Faculdade Santa Maria
Curso de Bacharelado em Sistemas de Informação

Fraudes na Internet: Uma proposta de identificação e prevenção.

Paulo Gabriel A. Jorge

Recife
2007

Paulo Gabriel A . Jorge

Fraudes na Internet: Uma proposta de identificação e prevenção.

Monografia apresentada ao Curso de Sistemas de Informações da Faculdade Santa Maria como requisito para a obtenção do grau de Bacharel em Sistemas de Informação.

Orientador: Márcio Nogueira

Recife
2007

AGRADECIMENTOS

Ao final deste estudo, quero agradecer profundamente a todas as pessoas que, direta ou indiretamente, colaboraram para a sua concretização.

Em razão do grande número de colaboradores, citar todos os nomes seria algo difícil , porém citarei alguns que de alguma forma me ajudaram bastante:

Marcio Nogueira, meu orientador, pela paciência e fabulosos ensinamentos.

Betânia Maciel pelo acompanhamento e dicas sempre preciosas.

Aos meus pais, Paulo Roberto e Maria Eunice, pela disciplina, educação, amor e , acima de tudo, pelo caráter ao longo de toda a vida.

Em especial, desejo agradecer à minha esposa Ester, pelo incentivo, companheirismo e amor verdadeiro sempre presente em cada momento.

Aos “Segundos Pais” Djanira, Nelson e Bernadete.

Aos meus queridos irmãos : Thiago, Lucas, Pedro e Gustavo.

As “irmãs” de perto e de longe: Raquel e Judith.

As minhas tias , tios, primos e primas.

Aos meus amigos de turma que sempre estiveram comigo durante toda a jornada.

E finalmente a Deus, por iluminar meu caminho nas horas difíceis e dar força nos momentos de desânimo.

RESUMO

O estudo *Fraudes na Internet: Uma proposta de identificação e prevenção* é direcionado a internautas, instituições financeiras, empresas e, de maneira geral a todo público interessado em segurança virtual. Trata-se de um conjunto de procedimentos na forma de tutorial que visa auxiliar a identificação e prevenção das fraudes na internet, através da segurança no acesso e manipulação das informações on-line.

Atualmente, com a falta de conhecimento deste tema, os usuários, empresas e instituições financeiras estão se tornando alvos em potencial dos vilões da internet. As maiores vítimas são os usuários que, pela ingenuidade e ávidos em conhecer novos horizontes, são induzidos a executarem ações que os colocam em situações difíceis, muitas vezes arcando com severos prejuízos. Assim, é necessário combinar esforços, investir na troca de informações e experiências, buscando uma eficiente educação de usuários. Este tutorial reúne procedimentos de segurança, tecnologias e legislação cujo conteúdo deverá ser do conhecimento de todos os usuários e instituições que usufruem dos benefícios da internet.

Com o avanço tecnológico e facilidade de comunicação proporcionada pela internet, foram surgindo novos tipos de atos ilícitos: As fraudes on-line. Delitos anteriormente praticados com armas de fogo, por contato pessoal, agora encontram na grande rede um meio atraente e abrangente, onde as distâncias não representam barreiras e o anonimato é supostamente garantido. O mundo digital requer precauções redobradas.

Desta forma, este estudo apresenta em sua totalidade, uma análise destas grandes ameaças globais que são as fraudes na internet. Utilizando-se uma ampla base técnica aliada a uma visão criteriosa do problema, de forma que possam ser expostas tecnologias de proteção, técnicas usadas pelos fraudadores, legislação e outras variáveis que, reunidas, proporcionam um eficiente tutorial na identificação e prevenção das fraudes na internet.

Palavras-chaves: fraudes, prevenção, malwares, phishing scam.

ABSTRACT

The study Fraud on the Internet: A proposal for the identification and prevention is targeted to Internet users, financial institutions, businesses and, in general to all public interested in virtual security. This is a set of procedures in the form of tutorial which aims to assist the identification and prevention of fraud on the Internet, through secure access and manipulation of information online.

Due to lack of knowledge users, companies and financial institutions are becoming targets of potential villains of the Internet. The main victims are the users who, for the naive, curious to know new horizons, are induced to implement actions that arise in difficult situations, often taking with severe damage. Is necessary to combine efforts, investing in the exchange of information and experience searching for a effective education of internet users. This tutorial meets security procedures, technologies, laws whose content should be aware of all users and institutions that enjoy the benefits of the Internet.

With technological advances and ease of communication offered by the Internet, new types of illicit acts emerged: The fraud online. Offenses previously charged with firearms, by personal contact, in the vast network now find a way attractive and comprehensive, where the distance does not represent barriers and anonymity is guaranteed. The digital world requires precautions a lot.

Thus, this study presents in its entirety, an analysis of these major global threats that are the fraud on the internet. By using a broad technical base coupled to a careful view of the problem, so that they can be exposed to protection technologies, techniques used by fraudsters, legislation and other variables that meeting, provide an effective tutorial in the identification and prevention of fraud in internet.

Key words: frauds, prevention, malwares, phishing scam.

LISTA DE ILUSTRAÇÕES

FIGURA 1: CRESCIMENTO DAS FRAUDES ON-LINE. 11
FIGURA 2 :ANÁLISE DE PRODUTOS DISPONÍVEIS PARA VENDA NO MERCADO INFORMAL 15
FIGURA 3: GRÁFICO DE INCIDENTES AO LONGO DOS ANOS. 16
FIGURA 4: TIPOS DE ATAQUES REGISTRADOS ENTRE JULHO E SETEMBRO DE 2007. 17
FIGURA 5: TOP 10 DOS PAÍSES COM MAIS SITES FRAUDADOS 19
FIGURA 6: SETORES QUE SOFRERAM AÇÃO DAS FRAUDES 22
FIGURA 7: ESTRUTURA DO CGI.BR E DO NIC.BR 27
FIGURA 8: ATIVIDADES DESEMPENHADAS PELO CERT.BR 29
FIGURA 9: TRATAMENTO DE INCIDENTES ENVOLVENDO TENTATIVAS DE FRAUDE. 30
FIGURA 10:QUADRO CRONOLÓGICO DE AÇÕES DA POLÍCIA FEDERAL 31
FIGURA 11: ESQUEMA TÉCNICO DAS FRAUDES FONTE: AUTORIA NOSSA, 2007. 34
FIGURA 12: O SPYWARE É USADO PARA EXTRAIR INFORMAÇÕES DOS USUÁRIOS 38
FIGURA 13: ESTRUTURA DE ATAQUE DO PHISHING 40
FIGURA 14: FRAUDES COM MENSAGENS E CARTÕES VIRTUAIS SÃO BASTANTE COMUNS. 41
FIGURA 15: TRAGÉDIAS, FOTOS DE TRAIÇÃO ATRAEM A ATENÇÃO DE MUITA GENTE. 41
FIGURA 16: GOLPES ENVOLVENDO SORTEIOS, PRÊMIOS SÃO COMUNS NA WEB. 42
FIGURA 17: BANCOS E EMPRESA DE TELEFONIA SÃO ALVOS CONSTANTES DE FRAUDES. 43
FIGURA 18: ESQUEMA DE PHARMING 45
FIGURA 19: OBSERVE OS LINKS E URL APRESENTADOS NO SITE. 48
FIGURA 20: O SITE DA RECEITA DISPONIBILIZA INFORMAÇÕES SOBRE A SITUAÇÃO ATUAL DA EMPRESA. 49
FIGURA 21:INFORMAÇÕES DISPONIBILIZADAS PELO REGISTRO.BR. 50
FIGURA 22: NO SITE DOS CORREIOS É POSSÍVEL VERIFICAR A VERACIDADE DO ENDEREÇO. 51
FIGURA 23: É IMPORTANTE VERIFICAR SE A EMPRESA POSSUI TELEFONE FIXO VÁLIDO. 52
FIGURA 24: SITES DE BUSCA SÃO ÓTIMOS PARA PESQUISAR QUALIFICAÇÕES OU PROBLEMAS. 52
FIGURA 25: HTTPS – INDÍCIO DA EXISTÊNCIA DE UMA CONEXÃO SEGURA. 54
FIGURA 26: O CADEADO FECHADO ATESTA QUE O SITE POSSUI UMA CONEXÃO SEGURA. 54
FIGURA 27: CLIQUE NO CADEADO FECHADO PARA EXIBIR O CERTIFICADO DE SEGURANÇA. 55
FIGURA 28 - BRASILEIROS TITULARES DE CONTAS CORRENTES/CARTÃO DE CRÉDITO 56
FIGURA 29: É POSSÍVEL DENUNCIAR FRAUDES PELO SITE DA POLÍCIA FEDERAL. 65
FIGURA 30: O CERT.BR DISPONIBILIZA MEIOS DOS USUÁRIOS DENUNCIAREM FRAUDES. 66

GLOSSÁRIO

ADWARE – Programa que exibe propagandas no computador

APWG -- Anti-Phishing Working Group

BACKBONE – Espinha dorsal, trecho de maior capacidade da rede que interliga várias redes locais

BOTS - Programa capaz de se propagar automaticamente através de vulnerabilidades ou falhas na configuração de softwares instalados em um computador.

BOTNET – É um grupo de computadores infectados com bots .Podem ser usados para envio de spam, esquemas de fraudes e outros delitos virtuais.

BROWSER - Programa para abrir e exibir as páginas da Web.Os mais conhecidos são o Mozilla Firefox e o Microsoft Internet Explorer, da Microsoft.

MALWARE – Código malicioso

Cert.Br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

CGI.br – Comitê Gestor da Internet no Brasil

CSIRT - **Equipe de Resposta a Tratamento de Incidentes de Segurança** (Computer Security Incident Response Team - CSIRT)

CHECKLIST – resumo com os pontos pertinentes as principais considerações sobre segurança na NET.

CYBERCRIME – Crimes cometidos na internet.

CRIPTOGRAFIA - Ciência e arte de escrever mensagens em forma cifrada ou em código.

DOMÍNIO - É o nome registrado em orgão oficial . Fapesp por exemplo

DNS – Domain Name System converte nomes Internet em seus números IPs correspondentes e vice-versa.

E-MAIL - Eletronic-mail ou Correio Eletrônico, que serve para o envio e recebimento de mensagens através da internet

EXPLOIT – Vulnerabilidades de softwares, falhas de programação.

HOME PAGE - É a página inicial de um site.

KEYLOGGERS - Programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador

IP – Internet Protocol – Protocolo padrão da internet

FIRST – Forum of Incident Response and Security Teams

NIC.Br – Núcleo de Informação e Coordenação do Ponto br

NBSO - NIC BR Security Office - Brazilian Computer Emergency Response Team

PHISHING – Técnica criada pelos fraudadores, onde “iscas” (e-mails) são usadas para

“pescar” senhas e dados financeiros de usuários da internet.

POP- UPS - Janela que surge separadamente quando navegamos em um determinado site, geralmente para apresentar um anúncio.

SCAM – Golpe, fraude.

SITE - Representa uma revista digital composta de várias páginas dispostas com o objetivo de fornecer serviços.

SPAM – Lixo eletrônico, propaganda não autorizada.

SPAMMERS – Autores de spam.

TROJAN – Cavalo de tróia .Programa, normalmente recebido como um “presente” que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas.

UNDERGROUND – Mercado Negro

URL – Uniform Resource Locator ou Endereço Eletrônico.

MS – Microsoft Corporation

WINDOWS – Sistema Operacional da Microsoft Corporation

WORM - Programa malicioso capaz de se propagar automaticamente através de redes, enviando copias de si mesmo de computador para computador.

SUMÁRIO

GLOSSÁRIO VI

CAPÍTULO 1 – INTRODUÇÃO 9

1.1 MOTIVAÇÃO 10
1.2 OBJETIVOS 11
1.2.1 Objetivos Gerais e Específicos 12
1.3 METODOLOGIA 12

CAPÍTULO 2 – FRAUDES: UMA AMEAÇA EM CRESCIMENTO 14

2.1 CENÁRIO ATUAL 14
2.2 FATORES QUE "ALIMENTAM" AS FRAUDES ONLINE. 18
2.3 PREJUÍZOS CAUSADOS PELAS FRAUDES ON-LINE. 21
2.4 LEGISLAÇÃO E ENTIDADES ANTIFRAUDES 24
2.4.1 A Legislação Brasileira sobre as fraudes. 25
2.4.2 As Organizações que identificam e combatem as fraudes on-line 27

CAPÍTULO 3 – PRINCIPAIS TÉCNICAS FRAUDULENTAS 32

3.1 ENGENHARIA SOCIAL 35
3.1.1 O que é Engenharia Social? 35
3.1.2 Como funciona? 36
3.2 SPYWARE 37
3.2.1 Definição. 37
3.2.1 Características 37
3.3 PHISHING SCAM 39
3.3.1 O que é Phishing Scam? 39
3.3.2 Como Funciona? 39
3.4 PHARMING 44
3.4.1 O que é Significa Pharming? 44
3.4.2 Como funciona o Ataque? 45

CAPÍTULO 4 – GUIA DE PROCEDIMENTOS ANTIFRAUDES 46

4.1.COMO IDENTIFICAR A CONFIABILIDADE DE UM SITE? 47
4.2. COMO VERIFICAR A SEGURANÇA DA CONEXÃO? 53
4.3. QUAIS OS CUIDADOS PARA REALIZAR COMPRAS E ACESSAR BANCOS PELA INTERNET? 55
4.5. TUTORIAL (CHECKLIST) ANTIFRAUDES PARA LEIGOS 59
4.6. FUI VÍTIMA DAS FRAUDES. O QUE FAZER? 63

CAPÍTULO 5 - CONCLUSÃO 68

REFERÊNCIAS BIBLIOGRÁFICAS 74

Capítulo 1 – INTRODUÇÃO

Este trabalho apresenta como tema: *Fraudes na Internet: Uma proposta de identificação e prevenção.* Tendo como público alvo os usuários e as empresas ligadas à internet e, de maneira geral interessados em segurança, visando identificar e prevenir o roubo de informações pessoais; correto acesso e manipulação de informações e outras conseqüências “maliciosas” das fraudes on-line.

A Crescente popularização do uso e acesso da internet trouxe inúmeros benefícios para o cotidiano das pessoas e organizações. A informação on-line tornou-se ágil, a relativa facilidade de propagação que temos hoje com a internet, a constante utilização de e-mail, sites de e-commerce e home banking, atingiu rapidamente um grande número de pessoas em âmbito mundial. Porém, devido à ampla diversidade e volume de informações diariamente circuladas, aliada às falhas de segurança em sites, programas, sistemas operacionais e a ausência de uma legislação específica, a internet vem se tornando cenário de inúmeras armadilhas e fraudes a estes usuários.

Neste estudo, o conceito de fraude adotado é definido pelo Aurélio, como uma palavra derivada do latim, que significa “*um golpe com o objetivo de enganar, prejudicar, roubar outrem*”.

Segundo (SIQUEIRA[37] , 2004):

> *“Quase a metade de tudo que circula na internet é lixo. Trocando em miúdos: no Brasil e no mundo, os usuários da internet estão sendo inundados por uma onda de spams, de vírus, de pornografia, de pedofilia, de propaganda nazista, de roubo de dados, de comercialização de produtos pirateados, de medicamentos falsos, de propostas mentirosas, de endereços e remetentes apócrifos e oferecimentos semelhantes.”*

A Internet está vulnerável a estas ameaças, e seus usuários aos riscos. Contudo, existem vários procedimentos que podem ser observados para identificar e prevenir estes tipos de golpes. Portanto, como identificar se um site, e-mail, ou propaganda é confiável?

A utilização confiável e segura de grande parte das informações que circula na rede mundial é um desafio complexo e contínuo, pois, devem-se enfrentar os fraudadores e sua grande diversidade de técnicas. Segundo a (FEBRABAN apud GOUVEIA[17], 2007) somente as instituições financeiras investem R$ 1,2 bilhão por ano para atualizar seus mecanismos de combate às fraudes eletrônicas.Uma das maneiras de reduzir as práticas fraudulentas é através de procedimentos que auxiliem na identificação e prevenção dos fraudadores, assim como, acionar autoridades responsáveis por combater estas práticas criminosas.

Desta maneira, este trabalho apresenta um estudo sobre a situação atual dessa grande ameaça mundial: as fraudes na internet, identificando suas causas, impactos econômicos, principais técnicas utilizadas pelos fraudadores, autoridades e legislação antifraudes com o intuito de reunir e estabelecer um conjunto de procedimentos que tornem mais fácil a identificação e prevenção destas práticas.

1.1 Motivação

Este estudo sobre as *Fraudes na Internet: Uma proposta de identificação e prevenção* tem como objetivo identificar os diversos tipos de fraudes existentes na internet e suas peculiaridades, dando ênfase às medidas de proteção. Ao final do estudo, almeja-se que as empresas e os usuários se tornem mais aptos a reconhecer e evitar as mais diversas fraudes que circulam na internet, assim como acionar autoridades para processar fraudadores e deter ataques.

Segundo (GHETLER apud PRADO[31], 2004):

> *"O mundo eletrônico é um mundo mais ou menos anônimo. Os bancos têm que recorrer a senhas ou a outras metodologias mais sofisticadas. A parte mais fraca, que é o usuário, o cliente, não dispõe de toda essa tecnologia dentro de casa. Então, eles são os alvos mais fracos".*

Os usuários, portanto, possuem função primordial nesse cenário, pois, apesar de as empresas de comércio eletrônico e bancos também serem vulneráveis às pragas cibernéticas, possuem tecnologias mais rígidas e sofisticadas de proteção.

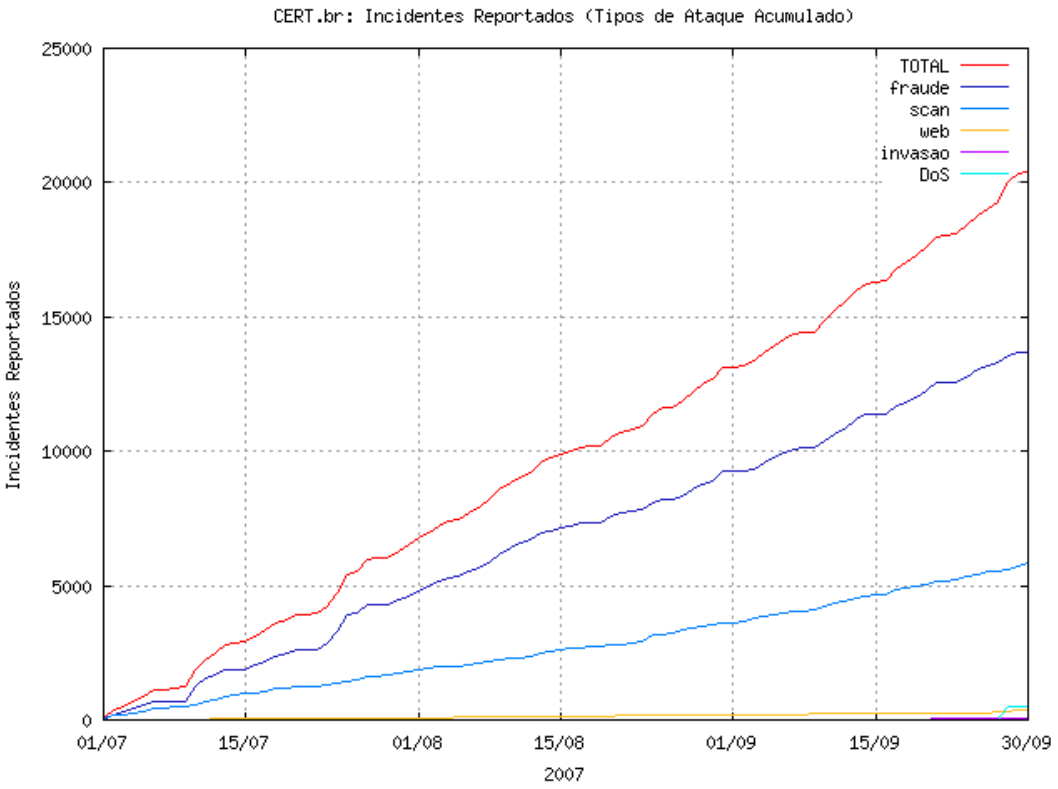

Figura 1: Crescimento das Fraudes on-line.

Fonte: Cert.Br, in: http://www.cert.br/stats/incidentes/2007-jul-sep/tipos-ataque-acumulado.html

Conforme dados da Figura 1, as pesquisas demonstram índices preocupantes: As fraudes envolvendo a internet deixaram o amadorismo para a ação crescente e coordenada de criminosos.O internauta maduro e bem informado estará menos propenso a ser mais um nas crescentes estatísticas deste cenário.

1.2 Objetivos

Um dos grandes questionamentos que se faz presente na internet atualmente é a precisa identificação dos interlocutores. Apesar da constante evolução da segurança no mundo digital, incluindo sistemas, sites e ferramentas usadas na

internet, os fraudadores são muito criativos, freqüentemente bem informados, flexíveis e adaptáveis a novas situações, com isso novas fraudes surgem freqüentemente, ajustando-se e aproveitando cada nova oportunidade.

Segundo (HOEPERS[18],2007, p.01):

> *"O número de notificações relacionadas a fraudes aumentou 46% em relação ao primeiro trimestre de 2007 e 3% se comparado ao mesmo período de 2006".*

Assim, torna-se constante a preocupação em ratificar a confiabilidade do site acessado; a verdadeira identidade do emissor de um e-mail e a confirmação da existência ou não de uma empresa vendedora de produtos, sendo estas as variáveis envolvidas neste estudo.

1.2.1 Objetivos Gerais e Específicos

Diante deste contexto, as empresas, principalmente ligadas ao comércio eletrônico, bancos, e os usuários vitimados ficam desacreditados perante seus clientes e parceiros comerciais quando as notícias se tornam públicas. Assim, a grande questão é saber se um interlocutor é "realmente quem ele diz ser", em síntese: *Como identificar e prevenir as fraudes on-line?* Para isto, este estudo tem como objetivo geral: Identificar e prevenir as fraudes on-line, e como objetivos específicos: identificar a confiabilidade de um site; identificar as técnicas usadas pelos fraudadores e estabelecer procedimentos para tornar a navegação mais segura, com o suporte do trabalho de autoridades e dispositivos da legislação brasileira que combatem as fraudes na internet.

1.3 Metodologia

A metodologia utilizada será baseada no plano de elaboração de um Tutorial

com procedimentos e orientações sobre as fraudes on-line e suas variáveis. Este tutorial é um guia, exemplificado e ilustrado, destinado a usuários de internet leigos ou especialistas, empresas e, qualquer público interessado, que servirá de referência técnica para identificar e prevenir as fraudes na internet.

A composição dessa metodologia abordará a pesquisa teórica, conhecimento científico sobre o assunto, documentação indireta: livros; jornais; teses; artigos científicos e revistas sobre segurança na web; normas padronizadas mundialmente; autoridades e leis antifraudes; sites especializados em fraudes; crimes cibernéticos e segurança da informação. Em síntese, o estudo será construído a partir de um arcabouço teórico, tendo como foco uma gama de informações relacionadas às fraudes on-line e suas ramificações disponíveis na web, bibliotecas, faculdades entre outras fontes comprovadamente eficientes.

Para isto, será realizado um estudo minucioso sobre as fraudes on-line e suas características, tendo como atividades de pesquisa o seguinte roteiro:

- Os fatores que, combinados, levam à ocorrência e proliferação das fraudes;
- Os prejuízos econômicos causados pelas fraudes on-line;
- A legislação brasileira e as autoridades responsáveis por combater e punir as fraudes na internet;
- Identificar as principais técnicas utilizadas pelos fraudadores;
- Definição de um conjunto de procedimentos que auxiliem na prevenção das fraudes.

O estudo transcorrerá conforme o estabelecido acima, ressaltando a constante preocupação em abranger o maior número de possibilidades, levantando a maior quantidade de recursos disponíveis, pois, o combate às fraudes on-line nunca será 100% eficiente, mas as conseqüências que as envolvem podem ser amenizadas com a implementação de um conjunto de procedimentos de segurança. Este tutorial deve buscar informar os internautas, as empresas, instituições financeiras e outros grupos a maneira correta de acessar e manipular a informação

que trafega na internet. Além disso, fornecerá um *checklist* de boas práticas para que uma proteção eficiente possa ser alcançada e mantida, assim como, divulgar autoridades e leis responsáveis pelo combate e punição dos fraudadores.

Capítulo 2 – Fraudes: Uma ameaça em crescimento

2.1 Cenário Atual

Nos dias atuais, ter um computador conectado a internet se tornou o sonho de consumo de boa parte da população. Com a valorização da moeda, queda nos preços e incentivos fiscais, a popularização dos computadores pessoais, principalmente, nas classes de baixa renda, tornou a inclusão digital uma realidade. Este processo, embora de grande importância para a sociedade, impulsionou o crescimento de fraudes na internet. TERZIAN[41] (2006) afirma que isto ocorre, pelo fato de que a maioria dos novos computadores adquiridos são imediatamente conectados à rede, porém, os internautas iniciantes pouco conhecem os procedimentos básicos de segurança on-line.

Nos últimos anos, o número cada vez maior de incidentes documentados por empresas especializadas em segurança como o CERT.Br (http://www.cert.br) e os constantes noticiários mostram que o cyber crime cresceu bastante no Brasil e no mundo. Apesar desta constatação, não há indícios de que esta tendência vá recuar nos próximos anos. Podemos estabelecer um breve histórico das fraudes via internet no Brasil. Segundo (CHAVES[8], 2006, p.37):

2001

- O surgimento dos keyloggers enviados por e-mail, ataques de força bruta;

2002-2003

- Casos de phishing e uso disseminado de servidores DNS

comprometidos;

2003-2004

- Aumento dos casos de phishing mais sofisticados;
- Dados eram enviados dos sites falsificados para sites coletores;
- Sites coletores processavam os dados e os enviavam para contas de e-mail;

2005-2006

- Spams usando nomes de diversas entidades e temas variados;
- Links para cavalos de tróia hospedados em diversos sites;
- Vítima raramente associa o spam recebido com a fraude bancária;

A situação atual vivencia a união de golpistas numa espécie de “crime organizado digital” injetando dinheiro na economia “underground”, aliciando *spammers* e invasores,utilizando como moeda informações sigilosas como senhas de administradores, novos *exploits*, senhas e contas bancárias, número de cartões de crédito entre outras.

Posição	Item	%	Gama de Preços
1	Cartões de Crédito	22%	$0.50 - $5
2	Contas Bancárias	21%	$30 - $400
3	Senhas de E-mail	8%	$1 - $350
4	Mailers	8%	$8 - $10
5	Endereços de E-mail	6%	$2/MB - $4/MB
6	Proxies	6%	$0.50 - $3
7	Identidades Completas	6%	$10 - $150
8	Scams	6%	$10/week
9	Números de Seguro Social	3%	$5 - $7
10	Shells UNIX comprometidas	2%	$2 - $10

Figura 2 :Análise de produtos disponíveis para venda no mercado informal

Fonte: *Symantec Corporation, in*: http://www.symantec.com/pt/br/enterprise/theme.jsp?themeid=threatreport

Somando-se a essa situação constatamos uma grande utilização de *Botnets*

para envio de phishing, spam, invasões e outros delitos, redes mal configuradas sendo manipuladas para disseminação de fraudes e a migração das armadilhas on-line do ambiente coorporativo para o usuário final.

O perfil dos atacantes aponta que ,em grande parte ,trata-se de pessoal com conhecimento técnico que utiliza informações e kits de ferramentas prontas provenientes do mercado underground explorando vulnerabilidades em sistemas operacionais e softwares desatualizados para realizar operações fraudulentas na internet.

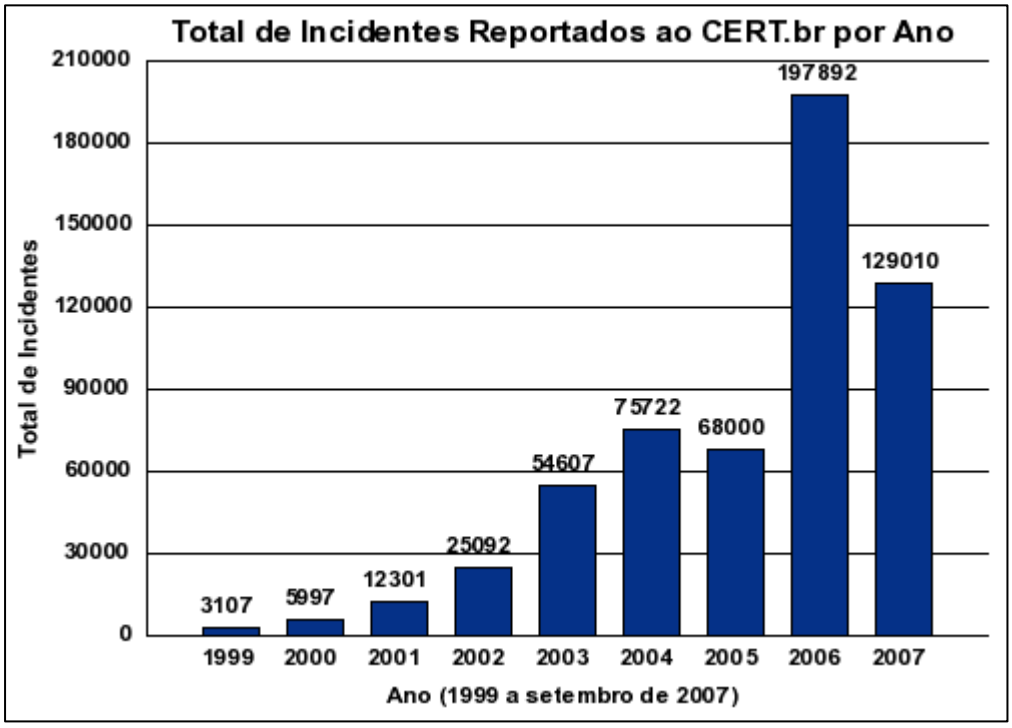

Figura 3: Gráfico de Incidentes ao longo dos anos.

Fonte: Hoepers & Steding- Jenssen, 2007, in: http://www.cert.br/docs/palestras/certbr-febraban2007.pdf

A web está se tornando uma das principais vias de ataque dos criminosos. Com isto, cresce a preocupação por parte dos usuários em proteger seus computadores de vírus e outras pragas virtuais. Navegar na Web está cada vez mais semelhante a passear pelas ruas das metrópoles: quem não andar com cuidado,

estiver constantemente informado, prestando atenção em indivíduos e atitudes suspeitas, pode cair em golpes ou arcar com enormes prejuízos. Segundo a empresa de segurança (SOPHOS[38], 2007):

> *"23.864 novas ameaças foram criadas no primeiro trimestre do ano, contra 9.450 do mesmo período do ano passado". De acordo com a companhia, em média, foram identificadas 5 mil novas páginas na web contaminadas por dia."*

Neste cenário preocupante, as fraudes ocupam uma parcela de destaque (40% do total) entre os incidentes de segurança registrados. Uma das explicações para justificar o aumento de tal prática criminosa, nos últimos anos, reside na ampla divulgação do assunto na mídia e das constantes prisões efetuadas pelos órgãos e autoridades competentes.

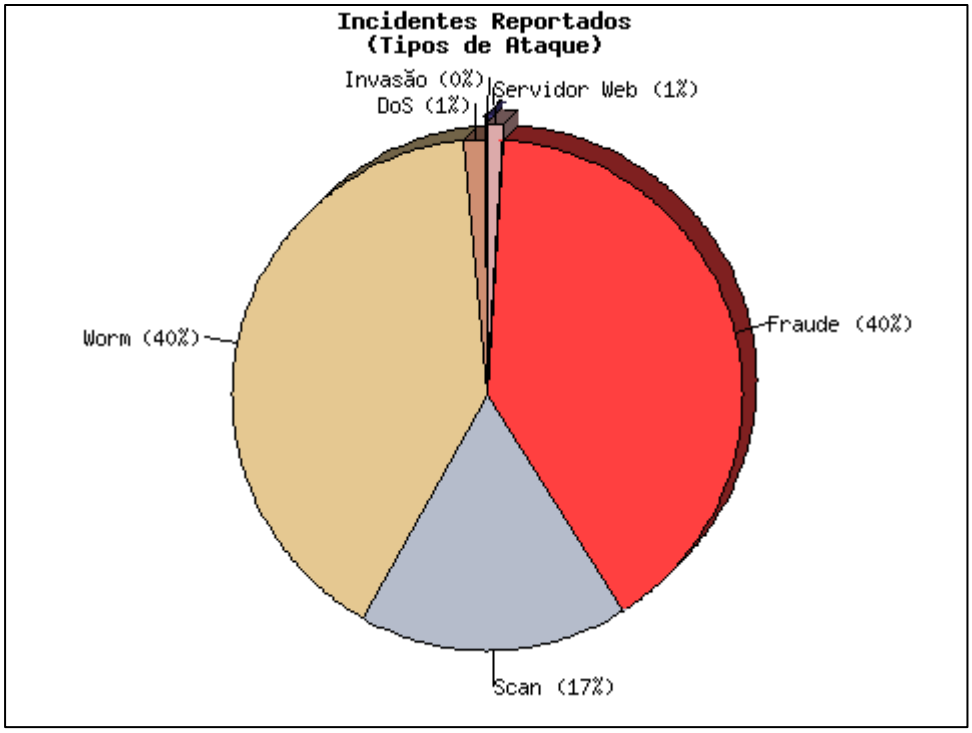

Figura 4: Tipos de Ataques registrados entre julho e setembro de 2007.

Fonte: Hoepers & Steding- Jenssen, 2007, in: http://www.cert.br/docs/palestras/certbr-febraban2007.pdf

Segundo (HOEPERS & JESSEN apud ROCHA[32], 2004):

> *"Todas as estatísticas do NBSO são de incidentes voluntariamente reportados. A divulgação na mídia e as várias prisões aparentemente têm estimulado um maior número de usuários de internet a reportar este tipo de atividade. Aliado a esse maior número de usuários notificando fraudes, está claro que esse tipo de incidente está aumentando".*

2.2 Fatores que “alimentam” as Fraudes online.

Os golpes on-line são resultados de um conjunto de variáveis de diferentes origens. Identificar precisamente o fator principal é algo bastante difícil. SÊMOLA[35] (2007) afirma que ,de um modo geral, as fraudes existem pela coexistência de três fatores fundamentais:

- A existência de golpistas motivados: Sensação de impunidade, a ineficácia das leis, a falta de regulamentação, pouca fiscalização, o volume de vítimas vulneráveis, a facilidade de aplicação dos golpes, a redução dos custos da fraude.
- A disponibilidade de vítimas adequadas e vulneráveis: Falta de informação adequada, ambição, ingenuidade, o despreparo para lidar com um ambiente eletrônico novo, desrespeito às leis, a ganância, credulidade, ignorância, entre outros.
- A ausência de controles de fraude eficazes: Despreparo das autoridades, falta de legislação, ausência de integração entre as autoridades responsáveis , reunir o conhecimento adquirido para agir preventivamente.

Segundo (HARRIS apud SANTOS[34], 2007):

> *“O Brasil é o número um do mundo na produção de golpes de phishing scam via e-mail destinados ao roubo de dados bancários. O volume e a variedade de mensagens com cavalos-de-tróia produzidos no país com objetivo de roubar informações bancárias têm crescido muito e já superam o de qualquer outro país”*

O Brasil ocupa o terceiro lugar no ranking mundial de produção de pragas virtuais (vírus, phishing, spywares, etc.) por país com 14,2% do total, atrás da China (30%) e dos Estados Unidos (35%). O Top 5 traz ainda Rússia (4,1%) e Suécia (3,8%).

Figura 5: TOP 10 dos Países com mais sites fraudados

*Fonte: APWG ,in:*http://www.apwg.org

Aliada aos 03 pilares principais citados anteriormente existem uma série de outros fatores que, contribuem para a ocorrência e proliferação dos golpes na internet.Segundo (D´ÁVILA[9], 2004) podemos destacar:

- A simplicidade com que um e-mail, site é falsificado e fraudado;
- Conhecimento técnico, capacidade de persuasão aprofundada dos fraudadores;
- Crescente profissionalização e comercialização de atividades maliciosas.Fraudes geram lucros cada vez maiores aos com kits, programas maliciosos;
- Ameaças são, cada vez mais, dinâmicas , adaptando-se sob medida para regiões específicas;
- Golpistas se utilizam de empresas sérias, entidades da confiança do usuário;

- Ampla diversidade de técnicas fraudulentas se utilizando de conteúdos sempre atualizados, evolvendo grande número de empresas e serviços;
- Ingenuidade e falta de preparo de grande parcela dos internautas para desconfiar dos perigos existentes devido ao baixo nível ou nenhum conhecimento técnico;
- A facilidade de hospedar na web qualquer conteúdo e arquivos maliciosos, principalmente em serviços gratuitos de hospedagem e que não exigem uma identificação legítima dos responsáveis;
- A proliferação de softwares e lista de e-mails encontradas na internet para envio de spam (propaganda não solicitada) em larga escala;
- Convergência dos métodos de ataque aumentando a chance do golpe ser bem sucedido;
- A carência de autoridades e legislação que propiciem um melhor gerenciamento da segurança on-line permitindo identificar, coibir e punir os crimes cibernéticos de forma rápida, eficaz e globalizada;

Empresas que usufruem do potencial da web como instituições bancárias, lojas de e-commerce , embora grandes prejudicadas pela ação dos golpistas pouco contribuem para reduzir a incidência de ataques.Entre os principais fatores para esta constatação estão:

- Deficiência na elaboração e/ou informação de políticas corporativas aos consumidores;
- Pouca divulgação de medidas que auxiliem o usuário a identificar se o e-mail ou site é autêntico: O usuário, muitas vezes, não é capaz de identificar se o e-mail é da instituição ou é se trata de um golpe;
- Ausência de uma autenticação mais rígida nos sites: Se as instituições não solicitam informações confidenciais dos clientes (CPF, data de nascimento) como requisito de acesso a um site, fica mais fácil para os golpistas atuar como usuário legítimo;
- Empresas não monitoram a Internet em busca de sites fraudados: Geralmente, o site fraudado aparece em algum lugar da Internet antes do envio dos e-mails relacionado ao golpe. Muitas vezes, esses sites se

apropriam indevidamente de marcas comerciais de empresas para parecerem legítimos.

- Inadequado investimento em soluções de segurança focado na Internet: Muitas empresas não possuem filtragem e bloqueio de spam e phishing evitando que mensagens e arquivos maliciosos se propagem na internet.

Fica evidente a necessidade de uma participação conjunta entre empresas, autoridades e usuários na criação e aplicação de regras que busquem diminuir a incidência de fraudes na internet.

2.3 Prejuízos causados pelas Fraudes on-line.

A internet se tornou sinônimo de agilidade e comodidade.No mundo eletrônico, no entanto, nem tudo são flores. Da mesma forma que as ferramentas tecnológicas contribuem para ampliar as fronteiras geográficas e possibilitam uma série de facilidades e vantagens, elas também podem expor empresas e usuários a grandes perigos e a prejuízos consideráveis.

Segundo (ARTHUR apud CARDILLI & CARPANEZ[3], 2007):

> *"O trabalho de redução das fraudes sofre uma pressão contrária, que é o aumento no número de transações e de internautas". Embora o número de transações aumentou de 2005 para 2006, os prejuízos permaneceram estáveis.*

Impulsionada pela globalização, a internet ampliou sua gama de serviços oferecidos, além de transações bancárias,comércio eletrônico ,empresas realizam pagamentos, negociam ações e outros serviços.Um campo vasto para golpistas.O Brasil apesar de ser uma das referências mundiais em proteção virtual, enfrenta várias ondas de fraudes na grande rede. Nos últimos dez anos, o número de transações financeiras cresceu rapidamente, porém, cresceu também os prejuízos causados pelas fraudes na internet. As empresas financeiras são as mais atacadas e acumulam prejuízos. JONES[23] (2006) afirma que Números precisos sobre o

custo global de crimes online são difíceis de serem apurados, em parte porque algumas organizações preferem ficar no anonimato do que publicar que suas redes foram atacadas.

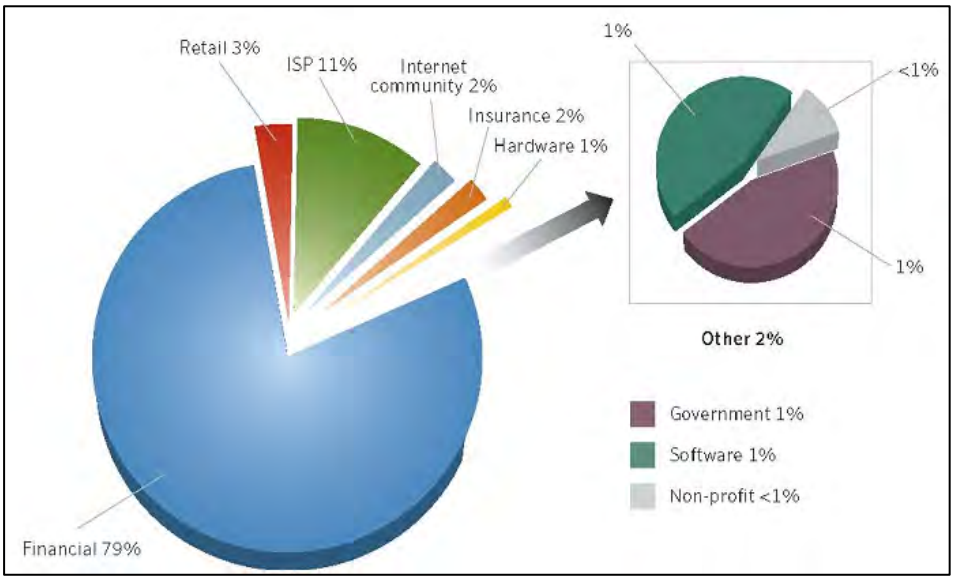

Figura 6: Setores que sofreram ação das fraudes

Fonte: Symantec Corporation,in http://eval.symantec.com/mktginfo/pt/br/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_exec_summary_09_2007-pt-br.pdf

Segundo a (FEBRABAN apud CARDILLI & CARPANEZ[3], 2007), o prejuízo de R$ 300 milhões em 2005 ocorreu em 327 mil operações fraudulentas, de um contingente de 23 bilhões de operações. Em 2006, segundo dados do IPDI (Instituto de Peritos em Tecnologias Digitais e Telecomunicações) criminosos causaram prejuízos na ordem de R$ 300 milhões em internet banking, cartão de crédito e de débito, o mesmo que no ano anterior. A previsão para o ano de 2007 é que os números se mantenham estáveis ou até haja queda. Podemos mencionar alguns números relacionados aos prejuízos decorrentes dos golpes pela internet, no Brasil e no mundo.(FEBRABAN et al[13], 2006)

- 300 milhões de reais é o prejuízo admitido pelos bancos com fraudes online no Brasil;

- 920 reais é o prejuízo médio de cada incidente;
- 630 milhões de dólares é a soma dos golpes registrados nos Estados Unidos (*);
- 850 dólares é o valor médio do desfalque nos golpes aplicados nos Estados Unidos (*);
- 7,9 milhões de mensagens de phishing são enviadas diariamente

A tendência de estabilidade e ate quedas nos prejuízos causados pelas fraudes on-line se deve principalmente ao usuário mais consciente e investimento de empresas em segurança para dificultar a trabalho dos fraudadores.Atualmente, os bancos gastam fortunas em tecnologias voltadas para segurança eletrônica. O investimento do setor bancário tem focado conscientizar seus clientes para trabalhar junto com eles na prevenção.

O comercio eletrônico também é vítima em potencial da ação dos fraudadores. Segundo a pesquisa do site Reclame Aqui, que reuniu 130 mil queixas de consumidores descontentes serviços prestados por empresas no país , os prejuízos de consumidores que compraram pela internet e não receberam já somam R$ 3 milhões neste ano. Ainda conforme estimativa do site indica que o prejuízo com falsas vendas online em todo Brasil pode chegar a R$ 300 milhões por ano. (NETTION[29], 2007)

Segundo (VARGAS[43], 2007):

> *"As principais causas desse quadro são o excesso de confiança do consumidor e a tentação de comprar produtos muito mais baratos que o normal. ´Como as quadrilhas não têm muito tempo até serem descobertas, elas precisam trabalhar com preços tentadores para atrair o máximo de público possível. Com isso, o consumidor acaba se esquecendo de checar vários detalhes para se certificar de que a empresa é realmente idônea e compra por impulso´".*

A perspectiva é de salto em potencial do comercio eletrônico alavanco pelo crescimento da venda de computadores e popularização do acesso a internet no Brasil. O faturamento projetado para o ano é de R$ 6,4 bilhões, 45,45% a mais que

em 2006. O número de compradores por meio eletrônico vai chegar a 9,5 milhões, ou 35% a mais que os sete milhões de brasileiros que fizeram compras via Internet em 2006. (ESCALENA[11], 2007)

Os prejuízos relacionados às fraudes, por outro lado, indicam tendência de queda, muito em função da preocupação do internauta em aprender a usar a grande rede de forma segura. Por isso, a fraude não cresce na mesma proporção que as vendas.

Segundo MATTOS[24], 2007:

> *"A reversão na curva de incidentes negativos tem a ver com o cuidado das pessoas com o e-mail, deixando de abrir e ver as mensagens criminosas.*E ainda, *No fundo, o principal meio para o processo de fraude é a comunicação por e-mail. A estratégia dos malfeitores não mudou muito nos últimos anos, o que muda é o conteúdo".*

A evolução da internet impulsiona o comercio eletrônico e negócios on-line. Embora o volume de dados trafegados tende a aumentar, os prejuízos decorrentes das fraudes no mundo virtual estão em queda .O primeiro passo está sendo dado, o usuário está mais precavido reconhecendo a estratégias de ataque dos golpistas.A caminhada contra as fraudes on-line , porém, é longa e cheia de obstáculos. É preciso combinar soluções e tecnologias, manter-se bem informado e investir numa legislação madura e abrangente.

2.4 Legislação e Entidades antifraudes

As ações dos fraudadores são difíceis de comprovar e serem enquadrados nas leis vigentes.A ausência de uma legislação brasileira específica que defina os diferentes tipos de delitos e facilite a obtenção de dados de usuários delituosos impede que os tribunais ajam com rapidez na punição de golpes na web. Segundo (FILHO[15], 2007):

> *"Precisamos aprovar a Lei Específica o quanto antes. Ela é um instrumento para trabalharmos com mais tranqüilidade. Todos têm de guardar dados. Vamos poder ser mais pró-ativos".*

2.4.1 A Legislação Brasileira sobre as fraudes

A Internet apresenta-se como a maior ferramenta de comunicação e revolução tecnológica desse milênio. A comunicação tornou-se ágil, usuários de diversas partes do mundo usam a rede para lazer, pesquisar, trocar informações e fechar negócios. Mas juntamente com o desenvolvimento tecnológico, novas modalidades de crimes surgiram. As fraudes via Internet e com auxílio de computadores, mostra-se sempre dinâmico, na medida em que está em constante atualização e mutação, caminhando junto com os avanços da tecnologia.

Em países desenvolvidos tecnologicamente, desde a mais simples tarefa até a movimentação financeira de milhões de dólares ou monitoração de vôos comerciais é operada por computadores, a preocupação com o funcionamento e confiabilidade dos computadores é permanente e crescente; Essa tendência se reflete também nos países em desenvolvimento, onde a informática também já faz parte do cotidiano e trabalho das pessoas.

Envio de e-mails em massa com objetivo de obtenção de dados pessoais, por exemplo, ainda não é considerado delito. Por não se enquadrar na definição de ação ou omissão típica, ilícita ou antijurídica e culpável,técnicas fraudulentas como *phishing*, *pharming* e *outra* só aparecem realmente como delito em projetos de lei.(SIMON[36], 2007)

Para (PRADO[31], 2007):

> *"O aumento de golpes ocorre de forma exponencial quando se tem a percepção de impunidade. Assim, dotar a legislação de mecanismos que possibilitem, entre outros, o rastreamento de mensagens (registros de operações nos provedores), a punição às tentativas de ataques, à violação de privacidade, e a tipificação das diversas modalidades de crimes eletrônicos é fundamental para o continuo desenvolvimento da internet".*

O início de uma lei específica sobre crimes na internet surgiu em 1999 : O Projeto de Lei 84/99, de autoria do Deputado Federal Luiz Piauhylino. O projeto, que dentre outros assuntos tipifica crimes virtuais, clonagem de telefone celular e cartões de créditos. (INVASÃO[22], 2007). Atualmente o Projeto de Lei 76/2000 relatado pelo Senador Eduardo Azeredo com a assessoria do Dr. José Henrique Santos Portugal é o mais completo texto legislativo já produzido no país para regular a repressão a crimes de informática.O projeto incorpora atualizações e contribuições de outros projetos de lei menos abrangentes e altera o Código de Processo Penal, o Código Penal Militar e a Lei de Interceptação de Comunicações Telefônicas. (TERRA[40], 2006)

Caso seja aprovado, a dificuldade de enquadrar condutas criminosas que até então carecem de cobertura penal específica deve ser em grande parte reduzida. Segundo Azeredo apud Brancatelli0 (2007) “A lei vai ajudar a disciplinar a internet e punir outros crimes tecnológicos como clonagem de cartão de crédito e celular”. A lista de delitos virtuais é ampla: Engloba desde a invasão de sistemas, phishing, difusão de vírus, quebra de privacidade de banco de dados, não armazenar dados de conexões, alteração de dados, guardar dados obtidos indevidamente à permitir acesso anônimo à rede.

Nessa luta contra as fraudes eletrônicas, cabe ao governo adequar rapidamente a legislação, agilizar projetos de lei que possibilitem fiscalizar e punir com o maior rigor os responsáveis.É preciso disciplinar a conduta na internet..Ao usuário, cabe exercer o papel investigativo: coletar e preservar as provas,salvar o site ou e-mail criminoso,procurar anotar o horário que a pessoa acessou a internet ou recebeu a mensagem ilícita. Enfim, coletar o maior número de provas possível para que haja possibilidade de identificação do responsável pela ação ilegal e posteriormente denunciar irregularidades as autoridades e órgãos competentes.

2.4.2 As Organizações que identificam e combatem as fraudes on-line

Nesta luta de identificação e prevenção das fraudes, existem autoridades sérias, competentes que auxiliam os usuários e empresa da internet a se protegerem das ameaças do mundo virtual.

À nível nacional destacamos o comitê de Gestão da internet no Brasil (CGI.br), Núcleo de Informação e Coordenação do Ponto BR (NIC.br), o Registro.br, o centro de estudos, resposta e tratamento de incidentes de segurança (CERT.br) , o SaferNet Brasil entre outras entidades do governo(dentre elas a polícia federal) e sociedade civil.

Embora todas as entidades possuam sua parcela de contribuição no combate aos crimes virtuais, O estudo enfocará as atribuições e responsabilidade do CGI.br, as atividades desenvolvidas pelo CERT.br e SafeNet Brasil além das autuações da polícias federal no combate aos golpes on-line.

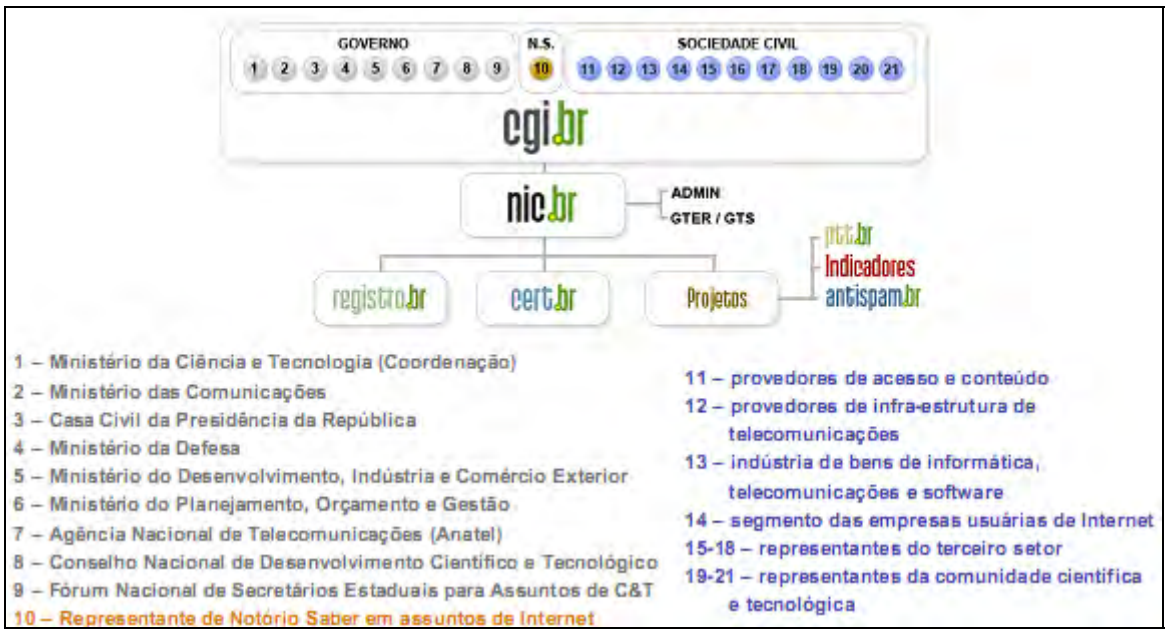

Figura 7: Estrutura do CGI.br e do NIC.br

Fonte : Cert.br in http://www.cert.br/docs/palestras/certbr-real2007.pdf

O **CGI.br** (Comitê gestor da internet no Brasil) foi criado pela Portaria Interministerial nº 147, de 31 de maio de 1995 e alterada pelo Decreto Presidencial nº 4.829, de 3 de setembro de 2003, visando coordenar e integrar todas as iniciativas de serviços Internet no país, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados. Tem como endereço virtual a Home Page: http://www.cgi.br. (CGI.br[6], 2007)

Dentre as Atribuições e responsabilidade do CGI.br se destacam:

- A proposição de normas e procedimentos relativos à regulamentação das atividades na Internet;
- Recomendação de padrões e procedimentos técnicos operacionais para a Internet no Brasil;
- Estabelecimento de diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil;
- Promoção de estudos e padrões técnicos para a segurança das redes e serviços no país;
- Coordenação da atribuição de endereços internet (IPs) e do registro de nomes de domínios usando <.br>;
- Coleta, organização e disseminação de informações sobre os serviços internet, incluindo indicadores e estatísticas.

O **CERT.br** (Centro de estudos, resposta e tratamento de incidentes de segurança) é um dos principais grupos de resposta a incidentes de segurança. Fundado em 1997 e mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil é responsável por tratar incidentes de segurança em computadores,envolvendo redes conectadas à Internet brasileira. Tem como endereço virtual a Home Page: http://www.cert.br. (CERT.br[5], 2005).

Suas Atividades Incluem(CERT.br[5], 2005):

- A proposição de normas e procedimentos relativos à regulamentação das atividades na Internet;
- Ponto de contato nacional para notificação de incidentes de

segurança;

- Provê o apoio necessário no processo de resposta a incidentes;
- Trabalho colaborativo com outras entidades, como os operadores da justiça provedores de acesso e serviços e backbones;
- Auxilia novos CSIRTs a estabelecerem e desenvolverem suas atividades.

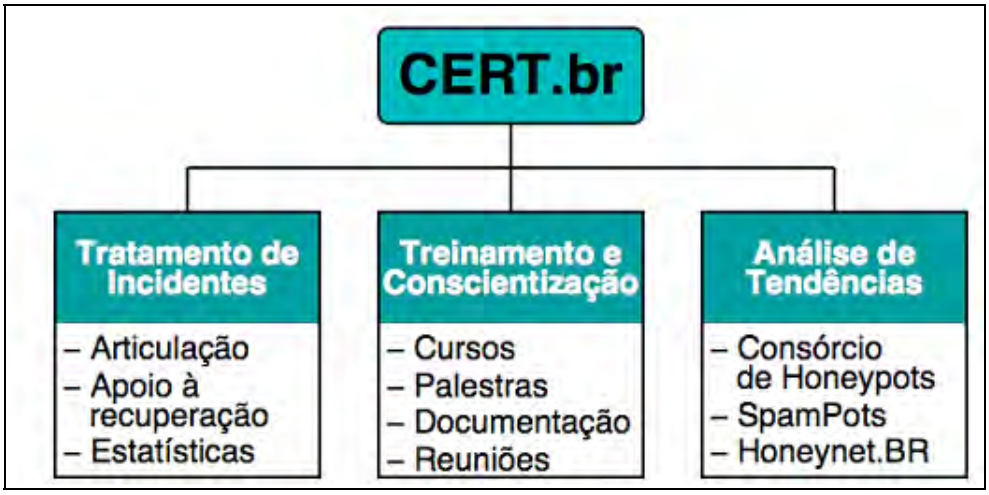

Figura 8: Atividades desempenhadas pelo CERT.br

Fonte : CERT.br in http://www.cert.br/docs/palestras/certbr-dualtec2007.pdf

O **SafeNet Brasil** (Central Nacional de Crimes Cibernéticos) é uma organização não governamental, fundada em 2005, sem fins lucrativos, que engloba cientistas da computação, professores, pesquisadores e bacharéis em Direito com a missão de defender e promover os Direitos Humanos na Sociedade da Informação no Brasil (SAFERNET[33], 2007).

A Organização visa oferecer uma resposta eficiente, consistente e permanente no Brasil aos graves problemas relacionados ao uso indevido dos serviços da rede Internet para a prática de crimes e violações contra os Direitos Humanos. Tem como endereço virtual a Home Page: http://www.sefernet.com.br. (SAFERNET[33], 2007).

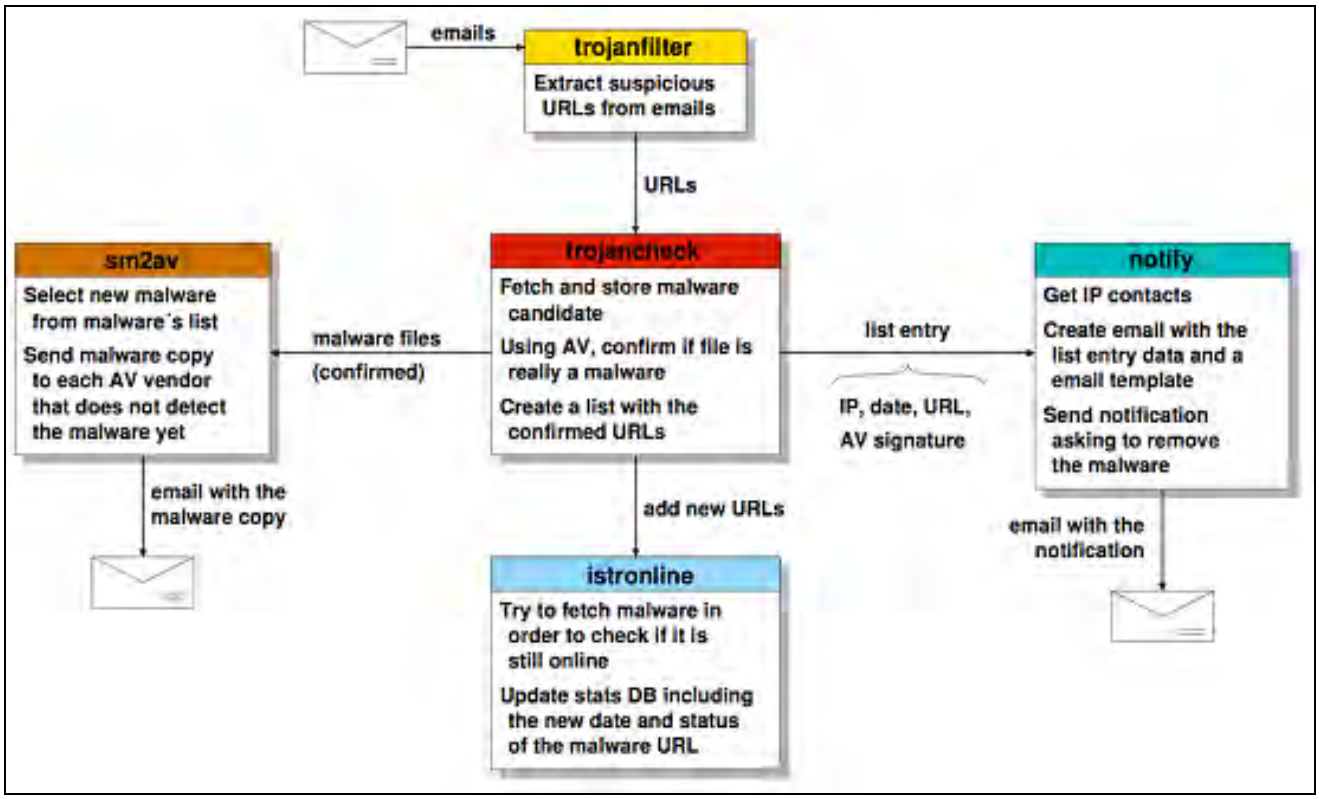

Figura 9: Tratamento de Incidentes Envolvendo Tentativas de Fraude.

Fonte : Cert.br in http://www.cert.br/docs/palestras/certbr-real2007.pdf

A **Polícia Federal** vem sendo uma das entidades mais ativas na identificação e combates aos delitos via internet. Nos últimos anos, a Polícia Federal desarticulou diversas quadrilhas brasileiras especializadas em invadir e desviar dinheiro de contas bancárias via web totalizando quase 600 criminosos virtuais. Tem como endereço virtual a Home Page: http://www.dpf.gov.br/. (DPF[10], 2007).

O quadro a seguir sintetiza as principais operações no combate às fraudes, nos últimos anos:

QUADRO CRONOLÓGICO DE AÇOES DA POLÍCIA FEDERAL		
2001 Operação Cash Net	As primeiras implementações de keylogger, ataques de força bruta.	17 pessoas presas
2003 Operação Cavalo de Tróia I	Spams, sites falsos, {key,screen} loggers,comprometimentos de DNS	27 pessoas presas
2004 Operação Cavalo de Tróia II	Organização criminosa, hierarquia, key e screenloggers sofisticados.	64 pessoas presas
2005 Operação Pégasus	key, screenloggers ainda mais sofisticados, sobreposição de tela.	85 pessoas presas
2006 Operação Scan	Líder tinha 19 anos, 9 eram menores de idade.	63 pessoas presas

Figura 10:Quadro cronológico de ações da Polícia Federal

Fonte: DPF, in: http://www.dpf.gov.br/ (modificação nossa).

No âmbito internacional existem autoridades igualmente respeitadas. Elas trabalham em parceria com entidades brasileiras na coleta,prevenção, e divulgação dos cybers crimes.Entre as principais parceiras podemos citar:

O **APWG** (Anti-Phishing Working Group) surgiu em novembro de 2003.Representa um grupo internacional formado por mais de 2600 membros, 1600 empresas, grandes instituições bancárias e empresas de tecnologia focadas na eliminação de fraudes e roubo de identidades resultantes de técnicas fraudulentas como phishing, pharming ,spywares, falsificação de e-mail (email spoofing) e outras atividades semelhantes. Oferece um cenário balanceado sobre perspectivas atuais e futuras das fraudes na Internet. Tem como endereço virtual a Home Page: http://www.antiphishing.org/. (APWG[1], 2007)

O ***FIRST*** (Forum of Incident Response and Security Teams) surgiu em 1990 após a crescente onda de vírus no final dos anos 80. Seus participantes buscam resolver continuamente falhas de seguranças relacionadas a ataques além de corrigir vulnerabilidades de segurança que afetam redes e computadores interligados pela internet. Além disso, Reúne uma grande variedade de incidentes de segurança além de “response teams” analisando produtos de segurança destinado a setores governamentais, comerciais e acadêmicos. Tem como endereço virtual a Home Page: http://www.first.org/. (FIRST[16], 2007)

O Honeynet Project é uma outra organização voltada para a segurança da internet. Fundada em 1999, exerce um trabalho voluntário dedicado a melhorar a segurança da Internet, sem qualquer custo para o público. Dentre os principais trabalhos, destaca-se a identificação e o relato das ameaças e vulnerabilidades existentes atualmente na internet. Através disso, busca conscientizar usuários e empresas sobre medidas básicas que podem ser tomadas para atenuar estas ameaças. Tem um endereço virtual, a Home Page: http://honeynet.org. (HONEYNET[21], 2007).

Enquanto leis específicas que combatem a criminalidade cibernética não são aprovadas em caráter final no Brasil,o usuário deve se precaver se mantendo bem informado.As autoridades citadas, demonstram ser um importante aliado, uma vez que disponibilizam grande variedade de informações e serviços na identificação e punição ao crime virtual no Brasil e no mundo.Informação é sempre um facilitador para que ,cada vez mais usuários, exerçam sua parcela de contribuição no combate aos fraudadores e suas armadilhas presentes na internet.

Capítulo 3 – Principais Técnicas fraudulentas

Neste capítulo abordaremos as principais técnicas utilizadas pelos fraudadores para a disseminação das fraudes na internet. Os golpes envolvendo a internet estão em constante evolução. Isto é constatado pela criatividade e flexibilidade dos fraudadores, o envolvimento de inúmeras empresas e serviços, conteúdo atual e bastante diversificado das mensagens.

Segundo a (SYMANTEC[39], 2007, p. 02):

> *“Os atacantes migraram de ataques feitos com o intuito de simplesmente perturbar o usuário ou de outros com finalidade destrutiva para ataques motivados por ganho financeiro. Os atacantes de hoje estão cada vez mais sofisticados e organizados e começaram a adotar métodos similares às práticas tradicionalmente usadas no desenvolvimento de softwares”.*

À medida que novas tecnologias de segurança são implementadas e divulgadas buscando uma eficiente proteção dos computadores de usuários e empresas, os golpistas rapidamente adaptam novas técnicas e estratégias para burlar tais medidas.

Os criminosos, principalmente, procuram explorar falhas de segurança em softwares aliada à ingenuidade dos usuários com relação aos e-mails recebidos e a execução de programas sem o conhecimento da origem.

Segundo (ROCHA[32], 2004):

> *"Os fraudadores vêm observando a utilização de novos artifícios para disseminação dessas fraudes. Existe uma tendência de novas fraudes que exijam menor interação por parte do usuário, explorando diretamente vulnerabilidades do browser ou leitor de e-mail, por exemplo".*

Dentre as principais armadilhas usadas pelos fraudadores podemos destacar:

- Engenharia Social: ligações telefônicas, usando para obter os dados do usuário (número da conta, senha, etc);

- Spywares: programas que recolhe informações sobre o usuário, sobre os seus costumes na Internet e transmite essa informação a uma entidade externa na Internet, sem o seu conhecimento nem o seu consentimento. Por outro lado, muitos vírus transportam spywares, que visam roubar certos dados confidenciais dos usuários.

- Phishing Scam: Representa o método mais utilizado. O usuário recebe e-mails falsos de empresas tentando convencê-lo a acessar determinada URL, onde posteriormente é redirecionado a uma página falsa solicitando dados confidenciais, como: número da conta, senha de acesso, senha do cartão , entre outras informações sigilosas

- Utiliza o nome de empresas conhecidas para tornar confiáveis as páginas falsas utilizadas e e-mails enviados para coleta dos dados. Podemos citar como exemplo : www.meubanco.gov.br é o site original,

enquanto e www.meubanco.br é o site fraudulento. Os e-mails das empresas também são alvos das falsificações.Enquanto o e-mail original do banco pode ser sac@meubanco.gov.br e o e-mail falso pode ser sac@meubanco.br .

- Pharming: Representa a “contaminação” do servidor de nomes (DNS).O usuário ao tentar acessar a página do seu banco é automaticamente redirecionando a uma página falsa, semelhante à página original do Banco, de onde o fraudador busca capturar seus dados sigilosos, tais como: número da conta, senha de acesso, senha do cartão, entre outras informações.

Podemos representar as técnicas e sua relação com os golpes virtuais na figura a seguir:

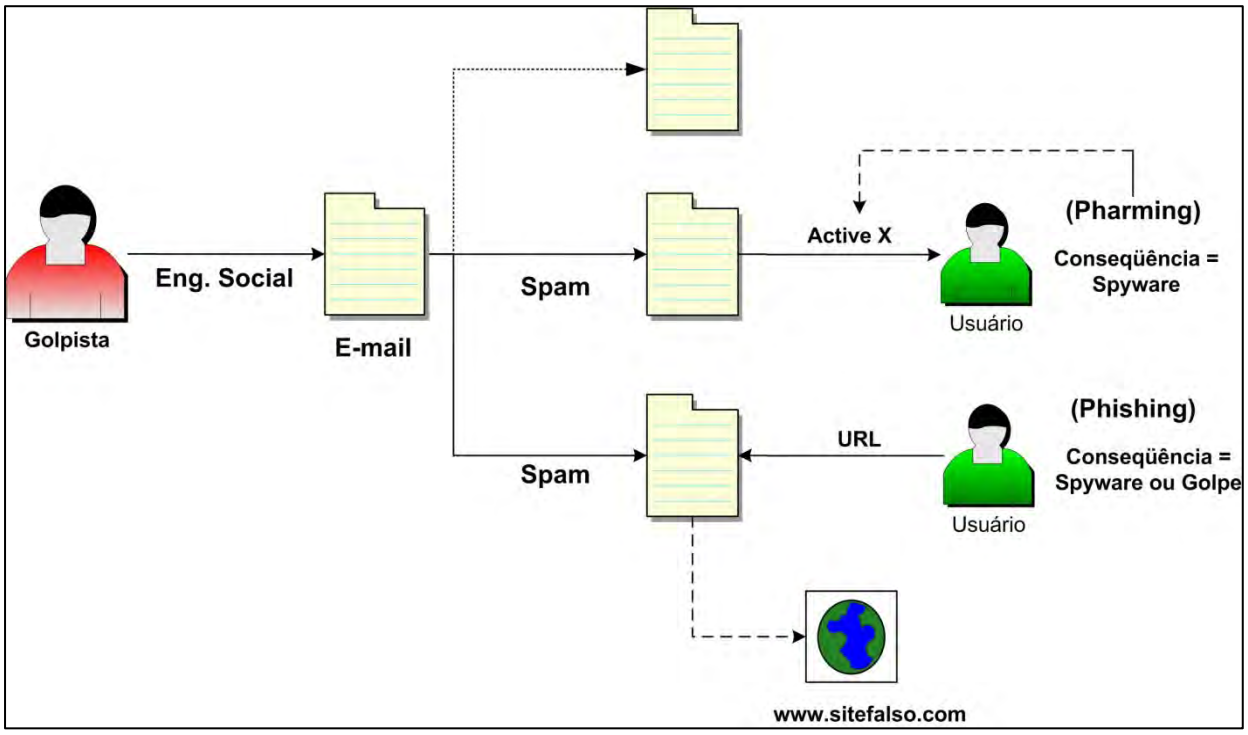

Figura 11: Esquema Técnico das Fraudes

Fonte: Autoria Nossa, 2007.

3.1 Engenharia Social

3.1.1 O que é Engenharia Social?

A engenharia social é uma técnica onde o fraudador explora a ingenuidade ou confiança do usuário, apresentando estórias e situações que o levam a fornecer dados sigilosos, posteriormente usados para se obter acesso não autorizado a computadores ou informações. As técnicas de engenharia social podem ser usadas em contatos pessoais, por telefone, e-mail, mensagens instantâneas ou chats.

Segundo (MITNICK[25], 2003, p.06):

> *"A engenharia social usa a influência e a persuasão para enganar as pessoas e convencê-las de que o engenheiro social é alguém que na verdade ele não e, ou pela manipulação. Como resultado, o engenheiro social pode aproveitar-se das pessoas para obter as informações com ou sem o uso da tecnologia".*

A Engenharia Social trata o elemento humano dentro de um ciclo de segurança como o elo mais vulnerável pois possui traços comportamentais e psicológicos que o torna susceptível a ataques de um engenheiro social,dentre destes traços podemos destacar:

- Vontade de ser útil - o ser humano comumente procura agir com cortesia bem como ajudar outros quando necessário.
- Busca por novas amizades - o ser humano costuma se agradar e sentir-se bem quando elogiado, ficando mais vulnerável a fornecer informações.
- Persuasão – compreende quase uma arte a capacidade de persuadir pessoas,onde se busca obter respostas específicas.

3.1.2 Como funciona?

Podemos então, traçar uma seqüência lógica explorada pelo engenheiro social para a realização de ataques utilizando fatores acima citados.

- Construção de um relacionamento;
- Desenvolvimento de um relacionamento para coleta de dados: O fraudador ou engenheiro social busca obter informações sigilosas dos usuários como, data de nascimento, RG, CPF, nome dos pais, senhas de cartões de crédito, dados de conta bancária entre outras;
- Execução do Ataque: De posse das informações obtidas é realizado o ataque ao usuário ou empresa.

As diversas formas de ataque da engenharia social estão presentes no cotidiano de usuários e empresas por meio de telefones de supostos bancos, serviços de telefonia, provedores de internet onde por trás da ligação pode estar uma pessoa mal intencionada visando colher informações preciosas das vítimas. Porém sem dúvida, a forma mais eficiente e destrutiva de ataque da engenharia social é feita através do e-mail, contribuindo para o aumento das fraudes on-line.

As fraudes pela internet não é uma ferramenta exclusiva do engenheiro social. Existem outras técnicas não menos eficazes e muitas vezes, mais sofisticadas e populares entre os fraudadores .Temos que reconhecer como nunca antes que o mundo é um lugar perigoso. Afinal de contas, a civilização é apenas um verniz superficial.

3.2 Spyware

3.2.1 Definição.

Caso o micro começe a freqüentemente apresentar panes, baixo desempenho, anúncios aparecendo constantemente enquanto navega na internet, é possível que você tenha sido vítima de spywares,um termo genérico usado para designar softwares que realizam atividades ,muitas vezes sem o consentimento do usuário, de anúncios, alterações na configuração do computador e coleta de informações pessoais.

Segundo (HONEYCUTT[20], 2004) Spyware é:

> *"Um software que envia suas informações pessoais para um terceiro, sem sua permissão ou conhecimento. Isso pode incluir informações sobre Web-sites que você visita ou algo mais sensível, como seu nome de usuário e senha. Em geral, as empresas inescrupulosas usam esses dados para lhe enviar anúncios direcionados e não-solicitados."*

3.2.1 Características

O objetivo do spyware é permanecer despercebido, ocultando-se ativamente ou simplesmente não se fazendo notar em um sistema conhecido pelo usuário.Spywares ou programas espiões podem entrar em seu sistema de vários métodos, dentre os mais comuns podemos destacar:

- O usuário é enganado, para que clique em um link que faz a instalação. Os links para estes programas comumente estão disfarçados. Por exemplo, um site que esteja tentando instalar o spyware no seu computador pode abrir uma janela dizendo que seu micro pode estar infectado com vírus e spyware , ao clicar ele engana o usuário e instala o spyware;

- Muitos freewares distribuídos na internet instalam um spyware, porém , é

importante frisar que nem todos os programas gratuitos contêm arquivos espiões ou publicitário. O usuário, ao instalar um programa gratuito de Peer-to-Peer (P2P), por exemplo, instala um spyware ocultamente no seu computador.

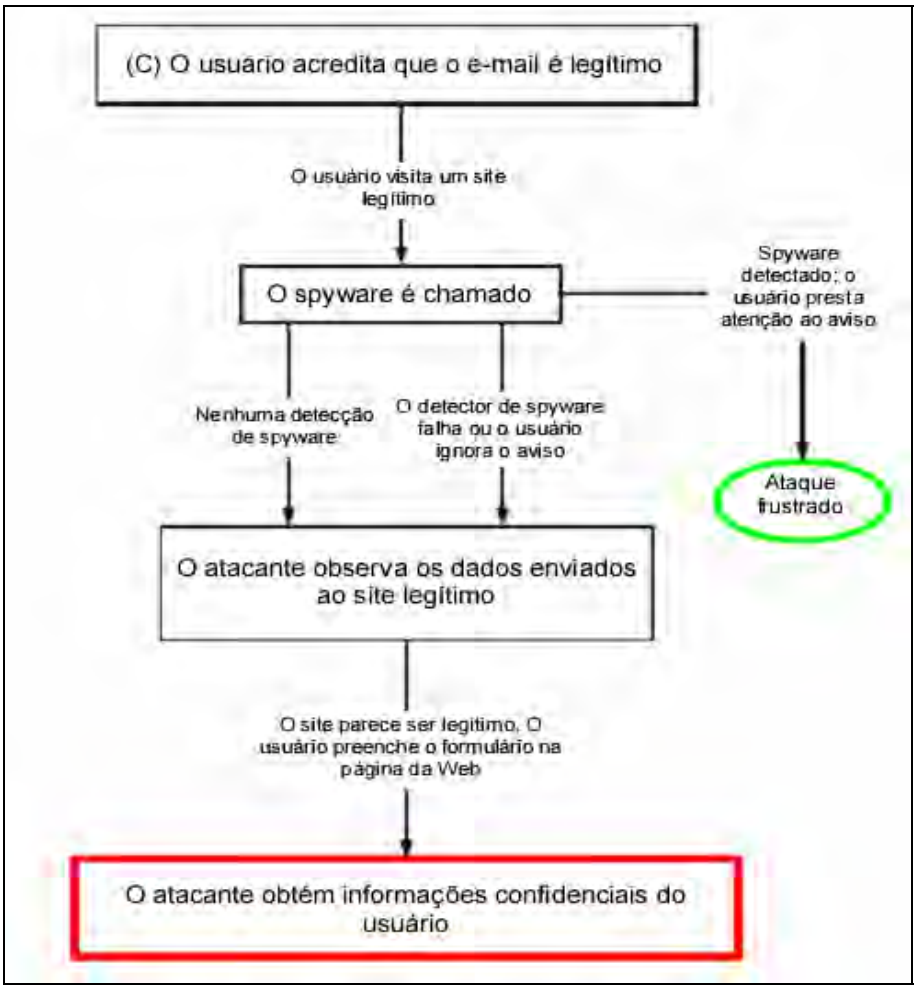

Figura 12: O Spyware é usado para extrair informações dos usuários

*Fonte:*http://www.nai.cl/es/partners/literature/wp_antiphishing_inst&consbp.pdf

Os spywares representam outra munição muito utilizada pelos fraudadores que nunca deve ser descartada.Muitos destes softwares espiões trabalham em conjunto com vírus e softwares de exibição de anúncios (chamado adware) buscando aplicar golpes na internet através do roubo de dados bancários, senhas pessoais, montam e enviam logs das atividades do usuário, roubam determinados arquivos ou outros documentos pessoais.

3.3 Phishing Scam

3.3.1 O que é Phishing Scam?

A técnica do phishing scam é umas das mais populares relacionadas às fraudes on-line. Phishing, na verdade é uma analogia ao termo “fishing”(Pescaria ou pesca). Scam significa falcatrua, embuste ou golpe.

Segundo a Cert.Br[4] (2005, p.05):

> *“Phishing, também conhecido como phishing scam ou phishing/scam, foi um termo originalmente criado para descrever o tipo de fraude que se dá através do envio de mensagem não solicitada, que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou site popular, e que procura induzir o acesso a páginas fraudulentas (falsificadas), projetadas para furtar dados pessoais e financeiros de usuários”.*

Nessa técnica e-mails são usados como “iscas” para “pescar” senhas e informações confidencias dos usuários na internet.

3.3.2 Como Funciona?

Para que o golpe funcione, o fraudador envia milhões de e-mails falsos que parecem vir de empresas e sites conhecidos, como sua empresa de telefonia, seu banco entre outras. Os sites e e-mails enviados são bastante fiéis aos originais levando os usuários a crer na sua legitimidade. Internautas mal informados acreditando que esses emails são legítimos, preenchem as solicitações com suas informações pessoais: nome completo, CPF, senhas e números de cartão de crédito entre outras.

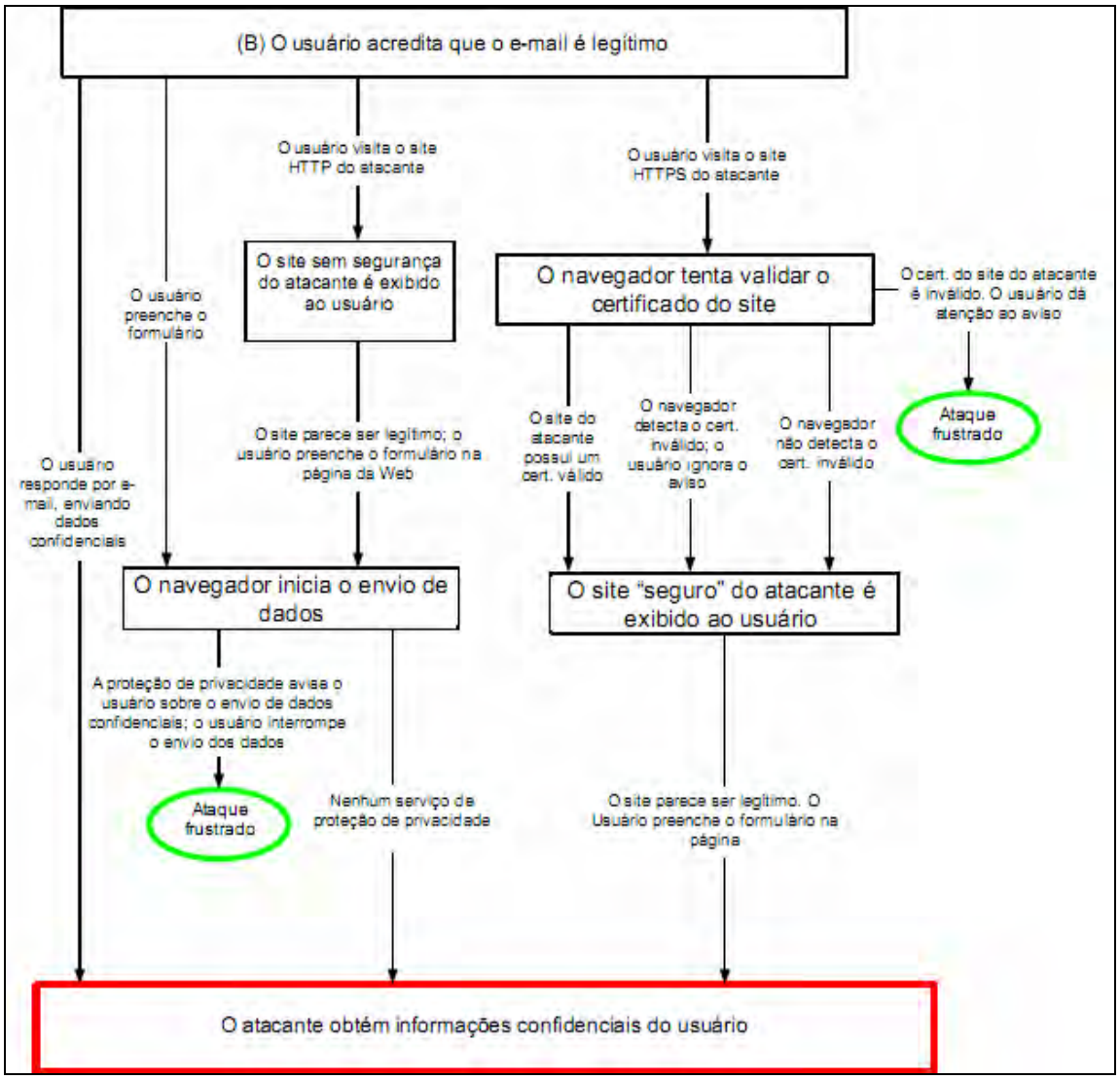

Figura 13: Estrutura de ataque do phishing

*Fonte:*http://www.nai.cl/es/partners/literature/wp_antiphishing_inst&consbp.pdf

A técnica de phishing é uma técnica em constante evolução obrigando o usuário a se manter informado através dos meios de comunicação em massa, como televisão, revistas, jornais e sites especializados sobre os diferentes tipos que vêm sendo utilizados pelos fraudadores.Segundo D'Ávila[9] (2007) podemos observar que existem inúmeras variantes para as situações apresentadas, dentre as quais podemos destacar:

- Cartões & Mensagens

"Você recebeu um cartão postal virtual", "um segredinho de amor", ou similar; e bastaria clicar no link para "visualizar a mensagem", isto é, na verdade receber o trojan. Esta é uma das fraudes mais comuns para levar ao download e execução de um programa malicioso. Com aparências que vão do grosseiro à imitação bem feita, fingindo ser originado de um serviço de cartões virtuais realmente existente ou muitas vezes nem isso, as variações são muitas.

Figura 14: Fraudes com mensagens e cartões virtuais são bastante comuns.

Fonte: D`Ávila, in: http://www.mhavila.com.br/topicos/seguranca/scam.html

- Informações Dramáticas ,Traição, Tragédias.

"Mensagens do tipo: Você está sendo traído!" "Osama Bin Laden foi preso!" Clicando no link fornecido na mensagem você veria "as imagens" em primeira mão; na verdade, daria uma mão ao malfeitor para instalar o trojan.Outro tipo de fraude nesta categoria é de mensagens de amor ou reencontro de alguém do passado, com um link para "ver fotos" desse falso alguém.

Figura 15: Tragédias, fotos de traição atraem a atenção de muita gente.

Fonte: D`Ávila, in: http://www.mhavila.com.br/topicos/seguranca/scam.html

- Sorteios , Solidariedade e prêmios.

Você é uma pessoa de sorte. Foi sorteada para um prêmio fabuloso ou convidada a participar de uma promoção incrível. E o seu e-mail foi "selecionado", junto com mais alguns milhões de outros, em uma lista de spam. Mensagens deste tipo instrui o usuário a clicar no link para preencher o "formulário eletrônico", mas na verdade seria para assinar um verdadeiro atestado de ingenuidade ao baixar e executar um programa malicioso.

Além das campanhas promocionais e de concursos, existem fraudes que apelam até para o tema de campanhas de solidariedade, como as que citam o Click Fome e a AACD. Ambas as instituições divulgaram alertas sobre a fraude em seus endereços na web.

Figura 16: Golpes envolvendo sorteios, prêmios são comuns na web.
Fonte: D`Ávila, in: http://www.mhavila.com.br/topicos/seguranca/scam.html

- Pendências Financeiras e cadastrais

Temas financeiros e cadastrais também são constantes nas fraudes: pendências de CPF, título eleitoral e de crédito, avisos de pagamentos, débitos e cobranças, transações de comércio eletrônico, orçamentos.

Por exemplo: "o seu CPF consta no Serasa", ou "foi cancelado pela Receita Federal". Misteriosamente, estas entidades descobriram o seu e-mail. E ainda escolheram o inseguro correio eletrônico como forma de notificá-lo de uma situação tão séria. O link supostamente levaria ao download de um

“relatório com detalhes e instruções para você regularizar sua situação” ou similar.

Outro tipo de phishing que se enquadra aqui é o de falso aviso de débito para um suposto pedido de compra on-line. O objetivo é igualmente alarmar o destinatário, neste caso sobre um possível débito indevido, levando-o a clicar em um link como “mais informações sobre o pedido/débito” para download do programa malicioso.

Fraudes com tema similar oferecem o download de um programa gratuito como “cadastro de clientes com consulta a SPC, Serasa, CCF”, “licitações eletrônicas” entre outros.

Figura 17: Bancos e empresa de telefonia são alvos constantes de fraudes.
Fonte: D`Ávila, in: http://www.mhavila.com.br/topicos/seguranca/scam.html

Cabe ressaltar que a lista de assuntos acima relacionados não é ampla,nem tampouco se aplica a todos os casos. Existem outros assuntos e novos temas podem surgir com a criatividade dos golpistas e velocidade da internet.O phishing é uma das técnicas mais utilizadas pelos fraudadores e sua diversidade de assuntos e empresas envolvidas apenas ratifica essa tendência.

Segundo TERZIAN[41] (2006) quase 8 milhões de e-mails de phishing são disparados para usuários de todo o mundo, em especial do Brasil e dos Estados Unidos.No primeiro semestre de 2005, a média diária era de 5,7 milhões de tentativas.Nota-se que o phishing não utiliza mecanismos de alta tecnologia para obter sucesso.Na verdade, o golpe se realiza com a ajuda e a cumplicidade da

vítima que, ingenuamente e muitas vezes mal informada, clica nos links suspeitos, transmite informações sigilosos para os golpistas

3.4 Pharming

3.4.1 O que é Significa Pharming?

Pharming é uma nova nomeclatura para designar um tipo de ataque conhecido no passado, que visava em modificar a relação que existe entre o endereço eletrônico de um site e seu servidor web correspondente.

O termo surgiu em analogia à "*farming*" um termo utilizado na indústria farmacêutica e agrícola, que trata da modificação genética de hospedeiros para incrementar a produção de drogas medicinais.SIMON[36], 2007 afirma que o nome do ataque surge da semelhança com a técnica desenvolvida, pois também se modifica o "hospedeiro" que detém informação para o funcionamento da rede. Os referidos "hospedeiros" se chamam Servidores de Nome de Domínio ou DNS.

Normalmente, o Pharming está relacionado a outras técnicas maliciosas.Pode haver desde a instalação de spywares para propaganda e publicidade nocivas, como também a junção com a técnica de phishing redirecionando para um de um site bancário falso como o objetivo de roubar os dados da vítima. Para Pereira [30](2007, p.26), o pharming é:

> *"(...) uma variante mais sofisticada de Phishing que explora vulnerabilidades dos browsers, dos sistemas operativos e dos servidores de DNS (Domain Name System) para conseguir conduzir os utilizadores a site s fictícios com o objetivo de obter os códigos de acesso".*

3.4.2 Como funciona o Ataque?

O ataque em servidores DNS explora as falhas de segurança, programação ou má configuração, que permitem "envenenar" a memória temporária (cache) do sistema atacado. Assim o intruso consegue manipular e alterar algumas configurações no servidor, atribuindo “nomes de domínio” a IP’s forjados e que são controlados pelo invasor. Por exemplo,o endereço IP associado ao domínio www.minhaempresa.com.br poderia ser alterado de 200.222.23.173 (IP legítimo) para 209.100.111.90 (IP falso) num servidor DNS atacado e ,conseqüentemente, quando o usuário digitasse no seu browser www.minhaempresa.com.br este seria redirecionado para a página forjada criada pelo golpista.

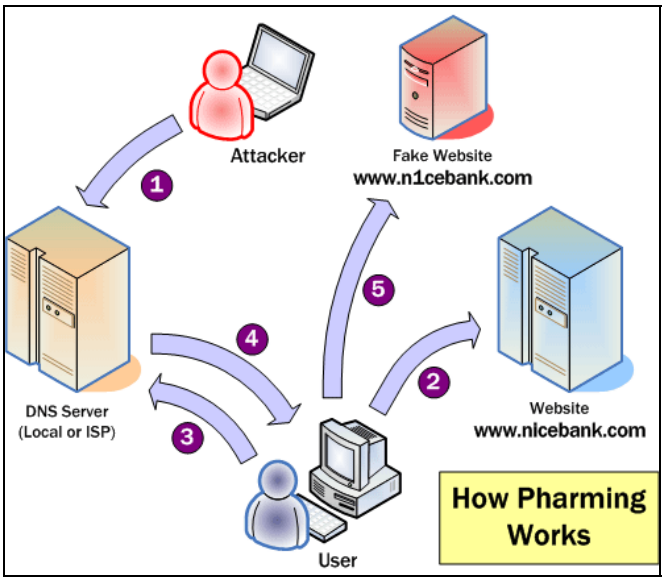

Figura 18: Esquema de Pharming

Fonte:http://palisade.plynt.com/issues/2006Mar/pharming/

A nível de usuários as invasões se dão no computador da vítima fazendo modificações no arquivo “*hosts*”. O Arquivo “hosts” está presente na maioria das versões do MS Windows e outros sistemas operacionais , Inclui uma relação de nomes de sites associados a determinadas URLs. Se estas URLs forem alteradas, o micro do usuário pode redirecioná-lo para um site falso sempre que o endereço de um site legítimo presente no arquivo for

digitado no browser .

Este tipo de ataque atualmente não preocupa tanto como o phishing. Depois de grandes investimentos das instituições financeiras e provedores de internet devido aos prejuízos no setor financeiro entre 2002 e 2003 conseguiram uma melhor gerência e respostas aos ataques. A partir de 2004, percebeu-se no cenário brasileiro uma queda brusca nas estatísticas de pharming.Porém, o internauta deve permanecer em alerta,principalmente ao baixar e instalar softwares e clicar em links desconhecidos para não correr o risco de ser mais uma vítima do pharming.

Atualmente o portfólio de ameaças está mais dinâmico e convergente que nunca.Os fraudadores são flexíveis, criativos , bem informados e adaptáveis a novas situações, por isso novos golpes surgem a cada dia, se ajustando e desfrutando cada nova oportunidade.

Capítulo 4 – Guia de Procedimentos Antifraudes

Conforme os ataques convergem e se tornam mais complexos do que antes, é importante fornecer proteção completa para computadores e redes das empresas. No passado, grupos diferentes eram freqüentemente responsáveis por vários aspectos de um esquema de segurança das empresas: proteção de desktop, servidores, redes, antivírus, anti-spam entre outros.Atualmente o ambiente digital exige uma convergência de esforços entre empresas e usuários.

As empresas devem estabelecer políticas corporativas, aprimorar a autenticação nos sites, monitorarem a internet em busca de sites fraudados, implementarem soluções de segurança de boa qualidade ,ou seja, fornecer um “pool” de medidas visando reduzir a vulnerabilidade do consumidor.O usuário, neste cenário, representa o ponto chave.O usuário precisa se manter sempre atualizado, seguir procedimentos que minimizem o risco de serem alvos em potencial dos

crimes no ambiente virtual.

4.1.Como identificar a Confiabilidade de um site?

As aparências enganam e na Internet esse ditado é ainda mais verdadeiro. Com um pouco de conhecimento técnico, um microcomputador, programas gráficos e muita criatividade,golpistas oferecem serviços e produtos mascarados em sites de aparência profissional normalmente envolvendo empresas conhecidas e idôneas.

Podemos destacar um conjunto de procedimentos que buscam verificar a confiabilidade de um site e ,conseqüentemente auxiliar internautas e empresas a se precaverem dos golpes aplicados na web:

1) Verifique se o endereço eletrônico (URL) digitado permanece inalterado no momento em que o conteúdo do site é apresentado no navegador do usuário.

2) Acostume-se a observar também os links em que você clica e os endereços que aparecem na barra de status e de endereços do seu navegador. Lembre-se que, assim como os e-mails, é possível disfarçar uma página ou URL dentro que qualquer link.

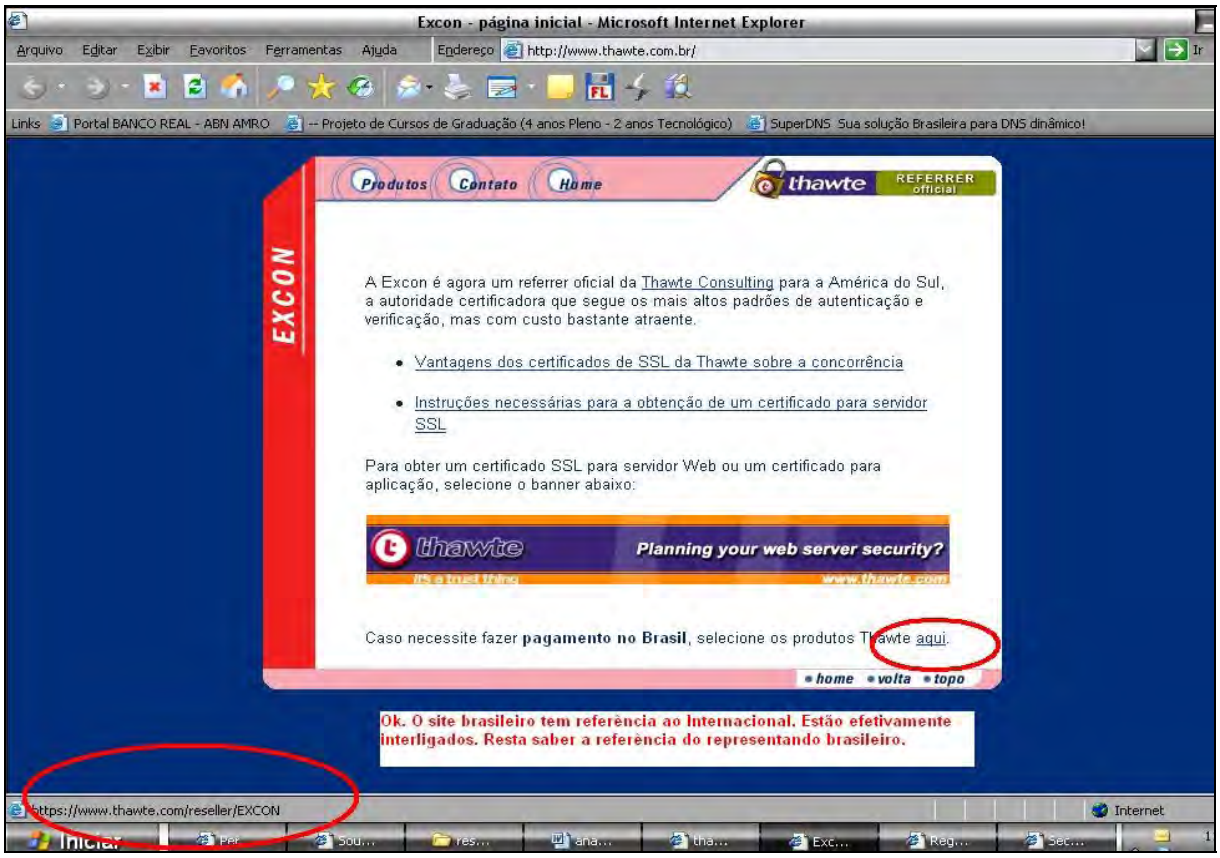

Figura 19: Observe os links e URL apresentados no site.

Fonte : Nogueira (2007)

3) Confirme o CNPJ da empresa vendedora no site da Receita Federal (http://www.receira.fazenda.gov.br).Se houver qualquer informação diferente da ficha cadastral da Receita, desconfie. Um endereço diferente indica que é um CNPJ falso. Qualquer depósito que tenha que ser feito deve constar a razão social da empresa; e caso peçam para fazer em outro nome, não faça.

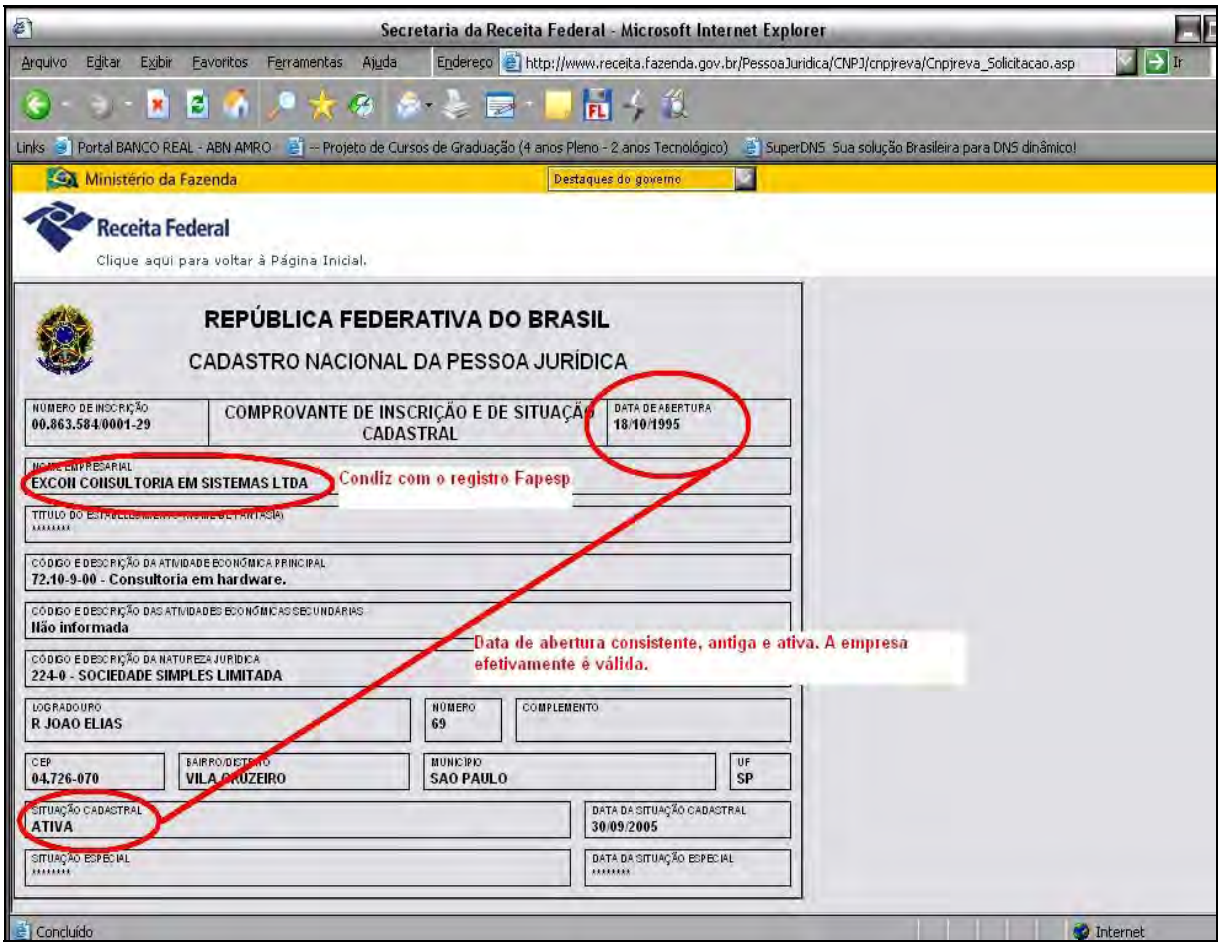

Figura 20: O site da receita disponibiliza informações sobre a situação atual da empresa.

Fonte : Nogueira (2007)

4) Observe algumas informações contidas no certificado como endereço do site, nome da instituição, prazo de validade. Além disso o internauta deve analisar se as informações apresentadas correspondem as da instituição que você realmente deseja acessar.

5) Cuidado com sites hospedados em provedores gratuitos, não há garantias de veracidade das informações. Empresas legítimas não hospedam seus sites em serviços gratuitos, pois, geralmente possuem seu próprio domínio. Caso “os domínios sejam próprios e terminados em “**.**br”, acostume-se a procurar as informações sobre os responsáveis nos sites do Registro.Br (http://registro.br) e da Receita Federal. Se forem domínios internacionais(.com,.net entre outros), há menores chances de confrontar os dados, mas você ainda poderá utilizar serviços na internet

para fazer diversas pesquisas sobre os sites, incluindo sua titularidade.

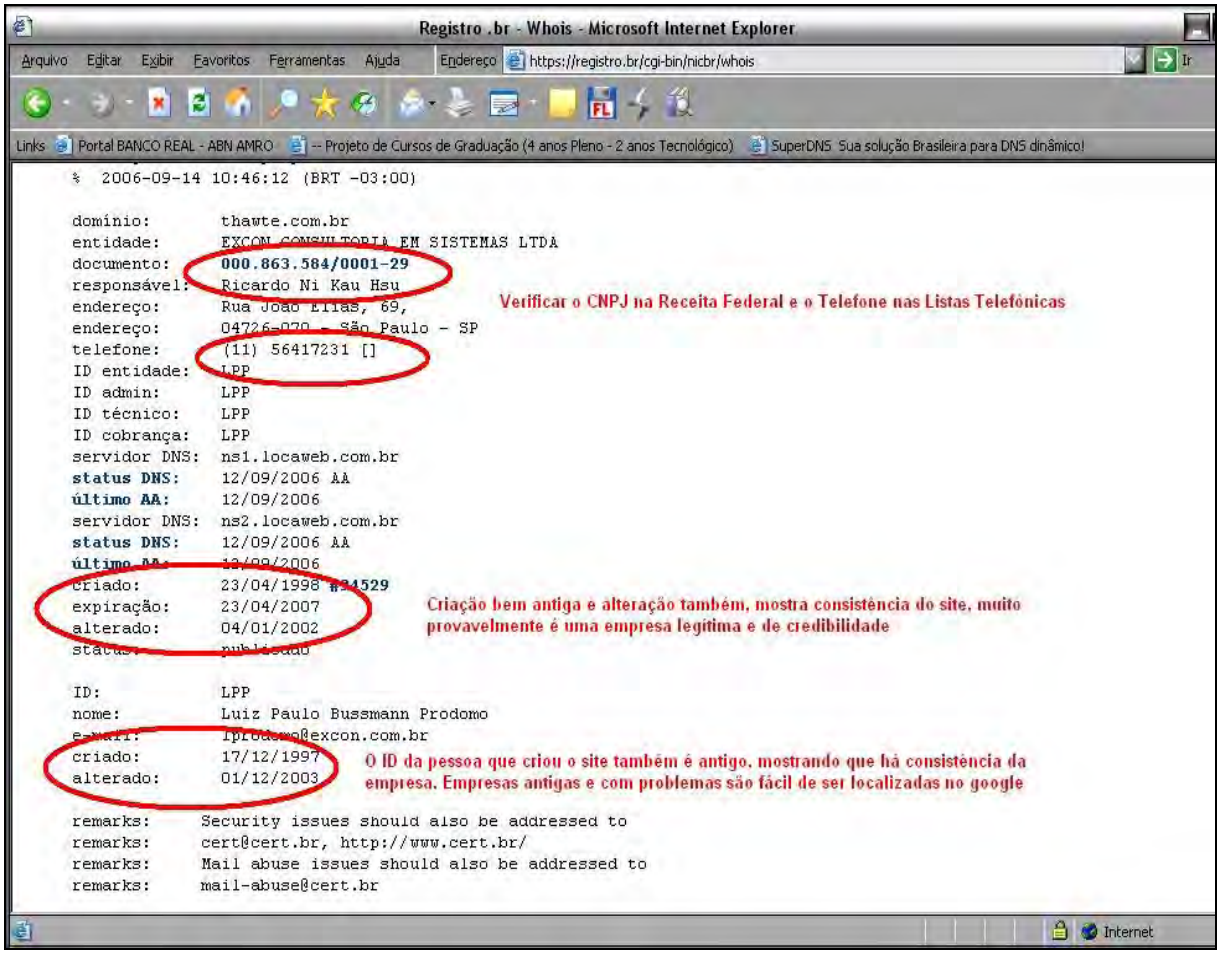

Figura 21:Informações disponibilizadas pelo registro.br.

Fonte : Nogueira (2007)

6) Pesquise no site dos correios (http://www.correios.gov.br), o CEP da empresa para ratificar seu endereço.Além disso é recomendável confrontar se endereço fornecido na receita federal (Cadastro de CNPJ) coincide com o endereço fornecido pelos correios.Dados discordantes são sinais de possíveis golpes.

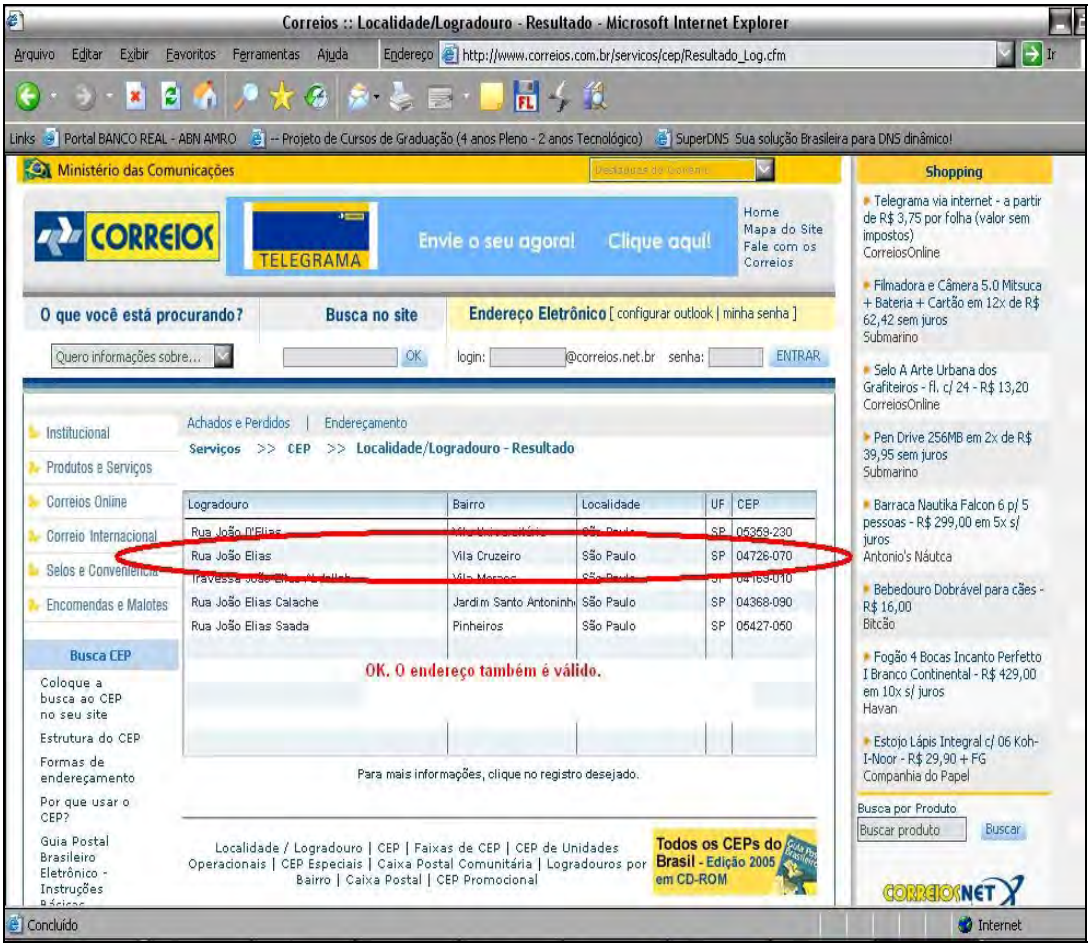

Figura 22: No site dos correios é possível verificar a veracidade do Endereço.

Fonte : Nogueira (2007)

7) Assim como o CEP, consultar um telefone da empresa em sites como *TeleLista.Net* (http://www.telelistas.net) e *ListaOnline* (http://www.listaonline.com.br) deve ser levado em consideração para assegurar ainda mais a confiabilidade do site.Sites de empresas legítimas, sempre disponibilizam algum telefone de contato para atender o consumidor. É comum encontrar sites fraudados a afirmação de que a o serviço ou promoção só é válida pela Internet, numa tentativa de evitar que o internauta entre em contato com a empresa real e descubra que o site é falso.

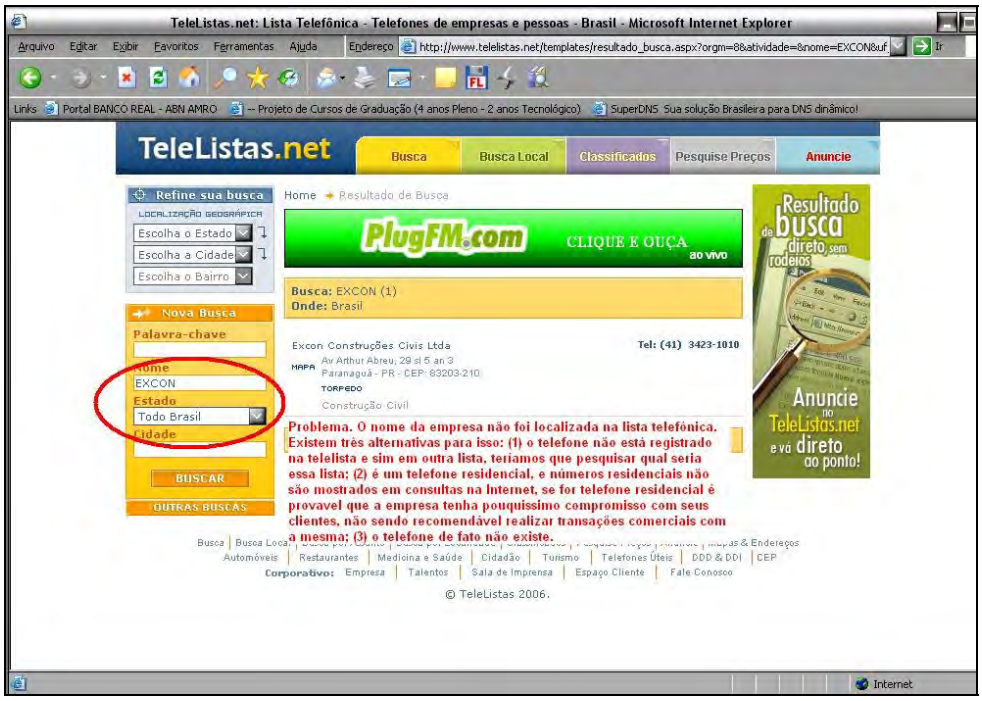

Figura 23: É importante verificar se a empresa possui telefone fixo válido.

Fonte : Nogueira (2007)

8) Pesquise em sites de busca informações importantes que atestam confiabilidade como: recomendações positivas, portfólio de clientes, reclamações de serviços relacionados à empresa analisada.

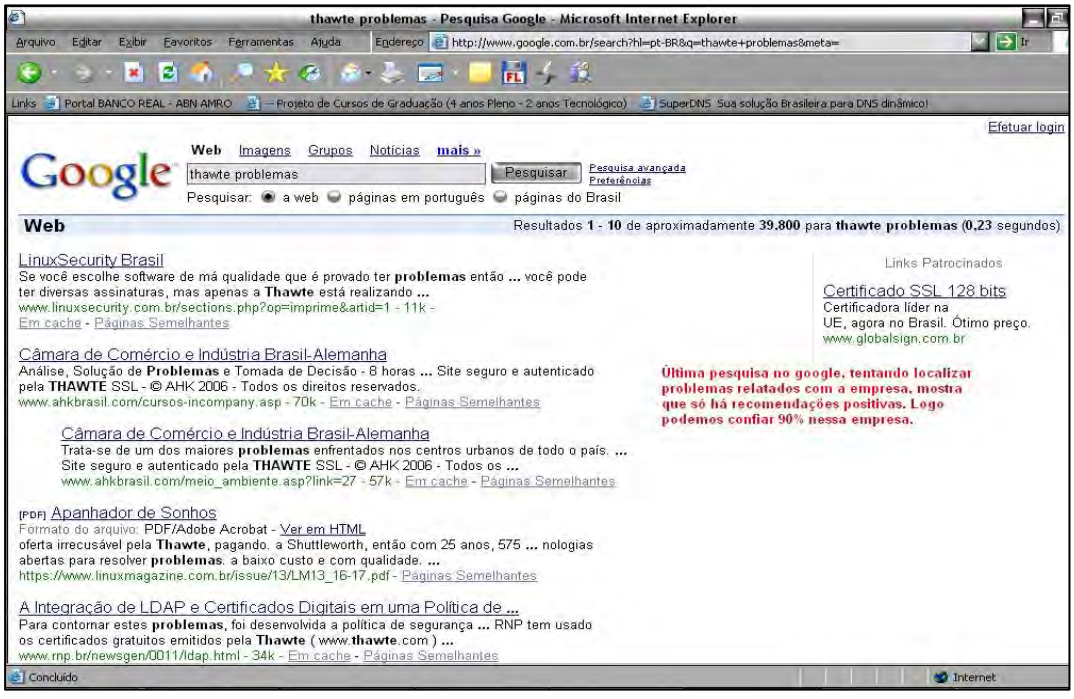

Figura 24: Sites de busca são ótimos para pesquisar qualificações ou problemas.

Fonte : Nogueira (2007)

9) Procure nos sites por erros de português e textos fora de formatação É muito comum encontrar erros grosseiros de português e texto com formatação estranha. Sites de empresas idôneas tomam cuidado para enviar textos bem escritos e formatados.

Identificar se um site é confiável é uma tarefa trabalhosa, que exige tempo e conhecimento. Tomando esses cuidados, é possível ficar mais seguro, minimizar as chances de ser enganado por um site falso e outras armadilhas digitais que surgem todos os dias.

4.2. Como verificar a segurança da Conexão?

Quando no referimos a serviços on-line que envolve transações financeiras (bancos , e-commerce) segurança é uma questão primordial. Sem segurança ,sites não fecham negócios.Ninguém ,em sã consciência, vai digitar seu número do cartão de crédito, senha bancária em qualquer site.Por esse motivo, site com conexão segura (Criptografia) é usada por lojas virtuais, operadoras de cartões de crédito e bancos como forma de garantir a seus clientes que os dados fornecidos são confidenciais.

O princípio de funcionamento de um site seguro é simples: os dados digitados pelo cliente no seu browser, são criptografados e transmitidos para o servidor. Apenas o servidor, que sabe como os dados foram criptografados, pode decodificar e ler as informações. A criptografia é fornecida através de um documento que o site fornece, denominado certificado digital.

Podemos identificar alguns aspectos de sites com conexão segura, auxiliando, desta forma, usuários a se certificarem da confidencialidade de suas informações:

- Em uma conexão segura,o endereço eletrônico (URL) no browser deve começar com ***https://*** (diferente do http:// presente nas conexões normais).O ***s*** adicionado ao http significa http seguro, os dados serão transmitidos através de uma conexão criptografada. Além disso, alguns browsers podem mudar a cor na barra de endereço do site.

Figura 25: https – Indício da existência de uma conexão segura.

Fonte : Cert.br,in:http://cartilha.cert.br/download/cartilha-04-fraudes.pdf (Modificação nossa)

- Nos browsers mais recentes, as conexões seguras são identificadas por uma imagem de **cadeado fechado**, apresentado na barra de status, na parte inferior da janela do navegador.Se o cadeado estiver aberto, a conexão não é segura.

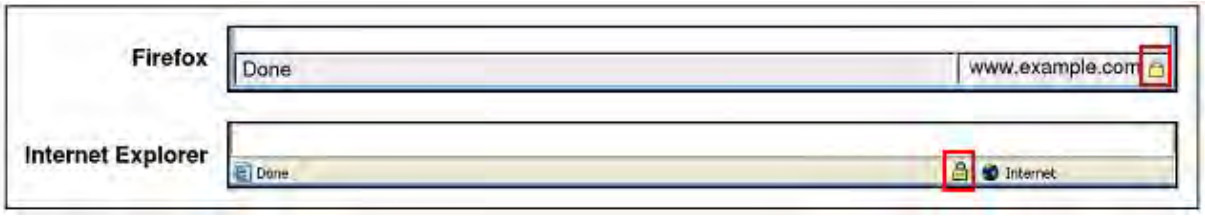

Figura 26: O cadeado fechado atesta que o site possui uma conexão segura.

Fonte : Cert.br,in:http://cartilha.cert.br/download/cartilha-04-fraudes.pdf (Modificação nossa)

- Outro ponto importante é clicar sobre o cadeado fechado, localizado na barra status do navegador para acessar as informações referentes ao certificado do site. Uma nova janela se abrirá às informações referentes a identidade do proprietário, endereço do site, tamanho da chave utilizada para criptografar os dados entre outras informações necessários para que assegura se a conexão é segura ou não.

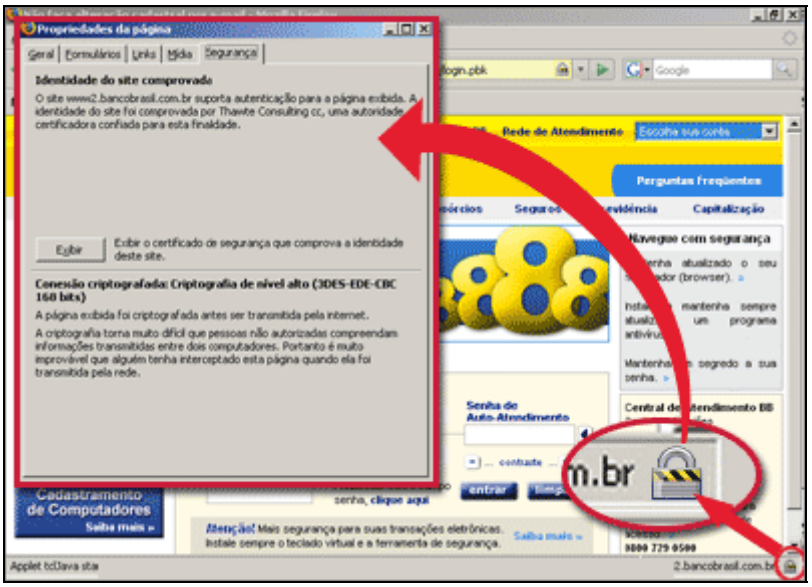

Figura 27: Clique no cadeado fechado para exibir o certificado de segurança.

Fonte:AcessaSP, in:http://www.acessasp.sp.gov.br/cadernos/Cadernos_Eletronicos_arquivos/PDFs/caderno08.pdf

A conexão segura (criptografada) não é uma garantia que o site é confiável. Uma conexão segura garante apenas a identidade do site, com base nas informações fornecidas pela organização de certificação. A privacidade ainda pode estar comprometida na maneira pela qual o site usa ou distribui suas informações.Portanto, é importante o usuário fornecer informações pessoais apenas para sites que você conhece e nos quais confia.

4.3. Quais os cuidados para realizar compras e acessar bancos pela internet?

O comércio eletrônico juntamente com os serviços bancários pela Internet vem crescendo rapidamente no Brasil e no mundo. Comodidade, Flexibilidade de horários, inexistência de filas estão entre os principais benéficos, porém, no outro lado da moeda a quantidade de fraudes vem crescendo assustadoramente. Realizar compras num site, acessar um internet banking não é uma tarefa trivial para a maiorias dos usuários.Desta maneira, os fraudadores focam em explorar as fragilidades do lado do usuário.

A noção de insegurança sobre o uso indevido de contas correntes também é grande entre os brasileiros. Cerca de 70% dos entrevistados declaram ter "grande" preocupação com as fraudes, enquanto 21% disseram ter preocupação "moderada". Apenas 9% dos entrevistados disseram não ter nenhum tipo de preocupação sobre o assunto.

Segundo a Unisys Corporation[42] (2005, Pág. 08):

> *"Cerca de um entre cada dez brasileiros titulares de cartões de crédito/contas bancárias já foi vítima de roubo de identidade. Ainda segundo o estudo os que conduzem transações bancárias pela Internet têm uma chance quase duas vezes maior de serem vítimas de roubo de identidade (13% em comparação com 8% dos que não conduzem operações pela Internet)."*

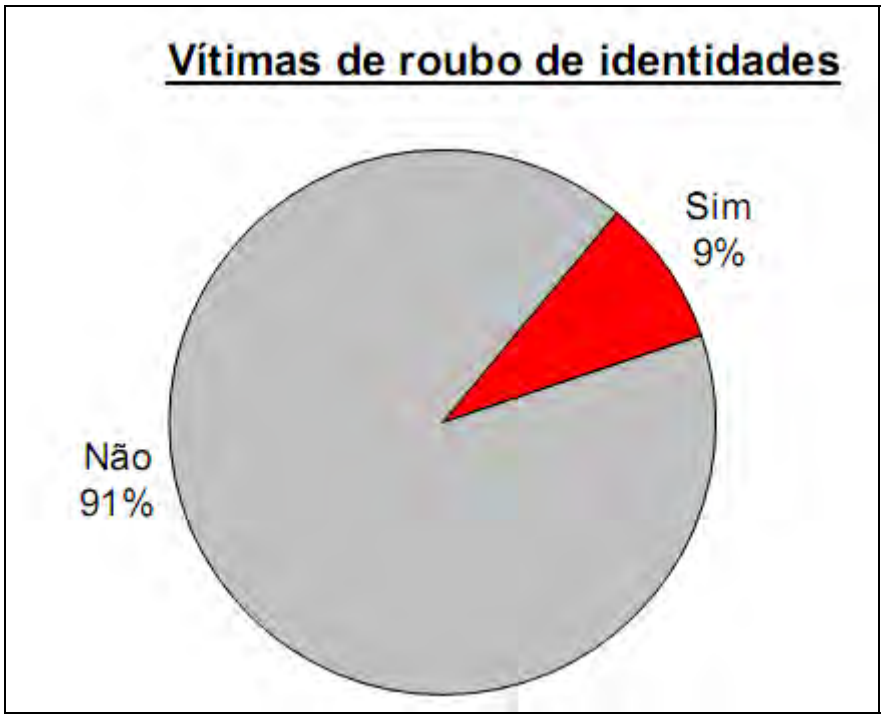

Figura 28 - Brasileiros titulares de contas correntes/cartão de crédito

Fonte: Unisys Corporation,in http://www.unisys.com.br/Identity_theft_Brazil_Port.pdf

Apesar de não ser uma tarefa simples atacar e fraudar dados em um servidor de e-commerce e instituições bancárias, os golpistas têm concentrado seus esforços na exploração de fragilidades dos usuários, para realizar fraudes comerciais e bancárias através da Internet. A FEBRABAN[14](2007), recomenda alguns cuidados

que deve ser seguidos pelos internautas ao acessar sites Internet Banking e comércio eletrônico:

- Sites de comércio eletrônico ou Internet Banking legítimos sempre utilizam conexões seguras quando solicitam informações sigilosas dos usuário.Portanto, se a página não utilizar conexão segura, desconfie imediatamente;
- Instalar e manter sempre atualizado uma suíte de aplicativos de segurança como antivírus, firewall e antispyware;
- Manter bem guardadas e seguras seus dados pessoais, principalmente senhas;
- Não executar programas obtidos pela Internet, ou recebidos por e-mail.
- Não utilizar computadores de terceiros ou procedência duvidosa;
- Nunca acessar bancos e fazer compras em locais aberto ao público como aeroportos, Lan Houses;
- Realizar compras, transações bancárias somente em sites de instituições que você considere confiáveis;
- Evitar deixar informações de cartão de crédito cadastradas nos sites de compra;
- Não fornecer detalhes de seus dados sigilosos na internet (senhas de sites, conta bancária) quando abordados por estranhos ,seja pessoalmente, telefone ou e-mail.
- Usar senhas longas e complexas, Além disso, trocá-las com freqüência;
- Verificar a existência de conexão segura (ícone cadeado fechado ou chave destacada);
- Ao acessar o site de comercio eletrônico e bancos, dedicar algum tempo a verificar a página, propagandas e dados solicitados, em busca de algo suspeito.
- Certificar-se de que o endereço eletrônico apresentado em seu browser corresponde ao site que você realmente quer acessar;
- Ficar atento aos comunicados oficiais de empresas de comercio eletrônico e bancos. Essas empresas sempre têm destacado nos seus sites, mensagens de sobre possíveis tentativas de fraude.

- Ao ser alvo de situações suspeitas (e-mails da empresa, contatos telefônicos solicitando senha ou conta bancária, erros consecutivos no acesso ao site), relate o ocorrido ao serviço de suporte ao usuário das empresas.
- Sempre manter atualizado o navegador utilizado;
- Desligar sua webcam ao acessar sites de compras e bancos;
- Solicite as empresas, bancos que envie um e-mail com todas as informações possíveis a respeito da compra ou transação efetuada;
- Analise se o domínio do e-mail coincide com o domínio do site;
- Verificar se o certificado foi emitido para a empresa ou banco que está sendo acessado e a data de validade do certificado. Recomenda-se também ficar atento às mensagens emitidas pelo seu navegador, verificando se este reconheceu a autoridade certificadora que emitiu o certificado ao site que você está acessando.
- Não descartar automaticamente as mensagens de aviso geradas pelo navegador em relação a certificados digitais e páginas criptografadas. A prática recomendada é ler atentamente tais mensagens e em caso de dúvidas interromper o processo, consultando o serviço de suporte ao usuário.
- Em sites de lojas virtuais e, principalmente, em leilões verifique as qualificações de compradores e vendedores ajudam a informar a confiabilidade da empresa.
- Prefira uma conversa por meio de um telefone fixo a um e-mail, principalmente se tratando de empresas hospedadas em provedores gratuitos que não garantem a veracidade das informações.
- Guarde os registros de suas compras e transações on-line, especialmente mensagens com confirmação de compra e entrega;
- Desconfie de preços muito abaixo dos praticados no mercado, na dúvida , não compre!
- Denuncie a empresa caso você se sinta lesado para conscientizar futuros compradores do site dos riscos envolvidos.

Fraudes envolvendo sites de empresas conhecidas e respeitadas surgem a cada dia.Fazer compras, efetuar pagamento, fechar negócios, todas essas atividades pela internet possuem características em comum: privacidade e

segurança redobrados.Sempre que há necessidade de expor dados pessoais ou financeiros, procedimentos de segurança devem ser adotados e seguidos. Com os cuidados apresentados o usuário estará mais consciente e, conseqüentemente, menos vulnerável ao acessar sites de comércio eletrônico ou Internet Banking.

4.5. Tutorial (Checklist) antifraudes para leigos

Buscando atingir um nível aceitável de segurança digital é fundamental , O internauta deve estar sempre bem informado, conhecer regras e ,acima de tudo, pô-las em prática quando estiver em seu computador seja no ambiente familiar ou de trabalho . Segundo estudo realizado pelo Instituto IPSOS[6] , 2005: 70,07% dos usuários brasileiros nunca fizeram curso de informática antes de navegar.É importante desta maneira, destacaremos um checklist com 20 dicas fundamentais sobre segurança digital buscando informar o internauta sobre os cuidados necessários para minimizar os riscos de não cair nos golpes da internet (MONITOR DAS FRAUDES[27], 2007):

1) Utilize um antivírus confiável e o mantenha constantemente atualizado. Além disso, configure o antivírus para realizar uma varredura, em tempo real, em todos os arquivos executados ou que entrem no micro.Programe semanalmente executar uma varredura completa no computador.

2) Instale e configure um bom programa antispyware. Certifique-se que o programa analise todos os arquivos executados ou que entrem no computador. O programa deverá ainda ser configurado para se atualizar automaticamente e para executar uma varredura completa diariamente.

3) Para completar a suíte de segurança, instale um bom programa de firewall e configure seu nível de proteção de acordo com as suas necessidades.

4) Verifique se o filtro anti-spam do seu provedor está ativado, ou se não for disponível adquira cliente de email que disponha dessa funcionalidade. Ter

um sistema capaz de filtrar as mensagens de spam de forma eficaz é importante pois grande parte dos emails com arquivos maliciosos anexados são normalmente identificados como spam.

5) Certifique que as configurações de segurança do seu navegador (Internet Explorer, Firefox,...) sempre solicite autorização e confirmação antes de baixar ou executar qualquer conteúdo na web. Não o autorize a instalação de nenhum software no qual não saiba a procedência. Evite realizar downloads ou executar códigos diretamente do seu navegador.

6) Ao realizar compras on-line, verifique se a loja virtual é confiável antes de fornecer dados dos seus cartões de credito.Procure informações sobre sua credibilidade, confiabilidade, solidez, segurança e eficiência nos sites de busca e compradores. Também verifique que o site utiliza conexão segura (figura do cadeado no browser) para a troca de dados e informações.

7) Desconfie e rejeite comunicados, propostas e ofertas milagrosas de qualquer tipo que possam chegar por qualquer meio (e-mail, MSN, icq, Orkut,...)

8) Nunca anote seus dados confidenciais como login, senhas e outras em lugares de fácil acesso ou visíveis.

9) Fraudadores costumam utilizar o nome de instituições sérias para desenvolver sites falsos com o intuito de enganar as vítimas desavisadas e de capturar suas senhas e dados sigilosos. Certifique-se que a URL digitada é a mesma da empresa e se esta permanece inalterada na hora que aparecer o site. Um procedimento auxiliar importante é tentar acessar o site utilizando uma senha propositalmente errada e ver se o site aceita esta senha. Sites fraudados não possuem controle dos dados, ou seja, aceitam qualquer informação digitada, já os verdadeiros sabem reconhecer a senha válida de uma errada.

10) Lembre-se que a enorme maioria dos casos de fraudes envolvendo compras on-line e internet banking acontece por descuidos do usuário Portanto tome sempre os devidos cuidados quando acessar sua conta e, de forma geral, usar o seu computador.

11) Ao acessar sua conta bancária e dados sigilosos utilize somente computadores confiáveis e que possuem sistemas de segurança instalados como antivírus, firewall. Evite usar computadores públicos ou de terceiros.

12) Evite navegar em sites arriscados e nunca baixe qualquer coisa de site que não conheça bem e que não sejam totalmente confiáveis. Geralmente , sites com material pornográfico, seriais de programas, hackers, pedófilos e outros crimes são suspeitos, pois, freqüentemente contém vírus, spyware ou outros malwares aos visitantes;

13) Nunca responda à emails não solicitadas spam nem para pedir sua remoção de listas de envio ou para reclamar ou solicitar qualquer informação. Eles usam sua resposta para confirmar a existência do seu endereço de email e aí sim que não irão parar nunca. Também não clique em links de descadastramento ou de forma geral em qualquer tipo de link ou site sugerido ou de outra forma presente nestas mensagens.

14) Nunca execute ou abra qualquer arquivo anexadas a mensagens de origem desconhecida ou não solicitadas. Sobretudo não abra arquivos de tipos suspeitos como: Exe, Pif, Bat, Com e Scr.Além disso, é importante configurar o seu cliente de email preferido para não executar automaticamente os anexos das mensagens, pois, estes anexos podem conter arquivos maliciosos como phishing, vírus e spywares.

15) Desconfie ao receber e-mails ameaçadores tipo cobranças, cancelamento de documentos pessoais, débitos em atraso entre outras. Fique em alerta com o recebimento de mensagens que aparentem ter sido enviada por sites de e-commerce, instituições financeiras, órgão do governo e outras empresa

com credibilidade no mercado.Empresas desta natureza jamais enviam mensagens por email com esta intenção. Sobretudo não clique em arquivos anexados a este tipo de emails ou qualquer link suspeito;

16) Não acredite em promessas milagrosas, preços abaixo dos praticados no mercado, propostas de dinheiro fácil ,vendas simplificadas de produtos ou serviços que deveriam estar sujeitos a fiscalização. Os fraudadores utilizam estes artifícios para praticar golpes, vender produtos falsificados e até perigosos.

17) Evite fornecer seu e-mail para publicação em fóruns, salas de bate papo e grupos de discussão. A mesma regra vale para informações pessoais como nome completo, data de nascimento CPF, RG. Entre outras

18) Evite sempre participar de qualquer tipo de correntes, sorteios de brindes pirâmides financeiras ,campanhas de solidariedade e artifícios deste tipo na internet. Também desconfie muito de qualquer oferta que lhe chegue pela rede e onde exista a solicitação de um pagamento adiantado.

19) Crie um endereço de email secundário em provedores gratuitos e utilize exclusivamente este endereço para cadastramento em sites, fóruns, blogs, bate-papos quando isso for inevitável.

20) Se recuse a abrir qualquer mensagem suspeita onde não seja claramente definida a identidade de quem a envia (endereços falsos, endereços omissos ou incompletos, assuntos com erros ou incongruentes...). A mesma regra vale para sites que proponham vendas de produtos ou serviços mas que tenham poucos dados, sem endereços e telefone de contato, sem nomes de empresas ou pessoas para contatar etc...

É importante também lembrar que, em qualquer mensagem de e-mail, o endereço do remetente é muito fácil de ser burlada. Por isso não confie automaticamente em mensagens que supostamente parecem ter sido enviadas por

seus contatos. Use seu senso crítico e um pouco de desconfiança pois existem muitos casos de fraude com e-mails que usam maliciosamente os nomes de pessoas conhecidas da vítima.

4.6. Fui vítima das fraudes. O que fazer?

Mesmo seguindo a guia de procedimentos, o usuário pode ser vítima dos fraudadores on-line.O internauta deve manter a calma e procurar minimizar as perdas seguindo um conjunto de recomendações.A Microsoft Segurança em casa[25] (2005) dispõe de um conjunto de passos que auxiliam o internauta as vítimas dos golpes on-line.Podemos destacar:

- **Feche quaisquer contas e cadastros afetados**

  Entre em contato com a empresa ou organização legítima se acreditar que deu informações confidenciais a uma fonte desconhecida que tenha se passado pela empresa ou organização. Se você entrar em contato com a empresa imediatamente, eles poderão aliviar os danos a você e terceiros.

  1.Consulte o departamento de segurança ou fraudes a respeito de quaisquer contas abertas ou acessadas em cada banco ou instituição financeira com a qual você negocia, incluindo empresas de cartão de crédito, serviços públicos, provedores de Internet e outros lugares em que você usa seu cartão de crédito.

  2.Dê seguimento com uma carta e guarde uma cópia. Ao abrir novas contas, use senhas seguras, e não senhas como o nome de solteira de sua mãe, junto com o novo número da conta.

  3.Altere as senhas de todas as suas contas online, iniciando por aquelas relacionadas a informações ou instituições financeiras.

- **Coloque um alerta de fraude em seus relatórios de crédito**

1. Obtenha uma cópia de seu relatório (vítimas de roubo de identidade podem receber cópias de seus relatórios de crédito gratuitamente) e solicite que nenhum crédito seja concedido sem sua aprovação.

2. Certifique-se de que sua conta esteja sinalizada com um indicador de "alerta de fraude" e uma "declaração da vítima" e insista para que o alerta permaneça ativo pelo máximo de sete anos.

3. Envie suas solicitações por escrito e guarde cópias. Ao receber seus relatórios, analise-os com cuidado. Procure solicitações que você não fez, contas que não abriu e dívidas inexplicáveis.

4. Entre em contato com a empresa envolvida, seu banco ou operadora de cartão de crédito que poderão orientar você sobre a organização ou agência relevante.

- **Entre em contato com as autoridades competentes**

1. Faça uma reclamação oficial. Se você for vítima de qualquer tipo de roubo de identidade, poderá denunciar o roubo ligando para autoridades competentes. Advogados orientarão você sobre como tratar dos problemas relacionados a crédito que poderão decorrer do roubo de identidade.

2. Faça um boletim de ocorrência na delegacia;

3. Obtenha uma cópia do boletim de ocorrência para notificar seu banco, empresa de cartão de crédito e outros credores de que você foi vítima de crime e que não abusa de crédito.

4. Dependendo de onde você mora, pode ser necessário fazer uma denúncia na jurisdição onde o crime realmente ocorreu.

5. Denuncie o golpe às autoridades que tratam de crimes praticados na internet como a polícia federal e o CERT.br. É importante, se possível, enviar o link do arquivo suspeito, cabeçalho da mensagem completo ou até mesmo, o próprio arquivo para que seja feita uma análise.

    a. A polícia federal disponibiliza o contato via website ou endereço eletrônico: *crime.internet@dpf.gov.br* para ajudar qualquer pessoa vítima de um crime na internet, como invasão para descoberta de senhas pessoais ou sites falsos.

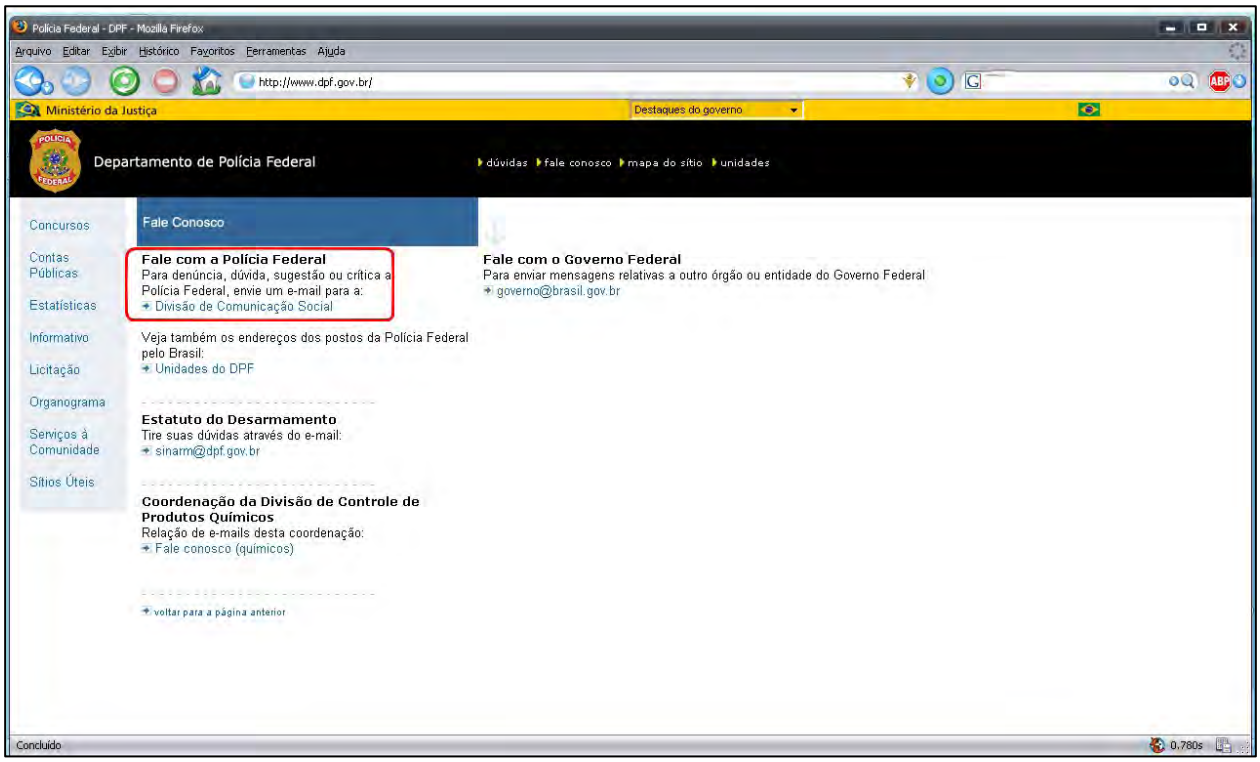

Figura 29: É possível denunciar fraudes pelo site da Polícia Federal.

Fonte: Polícia Federal,in; http://www.dpf.gov.br/ (Modificação Nossa)

    b. O CERT.br representa outra entidade bastante ativa no combate aos crimes virtuais.De modo semelhante a polícia federal o CERT.br disponibiliza o e-mail *cert@cert.br* para o usuários denunciar ataques fraudulentos e outros incidentes de segurança.

Figura 30: O CERT.br disponibiliza meios dos usuários denunciarem fraudes.
Fonte: CERT.br ,in: http://www.cert.br/contato.html (Modificação Nossa)

- **Registre e guarde tudo**

1. Ao completar esses passos para remediar a transgressão, sempre faça cópias de documentos, incluindo mensagens de email, correspondência e gravações de telefonemas, e guarde-os em local seguro.

2. Para conversas pessoais ou por telefone, dê seguimento por meio de cartas de confirmação com datas encaminhadas à organização e guarde uma cópia.

3. Declare na carta o que foi conversado e liste quaisquer itens de seguimento que você ou o representante se comprometeram a fazer na conversa.

Apesar de todos esses procedimentos, o mais importante é se manter em alerta.Caso o usuário suspeite que suas informações pessoais e sigilosas como

nome, CPF, senha de cartões de crédito, dados bancários estão sendo usados por golpistas entre em contato com a empresa envolvida (sua loja virtual , banco ou operadora do seu cartão de credito), informe-os sobre o caso e siga as orientações que serão divulgadas por eles.

Como dicas principais valem ressaltar também a importância de monitorar regularmente seus dados cadastrais e transações financeiras através de e-mails, extratos bancários e de cartões de credito em busca de cobranças, saques, ou débitos inesperados. Divulgue sua ocorrência em autoridades competentes que tratam e combatem as fraudes na internet com e, por fim, nunca descarte procurar uma delegacia de polícia, para registrar um boletim de ocorrência.

Capítulo 5 - Conclusão

Com base no estudo apresentado, podemos identificar um conjunto de fatores que costumam aparecer nas fraudes na internet e, conseqüentemente, representar indícios que auxiliam na sua identificação e prevenção.

Além de falta de conhecimento dos internautas, a ausência de uma legislação madura e abrangente,a inclusão digital se deu de maneira rápida e desorganizada. Todos querem usufruir dos benéficos da era digital, sem se importar com os riscos. Não há uma preparação e o ambiente virtual pode trazer alguns perigos aos novos navegantes. Diante do aumento de usuários ingênuos e ambiciosos, que são enganados com facilidade dentro do meio informático, surge um campo fértil aos golpistas.

Uma solução definitiva para as fraudes on-line envolve mudanças profundas na infra-estrutura e utilização da Internet cuja implementação está além da capacidade de qualquer instituição.Usuários e empresas continuarão usando por muitos anos variantes de hardware e software existentes hoje. É difícil pressupor que seja prático propor mudanças radicais nessa base instalada como parte de uma solução de curto prazo. Mas até que as expectativas de um desfecho definitivo se cumpram, as soluções devem ser baseadas na ajuda mútua entre internautas, empresas e autoridades.

- Internautas: Elaboração de um plano de conscientização claro e objetivo direcionado ao público mais suscetível à fraude;
- Empresas: Investimento contínuo em sistemas de segurança, treinamento, política de segurança, divulgação das políticas organizacionais;
- Autoridades: Criar leis específicas, Compartilhar informações e experiências, Monitorar e acompanhar tendências, atuar constantemente na investigação e punição dos fraudadores, divulgar nos meios de comunicação as operações

antifraudes realizadas.

De maneira geral, golpes cometidos pela Internet continuarão acontecendo, independentes das proteções que estão sendo utilizadas e desenvolvidas. O ser humano sua curiosidade e falta de cuidados, ainda continuarão sendo o elo mais fraco da corrente de segurança.

Com o presente estudo, o usuário estará certamente mais informado, ciente dos perigos da web e, conseqüentemente, de como não ser vítima dos cybers crimes.Porém, isto é apenas um dado pontual pertinente à segurança da informação, haja visto que o mundo das armadilhas on-line é imensamente vasto e representar todas as suas variáveis torna-se uma tarefa bastante difícil.

A melhor proteção é a prevenção e prevenção se consegue com informação. Navegar pela internet exige cautela, bom-senso e, acima de tudo, informação. Assim, a conscientização do usuário é o melhor caminho para que as boas práticas em segurança na internet reduzam significativamente o risco da ocorrência de fraudes.

Apesar da abrangência deste estudo,o tema fraudes na internet requer uma gama maior de discussões englobando detalhadamente tópicos como: botnets, worms, spams e outros malwares envolvidos na ocorrência dos golpes virtuais.Deve-se considerar que a tecnologia computacional está em constante aperfeiçoamento correspondendo à evolução dos métodos utilizados pelos fraudadores.

[1] APWG. Anti-Phishing Work Group**.** Disponível em: <http://www.apwg.org>. Acesso em: 15 Set. 2007.

[2] BRANCATELI, Rodrigo. **Comissão pode votar nesta quarta lei de crimes na internet.** Estadão. São Paulo, maio. 2007. Disponível em: <http://www.estadao.com.br/tecnologia/internet/noticias/2007/mai/29/378.htm>.Acesso em: 13 out.2007.

[3] CARDILLI, Juliana; CARPANEZ,Juliana**. Fraude virtual toma R$ 300 milhões em 2006.** Disponível em: <http://g1.globo.com/Noticias/Tecnologia/0,,MUL3537-6174,00.html>. Acesso em: 15 Out. 2007.

[4] Cert.br.**Cartilha de Segurança para Internet.Parte IV: Fraudes na Internet**. Disponível em: <http://www.cgi.br/sobre-cg/definicao.htm>. Acesso em: 12 Ago. 2007.

[5] _____. Missão. Disponível em:< http://www.cert.br./missao.html> Acesso em: 17 out.2007.

[6] Cetic.br. Centro de Estudos sobre as Tecnologias da Informação e da Comunicação. **TIC domicílios 2005.**2005.Disponível em:< http://www.cetic.br/usuarios/tic/2005/index.htm>. Acesso em: 24 Ago.2007

[7] CGI.br. **Sobre o CGI.br**. Disponível em: http://cgi.br/sobre-cg/definicao.htmAcesso em: 17 out.2007.

[8] CHAVES, Marcelo H. C. P. **Segurança na internet.** Disponível em: <www.conip.com.br/sp/2006/palestras/maracana/28-06/marcelo_chaves.pdf >. Acesso em: 11 Out 2007.

[9] D´ÁVILA, Márcio. **Scam - A fraude inunda o correio eletrônico**. **Scan**. São Paulo,28 Jun.2004. Disponível em: <http://www.mhavila.com.br/topicos/seguranca/scam.html> Acesso em: 15 Ago.2007.

[10] DEPARTAMENTO DE POLÍCIA FEDERAL. Disponível em: < : http://www.dpf.gov.br/>. Acesso em: 18 out.2007.

[11] ESCALENA. **Pode perder o medo de comprar pela internet**. São Paulo,30 out.2007. Disponível em: <http://www.escalena.com/comercioeletronico.asp?id=55 >Acesso em: 30 out.2007.

[12] FEBRABAN. **Guia de Referência Sobre Ataques Via Internet**.2000. Disponível em: <http://www.cyberbric.com/arquivos/Guia%20de%20Refer%C3%AAncia%20sobre%20Ataques%20Via%20Internet.pdf >. Acesso em: 16 Ago 2007.

[13] _____ et al. **Sua identidade corre perigo**. Disponível em: http://info.abril.com.br/aberto/infonews/082006/25082006-6.shl. Acesso em: 26 out. 2007.

[14] _____. **Os 20 mandamentos do acesso seguro às transações eletrônicas.** Disponível em:< http://www.febraban.org.br/seguranca_site/20_mandamentos.asp> Acesso em: 13 set.2007.

[15] FILHO, Mariano. **Brasil subestima o impacto dos crimes eletrônicos**. PBI. Porto Alegre, 19 Out. 2007. Disponível em: http://www.pbi.com.br/site/interno_alerta_leitura.php?id=401. Acesso em: 12 set. 2007.

[16] FIRST. About First. Disponível em: http://www.first.org/about/history. Acessado em: 17 out. 2007.

[17] GOUVEIA, Flávia.**Não Morda a Isca!**.2007. Disponível em:<http://www.comciencia.br/comciencia/handler.php?section=8&edicao=20&id=218>. Acesso em: 08 Set.2007

[18] HOEPERS, Cristine. **Atuação de CERT.br.** Disponível em: < http://www.cert.br/docs/palestras/certbr-dualtec2007.pdf >. Acesso em: 11 Out 2007.

[19] HOEPERS, Cristine. JESSEN, Klaus.S. **Vulnerabilidades e Proteção dos Usuários.** Disponível em: < http://www.cert.br/docs/palestras/certbr-febraban2007.pdf >. Acesso em: 12 Out 2007.

[20] HONNEYCUTT, Jerry. **Como Proteger seu Computador do Spyware e do Adware** Disponível em: < http://www.microsoft.com/brasil/windowsxp/using/security/expert/honeycutt_spyware.mspx>. Acesso em: 19 Out 2007.

[21] HONEYNET Project. **About the project**. Disponível em: < http://honeynet.org./misc/project.html>. Acesso em: 18 out. 2007.

[22] INVASÃO. **Projeto de lei para crimes virtuais.** Disponível em: < http://www.invasao.com.br/coluna-proj-lei.htm>. Acesso em : 16 out.2007.

[23] JONES, Matthew . **Cibercrime está se tornando mais organizado**.2006. Disponível em:< http http://info.abril.uol.com.br/aberto/infonews/092006/15092006-7.shl>. Acesso em: 29 Out.2007.

[24] MATTOS, Gastão apud CARDILLI, Juliana; CARPANEZ,Juliana**. Fraude virtual toma R$ 300 milhões em 2006**. G1. Disponível em: <http://g1.globo.com/Noticias/Tecnologia/0,,MUL3537-6174,00.html>. Acesso em: 15 Out. 2007.

[25] Microsoft Segurança em casa. **O que fazer se você for vítima de fraude de cartão de crédito ou outros tipos de esquemas online**.2005. Disponível em:< http://www.microsoft.com/brasil/athome/security/privacy/fraudvictim.mspx>. Acesso em: 01 Set.2007.

[26] MITNICK, Kevin D.**A Arte de Enganar**. Makron Books .2003. ISBN: 85-346-1516-0

[27] Monitor das Fraudes. **Introdução ao Mundo das Fraudes**. 2007. Disponível em: < http://www.fraudes.org/showpage1.asp?pg=2 >. Acesso em: 04 Set.2007.

[28] Monitor das Fraudes.**Vinte dicas de segurança digital**. 2007. Disponível em: < http://www.fraudes.org/showpage1.asp?pg=14 >. Acesso em: 15 set.2007.

[29] NETTION. **Prejuízos com compras feitas em sites falsos somam R$ 300 milhões**. Disponível em: <http://www.nettion.com.br/?m=noticias&s=noticia&cod_noticia=73>. Acesso em: 14 set.2007.

[30] PEREIRA, João. Introdução a programação em WML. In: Revista Programar,n°7, Portugal, março. 2007. Disponível em: http://www.portugal-a-programar.org/revista-programar/edicoes/Revista_PROGRAMAR_-_7a_edicao_Marco_2007.pdf. Acesso em: 14 set. 2007.

[31] PRADO, Cláudio Almeida. **Dicas para não ser vítima de golpes na Internet.Netmarkt**. São Paulo. 2004. Disponível em: < http://www.pulso.com.br/index.php?option=com_content&task=view&id=46&Itemid=91>. Acesso em: 28 Ago.2007.

[32] ROCHA, Luis F. **NBSO revela o cenário do terceiro trimestre: fraudes e scans pela porta 22/TCP**. **Cert**. São Paulo, nov.2004. Disponível em: http://www.cert.br/docs/reportagens/2004/2004-11-01a.html. Acesso em: 25 Set.2007.

[33] SAFERNET**. Quem somos.** Disponível em: < http://www.safernet.com.br/twiki/bin/view/SaferNet/QuemSomos. Acesso em: 17 out.2007.

[34] SANTOS, Daniel dos. **Brasil é líder em golpe via e-mail.** Disponível em:<http://pcworld.uol.com.br/especiais/secworld/archive/2007/02/08/brasil--lder-em-golpe-via-e-mail/>. Acesso em 18 Set. 2007.

[35] SÊMOLA, Marcos. **Inteligência da fraude**. Disponívem em: <http://www.semola.com.br/disco/Coluna_IDGNow_93.pdf>. Acesso em: 06. nov.2007.

[36] SIMON, Cláudio Antônio de paiva**. Scam, phishing e pharming: as fraudes praticadas no ambiente Internet Banking e sua recepção no Brasil**. 2007. Disponível em: < http://www.alfa-redi.org/rdi-articulo.shtml?x=9077>. Acesso em: 08 Set.2007.

[37] SIQUEIRA, Ethevaldo. **A luta mundial contra a fraude na internet**. 2004. Disponível em: http://clipping.planejamento.gov.br/Noticias.asp?NOTCod=148639>. Acesso em: 01 Set.2007.

[38] SOPHOS. **Número de pragas virtuais cresce 152%. Disponível em: <**http://gsisic.serpro.gov.br/destaque/20070425_01>. Acesso em: 04 Set. 2007.

[39] Symantec Corporation.**Relatório Symantec Sobre Ameaças à Segurança na Internet**. 2007. Disponível em:<http://eval.symantec.com/mktginfo/pt/br/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_exec_summary_09_2007-pt-br.pdf>. Acesso em: 28 Out.2007.

[40] TERRA. **Entenda a lei que coíbe crimes na Internet.** São Paulo.19 set.2006. Disponível em: <http://infomediatv.terra.com.br/infomediatv/?section=10&article=108 >.Acessado em: 17 out.2007.

[41] TERZIAN, Françoise .**Sua identidade digital corre perigo.**2006 InfoExame. Disponível em:< http://info.abril.com.br/aberto/infonews/082006/25082006-6.shl>. Acesso em: 29 Out.2007.

[42] Unisys Corporation. **Relatório sobre Fraudes bancárias de "Roubo de Identidades"**. 2005. Disponível em:< http://www.unisys.com.br/Identity_theft_Brazil_Port.pdf >. Acesso em: 29 Out.2007.

[43] VARGAS, Maurício. Prejuízos com compras feitas em sites falsos somam R$ 300 milhões. **Nettion**, São Paulo. Disponível em: http://www.nettion.com.br/?m=noticias&s=noticia&cod_noticia=73. Acesso em: 07 out.2007.

REFERÊNCIAS BIBLIOGRÁFICAS

ALFA-REDI. **Scam, phishing e pharming: as fraudes praticadas no ambiente Internet Banking e sua recepção no Brasil**. Revista de derecho informático. Abr. 2007. Disponível em: http://www.alfa-redi.org/rdi-articulo.shtml?x=9077. Acesso em 04 set.2007.

APWG**. Anti-Phishing Work Group.** Disponível em: <http://www.apwg.org>. Acesso em: 15 Set. 2007.

BARBOSA, Alexandre . **Cuidado, a internet está viva!-os incríveis cenários para o futuro desse fenômeno**.Ed Mostarda.2006

BRANCATELI, Rodrigo. **Comissão pode votar nesta quarta lei de crimes na internet**. Estadão. São Paulo, maio. 2007. Disponível em: http://www.estadao.com.br/tecnologia/internet/noticias/2007/mai/29/378.htm.Acesso em 13 out.2007.

Cadernos Eletrônicos.**Navegação Segura**. Disponível em: < http://www.acessasp.sp.gov.br/cadernos/Cadernos_Eletronicos_arquivos/PDFs/caderno08.pdf>. Acesso em: 01 Nov. 2007.

CARMARGO,Francisco .**Salve-se dos hackers quem puder.** .. Comento que, Fonte: Gazeta Mercantil de 29 de agosto de 2006. Caderno A – p. 3.

CARDILLI, Juliana; CARPANEZ,Juliana**. Fraude virtual toma R$ 300 milhões em 2006.** Disponível em: <http://g1.globo.com/Noticias/Tecnologia/0,,MUL3537-6174,00.html>. Acesso em: 15 Out. 2007.

CHAVES, Marcelo H. C. P. **Segurança na internet.** Disponível em: <www.conip.com.br/sp/2006/palestras/maracana/28-06/marcelo_chaves.pdf >. Acesso em: 11 Out 2007.

Cert.br.**Cartilha de Segurança para Internet.Parte IV: Fraudes na Internet**. Disponível em: <http://www.cgi.br/sobre-cg/definicao.htm>. Acesso em: 12 Ago. 2007.
Cetic.br. Centro de Estudos sobre as Tecnologias da Informação e da Comunicação. **TIC domicílios 2005.**2005.Disponível em:< http://www.cetic.br/usuarios/tic/2005/index.htm>. Acesso em: 24 Ago.2007

CGI.br, Comitê Gestor da Internet no Brasil. **Sobre o CGI.br**. Disponível em: <http://www.cgi.br/sobre-cg/definicao.htm>. Acesso em: 23 Out. 2007.

CORRÊA, Nelson. **PHISHING SCAM, o que é isso?**. Disponível em: < http://www.nelsoncorrea.com/Documents/NelsonCorrea_Phishing_Scam.pdf>. Acesso em: 29 Set. 2007.

D´ÁVILA, Márcio**. Scam - A fraude inunda o correio eletrônico**. **Scan**. São Paulo,28 Jun.2004. Disponível em: <http://www.mhavila.com.br/topicos/seguranca/scam.html> Acesso em: 11 Ago out.2007.

ESCALENA. **Pode perder o medo de comprar pela internet**. São Paulo,30 out.2007. Disponível em: <http://www.escalena.com/comercioeletronico.asp?id=55 >Acesso em: 30 out.2007.

FÁBIO S. **Pharming.** Disponível em: <http://www.hipermail.com/blog/archives/200504.html#003492>. Acesso em 24 Set 2007.

FEBRABAN. **Guia de Referência Sobre Ataques Via Internet**.2000. Disponível em: <http://www.cyberbric.com/arquivos/Guia%20de%20Refer%C3%AAncia%20sobre%20Ataques%20Via%20Internet.pdf >. Acesso em: 16 Ago 2007.

_____ et al. **Sua identidade corre perigo**. Disponível em: http://info.abril.com.br/aberto/infonews/082006/25082006-6.shl. Acesso em: 26 out. 2007.

FILHO, Mariano. **Brasil subestima o impacto dos crimes eletrônicos**. PBI. Porto Alegre, 19 Out. 2007. Disponível em: http://www.pbi.com.br/site/interno_alerta_leitura.php?id=401. Acesso em: 12 set. 2007.

G Tally, R Thomas, T Van Vleck. **Anti-Phishing:Práticas Recomendadas para Instituições e Consumidores**.2004. Disponível em: < http://www.nai.cl/es/partners/literature/wp_antiphishing_inst&consbp.pdf>.Acesso em: 25 Set.2007.

HOEPERS, Cristine. **Atuação de CERT.br.** Disponível em: < http://www.cert.br/docs/palestras/certbr-dualtec2007.pdf >. Acesso em: 11 Out 2007.

HOEPERS, Cristine. JESSEN, Klaus.S. **Vulnerabilidades e Proteção dos Usuários.** Disponível em: < http://www.cert.br/docs/palestras/certbr-febraban2007.pdf >. Acesso em: 12 Out 2007.

HONNEYCUTT, Jerry. **Como Proteger seu Computador do Spyware e do Adware** Disponível em: < http://www.microsoft.com/brasil/windowsxp/using/security/expert/honeycutt_spyware.mspx>. Acesso em: 19 Out 2007.

IBP Brasil. **Segurança no comércio**. 2007.Disponível em: < http://www.ibpbrasil.com.br/comercioeletronico/index.html>. Acesso em: 25 Ago.2007.

InfoGuerra. **O que fazer se você for vítima de fraude online**. 2007.Disponível em: < http://www.infoguerra.com.br/infonews/viewnews.cgi?newsid1135216800,17740,>. Acesso em: 05 Ago.2007.

INVASÃO. **Projeto de lei para crimes virtuais.** Disponível em: < http://www.invasao.com.br/coluna-proj-lei.htm>. Acesso em : 16 out.2007.

MATTOS, Gastão apud CARDILLI, Juliana; CARPANEZ,Juliana**. Fraude virtual toma R$ 300 milhões em 2006.** G1. Disponível em: <http://g1.globo.com/Noticias/Tecnologia/0,,MUL3537-6174,00.html>. Acesso em: 15 Out. 2007.

Mcafee. **Práticas recomendadas de combate a ataques de phishing**.2007. Disponível em: < http://www.mcafee.com/br/security_insights/best_practices_fighting_phishing_attacks.html>. Acesso em: 22 Ago.2007.

Monitor das Fraudes.**VINTE dicas de segurança digital**. Ago. 2007. Disponível em: < http://www.fraudes.org/showpage1.asp?pg=14 >. Acesso em: 15 set.2007.

Módulo Security Solutions.**9º Pesquisa nacional de segurança da informação**.2004. Disponível em:<http:// www.modulo.com.br/pdf/nona_pesquisa_modulo.pdf>. Acesso em: 25 Ago.2007.

MITNICK, Kevin D.**A Arte de Enganar**. Makron Books .2003. ISBN: 85-346-1516-0

Monitor das Fraudes. **Introdução ao Mundo das Fraudes**. 2007. Disponível em: < http://www.fraudes.org/showpage1.asp?pg=2 >. Acesso em: 04 Set.2007.

NETTION. **Prejuízos com compras feitas em sites falsos somam R$ 300 milhões**. Disponível em: <http://www.nettion.com.br/?m=noticias&s=noticia&cod_noticia=73>. Acesso em: 14 set.2007.

NIC.br. **CERT.br registra aumento de 46% nas tentativas de fraudes reportadas no segundo trimestre**. 2007.Disponível em: <http://www.nic.br/imprensa/releases/2007/rl-2007-10.pdf>. Acesso em: 26 Ago.2007.

PEREIRA, João. Introdução a programação em WML. In: Revista Programar,n°7, Portugal, março. 2007. Disponível em: http://www.portugal-a-programar.org/revista-programar/edicoes/Revista_PROGRAMAR_-_7a_edicao_Marco_2007.pdf. Acesso em: 14 set. 2007.

PRADO, Cláudio Almeida. **Dicas para não ser vítima de golpes na Internet**.Netmarkt. São Paulo. 2004. Disponível em: < http://www.pulso.com.br/index.php?option=com_content&task=view&id=46&Itemid=91>. Acesso em: 28 Ago.2007.

ROCHA, Luis F. **NBSO revela o cenário do terceiro trimestre: fraudes e scans pela porta 22/TCP**. **Cert**. São Paulo, nov.2004. Disponível em: http://www.cert.br/docs/reportagens/2004/2004-11-01a.html. Acesso em: 25 Set.2007.

RODRIGUES, Giordani. **As armadilhas para internautas - como se proteger**. 2002. Disponível em: < http://www.infoguerra.com.br/infonews/viewnews.cgi?newsid1041076128,7378,/1>. Acesso em: 15 Ago.2007.

SANTOS, Daniel dos. **Brasil é líder em golpe via e-mail.** Disponível em:<http://pcworld.uol.com.br/especiais/secworld/archive/2007/02/08/brasil--lder-em-golpe-via-e-mail/>. Acesso em 18 Set. 2007.

SCHNNOR, Tatiana. **Febraban monta cartilha para ensinar Internauta a fazer as compras online de Natal.** WNews. Disponível em:<http://pcworld.uol.com.br/especiais/secworld/archive/2007/02/08/brasil--lder-em-golpe-via-e-mail/>. Acesso em 14 Nov. 2007.

SÊMOLA, Marcos. **Inteligência da fraude**. Disponívem em: <http://www.semola.com.br/disco/Coluna_IDGNow_93.pdf>. Acesso em: 06. nov.2007.

SIMON, Cláudio Antônio de paiva**. Scam, phishing e pharming: as fraudes praticadas no ambiente Internet Banking e sua recepção no Brasil**. 2007. Disponível em: < http://www.alfa-redi.org/rdi-articulo.shtml?x=9077>. Acesso em: 08 Set.2007.

SIQUEIRA, Ethevaldo. **A luta mundial contra a fraude na internet**. 2004. Disponível em: http://clipping.planejamento.gov.br/Noticias.asp?NOTCod=148639>. Acesso em: 01 Set.2007.

SOPHOS. **Número de pragas virtuais cresce 152%. Disponível em: <**http://gsisic.serpro.gov.br/destaque/20070425_01>. Acesso em: 04 Set. 2007.

Symantec **Corporation**.**Relatório Symantec Sobre Ameaças à Segurança na Internet**. 2007. Disponível em:<http://eval.symantec.com/mktginfo/pt/br/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_exec_summary_09_2007-pt-br.pdf>. Acesso em: 28 Out.2007.

TERRA**. Entenda a lei que coíbe crimes na Internet**. São Paulo.19 set.2006. Disponível em: <http://infomediatv.terra.com.br/infomediatv/?section=10&article=108 >.Acessado em: 17 out.2007.

TERZIAN, Françoise .**Sua identidade digital corre perigo.**2006 InfoExame. Disponível em:< http://info.abril.com.br/aberto/infonews/082006/25082006-6.shl>. Acesso em: 29 Out.2007.

The Honey Project**. About the Project**.**.** Disponível em: < http://www.honeynet.org/misc/project.html>. Acesso em: 03 Set.2007.

Unisys Corporation. **Relatório sobre Fraudes bancárias de "Roubo de Identidades"**. 2005. Disponível em:< http://www.unisys.com.br/Identity_theft_Brazil_Port.pdf >. Acesso em: 29 Out.2007.

VARGAS, Maurício. **Prejuízos com compras feitas em sites falsos somam R$ 300 milhões**. **Nettion**, São Paulo. Disponível em: http://www.nettion.com.br/?m=noticias&s=noticia&cod_noticia=73. Acesso em: 07 out.2007.

VIEIRA, Berenice, NIQUE, Walter**. E-Commerce: Atributos Determinantes na Utilização da Internet como Canal de Compra.** In.: ENCONTRO NACIONAL DA ANPAD, 23, 1999.