos importantes não foram discutidos, e que podem ser desenvolvidos por pesquisadores interessados sobre o tema de fraude no ambiente *Internet Banking*. As abordagens que podem ser adotadas por pesquisadores podem se basear nos seguintes contextos:

- **Jurídico.** Uma análise baseada sob o contexto jurídico, permite reconhecer a fraude como ato ilícito na esfera penal, onde sansões podem ser adotados pelo direito civil aos responsáveis pela aplicação da fraude em usuários do ambiente Internet. A contribuição de uma pesquisa baseada nesta esfera permite materializar conhecimentos de informática aos profissionais que atuam na área jurídica;
- **Computacional.** A análise detalhada dos ambientes computacionais utilizados pelo fraudador tanto para a disponibilidade de cavalos de tróia quanto páginas falsificadas é um assunto vasto, pois aborda as vulnerabilidades existentes em arquiteturas de rede e sistemas operacionais que permitem a hospedagem de arquivos ilícitos, direcionados a captura de dados pessoais de vítimas do ambiente *Internet Banking*. Outra ótica que pode ser adotada na visão computacional é compreender a evolução de cavalos de tróia através do período de 2002 ao momento atual; permitindo analisar os mecanismos utilizados na instalação, execução, captura de dados e envio destas informações ao fraudador. Considerações devem ser adotadas na produção de um trabalho acadêmico envolvendo este contexto, pois as informações coletadas pelo pesquisador tanto podem esclarecer o assunto aos interessados na contenção de fraudes, quanto à disseminação do conhecimento para efetivação da fraude a leitores mal intencionados, fomentando novos grupos para ações fraudulentas;

- **Serviço *Internet Banking*.** A compreensão de detalhes no serviço oferecido por instituições financeiras permite readequação do produto de *Internet Banking* ofertado ao cliente. Esta adequação não está baseada apenas na adoção de tecnologias que dificultam a efetivação da fraude neste ambiente, pois regras de negócio são fundamentais sobre este produto limitando o encorajamento de fraudadores em efetivar fraudes sobre instituições financeiras. O resultado de um trabalho sob esta ótica permite a disseminação do conhecimento aos gestores de produtos bancários e provedores de soluções de informática, permitindo um maior fortalecimento do produto *Internet Banking* no mercado brasileiro.

Dentre as linhas de trabalhos futuros propostos, é importante considerar que a visão computacional é uma das mais promissoras, pois permite o detalhamento sobre o método utilizado pelo fraudador e sua relação com processo evolutivo. Os resultados sobre esta linha de pesquisa pode ainda considerar possíveis caminhos para o aperfeiçoamento dos ataques, permitindo a adoção de contra medidas pelas instituições financeiras, provedores e órgãos públicos de repressão, possibilitando também o fomento de subsídios aos fraudadores através do conhecimento disponível neste tipo de trabalho.

5.2 CONCLUSÕES

É possível afirmar a ocorrência de constante e rápida evolução dos métodos utilizados para efetivação da fraude sobre o ambiente *Internet Banking* desde o ano de 2002. Constatou-se que a evolução dos métodos ocorreu em virtude de melhorias no produto *Internet Banking*, promovido pelas instituições financeiras. Além disto, no cenário externo, foi possível encontrar indícios de exportação de tecnologia para disseminação destes golpes em outros países utilizando as mesmas técnicas aplicadas sempre em primeiro lugar no Brasil para efetivação posterior da fraude sobre clientes do serviço *Internet Banking* no restante mundo.

A partir dos dados de *SCAM* e *PHISHING* apresentados neste trabalho, é possível afirmar que a maior ameaça aos clientes do serviço de *Internet Banking* está relacionada aos ataques de *SCAM*, que demonstra aumento consistente no número de incidentes registrados. Estes ataques baseados na infecção do computador da vítima com cavalos de tróia apresentaram neste trabalho concentração de hospedagem em provedores que não apresentavam mecanismos robustos de detecção destas ameaças, onde são três as extensões de arquivos (.EXE, .ZIP e .SCR) mais utilizadas pelos fraudadores.

Em contrapartida é possível afirmar que mitigação da fraude sobre o ambiente *Internet Banking* está baseada em três ações:

- **Sobre o usuário final:** Se recomenda a preparação de um plano de conscientização adequado à compreensão do cliente e dirigido ao público mais suscetível à fraude;
- **Sobre os provedores:** É necessário que todos os envolvidos na disponibilidade do serviço bancário na Internet atuem como co-responsáveis se comprometendo pela melhoria da segurança de todo o ambiente *Internet Banking* e;
- **Sobre os fraudadores:** Os órgãos públicos de repressão ao crime civis e federais necessitam atuar constantemente na investigação e punição, com apoio da imprensa na divulgação das operações realizadas pela polícia.

É importante mencionar que não há possibilidade de se mitigar a fraude apenas com a adoção de medidas pontuais, pois tanto órgãos públicos de repressão, quanto provedores de tecnologias e serviços, e usuários do ambiente Internet devem se mobilizar para buscar soluções e participar do processo de proteção contra a efetivação da fraude no ambiente *Internet*. *Banking.*

6 REFERÊNCIAS BIBLIOGRÁFICAS

APWG – **Anti-Phishing Working Group.** Disponível em: <http://www.antiphishing.org> Acesso em: 16 mai. 2005.

APWG – **Phishing Activity Trends Report – March, 2005. Anti-Phishing Working Group.** Disponível em: < http://antiphishing.org/APWG_Phishing_Activity_Report_March_2005.pdf > Acesso em: 16 mai. 2005.

BANCO SANTANDER – **Banco Santander.** Disponível em: <http://www.santander.com.br> Acesso em: 02 nov. 2005.

BASEL - **Risk Management Principles for Electronic Banking**. Basel Commitee on Banking Supervision. Disponível em: <http://www.bis.org/publ/bcbs98.pdf> Acesso em: 30 nov. 2004.

BASEL - **Risk Management Principles for Electronic Banking and Electronic Money Activities**. Basel Commitee on Banking Supervision. Disponível em: <http://www.bis.org/publ/bcbs35.pdf> Acesso em: 02 mar. 2005.

BITS - **Fraud Prevention Strategies for Internet Banking**. Fraud Reduction Steering Committee. Disponível em: <http://www.bitsinfo.org/mointernetwp.pdf> Acesso em 02 dez. 2004.

Bruce Schneier - **The Failure of Two-Factor Authentication**. Disponível em: <http://www.schneier.com/crypto-gram-0503.html#2> Acesso em 06 out. 2005

CALLAO, Gonzalo Rolando Archondo - **O Protocolo SSL**. Disponível em: < http://equipe.nce.ufrj.br/gonzalo/SSL/ssl.htm > Acesso em 18 mar. 2005.

CERT.br - **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil.** Disponível em: <http://www.cert.br/> Acesso em: 07 set. 2005.

CERT.br - **Incidentes Reportados ao CERT.br -- Outubro a Dezembro de 2004**. Disponível em: <http://www.cert.br/stats/incidentes/2004-oct-dec/tipos-ataque.html> Acesso em: 07 set. 2005.

CERT.br - **Incidentes Reportados ao CERT.br -- Janeiro a Março de 2005**. Disponível em: <http://www.cert.br/stats/incidentes/2005-jan-mar/tipos-ataque.html> Acesso em: 07 set. 2005.

CERT.br - **Incidentes Reportados ao CERT.br -- Abril a Junho de 2005.** Disponível em: < http://www.cert.br/stats/incidentes/2005-apr-jun/tipos-ataque.html> Acesso em: 07 set. 2005.

CERT.br - **Incidentes Reportados ao CERT.br -- Julho a Setembro de 2005.** Disponível em: < http://www.cert.br/stats/incidentes/2005-jul-sep/tipos-ataque.html> Acesso em: 02 nov. 2005.

CERT.br – **Cartilha de Segurança para Internet**. Versão 3.0 – Setembro de 2005. Disponível em: <http://cartilha.cert.br> Acesso em: 08 set. 2005.

CERT.br – **Entrevistas e Reportagens sobre o CERT.br**. Disponível em: <http://www.cert.br/docs/reportagens/> Acesso em: 02 nov. 2005.

CIARDHUÁIN, Séamus Ó - **An Extended Model of Cybercrime Investigations.** International Journal of Digital Evidence. Summer 2004, Volume 3, Issue 1. Disponível em: <http://www.ijde.org/docs/ociardhuain.pdf> Acesso em: 18 mar. 2005.

CITIBANK.COM – **Welcome to Citibank**. Disponível em: <http://www.citibank.com> Acesso em: 02 nov. 2005.

E-COMMERCEORG - **Dados estatísticos sobre a Internet e Comércio Eletrônico**. Disponível em: <http://www.e-commerce.org.br/STATS.htm> Acesso em 02 dez. 2004.

FDIC - **Putting an End to Account-Hijacking Identity Theft**. Federal Deposit Insurance Corporation. Disponível em: <http://www.fdic.gov/consumers/consumer/idtheftstudy/> Acesso em 03 fev. 2005.

FEBRABAN - **Número de contas, cartões de débito e clientes com Internet Banking.** Federação Brasileira de Bancos. Disponível em: <http://www.febraban.org.br/Arquivo/Servicos/Dadosdosetor/tecnologia_2003_dadossetor.asp> Acesso em 02 dez. 2004.

FEBRABAN - **Segurança no uso da Internet.** Federação Brasileira de Bancos. Disponível em: <http://www.febraban.org.br/Arquivo/Servicos/Dicasclientes/dicas7.asp> Acesso em 18 mar. 2005.

FEBRABAN – **Você e seu banco – Um guia que vai facilitar seu relacionamento com os bancos.** Edição 2 – 2004. Federação Brasileira de Bancos. Disponível em: < http://www.febraban.org.br/Arquivo/Cartilha/Manual Febraban 2004 Y.pdf > Acesso em: 22 mar. 2005.

FORTUNA, Eduardo - **Mercado Financeiro: produtos e serviços.** 15ª. Edição – Rio de Janeiro: Qualitymark Ed. 2002

FRANKLING SAVINGS BANK - **Internet Banking System Security**. Disponível em: <http://www.franklinsavingsbank.com/site/security.html> Acesso em 18 mar. 2005.

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.

GLOBO.COM - **Capital dos Hackers**. Fantástico, 24 out. 2004. Disponível em:<http://fantastico.globo.com/Fantastico/0,19125,TFA0-2142-5650-192470,00.html> Acesso em 10 mar.2005

HALLAM-BAKER, Phillip - **Prevention strategies for the next wave of cyber crime.** Network Security - Volume 2005 - Edição 10 - Outubro 2005.

HUNTER, Philip - **Microsoft declares war on phishers**. Computer Fraud & Security. Volume 2006 - Edição 5 - Maio/2006.

HUSCH, Jonathan J. - **The "Social Engineering" of Internet Fraud** – Internet Society. Disponível em: <http://www.isoc.org/isoc/conferences/inet/99/proceedings/3g/3g_2.htm> Acesso em: 15 mar. 2005.

IBGE - **Pesquisa Nacional Por Amostra de Domicílios – PNAD 2002**. Disponível em: < http://www.ibge.gov.br/home/presidencia/noticias/10102003pnad2002html.shtm> Acesso em 07 set. 2005.

IEEE - **Information Security: An Integrated Collection of Essays**. IEEE Computer Society Press. Disponível em: <http://www.acsac.org/secshelf/book001/book001.html> Acesso em 02 fev. 2005

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

INTERNET SEGURA – **Movimento Internet Segura**. Disponível em: <http://www.internetsegura.org/> Acesso em: 02 nov. 2005.

ISS - **Guia de referência sobre ataques via Internet.** Febraban / Internet Security Systems. Disponível em: < http://www2.dem.inpe.br/ijar/GuiaFebraban.pdf> Acesso em 17 mar. 2005.

ITSECURITY - **How to Survive in Internet Banking – The Threats and Solutions to Online Security**. Disponível em: < http://www.itsecurity.com/papers/argus.htm > Acesso em 18 mar. 2005.

JANE, Edward J. - **Difficulties of transferring risk-based capital requirements to developing countries**. Pacific-Basin Finance Journal. Volume 3 - Edição 2-3, Julho 1995.

L8455. **Alteração dos dispositivos da Lei 5869, de 11 de janeiro de 1973 – Código do Processo Civil, referentes à prova pericial**. Presidência da República. Disponível em: < https://www.planalto.gov.br/ccivil_03/Leis/1989_1994/L8455.htm > Acesso em: 15 nov. 2005

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

MAIA, LUIZ PAULO; PAGLIUSI, PAULO SERGIO - **Criptografia e Certificação Digital.** Disponível em: < http://www.training.com.br/lpmaia/pub_seg_cripto.htm> Acesso em 18 mar. 2005.

MANN, Paul - **Cybersecurity – the CTOSE project**. Computer Law & Security Report. Volume 20 - Edição 2, Março / Abril 2004.

NETO, Beraldo Crisante e CRESTO, Vicente - **Risco Operacional: o porquê de se registrarem perdas.** Resenha BM&F n. 156. Disponível em: <http://www3.bmf.com.br/pages/Educacional1/publicacoes/Resenha1/PDFs/Res156/artigo02.pdf> Acesso em 03 dez. 2004.

NIC.br - **Pesquisa Tecnologias da Informação e da Comunicação (TIC) Domicílios – IPSOS**. Agosto / Setembro de 2005. Disponível em: <http://www.nic.br/indicadores/usuarios/index.htm> Acesso em: 27 nov. 2005.

POTTER, Bruce - **User education – how valid is it?** - Network Security. Volume 2006 - Edição 4 - Abril 2006.

QUALISOFT - **Case Banco Santos**. Disponível em: < http://www.qualisoft.com.br/casos/bancosantosSG2.asp > Acesso em 18 mar. 2005.

RNP - **Alerta do CAIS ALR-02042003 – Fraudes em Internet Banking.** RNP/CAIS. Disponível em: < http://www.itsecurity.com/papers/argus.htm > Acesso em 18 mar. 2005.

ROBERT K. YIN, **Case Study Research: Design and Methods**, 3.edição. Thousand Oaks, CA: Sage Publications, 2002.

RSA Security - **The Cryptographic Smart Card: A Portable, Integrated Security Platform** Disponível em: < http://www.rsasecurity.com/products/securid/whitepapers/smart/CSC_WP_0301.pdf > Acesso em 06 out. 2005.

RUSCH, Jonathan J. - **The complete cyber-angler: a guide to phishing**. Computer Fraud & Security - Volume 2005 - Edição 1 - Janeiro 2005.

SILVIA GIURLANI – **Crime virtual, castigo real**. Security Review, n. 1, p.31, mar. / abr. 2005

STEIN, Lincoln D.; STEWART, Jowh N - **The World Wide Web Security FAQ.** W3C . Disponível em: < http://www.w3.org/Security/Faq/www-security-faq.html> Acesso em 21 mar. 2005.

STS - **A smart answer to online fraud?** - Card Technology Today - Volume 18 - Edição 5 Maio-2006.

SYMANTEC - **Symantec Host IDS**. Disponível em: < http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=48&EID=0>. > Acesso em 18 mar. 2005.

UOL-MICHAELIS - **Moderno dicionário da língua portuguesa**. Disponível em: <http://www2.uol.com.br/michaelis/> Acesso em 03 mar. 2005.

U.S. DEPARTMENT OF JUSTICE - **Internet Fraud.** Disponível em: <http://www.internetfraud.usdoj.gov/> Acesso em 03 mar. 2005.

VOIT, Johannes - **From Brownian motion to operational risk: Statistical physics and financial markets.** Physica A: Statistical Mechanics and its Applications. Volume 321 - Edição 1-2 - 1 Abril 2003.

WAHLSTRÖM, Gunnar - **Worrying but accepting new measurements: the case of Swedish bankers and operational risk**. Critical Perspectives on Accounting. Volume 17 - Edição 4 - Maio 2006.

WIKIPÉDIA - **Sistema de detecção de intrusos** .Disponível em: < http://pt.wikipedia.org/wiki/Sistema_de_detec%C3%A7%C3%A3o_de_intrusos> Acesso em 18 mar. 2005.

WHOIS.WS – **Whois.ws: Universal Whois Lookup.** Disponível em: < http://www.whois.ws/> Acesso em: 16 mai. 2005.

ZWICKY, Elizabeth D. - **Building Internet firewalls**. O'Reilly. Edição 2 - Junho 2000.