UNIVERSIDADE DO EXTREMO SUL CATARINENSE – UNESC
CURSO DE CIÊNCIA DA COMPUTAÇÃO

LUCAS URGIONI NIEHUES

AMEAÇAS DIGITAIS: UM ESTUDO DOS RISCOS ENVOLVIDOS NO USO DA INTERNET, SEUS IMPACTOS E FORMAS DE PROTEÇÃO

CRICIÚMA, JUNHO DE 2007.

LUCAS URGIONI NIEHUES

AMEAÇAS DIGITAIS: UM ESTUDO DOS RISCOS ENVOLVIDOS NO USO DA INTERNET, SEUS IMPACTOS E FORMAS DE PROTEÇÃO

Trabalho de Conclusão de Curso apresentado para obtenção do Grau de Bacharel em Ciência da Computação da Universidade do Extremo Sul Catarinense.

Orientador: Prof. M.Sc. Rogério Antônio Casagrande

CRICIÚMA, JUNHO DE 2007.

Aos meus pais, Celso Niehues e Anadir Urgioni Niehues, meus irmãos, e a minha namorada Marcele Casagrande Brunel.

AGRADECIMENTOS

A Deus, pela vida e pela saúde, pois por meio delas consegui, não só realizar este trabalho, como também me dedicar aos anos de estudo.

Aos meus familiares, especialmente meus pais e meus irmãos, pelo apoio, pelo amor, pela dedicação e por propiciar todas as condições para que eu tivesse capacidade de realizar este trabalho.

A minha namorada, pela paciência, compreensão, carinho, estímulo e por me oferecer importantes sugestões.

Ao meu orientador, Rogério Antônio Casagrande, pela dedicação e empenho fornecido durante a realização deste trabalho.

Aos amigos e companheiros de turma, que compartilharam das mesmas preocupações, dúvidas e descobertas.

Enfim, a todos que me ajudaram em mais esta etapa.

“Um computador seguro é aquele que está desligado.”

(Kevin Mitnick)

RESUMO

O aumento do uso da Internet proporcionou um crescimento significativo no número de fraudes por este meio. As ameaças digitais causam inúmeros problemas uma vez que muitos usuários deixam de utilizar a Internet para executar tarefas que envolvam uso de dados pessoais e principalmente financeiros. Estes problemas são ainda maiores quando uma fraude é concretizada.

Esta pesquisa apresenta as principais ameaças digitais existentes, seus sintomas e procedimentos de defesa.

Para verificar o comportamento dos usuários perante as ameaças digitais, foi realizada uma pesquisa de campo com base em questionário onde os resultados são apresentados e discutidos.

Por fim esta pesquisa apresenta uma simulação de fraude que utiliza *phishing*, cavalo de tróia, *pharming* e *site* falso e procedimentos de defesa.

Palavras-chave: Segurança; Fraudes digitais; *Pharming*; *Phishing*; Cavalo de Tróia.

ABSTRACT

The increase of the use of the Internet provided a significant growth in the number of frauds for this way. The digital threats cause innumerable problems a time that many users leave to use the Internet to execute tasks that involve use of personal datas and mainly financial. These problems are still bigger when a fraud is materialize.

This research presents the main existing digital threats, its symptoms and procedures of defense.

To verify the behavior of the users before the digital threats, questionnaire was carried through a field research on the basis of where the results are presented and argued.

Finally this research presents a fraud simulation that uses phishing, trojan, pharming and false site and procedures of defense.

Keywords: Security; Digital frauds; Pharming; Phishing; Trojan.

LISTA DE ILUSTRAÇÕES

LISTA DE SIGLAS

ADSL	*Asymmetric Digital Subscriber Line*
APWG	*Anti-Phishing Working Group*
CERT	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CETIC	Centro de Estudos sobre as Tecnologias da Informação e da Comunicação
CIA	*Confidentiality, Integrity and Availability*
DNS	*Domain Name System*
FTP	*File Transfer Protocol*
HTTPS	*HyperText Transfer Protocol Secure*
IP	*Internet Protocol*
IRC	Internet *Relay Chat*
MP3	MPEG-1/2 *Audio Layer*
NIC	Núcleo de Informação e Coordenação
P2P	*Peer-to-Peer*
SSL	*Secure Socket Layer*
SGSI	Sistema de Gestão de Segurança da Informação
TCP	*Transmission Control Protocol*
UNESC	Universidade do Extremo Sul Catarinense

SUMÁRIO

1 INTRODUÇÃO

Diariamente usuários da rede mundial de computadores estão sujeitos a inúmeras ameaças como engenharia social, vírus, *worms, malwares, spywares, backdoors, keyloggers, bots, rootkits, phishing,* entre outros, provenientes de *e-mails*, *browsers*, programas de troca de mensagens, programas de distribuição de arquivos e outras ferramentas desenvolvidas para Internet.

Estas ameaças causam uma série de problemas, já que o usuário com receio, deixa de utilizar ferramentas importantes como *sites* de Comércio Eletrônico e Internet *Banking,* trazendo perdas a todos os envolvidos neste processo.

O tempo perdido com os problemas causados por estas ameaças digitais também é outro ponto importante, pois normalmente quando infectados os computadores apresentam falhas impossibilitando o seu funcionamento ideal.

Os investimentos constantes em tecnologias na tentativa de minimizar ao máximo estes problemas e garantir a confidencialidade, integridade e disponibilidade das informações, poderiam estar sendo destinados ao desenvolvimento de novas ferramentas e assim proporcionando maior crescimento dos recursos computacionais e não apenas auxiliando o funcionamento de forma segura dos já existentes.

Estes e outros aspectos estão apresentados nesta pesquisa, que destaca um estudo das principais ameaças digitais e formas de proteção, juntamente com uma pesquisa de campo que apresenta os hábitos de navegação na Internet e o grau de conhecimento das ameaças por parte dos usuários.

Com intuito de demonstrar a possibilidade, o funcionamento e formas de proteção de uma fraude digital, foi desenvolvida uma simulação de ataque que utiliza técnicas de captura de informações.

1.1 OBJETIVO GERAL

Identificar os riscos das ameaças digitais existentes na Internet e demonstrar a possibilidade da execução de ações ilícitas por meio de simulação.

1.2 OBJETIVOS ESPECÍFICOS

Esta pesquisa possui como objetivos específicos:

a) identificar as principais ameaças digitais;
b) compreender o funcionamento dos ataques;
c) propor soluções existentes para minimizar o número de fraudes;
d) realizar pesquisa de campo buscando identificar hábitos de navegação na Internet e o grau de conhecimento das ameaças por parte dos usuários;
e) simular ataque baseado em técnicas de captura de informações e demonstrar procedimentos de defesa.

1.3 JUSTIFICATIVA

O crescimento e a popularização da Internet criaram um cenário ideal para propagação de ameaças digitais. Segundo o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT) o número de incidentes identificados subiu de 5.997 em 2000 para 197.892 em 2006 (CERT, 2007), apresentados na Figura 1.

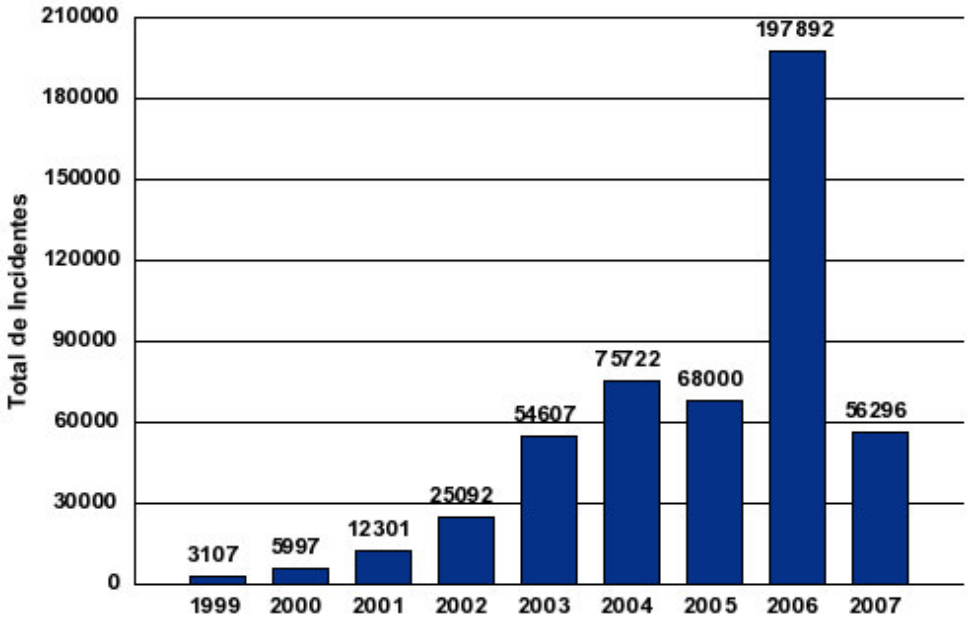

Figura 1. Incidentes de segurança reportados ao CERT
Fonte: CERT

Os veículos de comunicação têm alertado muito sobre este problema, mas dificilmente propõem medidas para que os usuários possam se defender, ou quando o fazem tratam superficialmente.

Conhecer o funcionamento das principais formas de ataque e procedimentos de defesa pode proporcionar maior confiança aos usuários e consequentemente aumentar o volume de negociações feitas pela Internet, diminuir os custos com incidentes e principalmente proporcionar maior confidencialidade, integridade e disponibilidade das informações.

A falta de conhecimento também favorece a propagação destas ameaças digitais, e ainda cria inúmeros riscos nas redes internas das organizações, já que muitas vezes funcionários por descuido abrem portas importantes para ataques externos.

1.4 ESTRUTURA DO TRABALHO

Este trabalho é composto por sete capítulos. No Capítulo 1 há uma introdução ao tema proposto, os objetivos e justificativas para realização deste projeto.

Nos Capítulos 2, 3 e 4 são abordados temas relacionados a segurança da informação, sintomas de sistemas infectados e procedimentos de defesas respectivamente.

O Capitulo 5 traz uma pesquisa de campo com base em questionário, que apresenta dados sobre o comportamento dos usuários mediante aos problemas com as ameaças digitais.

A implementação do projeto se encontra no Capítulo 6, que mostra uma simulação de fraude utilizando *phishing*, cavalo de tróia, *pharming* e site falso, e procedimentos de defesa.

Por fim, há uma conclusão e as possibilidades de trabalhos futuros.

2 SEGURANÇA DA INFORMAÇÃO

A informação hoje é talvez o que se tenha de mais valioso, tanto para as pessoas, quanto para os negócios, e desta forma deve ser muito bem protegida.

Antigamente, a informação existente era quase totalmente escrita em papel, e exigia segurança principalmente física. Com o passar dos anos, os avanços tecnológicos computacionais permitiram que a informação se tornasse algo muito mais fácil de ser armazenada, controlada e disponibilizada, porém, muito mais difícil de ser restringido o acesso.

A segurança da informação deve ser feita fisicamente e logicamente. O controle físico, como o próprio nome já diz, deve garantir que nenhuma pessoa não autorizada tenha acesso físico a determinada informação, utilizando uma infra-estrutura que permita esta limitação. O controle lógico também limita o acesso, porém é normalmente eletrônico, e exige sistemas computacionais projetados a fim de garantir que ninguém, não autorizado, tenha acesso, principalmente quando estas informações podem ser acessadas por meio da Internet, o que aumenta o grau de risco.

Nos dias de hoje, as pessoas e principalmente as organizações dependem cada vez mais dos sistemas de informações e da Internet para fazer negócios. “Um incidente de segurança pode impactar direta e negativamente as receitas de uma corporação, a confiança de seus clientes e o relacionamento com sua rede de parceiros e fornecedores.” (ZAPATER; SUZUKI, 2005).

A necessidade de proteger a informação gerada por qualquer pessoa ou organização, vem do objetivo de garantir o funcionamento de alguma tarefa ou continuidade de um negócio, minimizando os danos causados e aumentando o retorno gerado.

Com o aumento do uso da Internet, de ferramentas para disponibilizar informações e também aplicações, a segurança tornou-se vital para um grande número de empresas, como por exemplo, os bancos, que lidam com informações extremamente sigilosas e necessitam disponibilizá-las aos seus clientes por meio da Internet.

2.1 CONCEITOS DE SEGURANÇA

A segurança da informação está ligada à proteção das informações de uma determinada pessoa ou organização.

A informação é qualquer dado que possa ser útil para alguém ou para uma aplicação, e é um dos produtos mais valiosos para gestão de uma organização (FOINA, 2001).

Segundo Dias (2000) segurança "é a proteção de informações, sistemas e serviços contra desastres, erros e manipulação não autorizada, de forma a reduzir a probabilidade e o impacto de incidentes de segurança".

A segurança de determinada informação está ligada a fatores comportamentais, do ambiente e da infra-estrutura existente para que a mesma permaneça confidencial, íntegra e disponível.

A tríade *Confidentiality, Integrity and Availability* (CIA) - Confidencialidade, Integridade e Disponibilidade - representa as propriedades atuais que orientam o planejamento e implementação da segurança de determinada informação.

Os conceitos básicos podem ser explicados conforme os itens abaixo, segundo Moreira (2001 apud QUINTELLA et al, 2003):

a) **confidencialidade**: propriedade que visa manter o sigilo ou a privacidade das informações, limitando o acesso somente a pessoas autorizadas;

b) **integridade**: consiste em proteger a informação contra alterações sem a autorização explícita do autor da mesma, garantindo que mantenha todas as características originais estabelecidas;

c) **disponibilidade**: a informação deve estar disponível no momento que for necessário aos usuários autorizados.

Um sistema computacional é considerado seguro quando atende todas as propriedades listadas.

2.2 IMPORTÂNCIA DA SEGURANÇA

A evolução dos recursos computacionais e as melhorias na produtividade causadas pelos sistemas de informação, criaram uma dependência muito grande, principalmente quando se fala em Internet. Esta dependência cria problemas quando os sistemas não estão em funcionamento pleno, devido a ataques ou outros incidentes provocados pela falta de segurança.

É necessário que os três conceitos básicos da segurança da informação sejam respeitados, assim, o grau de risco que uma organização ou um usuário doméstico possuem torna-se muito menor.

Notadamente, hoje o usuário doméstico, por falta de conhecimento e estrutura para proteção, está muito mais vulnerável aos ataques em sistemas computacionais. O medo constante de ser vítima de fraudes, principalmente na Internet, faz com que ele deixe de utilizar ferramentas e efetuar transações, como por exemplo, uma compra *on-line* utilizando o seu cartão de crédito.

Outras inúmeras ameaças que colocam em risco a segurança da informação estão presentes nos sistemas computacionais. A proteção efetiva requer cuidados que envolvem recursos tecnológicos, gerenciamento, procedimentos e principalmente

conhecimento dos riscos existentes, para que os recursos disponíveis sejam utilizados para garantir o controle de qualquer ameaça.

2.3 NORMAS E POLÍTICAS DE SEGURANÇA

Adotar normas e políticas de segurança da informação é fundamental para que uma série de requisitos sejam implementados no auxílio da manutenção da segurança, principalmente nas organizações. As normas fornecem recomendações na gestão da segurança para uso dos responsáveis pela mesma e a todos os usuários que são também peças fundamentais no combate às ameaças existentes, e também contêm orientações detalhadas sobre um Sistema de Gestão de Segurança da Informação (SGSI).

A norma NBR/ISO IEC, que é a versão nacional da norma internacional ISO 17799, cuja última versão é a ABNT NBR ISO/IEC 17799:2005, detalha "as melhores práticas sobre gerenciamento de segurança e oferece uma linha mestra de como as medidas de segurança devem ser implementadas". Esta norma aborda regras de termos e definições, política de segurança da informação, classificação e controle dos ativos de informação, segurança física e do ambiente, gerenciamento das operações e comunicações, conformidades da lei, controle de acesso entre outros.

> A tendência é que a Norma ISO/IEC 17799 tenha rápida expansão, no médio prazo, e que venha a se tornar uma exigência comum para a contratação de serviços ou até mesmo para a análise do risco financeiro de uma companhia. (ZAPATER; SUZUKI, 2005).

Juntamente com as normas, uma política de segurança deve definir as responsabilidades a todos os envolvidos no processo. Segundo Lemos (2001), as políticas de segurança fornecem um conjunto de normas, métodos e procedimentos que

devem ser utilizados para a manutenção da segurança da informação, devendo esta ser documentada e de conhecimento de todos.

Por fim, a adoção de normas e políticas no uso dos sistemas computacionais, permite criar formas eficazes de padronizar o gerenciamento da segurança da informação, e podem não só ser utilizada por organizações de qualquer porte, mas também por usuários domésticos, na busca constante de minimizar as ocorrências de incidentes de segurança.

2.4 PRINCIPAIS AMEAÇAS DIGITAIS

A Internet sem dúvida revolucionou a vida da sociedade contemporânea. Com ela uma infinidade de recursos foram disponibilizados, seja para execução de tarefas profissionais, lazer, entretenimento ou muitas outras atividades.

Mas apesar de beneficiar uma grande parte da população, servindo como auxílio na realização de inúmeras tarefas, a Internet também trouxe consigo um grande número de problemas, associados a segurança dos dados de seus usuários. Hoje o número de ameaças existentes cresce a cada dia, ficando difícil identificar e controlar até mesmo para usuários que estão envolvidos profissionalmente com estes problemas.

Segundo (CERT, 2007), o número de tentativas de novas fraudes digitais detectadas durante o ano de 2006 atingiu 197.892 notificações. Boa parte destas fraudes poderiam ter sido evitadas caso não houvesse tanta falta de conhecimento por parte dos usuários da Internet.

> Os principais problemas de segurança que acontecem nos computadores domésticos são causados, em sua maioria, pela falta de conhecimento do usuário sobre os códigos maliciosos que proliferam por aí e sobre o próprio sistemas operacional que ele usa. Ainda há muito despreparo quanto a melhores práticas e procedimentos cotidianos no computador e na navegação Internet. (MACHADO; FREIRE, 2006).

O número de fraudes que podem ser evitadas simplesmente com conhecimento é grande, já que muitos ataques dependem da ajuda dos usuários para que ocorram, seja clicando em algum *link* de Internet ou executando alguma aplicação desconhecida. Um usuário informado e atento deixaria de executar estas ações e poderia estar evitando, por exemplo, a entrada de um *software* malicioso em seu computador. Segundo Zapater e Suzuki (2005), o elo fraco da corrente da segurança são as pessoas. "Sempre que a informação necessita ser manuseada por uma pessoa, ela está potencialmente em risco."

O conhecimento também facilita e estimula o usuário a instalar *softwares* que auxiliam na segurança como antivírus, *firewalls* pessoais, sistemas de detecção de intrusão, e outros.

Segundo Machado e Freire (2006) hoje a maioria das pessoas estão com seus computadores contaminados sem saber, e nem mesmo usuários mais experientes e acostumados a trabalhar *on-line* estão distantes das ameaças digitais, sendo que muitos relatam já terem passado por problemas deste tipo. "Isso acontece porque, por mais experientes que sejam, eles não tiveram cuidados suficientes ao manipular seus arquivos. Em suma, ninguém está livre de um ataque virtual".

O funcionamento destes ataques digitais varia de técnica para técnica, utilizada pela pessoa mal intencionada. Segundo (CERT, 2006), 59% dos ataques identificados hoje são provenientes de *worms,* que "é um programa capaz de se propagar automaticamente por meio de redes, enviando cópias de si mesmo de computador para computador." (CERT, 2006). Estes *worms* podem propagar uma série de pragas digitais de forma muito rápida por toda Internet.

Existe na Internet desde aplicativos que simplesmente incomodam o usuário danificando o sistema operacional, como alguns vírus, ou ferramentas de ataque mais

perigosas, que podem monitorar o que o usuário está fazendo no computador e, por exemplo, roubar informações bancárias quando o acesso ao Internet *Banking* for feito.

Estes e outros tipos de ataque serão citados a seguir, em suas diferenças e formas de funcionamento.

2.4.1 Engenharia Social

A engenharia social é um método antigo e utilizado não só em fraudes na Internet, mas também já conhecido em outros exemplos de fraudes, como telefônicas, por exemplo. Procura-se induzir o usuário a realizar alguma tarefa ou fornecer alguma informação que depois será utilizada na ação fraudulenta (MACHADO; FREIRE, 2006).

> O termo é utilizado para descrever um método de ataque, onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações. (CERT, 2006).

Pode-se citar como exemplo a seguinte situação. O usuário recebe um *e-mail* informando que existe uma atualização do sistema operacional que ele deve fazer para melhorar o funcionamento do seu sistema. Este *e-mail* informa um *link* que supostamente deveria ser do aplicativo que faria a atualização, mas na verdade é de um vírus que executado se instala na máquina.

Este tipo de ataque é quase sempre fácil de identificar, e basta um pouco de atenção e conhecimento para que uma decisão errada não comprometa a segurança do computador em questão, ou a rede de uma organização.

2.4.2 Vírus

Os vírus são pequenos programas ou *scripts*[1] que apresentam códigos executáveis e maliciosos que infectam sistemas computacionais (CRONKHITE; MCCULLOUGH, 2001).

Um vírus se diferencia de outra praga digital por sua capacidade de auto-reprodução, que torna possível infectar outros computadores, mas sempre por intermédio de alguma intervenção do usuário. Alguns vírus têm a capacidade de se propagar rapidamente pela Internet, infectando diferentes computadores no mundo inteiro em questão de minutos.

> Na terminologia da segurança de computadores, um vírus é um pedaço de um programa que, como um vírus biológico, faz cópias de si mesmo e se espalha anexando-se a um hospedeiro, o programa infectado. O programa infectado é um programa de computador que pode fazer parte do Sistema Operacional. Este programa infecta outros programas que permitem a propagação do vírus. (WIKIPEDIA, 2006a).

Os primeiros vírus foram criados antes mesmo do surgimento da Internet, e se propagavam normalmente por meio de compartilhamento de discos flexíveis (disquetes). Com o advento da Internet e a capacidade de troca de arquivos pela rede, os vírus ganharam um forte veículo de propagação.

Segundo Serrano (2001), o primeiro vírus de computador nasceu em 1987 e se chamava Brain. Ele danificava o setor de *boot* dos disquetes, e utilizava técnicas para passar despercebido pelo sistema. No final de 2005, segundo dados da Wikimedia Commons (2007), o número de vírus identificados ultrapassou a casa dos 70.000, como mostra a Figura 2.

---

[1] Roteiros, procedimentos ou pequenos programas que executam determinadas operações.

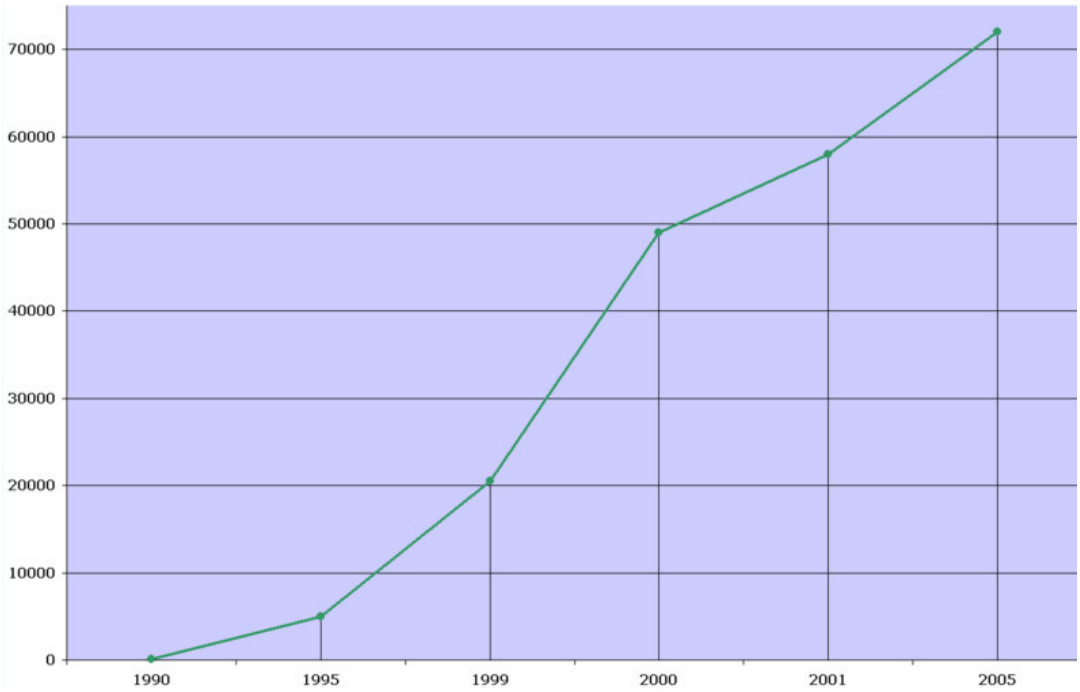

Figura 2. Evolução do número de vírus identificados de 1990 a 2005
Fonte: Wikimedia Commons.

Um vírus pode executar diferentes tarefas em um sistema computacional, entre elas:

a) excluir arquivos pessoais ou do sistema;

b) provocar perda de desempenho do computador;

c) alterar o conteúdo de arquivos;

d) liberar acesso às informações confidenciais a pessoas não autorizadas;

e) monitorar a utilização do computador;

f) diminuir o desempenho da rede (local e Internet);

g) desconfigurar o Sistema Operacional;

h) impossibilitar o uso de periféricos.

2.4.3 *Worms*

Worms (vermes) são programas maliciosos que podem ser projetados para vários fins, assim como os vírus, porém podem se reproduzir de forma rápida sem necessariamente uma intervenção do usuário. Um *worm* é um programa completo, e, diferente de um vírus, não necessita de um outro programa para se propagar (CERT, 2006).

> Enquanto o vírus precisa da intervenção do usuário para entrar na máquina, o *Worm* a dispensa. Não precisa nem de um clique; chega ao micro quando o usuário menos espera. Como explora falhas no sistema operacional, o usuário nada precisa fazer para ser infectado. (MACHADO; FREIRE. 2006).

Possuindo estas atribuições, os *worms* são mais difíceis de serem identificados, e também se espalham de forma muito mais rápida, dificultando o controle do problema. Em questão de minutos um *worm* pode, por *e-mail*, por exemplo, se propagar por diferentes lugares no mundo em progressão geométrica.

Um *worm* normalmente possui algoritmos inteligentes, podendo não só explorar um sistema operacional falho, mas também explorar sistemas em outras máquinas disponíveis.

2.4.4 Cavalos de Tróia

Um cavalo de tróia, também conhecido como *trojan*, é um programa que entra no computador escondido em algum arquivo qualquer que o usuário executa, abrindo portas que possibilitam acesso a informações e até ao controle do sistema (HATCH et al, 2002).

O nome cavalo de tróia teve origem na lenda da conquista de Tróia pela Grécia, onde um cavalo de madeira oco e cheio de soldados escondidos foi deixado nas

muralhas de Tróia. Os Troianos acreditavam ser um presente como sinal de rendição do exército grego, e levaram o cavalo para dentro da fortaleza. Porém a noite, soldados saíram de dentro do cavalo e abriram os portões de Tróia, e o exército grego pode sem muito esforço destruir e incendiar a fortaleza.

Assim como aconteceu em Tróia, hoje estes programas provocam inúmeras destruições nos sistemas computacionais. Qualquer arquivo executável de um sistema pode ser alvo desta ameaça.

Apesar de provocar problemas parecidos com os causados por vírus e *worms*, os cavalos de tróia não criam cópias de si mesmo, e não se espalham pela rede de forma descontrolada. Normalmente este tipo de ataque é utilizado não para causar falha no funcionamento do sistema computacional, mas sim para abrir portas em busca de informações sem que o usuário perceba.

Para Machado e Freire (2006) hoje o cavalo de tróia é a principal ameaça digital, já que possibilita o roubo de arquivos e informações do disco rígido, de *e-mail*, de textos, sendo os dados financeiros os mais visados.

Com acesso ao computador da vítima, o invasor pode, além de muitas outras coisas, saber, por exemplo, tudo que o mesmo digita no seu teclado, utilizando para isso um *Keylogger*, que armazena as informações e envia ao invasor por meio da Internet.

2.4.5 *Phishings*

Um *phishing*, também conhecido como *phishing scam*, é uma fraude digital desenvolvida para roubar informações de usuários da Internet (CERT, 2006). O fraudador mal-intencionado envia uma mensagem que pode ser um *e-mail*, e, utilizando técnicas de Engenharia Social, se faz passar por alguma instituição conhecida, como um

banco, provedor de Internet, ou qualquer *site* popular, tentando induzir o acesso a páginas falsas, criadas para furtar dados pessoais, financeiros, entre outros.

O termo *phishing* surgiu da palavra "pescar" (*fish*), dando idéia de roubar as informações dos usuários.

Normalmente um *phishing*, enviado por *e-mail*, solicita que o usuário efetue ou atualize um cadastro, fornecendo assim seus dados, que serão na verdade enviados para o invasor. Este *e-mail* pode também conter *links* falsos para programas ou *scripts* maliciosos.

De acordo com a pesquisa divulgada pelo *Websense Security Labs* (2006), só em junho deste ano de 2006 surgiram 1.422 novos *phishings* na Internet.

Quase sempre o *site* falsificado ou *e-mail* enviado, usa exatamente toda identidade visual da entidade verdadeira, fazendo com que a vítima não desconfie em momento algum que está sendo fraudada.

2.4.6 *Sniffing*

O *sniffing* é uma técnica que utiliza escutas em redes locais, para monitorar todo tráfego de dados e possibilitar assim a captura de qualquer informação, como senhas e dados confidenciais (GOMES, 2000).

Apesar de ser uma técnica voltada para ataques em redes locais, o *sniffing* pode ser utilizado em *links* de Internet via cabo e outros que utilizam uma pequena rede local, normalmente em condomínios e prédios onde a Internet é compartilhada.

> A Internet a cabo ou a rádio compartilhada com outras pessoas, assim, constitui grande perigo. Se estiver nesse trecho compartilhado um *software* do tipo "*sniffer*", que é um analisador de protocolos, será possível ler *e-mails* dos usuários, pegar senhas, e assim por diante (MACHADO; FREIRE, 2006).

Por este motivo, conexões *Asymmetric Digital Subscriber Line* (ADSL) são muito mais seguras do que as via cabo ou rádio. Praticar um *sniffing* em uma conexão ADSL é mais complicado, pois ela utiliza linha telefônica para acesso, só tornando possível a escuta do provedor em diante, afirma Machado e Freire (2006).

Utilizar *sites* que possuam proteção *HyperText Transfer Protocol Secure* (HTTPS) e que contenham dados criptografados é importante para garantir que as informações não sejam visualizadas mesmo que um *sniffing* seja utilizado, já que o invasor não terá como descriptografar a informação roubada.

2.4.7 Ataques de Força Bruta

Em um ataque de força bruta é feita a tentativa de descobrir o nome de usuário e senha de um sistema de acesso restrito, como por exemplo, um serviço de *e-mail* (MACHADO; FREIRE, 2006).

Primeiro o nome de usuário é descoberto, e no caso de um serviço de *e-mail* isso é bastante simples, já que o usuário de uma conta de *e-mail* normalmente é o próprio *e-mail*. Após descobrir o usuário, tentativas sucessivas de acesso com diferentes senhas são feitas, até que a senha correta seja validada e o acesso permitido.

Devido este motivo, é tão importante que a escolha de senhas seja feita com bastante cuidado, para que as muito fáceis não sejam utilizadas. Em um ataque como este, quanto maior número de caracteres diferentes na senha, mais difícil será "quebra-la", por isso denomina-se força bruta.

Apesar de ser relativamente simples, esta técnica vem perdendo espaço, já que é também fácil de ser combatida. A grande maioria dos servidores já bloqueia tentativas sucessivas de acesso com falhas por dados incorretos.

2.4.8 *Bots* e *Botnets*

Um *bot* é um programa que assim como um *worm*, é capaz de se propagar automaticamente, explorando vulnerabilidades existentes ou falhas na configuração de *softwares* instalados em um computador (CERT, 2006).

O que diferencia um *bot* de um *worm*, é que ele dispõe de mecanismos que possibilitam a comunicação com o invasor, fazendo com que ele controle o *bot* remotamente[2].

Segundo (CERT, 2006), normalmente um *bot* se conecta a um servidor de *Internet Relay Chat* (IRC) e entra em um canal (sala). Então, ele aguarda por instruções do invasor, e fica monitorando as mensagens que estão sendo enviadas. Ao se conectar ao mesmo servidor de IRC, o invasor entra no mesmo canal, e envia mensagens compostas por seqüências especiais de caracteres, que são interpretadas pelo *bot*, e correspondem a instruções que devem ser executadas pelo *bot*.

O invasor que possui controle remoto ao *bot*, pode enviar instruções para que ele realize diversas atividades, como desferir ataques na Internet, furtar dados do computador onde está sendo executado, enviar *e-mails* de *phishing* e SPAM entre outros.

Quando são formadas redes de computadores infectados com *bots* tem-se as chamadas *botnets*. Estas redes podem ser compostas por milhares de computadores, e um invasor que tenha controle sobre uma *botnet* pode utilizá-la para aumentar a potência dos ataques (CERT, 2006).

---

[2] Acesso à distância entre um terminal ou computador e uma rede.

2.4.9 *Pharming*

Um *pharming* é um programa capaz de redirecionar o tráfego da Internet de um *site* para outro, de forma que o usuário imagine estar visitando o *site* legítimo (MICROSOFT, 2006).

O *pharming* pode parecer semelhante ao *phishing*, executado por correio eletrônico, porém ele é mais insidioso, uma vez que redireciona a vítima para um *site* falso, sem que o usuário ao menos desconfie disso.

Um ataque de *pharming* pode manipular o serviço de *Domain Name System* (DNS) que é responsável por traduzir um nome alfanumérico para um número *Internet Protocol* (IP), que determina a localização de um servidor, alterando-o de acordo com os desejos do atacante.

Com a tradução comprometida é possível que o usuário da Internet introduza o endereço do *site* que deseja visitar, mas seja redirecionado para um servidor diferente do pretendido, controlado pelo atacante, e que pode conter um *site* idêntico ao da entidade verdadeira. Assim, o atacante pode armazenar informações confidenciais do visitante, sem que ele perceba.

2.4.10 *Sites* falsos

Um *site* falso, como o próprio nome diz, é um *site* parecido ou até mesmo idêntico ao *site* da entidade verdadeira, desenvolvido com o propósito de furtar informações sigilosas dos usuários que o utilizam (MACHADO; FREIRE, 2006).

Uma pesquisa do instituto americano *Anti-Phishing Working Group* (APWG) aponta que os *sites* fraudulentos crescem em média 50% por mês, o que é bastante preocupante devido a este índice.

O *site* falso normalmente chega até a vítima por meio de um *phishing* ou envenenamento de *cache* (*pharming*), e utiliza interfaces parecidas ou até mesmo idênticas às da empresa que está sendo utilizada como intermédio para o ataque, para induzir o usuário a clicar em um *link* e entrar no *site* falso.

Quando o ataque é feito por meio de um *link* de Internet, normalmente ele difere pouca coisa do endereço real, sem que o usuário perceba se não estiver bastante atento. Por exemplo, o *site* "www.unesc.net" poderia ser utilizado como "www.umesc.net", ou ainda trocando a extensão do domínio "www.unesc.com", que seria apontado para o *site* falso. Se o usuário utilizasse este *site* e inserisse seus dados de nome de usuário e senha, o invasor depois poderia utilizar estes dados para efetuar tarefas restritas e ilícitas.

2.4.11 *Exploits*

Um *exploit* é um programa de computador que contém códigos que exploram falhas do sistema operacional e também de outros aplicativos, e se aproveitam das vulnerabilidades (CERT, 2006).

Segundo Wikipedia (2006b), até meados dos anos 90, acreditava-se que os *exploits* exploravam exclusivamente problemas em aplicações e serviços voltados para as plataformas Unix. "A partir do final da década, especialistas demonstraram a capacidade de explorar vulnerabilidades em plataformas de uso massivo, por exemplo, sistemas operacionais Win32 (Windows 9x, NT, 2000 e XP)".

2.4.12 Ataques de *Buffer Overflow*

Os ataques de *buffer overflow* (estouro de pilha) são utilizados para comprometer o espaço de endereçamento de memória de um computador, e assim permitir que os dados que excederam o limite da pilha sejam executados como código pelo processador (HATCH et al, 2002).

Uma vez que o endereçamento de memória chega ao seu limite, o sistema permite que um invasor possa interagir com o sistema operacional, e assim possibilitar que o mesmo execute tarefas ilícitas.

> Executam-se instruções de modo que a aplicação responsável por elas se confunda e traga mais informações do que pode suportar. O *hacker*[3], aí, interage com a aplicação e obriga o sistema operacional a fazer o que ele quer – dando-lhe o acesso de administrador (MACHADO; FREIRE, 2006).

2.4.13 *Spyware*

Um *spyware* é um programa que possibilita a busca de informações sobre o usuário, seus hábitos e costumes na utilização da Internet e transmite estas informações à entidade que está fazendo o levantamento, ou ao invasor interessado em alguma informação, isso tudo sem que o usuário perceba (CERT, 2006).

Segundo Machado e Freire (2006), a cada dez ameaças encontradas hoje na Internet, três são *spyware*, e o Brasil é o quinto país com mais incidência deste problema.

Existem *spywares* desenvolvidos por empresas, que monitoram as preferências do usuário, para poder fornecer produtos de acordo com o perfil de cada

---

[3] Termo originário do inglês usado para designar um especialista em informática.

pessoa, fazendo assim com que as vendas aumentem. Eles utilizam análise dos *cookies*[4] armazenados no navegador ou ainda verificam o *cache* do mesmo, podendo assim saber o histórico de *sites* visitados.

Por outro lado, existem também vírus com *spywares*, que utilizam de suas características para roubar dados confidenciais dos usuários, como *logins*[5] de sistemas autenticados.

Segundo Wikipedia (2006c), os *spywares* podem ser introduzidos mediante a instalação de programas *shareware* ou *freeware*, uma vez que o sistema é gratuito, a empresa que o desenvolveu acaba lucrando com a venda de informações dos usuários.

2.4.14 *Adware*

Adware é uma maneira curta de dizer *Advertising Software*, ou seja, *software* de publicidade. É um *software* que mostra anúncios de diferentes tipos e formas no computador. Propagandas de empresas, produtos, serviços e outros, exibidos por meio de *banners*[6] e inúmeras outras maneiras (CERT, 2006).

O *adware* muitas vezes é confundido com o *spyware*, talvez pelo fato de utilizar as informações geradas pelos *spywares* para mostrar o anúncio de acordo com o perfil do usuário. Os *spywares*, ao contrário dos *adwares*, não mostram anúncios, apenas roubam informações. Alguns *adwares* modernos fazem também o papel de *spyware*, monitorando as ações do usuário para ter acesso ao seu perfil, e assim poder exibir propagandas de acordo com o mesmo.

---

4 Pequeno conjunto de informações armazenado no computador por alguns sites.
5 Nome que o usuário usa para acessar uma área restrita.
6 Imagens gráficas de pequeno tamanho utilizadas como anúncio nos sites.

Assim como os *spywares*, os *adwares* também podem ser instalados no computador juntamente com *softwares* gratuitos, e assim tornam possível o lucro da empresa que o desenvolveu, por meio de anúncios.

Os *adwares* normalmente são programas que não provocam problemas no sistema computacional, apenas incomodam com a exibição de anúncios não desejados. Porém, segundo Wikipedia (2006c), hoje já existem *adwares* muito mais sofisticados, de remoção complexa, que produzem alterações no registro do sistema operacional e depois somem para garantir que as alterações não sejam desfeitas, tornando necessário não mais a ação de um *software* de rastreamento de *adwares*, mas sim de um reparador do registro do sistema.

2.4.15 *Rootkits*

Rootkit é um programa como cavalo de tróia, que se esconde de *softwares* de segurança, utilizando técnicas de programação avançada, não tornando possível a visualização de suas chaves de registro e nem seus processos, o que torna a identificação e a remoção desta praga muito complexa (HATCH et al, 2002).

Uma vez que o *rootkit* está instalado no computador, ele pode executar inúmeras tarefas sem que o usuário perceba, como abrir portas, ativar ou desativar serviços, criar novas contas de usuário, entre outras ações, todas administradas remotamente pelo invasor.

2.4.16 *Backdoors*

Backdoors são partes de código fonte mal-intencionado, que provocam falhas de segurança e permitem acesso ao sistema operacional à pessoas não

autorizadas. Estes códigos abrem portas de acesso para que o invasor possa executar diversas tarefas (CERT, 2006).

O *backdoor* também torna possível que o fraudador consiga retornar ao computador comprometido, sem precisar recorrer novamente aos métodos utilizados na realização da primeira invasão.

Em alguns casos, fabricantes de aplicativos incluem *backdoors* em seus produtos alegando necessidades adversas, como verificação de atualizações de versão. Porém, mesmo no caso de fabricantes conhecidos, o uso desta ferramenta acaba sendo uma ameaça para segurança de um computador, mesmo porque muitas vezes não só a empresa que desenvolveu o aplicativo obtém acesso ao computador, mas também outras pessoas mal intencionadas.

2.4.17 *Keyloggers* e *Screenlogger*

Keyloggers são *softwares* que monitoram tudo que é digitado no teclado de um computador, e criam um arquivo com estas informações, que podem ser posteriormente enviadas por meio da Internet, permitindo assim roubar senhas, *logins*, números de conta corrente e cartões de crédito, endereços de *e-mail*, enfim, tudo que for digitado (MACHADO; FREIRE, 2006).

Normalmente os *keyloggers* chegam até o computador da vítima por meio de um cavalo de tróia, escondido em algum outro aplicativo necessitado pelo usuário. Uma vez executado ele inicia a gravação de tudo que é digitado e envia para a pessoa que está fazendo o ataque por meio de correio eletrônico ou *File Transfer Protocol* (FTP), por exemplo, isso em intervalos de tempo pré-definidos.

A pessoa que está fazendo uso das informações geradas pelo *keylogger*, ainda pode filtrar o conteúdo que o mesmo armazena, fazendo com que ele grave, por exemplo, apenas senhas digitadas.

Devido ao alto índice de fraudes digitais executadas por meio da utilização de informações geradas por *keyloggers*, os *sites* que exigem um grau de segurança maior, que é o caso de instituições financeiras, desenvolveram teclados virtuais para que os seus clientes não precisem digitar a senha, e sim selecionar as teclas com o *mouse*. Mediante isso, os *keyloggers* evoluíram para os chamados *screenlogger*.

Um *screenlogger* é capaz de armazenar a posição do cursor do *mouse* no momento em que o botão é clicado, e também gerar imagens destas regiões, fazendo com que a segurança imposta pelos teclados virtuais diminua bastante (CERT, 2006).

2.4.18 *Hoaxes*

Os *hoaxes* são boatos, lendas, ameaças e mentiras que circulam pela Internet, principalmente por meio de correntes de *e-mail* (CERT, 2006). São mensagens com assuntos normalmente interessantes e conteúdo alarmante, como por exemplo, uma mensagem informando que o *site* de comunidade virtual Orkut irá excluir os usuários inativos que não encaminharem aquele *e-mail* para 20 pessoas de sua lista de contato.

Alguns *hoaxes* fazem alertas de vírus inexistentes, solicitando também que o usuário encaminhe a mensagem a seus contatos, caso contrário terão sérios problemas com seus computadores. Uma grande mentira.

Os *hoaxes* podem também serem definidos como um vírus social, que utiliza a boa fé dos usuários para se propagar. Alguns apenas com o intuito de ver a sua mensagem provocar pânico em questão de dias, já que estas mensagens se alastram em progressão geométrica de forma muita rápida, outros muitas vezes com objetivos de se

beneficiar, como é o caso de muitas campanhas falsas de arrecadação de fundos espalhadas pela Internet.

3 SINTOMAS DE SISTEMAS INFECTADOS

Normalmente sistemas infectados apresentam uma série de características que facilitam a identificação de problemas relacionados à segurança, por este motivo, é importante ficar atento a estes sintomas, que denunciam o comprometimento do computador.

A seguir estão alguns sintomas comuns que devem ser analisados.

3.1 ALERTAS DE ANTIVÍRUS

Softwares antivírus costumam rastrear os arquivos que estão no computador, os *e-mails* que são recebidos, e os dados que estão sendo acessados, alertando quando encontram algum tipo de vírus. Por isso é fundamental prestar atenção a estes alertas, e não ignorá-los.

Assim como os antivírus, outros *softwares* de segurança como alguns *anti-spyware*, também costumam fazer alertas quando há alguma situação de perigo, e é importante analisá-los, até mesmo porque eles são um sinal de que o usuário pode estar sendo vítima de algum tipo de ataque, e às vezes é necessário não apenas tomar as medidas indicadas pelo *software* de segurança, mas outras mais ousadas, como por exemplo, retirar o computador da rede até que o problema seja solucionado, evitando que outras máquinas possam ser infectadas.

3.2 ARQUIVOS CRIADOS AUTOMATICAMENTE

É importante ficar atento a qualquer arquivo ou diretório criado no computador que não foram solicitados pelo usuário. Estes arquivos normalmente são

criados dentro do diretório raiz do sistema de arquivos e podem significar uma invasão (MACHADO; FREIRE, 2006).

3.3 EDIÇÃO E EXCLUSÃO DE ARQUIVOS

Quando ocorre a exclusão ou edição de qualquer arquivo do sistema sem a solicitação do usuário, pode ser um sinal de que alguma intervenção externa está ocorrendo. A manipulação de arquivos pode ser causada por vírus ou ainda por acesso não autorizado.

3.4 LENTIDÃO

Aplicativos como *spywares*, *rootkits* e cavalos de tróia, costumam executar processos escondidos, e às vezes estas tarefas deixam o computador mais lento que o normal. O uso da Internet como forma de envio e recebimento de informações por estes aplicativos, também pode ser um forte indício de sistemas infectados, já que a velocidade de navegação pode diminuir bastante nestes casos. Por este motivo é fundamental ficar atento à velocidade de resposta de uma solicitação.

3.5 COMPARTILHAMENTO DE PASTAS

Algumas técnicas de invasão costumam utilizar pastas que são compartilhadas no computador para buscar arquivos. É importante uma maior atenção aos compartilhamentos existentes, principalmente quando estes não foram feitos pelo usuário do computador.

3.6 REDIRECIONAMENTO DE SITES

É natural errar o endereço digitado na barra de endereços do navegador de Internet no momento que um *site* é acessado. Em um computador com sistema operacional Windows não infectado, seria mostrada a página de erro padrão da Microsoft, informando a inexistência do endereço acessado. Em computadores infectados por *spywares*, ao invés de exibir a página de erro, o usuário é redirecionado para um outro *site*, normalmente com exibição de anúncios de produtos ou serviços.

3.7 EXIBIÇÃO DE ANÚNCIOS E PROPAGANDA

Spywares e *adwares* costumam exibir anúncios de diversas formas. Em uma máquina infectada por estas pragas, é natural abrir janelas do navegador com páginas pornográficas, de vendas de produtos ou serviços, entre outras, o que é bastante fácil de identificar, até mesmo porque são repetitivas. Alguns *spywares* também instalam barras de ferramentas de empresas no navegador de Internet.

3.8 EXCESSO DE APLICATIVOS NO *STARTUP* DO SISTEMA OPERACIONAL

Quando um computador é ligado e um sistema operacional é inicializado, vários aplicativos são executados para possibilitar o funcionamento do sistema e também facilitar algumas tarefas do usuário, quando *softwares* que ele costuma utilizar já são automaticamente executados.

Alguns aplicativos maliciosos necessitam ser novamente executados quando o computador é reinicializado. A lista de aplicativos executada na inicialização do sistema operacional pode ser acessada pelo usuário, assim este pode verificar os

softwares que estão sendo inicializados no momento que o computador é ligado, e desativar os que são suspeitos. Isso, além de possibilitar o não funcionamento de algumas pragas digitais, pode contribuir com a melhoria do desempenho do sistema, já que o usuário pode tirar da lista de inicialização aplicativos que não utiliza. Algumas pragas mais sofisticadas, não são mostradas na lista de *startup*, pois trabalham de forma oculta.

A lista de *startup* do sistema operacional Windows, da Microsoft, pode ser acessada no menu Iniciar, Executar, "msconfig", aba "Inicializar".

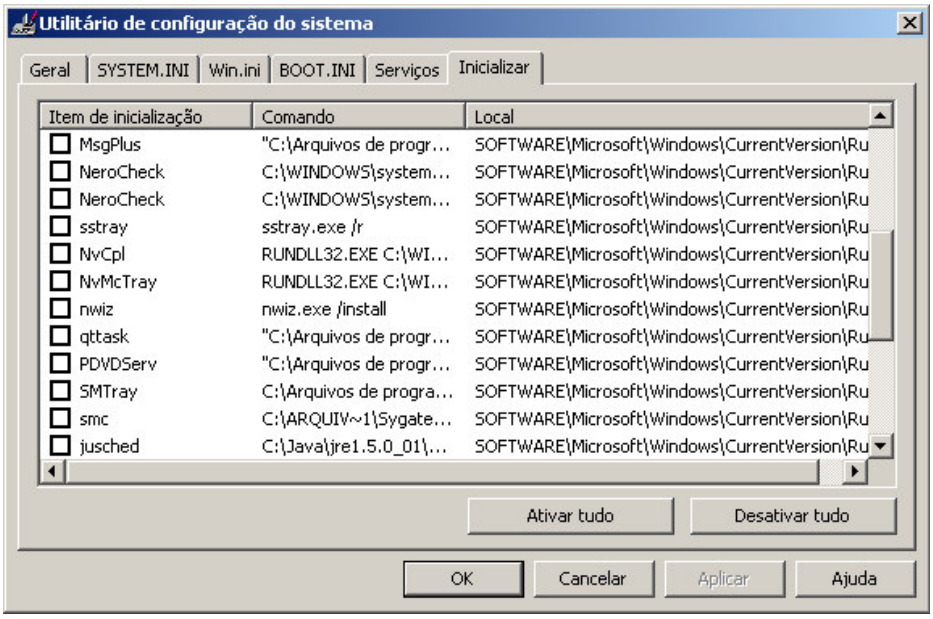

Figura 3. Lista de *startup* do sistema operacional Windows da Microsoft
Fonte: Microsoft (2006).

3.9 NOVOS USUÁRIOS

Quando alguma invasão ocorre, é possível aparecerem novos usuários com acesso ao sistema, que não foram criados pelo administrador do computador. Segundo Machado e Freire (2006), isso ocorre para que o invasor possa ter acesso ao sistema mesmo que um antivírus localize o código malicioso e o destrua. Por mais que o

problema com o vírus seja tratado, o usuário criado normalmente não é localizado pelo antivírus.

3.10 PROCESSOS DESCONHECIDOS

Todo processo que está sendo executado pelo computador fica disponível para que o usuário possa visualizar. No Windows estes processos podem ser visualizados no Gerenciador de Tarefas, acessado utilizando as teclas “Ctrl + Alt + Delete."

Fazendo o controle dos processos que estão sendo executados, é possível identificar e parar um processo suspeito, porém, assim como na lista de *startup*, alguns programas são executados de forma oculta, não aparecendo no gerenciador de processos.

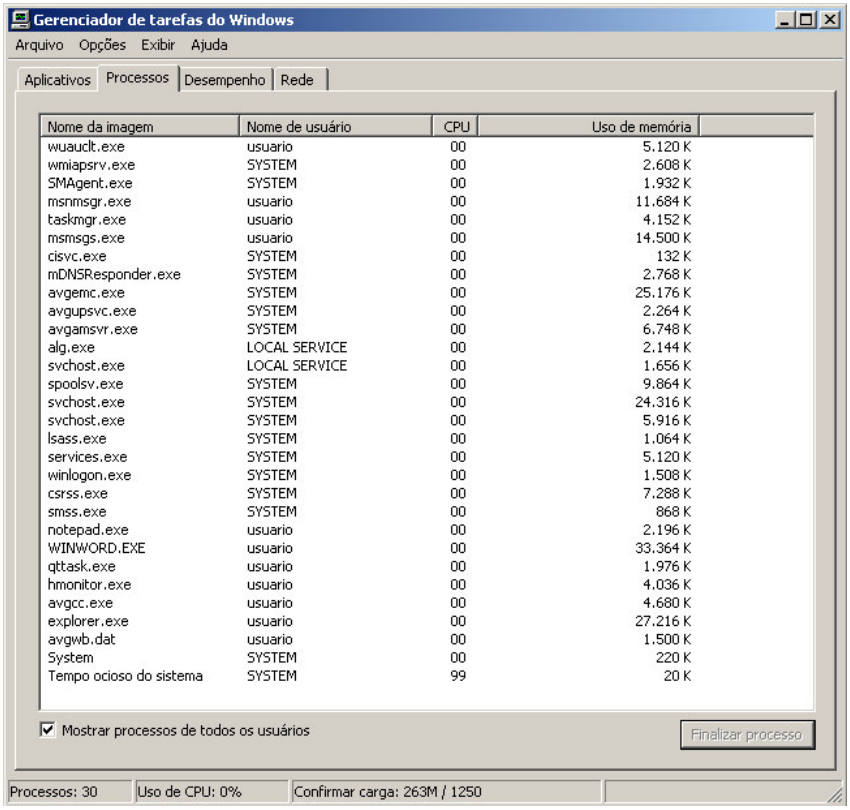

Figura 4. Lista de processos do sistema operacional Windows da Microsoft
Fonte: Microsoft (2006).

4 PROCEDIMENTOS DE DEFESA

Apesar do número de técnicas utilizadas para quebra da segurança ser bastante grande, boa parte das ações criminosas praticadas na Internet podem ser evitadas com um pouco de conhecimento e cuidado por parte dos usuários.

Segundo pesquisa do Núcleo de Informação e Coordenação (NIC, 2005) apenas 19,33% dos usuários da Internet no Brasil, fazem uso de *Firewalls* Pessoais (*Softwares* que controlam o tráfego da Internet, impedindo que usuários não autorizados tenham acesso a determinadas informações), o que acaba facilitando a incidência de casos de problemas com segurança.

Por outro lado, a pesquisa citada mostra que quase 70% dos usuários de Internet possuem algum antivírus instalado em seu computador, talvez porque sejam *softwares* de defesa utilizados a mais tempo e mais difundidos.

A seguir serão abordadas algumas ações que auxiliam na segurança de em computador, desde simples cuidados na navegação a instalação de *softwares* mais elaborados.

4.1 CUIDADOS DURANTE A UTILIZAÇÃO DA INTERNET

A grande maioria das ameaças existentes na Internet, só manifestam-se e obtém sucesso, mediante a intervenção do usuário, seja clicando em algum *link,* executando algum arquivo desconhecido, ou inúmeras outras tarefas. Por este motivo, são fundamentais alguns cuidados durante a utilização da Internet, para assim diminuir significativamente o número de incidentes de segurança.

4.1.1 Recebimento de *e-mails*

O *e-mail* é talvez uma das portas de acesso mais utilizadas para que as pragas digitais cheguem até as vítimas, devido a facilidade que se tem em enviar um *e-mail* a qualquer pessoa sem que a mesma solicite ou autorize.

Um *e-mail* pode conter informações falsas de engenharia social, *links* de Internet falsos ou mascarados, arquivos infectados em anexo, e outras pragas que podem acarretar a contaminação do computador e levar o usuário a se tornar vítima de um golpe virtual. É importante tomar alguns cuidados, tais como:

a) desconfiar sempre do conteúdo dos *e-mails* recebidos, tentativas de engenharia social podem ser utilizadas;
b) não clicar em *links* de Internet que não tenha plena certeza da sua procedência, mesmo que o endereço mostrado seja de um *site* conhecido, o endereço que está no *link* pode estar mascarado e levar a um *site* diferente do apresentado;
c) não abrir arquivos anexos que não se saiba exatamente o que é e de onde vem. Eles podem conter vírus, cavalos de tróia e outras pragas digitais;
d) observar a extensão dos arquivos anexos. Cuidado principalmente com arquivos .bat, .com, .cmd, .exe, .pif e .scr. São os mais comuns por serem executáveis, podendo conter códigos maliciosos;
e) utilizar um antivírus que verifica as mensagens do *software* utilizado para receber *e-mails*;
f) se possível, ler e-mails em modo texto, e não em formato HTML;
g) manter a versão do *software* leitor de *e-mail* sempre atualizada.

4.1.2 Navegação em *sites*

A navegação por meio de *browsers* pode causar muitos problemas se alguns cuidados não forem tomados. A Internet possui milhares de *sites*, e neles podem estar contidos várias pragas, principalmente naqueles com conteúdo desconhecido.

É recomendável:

a) navegar por *sites* oficiais, de entidades conhecidas. Evitar *sites* com conteúdo pornográfico, jogos, *hacker*, de pirataria e afins;

b) evitar clicar em *links* desconhecidos;

c) tomar cuidado com *sites* falsos. Verificar se o *site* que está visitando tem todas as características encontradas em navegações anteriores;

d) evitar preencher cadastros com dados pessoais se não for extremamente necessário;

e) desativar, se possível, a execução de *JavaScripts*[7] antes de entrar em uma página desconhecida. Isso evita que muitos códigos maliciosos sejam executados;

f) em *sites* de bancos, lojas virtuais e outros onde é necessário realizar transações com dados financeiros, verificar se existe certificação digital. Os *sites* com certificação de segurança válido, exibem um ícone de cadeado fechado no canto do navegador (*browser*) e mudam o início do endereço do *site* para “https”;

g) manter a versão do navegador de Internet (*browser*) sempre atualizada.

---

[7] Linguagem de scripts utilizada com freqüência na construção de páginas na Internet.

4.1.3 *Download* de arquivos

O *download* de arquivos desconhecidos pode trazer escondidas pragas digitais de diversos tipos, como por exemplo, os cavalos de tróia, que são inseridos em aplicativos executáveis. É recomendável:

a) fazer o *download* de aplicativos diretamente do *site* do fabricante. Isso evita cópia de *software* comum modificado por alguém mal intencionado;
b) evitar fazer *download* de arquivos desconhecidos, principalmente se forem executáveis;
c) executar um *software* antivírus nos arquivos que fizer *download* antes de abrí-los.

4.1.4 Compartilhamento e troca de arquivos

Segundo Machado e Freire (2006) a proliferação de serviços que possibilitam compartilhar arquivos de vários tipos, hoje é um dos maiores canais de infecção de computadores.

Estes arquivos compartilhados por *softwares peer-to-peer* (P2P), como o Kazaa, eMule, Shareaza, podem ser provenientes de usuários mal intencionados.

É preciso tomar cuidado principalmente com arquivos executáveis, pois estes podem conter cavalos de tróia, que são instalados juntamente com a aplicação necessitada.

Outro problema é que, para que estes *softwares* possam funcionar, são abertas portas altas[8] no computador, e isso pode facilitar a ação de um invasor.

O ideal é evitar a utilização de *softwares* P2P, ou pelo menos a cópia de aplicativos por meio deles, já que outros arquivos como MPEG-1/2 *Audio Layer* (MP3), por exemplo, não costumam apresentar códigos maliciosos.

4.1.5 Comunicação em sistemas de mensagem instantânea

Programas de comunicação instantânea, como o MSN Messenger da Microsoft, estão cada vez mais populares entre os usuários da Internet, já que as facilidades que eles trazem são inúmeras.

Mas apesar de facilitar a comunicação, estes *softwares* costumam abrir portas importantes para entrada de pragas digitais, como é o caso dos *worms.* É importante tomar os seguintes cuidados para evitar problemas:

a) não clicar em *links* desconhecidos, enviados por pessoas que estão na lista de contatos. Eles podem ser provenientes de usuário infectados por *worms.* Existem *worms* que quando executados, enviam mensagens de texto a toda lista de contatos, com um *link* falso que contém o arquivo infectado;

b) não aceitar o recebimento de arquivos desconhecidos;

c) não aceitar o cadastro de contatos de pessoas desconhecidas. Elas podem estar querendo abrir uma porta de comunicação com o computador para possibilitar ações ilícitas.

---

8 Porta é uma abstração utilizada por vários protocolos de Internet para permitir a distinção entre as diversas conexões simultâneas feitas a um único computador destino. Existem 65.536 portas *Transmission Control Protocol* (TCP), numeradas de 1 a 65536. As portas altas são as maiores que 1024.

4.2 ANTIVÍRUS

Os antivírus são *softwares* desenvolvidos para localizar e eliminar vírus, cavalos de tróia, *worms* e vários outros códigos maliciosos existentes no computador (CRONKHITE; MCCULLOUGH, 2001).

Existe uma grande variedade de *softwares* antivírus disponível, alguns gratuitos outros comerciais, soluções corporativas ou domésticas, cada um com suas peculiaridades, mas todos com o objetivo de afastar os riscos existentes com aparecimento de vírus.

Para localizar um vírus, o antivírus verifica cada arquivo do computador e compara com uma lista chamada lista de definição, que contém um banco de dados com informações de todos os vírus conhecidos. Este banco de dados é fornecido pela empresa que desenvolve o aplicativo, e constantemente localiza novos vírus e cria vacinas para eles. Por este motivo é tão importante manter o antivírus atualizado, já que um vírus recente pode não ser identificado caso não esteja na lista de definição.

4.3 ANTI-SPYWARE E ANTI-ADWARE

Os *anti-spyware* e *anti-adware* são *softwares* que se assemelham aos antivírus, porém como o nome já diz, são específicos para localizar e eliminar *spywares* e *adwares* (MACHADO; FREIRE, 2006).

Alguns antivírus incorporam funções para remover *spywares* e *adwares*, porém segundo (UOL, 2006) “um *anti-spyware* específico ainda faz parte da programação de segurança da maioria dos usuários”.

Assim como os antivírus, os *anti-spyware* e *anti-adware* também guardam uma base de informações, e devem ser atualizados constantemente, para que possam identificar as últimas ameaças existentes.

4.4 FIREWALL

Firewall (parede de fogo) é um importante dispositivo de segurança que monitora o tráfego da rede, possibilitando impedir a transmissão de dados nocivos ou não autorizados (HATCH et al, 2002).

Um *firewall* pode analisar pacotes recebidos de vários protocolos, e assim, desempenhar várias ações condicionais que podem ser configuradas por meio de regras.

O administrador do *firewall* pode determinar por meio de regras o que pode e o que não pode trafegar na rede, bloqueando portas de acesso, números IP, palavras censuradas, determinados tipos de arquivos entre outros.

Um *firewall* pode ser um *hardware* com um *software* interno, ou simplesmente um *software* instalado em um computador, que pode ser um servidor de uma rede corporativa que monitora todo o tráfego da rede, ou ainda um computador pessoal, onde se pode instalar *firewalls* pessoais.

O *firewall* pessoal monitora tudo o que trafega na máquina do usuário onde o mesmo está instalado, e isso torna possível evitar a ação de muitas pragas digitais. Os *keyloggers*, por exemplo, armazenam tudo que é digitado no teclado do computador, e enviam estes dados normalmente por meio de FTP. Em uma máquina com um *firewall* instalado, este irá notificar a tentativa de envio de informações por meio da porta 21 para um IP desconhecido, e esta ação poderá ser autorizada ou negada pelo usuário, evitando assim o envio de informações não autorizadas.

Além de verificar o tráfego de saída, o *firewall* pessoal pode monitorar todo o tráfego de entrada, e assim todas as ações suspeitas podem ser bloqueadas.

4.5 ATUALIZAÇÕES DO SISTEMA

Não basta utilizar várias ferramentas de defesa contra ameaças digitais, se estas ferramentas e também seus aplicativos não estiverem devidamente atualizados.

Softwares de defesa como antivírus e *anti-spyware*, precisam ser atualizados frequentemente, uma vez que novas ameaças são criadas todos os dias.

Em sistemas computacionais, principalmente no sistema operacional, as descobertas de vulnerabilidades não percebidas no momento da criação são freqüentes, e estas são corrigidas por meio de *patches* de atualização, fornecidos pela empresa desenvolvedora.

Estes *patches* normalmente podem ser adquiridos facilmente por *download*, de forma automática, basta que o usuário aceite a atualização, sendo importante que o faça.

5 PESQUISA DE CAMPO

A pesquisa apresentada neste projeto teve natureza quali-quantitativa e aconteceu por meio de um processo de coleta de dados de um público alvo específico, que foram analisados e discutidos a partir da fundamentação teórica.

5.1 PÚBLICO ALVO

Os sujeitos da pesquisa foram acadêmicos de graduação da Universidade do Extremo Sul Catarinense (UNESC), divididos de acordo com as áreas de conhecimento de seus cursos. A faixa etária média variou dos 18 aos 35 anos e o questionário foi aplicado para ambos os sexos.

5.2 COLETA DE DADOS

Foram aplicados como instrumento de coleta de dados, questionários semi-estruturados, com questão abertas e fechadas. Os questionários (Apêndice A) foram entregues pessoalmente a cada um dos participantes depois de aceitarem participar desta pesquisa.

Foram aplicados um total de 260 questionários, o que segundo Barbetta (1998) gera um erro amostral estatístico de 6 pontos percentuais, seguindo a fórmula apresentada na Figura 5.

$$n_0 = \frac{1}{E_0^2} \qquad n = \frac{N \,.\, n_0}{N + n_0}$$

N tamanho da população
n tamanho da amostra
n_0 uma primeira aproximação
e_0 erro amostral tolerável

Figura 5. Fórmulas para cálculo do erro amostral estatístico.

5.3 ANÁLISE DOS DADOS

Os dados foram catalogados, agrupados e analisados. O resultado da pesquisa será discutida conforme a relevância das questões e apresentada em forma de gráficos.

5.4 RESULTADOS

Ao serem questionados sobre o hábito de fazer compras pela Internet, 26% disseram que não têm este hábito, enquanto 74%, um número considerável, afirmaram comprar por este meio, como mostra a Figura 6.

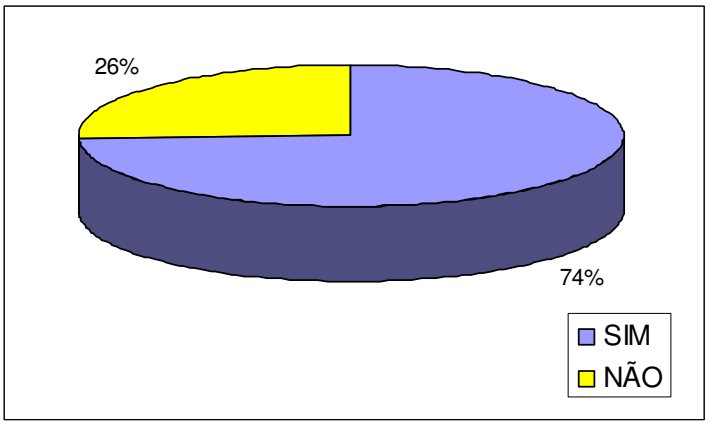

Figura 6. Prática de fazer compras pela Internet

O segundo gráfico apresentado na Figura 7, demonstra que 63% dos entrevistados já deixaram de comprar pela Internet com medo de exporem seus dados pessoais, 20% nunca deixaram e 17% não deixaram de comprar, porém tiveram receio. Estes dados mostram que as negociações realizadas na Internet são diretamente prejudicadas pela insegurança que os usuários têm em utilizar este recurso na compra.

Segundo dados do grupo de pesquisas e-bit (2007), o comércio eletrônico no Brasil movimentou 4,4 bilhões de reais em 2006. Este valor poderia ser

aproximadamente três vezes maior considerando que as pessoas que responderam não utilizar a Internet para fazer compras por medo, não tivessem este problema.

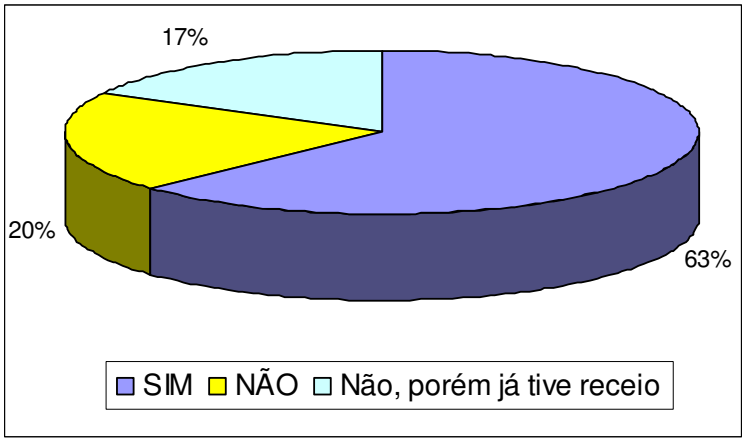

Figura 7. Deixar de comprar por medo de expor dados pessoais

A compra pela Internet vem utilizando cada vez mais o cartão de crédito como meio de pagamento. A Figura 8 demonstra os resultados da pesquisa que se referem a este aspecto.

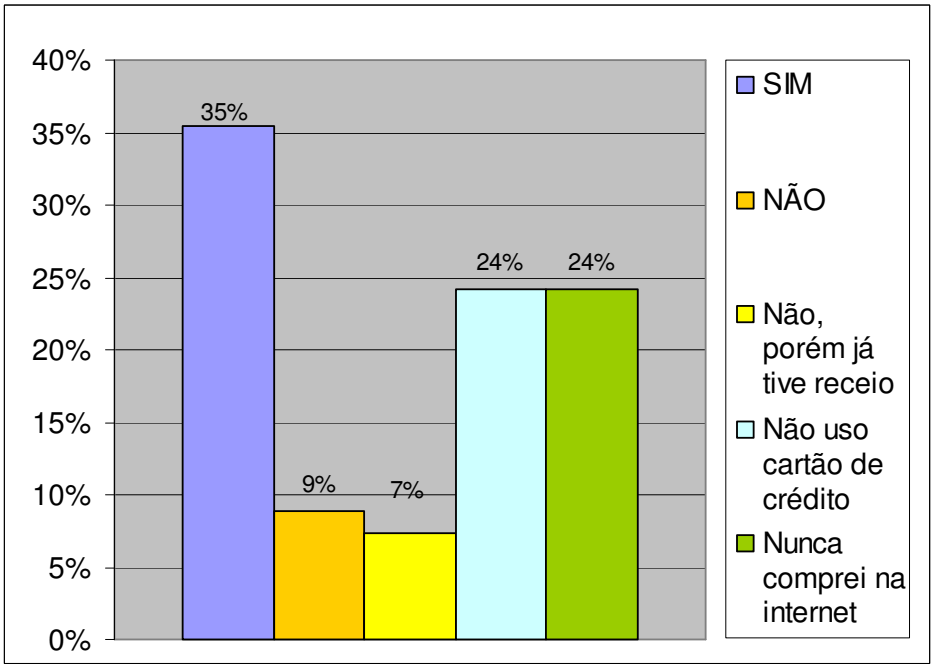

Figura 8. Deixar de comprar com cartão de crédito

Por medo de serem fraudados, 35% dos entrevistados já deixaram de comprar na Internet usando este recurso para pagamento, 9% não deixaram de utilizar o cartão de crédito, 7% não deixaram de usar, mas tiveram receio, 24% não utilizam cartão de crédito e 24% não compram pela Internet. Este resultado está apresentado na Figura 8.

O cartão de crédito é talvez a forma mais simples de efetuar pagamento, principalmente tratando-se de compras na Internet. Por ser fácil fazer este tipo de transação simplesmente possuindo o número do cartão, o código de segurança e a validade, os dados do cartão de crédito são bastante visados por *crackers*[9], e talvez por isso causem receio ao usuário em utilizá-lo.

A não utilização do cartão faz com que o usuário e a empresa tenham que optar por uma forma de pagamento não tão simples operacionalmente, e consequentemente geram custos desnecessários.

A pesquisa também focou a utilização do *site* do banco para pagamentos, transações e consultas nas contas por meio da Internet. De todos os entrevistados, 16% disseram que utilizam com freqüência, a mesma quantidade (16%) afirmou utilizar poucas vezes e a maioria (68%), conforme a Figura 9, não utilizam o *site* do banco via Internet para estes fins.

[9] Pessoa que possui conhecimentos avançados de informática e utiliza esses conhecimentos para destruir sistemas alheios, sem se preocuparem com os resultados dos seus atos.

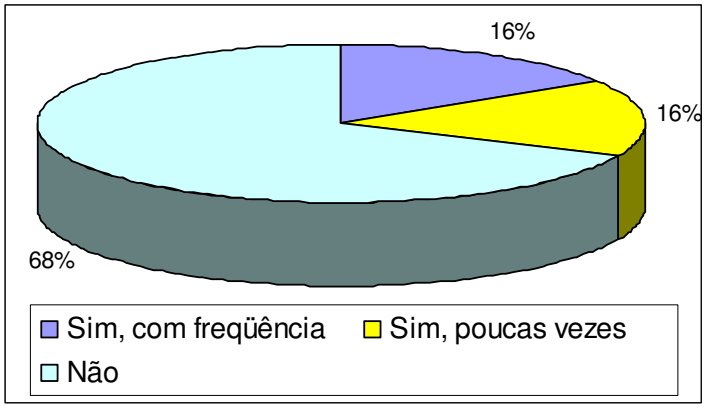

Figura 9. Utilização do *site* do banco para transações, pagamentos e consultas

Segundo Lira (2007), o auto-atendimento do cliente bancário que utiliza a Internet se torna mão-de–obra para o banco, que deixa de disponibilizar funcionários e estrutura física para atendê-lo, e isso acarreta uma economia de custos significativa. Lira (2007) ainda cita que "é provável que, se dependesse apenas das instituições financeiras, todas as agências como as que existem hoje seriam fechadas e os clientes fariam as suas operações por meios eletrônicos".

A Figura 10 representa os resultados encontrados na questão 6 do questionário aplicado e demonstra que 20% dos entrevistados já deixaram de fazer transações financeiras por meio do *site* do banco pela Internet com o receio de serem furtados, 16% se mostraram indiferentes respondendo que não, 8% afirmaram que não, porém tiveram receio e 57% não costumam utilizar o *site* do banco na Internet.

É muito provável que boa parte dos 57% que não utilizam o banco na Internet, também deixam de utilizar por medo de serem furtados, unindo-se aos 20% que já citam ter receio. Estes números, levando em consideração o custo menor que as instituições financeiras têm com os clientes que utilizam o Internet *Banking*, mostram que o prejuízo provocado pela não utilização é bastante grande.

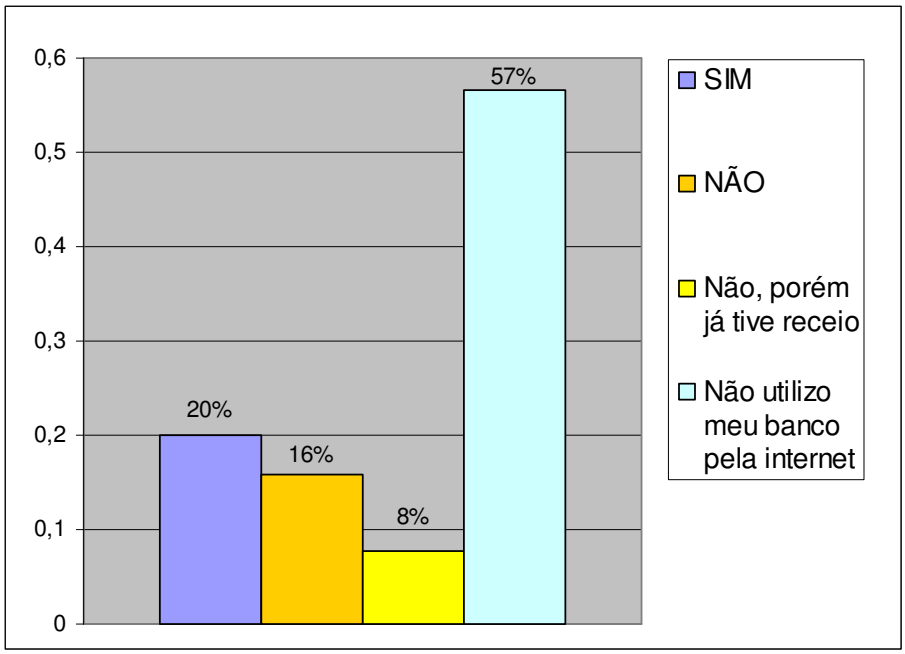

Figura 10. Não fazer transação financeira pela Internet por medo de ser furtado

Por meio dos resultados encontrados nas questões relativas a utilização da Internet no trabalho e o alerta das próprias empresas sobre os riscos e formas de proteção, que estão representados respectivamente nas Figuras 11 e 12, é possível afirmar que a maioria utiliza Internet no trabalho (65%), 19% não utilizam e 16% não trabalham, conforme a Figura 11.

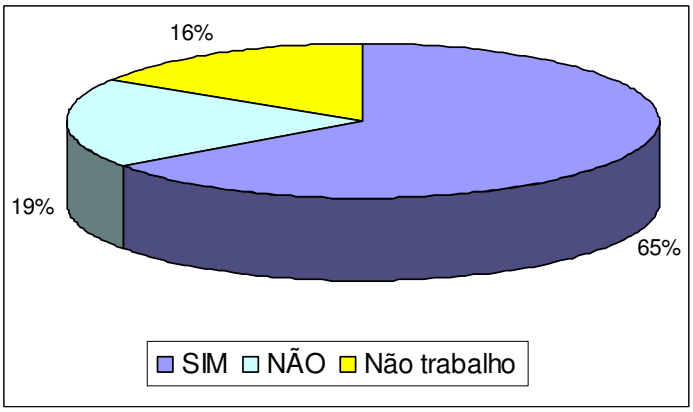

Figura 11. Utilização da Internet no trabalho

A Figura 12 apresenta os resultados referentes aos alertas das empresas sobre os riscos da utilização da Internet. Estes mostram que 30% não utilizam a Internet

no trabalho, 45% são alertados pelas empresas, porém 26% muitas vezes e 19% poucas vezes, e 25% disseram nunca receber este tipo de informação por parte da empresa onde trabalham.

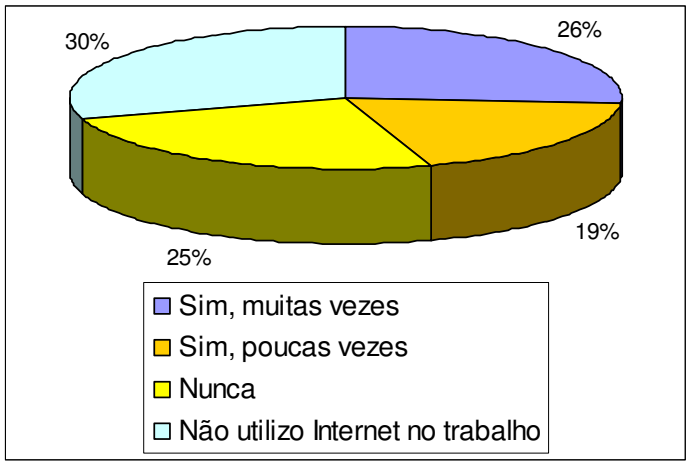

Figura 12. Alerta das empresas sobre riscos e formas de proteção

Conforme já citado nesta pesquisa, a falta de conhecimento e a utilização incorreta da Internet nas empresas, além de apresentar perigo aos próprios usuários, pode também abrir portas importantes para o acesso externo de pessoas mal intencionadas. Por este motivo é tão importante que os alertas sejam feitos.

No âmbito da segurança os resultados revelaram que 42% conhecem várias ferramentas para aumentar a segurança ao utilizar a Internet, enquanto 58% afirmaram não conhecer nada referente a isto, conforme mostra a Figura 13, o que é um dado preocupante, já que mais da metade dos usuários não conhecem nenhuma ferramenta que os auxilie na sua segurança durante a utilização da Internet.

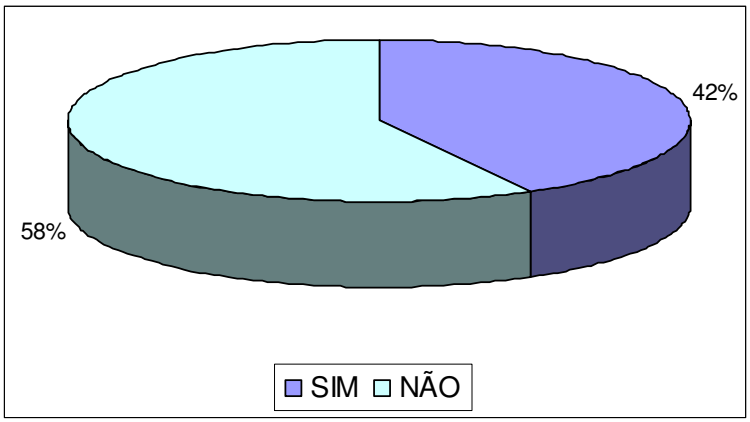

Figura 13. Conhecimento de ferramentas de defesa

Dos exemplos citados, entre os 42% apresentados na Figura 13 que tem este conhecimento de ferramentas para aumentar a segurança na utilização da Internet, o antivírus foi o mais indicado (52%), depois o *Firewall* (18%) e em seguida o *Anti-spyware* (17%), e ainda 13% não citaram exemplos. Estes dados são representados na Figura 14.

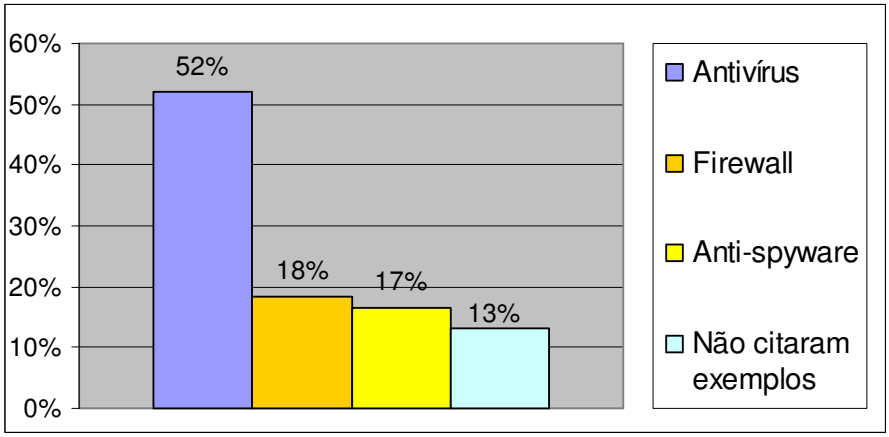

Figura 14. Exemplos de ferramentas de defesa

Segundo o Centro de Estudos sobre as Tecnologias da Informação e da Comunicação (CETIC, 2007), 97% das empresas utilizam Antivírus como forma de proteção, seguidos do *Anti-spyware* com 59% e do *Firewall* com 54%. Apesar de nesta pesquisa o questionamento ser a respeito do conhecimento e não da utilização, pode-se perceber que a proporção é bastante parecida. É claro que, como o CETIC informa os

dados de empresas, estes valores são maiores, já que normalmente as empresas investem mais em segurança que usuários domésticos.

Outro questionamento feito durante a pesquisa referente aos conhecimentos sobre segurança, revelou que 46% conhecem várias ações para se proteger durante a navegação na Internet, 44% conhecem poucas e 10% não conhecem nenhuma forma de proteção, relativo a ações dos próprios usuários, como apresenta a Figura 15.

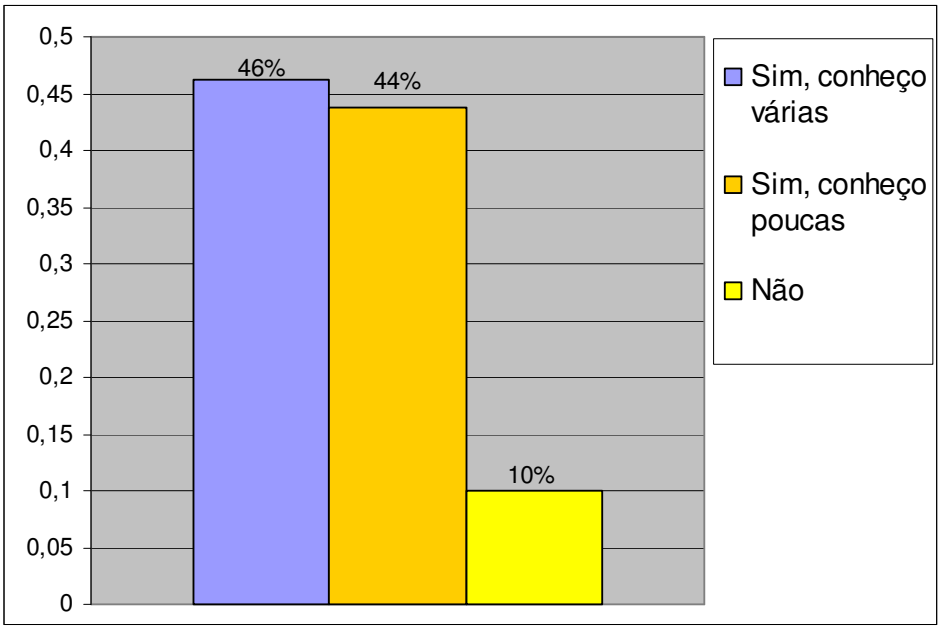

Figura 15. Conhecimento de ações de defesa ao navegar na Internet

Estes dados são importantes, já que grande parte das fraudes digitais necessitam da intervenção do usuário em algum momento para serem concretizadas, e o conhecimento faz com que os mesmos consigam observar uma possível tentativa de fraude.

Destes conhecimentos sobre ações de proteção e segurança, o hábito de verificar a existência do certificado *Secure Socket Layer* (SSL) nos *sites* que exigem maior grau de segurança é focado com destaque em uma das perguntas do questionário aplicado na pesquisa. De todos os entrevistados, 30% verificam a existência do

certificado SSL nos *sites* onde existe maior risco de serem prejudicados por fraudes, 47% não tem este costume e 23% não conhecem este item, conforme a Figura 16.

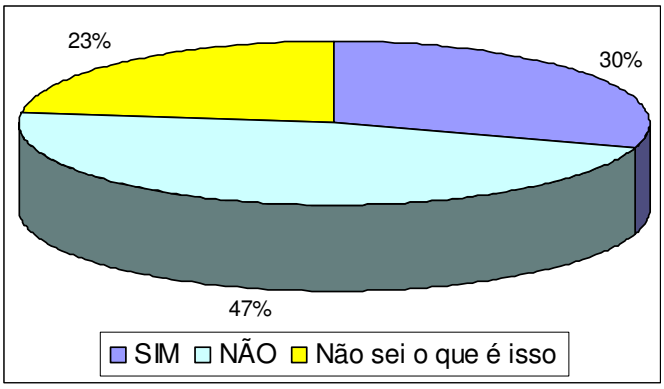

Figura 16. Verificar existência do certificado SSL nos *sites* que exigem maior segurança

A verificação do certificado SSL é um item importante, porque além de garantir a criptografia dos dados que são transferidos na rede, tornando a navegação mais segura. Sua inexistência pode fazer com que outras fraudes sejam identificadas, como por exemplo, a navegação em um *site* falso. Normalmente os *sites* verdadeiros que possuem o certificado, quando fraudados passam a não apresentar este item.

Na Figura 17, que apresenta os resultados obtidos na questão 12 do questionário utilizado na pesquisa, 80% afirmam que utilizariam mais a Internet para compras e transações financeiras se tivessem mais conhecimento sobre segurança e 20% já se sentem seguros.

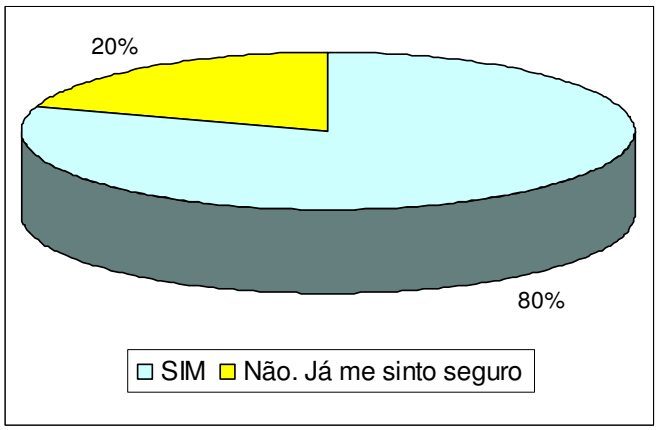

Figura 17. Utilizar mais a Internet para compras e transações financeiras

Esta questão traz a tona o problema econômico provocado pela insegurança dos usuários em utilizar serviços *on-line.* Assim como para as instituições financeiras, para as lojas, a venda pela Internet apresenta um custo operacional inferior em relação a venda física, que, em uma loja envolve vários custos, dispensados pela Internet, como estrutura física e funcionários para atendimento.

Este custo também é menor para quem compra, já que não existe a necessidade de deslocamento, e na grande maioria dos casos os preços dos produtos na Internet são também menores, levando em conta a economia que a loja tem.

Alguns *sites*, como de bancos ou lojas virtuais, oferecem informações sobre segurança aos seus usuários, porém dos que utilizam estes *sites*, 39% revelaram nunca lerem estas dicas, 42% leram poucas vezes e 19% já leram várias vezes, de acordo com a Figura 18. Levando-se em conta que o acesso a estas informações no *site* é fácil, a falta de interesse dos usuários, que estes dados mostram, é também fator importante para aumentar o número de fraudes.

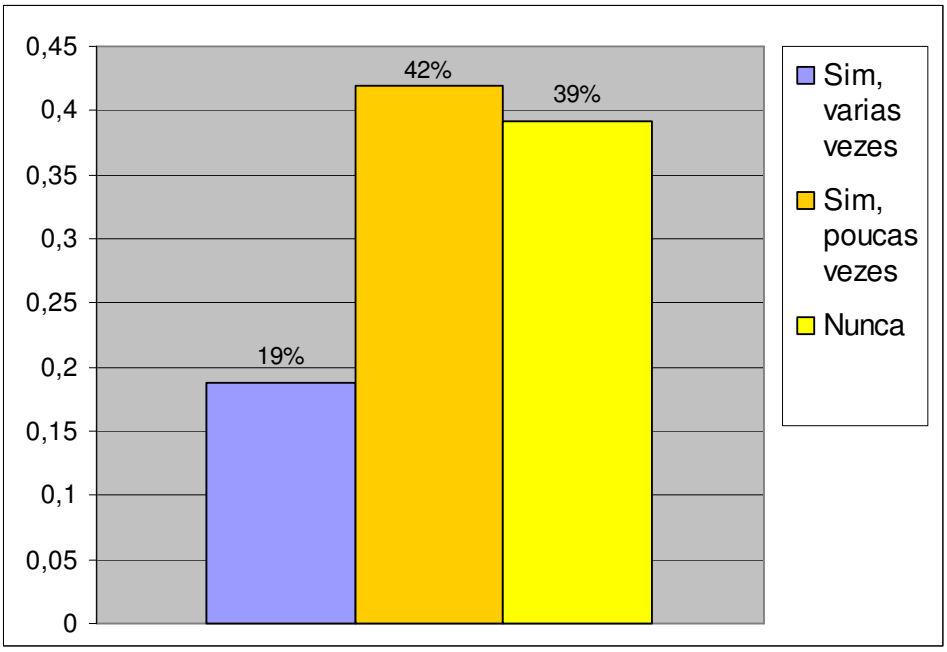

Figura 18. Hábito de ler dicas e manuais de segurança na Internet

Muitos dos entrevistados deram sugestões sobre possíveis maneiras de diminuir o número de incidentes relacionados à segurança na Internet, que são apresentadas na Figura 19.

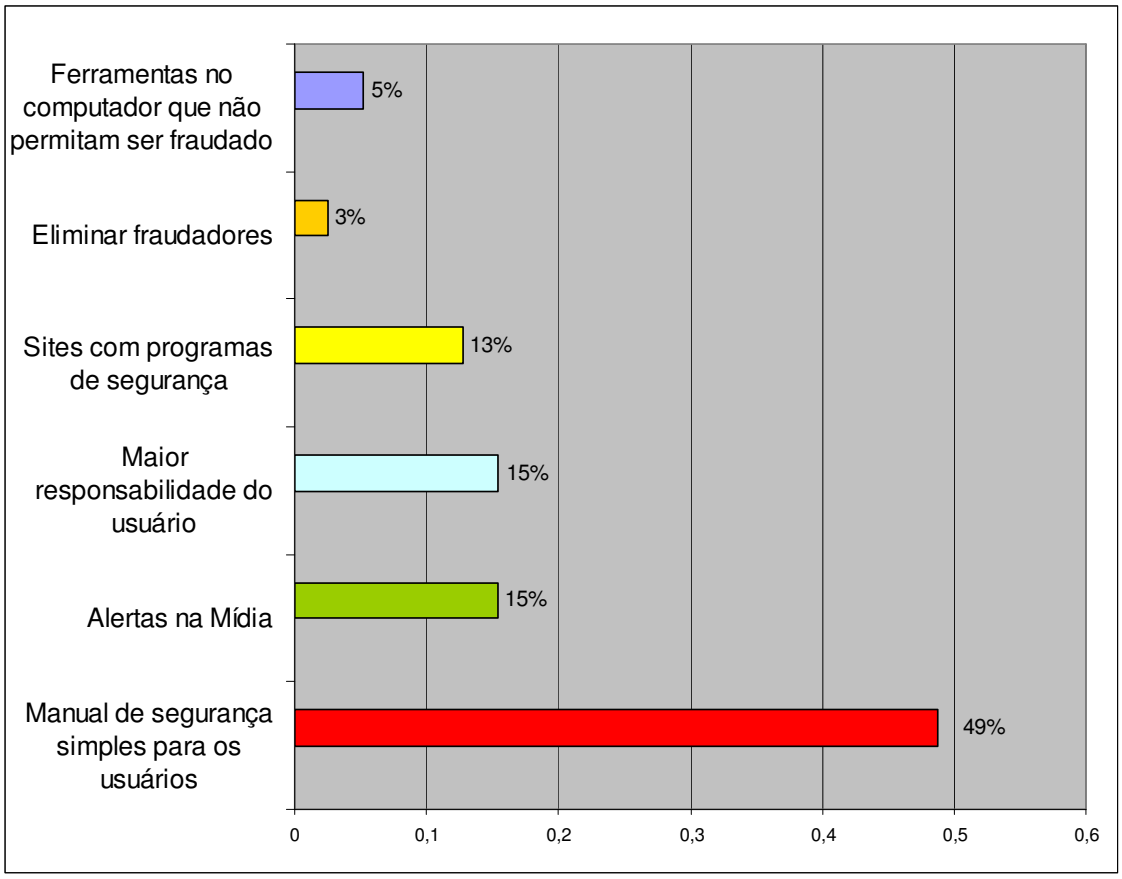

Figura 19. Sugestões apresentadas

Dos que sugestionaram, o comentário mais freqüente (49%) foi para criação de manuais de segurança com linguagem simples para os usuários, a seguir com 15% destacaram alertas na mídia e maior responsabilidade do próprio usuário. Outros exemplos foram citados como: os *sites* possuírem programas de segurança (13%); eliminação dos fraudadores (3%) e criação de ferramentas para o computador que não permitam que o mesmo seja fraudado (5%).

O que a grande maioria dos entrevistados citou como importante para diminuir o número de incidentes, realmente pode apresentar bons resultados. A leitura

destes manuais iria expandir o conhecimento e provavelmente mudar algumas ações dos usuários no momento da navegação, e como já comentado nesta pesquisa, a não intervenção do usuário em alguma tentativa de fraude pode impossibilitá-la.

6 SIMULAÇÃO DE FRAUDE UTILIZANDO *PHISHING*, CAVALO DE TRÓIA, *PHARMING* E *SITE* FALSO, E PROCEDIMENTOS DE DEFESA

A pesquisa desenvolvida simula um procedimento de ataque que une técnicas de *phishing*, cavalo de tróia, *pharming* e *site* falso, aliado a procedimentos que podem ser utilizados para impossibilitar o sucesso deste ataque.

Um *phishing* enviado por *e-mail*, utiliza uma identidade visual parecida com a de uma empresa conhecida, e contém um *link*[10] para um cartão virtual animado em formato executável, compactado, desenvolvido utilizando o *software* Macromedia Flash da Adobe. Este arquivo, além do cartão virtual, contém um Cavalo de Tróia inserido com auxílio de um *Joiner*[11], e dentro deste um *pharming*, que quando executado infecta o arquivo de *hosts* do sistema operacional Windows no computador local. O *pharming* cria resoluções falsas para o IP do domínio e subdomínios do *website* da UNESC, que foi utilizado como alvo na execução desta fraude. Quando o acesso ao *site* é realizado, uma vez que existem regras de resolução DNS daquele domínio na própria máquina, a busca pelo domínio é realizada no IP falso inserido no arquivo de *hosts*, e ao invés do *site* real ser mostrado, leva até um *site* falso em outro servidor, desenvolvido utilizando toda identidade visual do *site* verdadeiro, para que o usuário não desconfie que está sendo vítima de uma fraude.

Quando os dados de acesso restrito do usuário forem inseridos no *site*, no mesmo instante serão enviados por *e-mail* para o fraudador, e será mostrado ao usuário uma mensagem de erro de incompatibilidade no navegador de Internet, finalizando o processo.

---

10 Atalho, caminho ou ligação para determinado endereço na Internet.
11 Programa capaz de unir dois ou mais arquivos executáveis.

Todos os aplicativos, códigos fonte e outras ferramentas utilizadas no desenvolvimento deste projeto estão presentes no CD-ROM que o acompanha.

6.1 DEFINIÇÃO DA EMPRESA ALVO

A primeira etapa do desenvolvimento deste projeto foi a escolha da empresa que seria utilizada como alvo para desenvolvimento do *site* falso.

A idéia inicial era utilizar o *site* de um banco, uma vez que são instituições visadas por fraudadores e que exigem um grau de segurança elevado por trabalharem com informações absolutamente restritas e transações financeiras.

Por se tratar de um trabalho científico e público, é evidente a necessidade de autorização jurídica da empresa que seria utilizada como alvo para o ataque, e foi esta necessidade que inviabilizou o desenvolvimento do *site* falso de um banco. Todos os contatos realizados com diferentes bancos só foram suficientes para conseguir a informação de que seria muito difícil a concessão de uma autorização desta natureza.

Não apenas em bancos, mas em outras empresas também não seria fácil esta autorização, já que as pessoas têm receio de expor o nome de sua instituição em um trabalho como este.

Devido à dificuldade de conseguir autorização de uma empresa conhecida, foi utilizado como alvo desta fraude o *site* da UNESC, que se mostrou aberta em contribuir para o desenvolvimento científico desta pesquisa.

Apesar de ser utilizado o *site* da UNESC como *site* falso, isso não identifica problemas de segurança no desenvolvimento de suas aplicações, uma vez que este tipo de fraude poderia ser desenvolvida utilizando qualquer *site*.

6.2 CONFIGURAÇÃO DOS DNSs DO DOMÍNIO DA EMPRESA ALVO NO SERVIDOR FALSO

Para que o IP inserido no *pharming* desenvolvido respondesse pelos domínios e subdomínios informados, foi necessário efetuar a liberação do serviço de DNS para o domínio "unesc.net" no servidor falso. Assim tanto o servidor verdadeiro quanto o falso respondem pelo domínio normalmente.

Nos dias atuais é fácil abrir uma conta de hospedagem de qualquer domínio na Internet, até mesmo fornecendo informações falsas, principalmente de domínios internacionais e em empresas internacionais de hospedagem do *sites*.

O domínio "unesc.net" e seus subdomínios foram devidamente configurados para responderem no IP 209.67.x.x, local onde estão os arquivos do *site* falso, idênticos ao verdadeiro.

6.3 DESENVOLVIMENTO DO *PHARMING*

O *pharming* foi desenvolvido em linguagem de programação C++, utilizando o *software* Bloodshed Dev-C++.

A aplicação quando executada cria novas linhas no arquivo de *hosts* do sistema operacional Windows, que fica localizado no diretório "c:\windows\system32\drivers\etc". Quando o usuário for acessar o *site*, ao invés do sistema verificar para qual IP aponta o domínio verdadeiramente, ele irá antes verificar o arquivo de *hosts*, e nele irá buscar os IPs falsos configurados, onde está o *site* falso.

A Figura 19 mostra a lista de domínios e subdomínios que são inseridos no arquivo de *hosts* após a infecção pelo *pharming*.

Domínio ou subdomínio	IP verdadeiro	IP falso configurado
www.unesc.net	200.18.x.x	209.67.x.x
webmail.unesc.net	200.135.x.x	209.67.x.x
ead.unesc.net	Inexistente	209.67.x.x
www.ead.unesc.net	200.18.x.x	209.67.x.x

Figura 20. Domínios e subdomínios inseridos com IP falso no arquivo de *hosts*

6.4 DESENVOLVIMENTO DO *SITE* FALSO

O *site* falso desenvolvido utiliza uma identidade visual idêntica ao *site* real, o que torna a identificação da fraude bastante difícil, pelo menos no início da navegação.

Para seu desenvolvimento, foi utilizado o *software* Macromedia Dreamweaver da Adobe e programação HTML, JavaScript, CSS e PHP.

Boa parte do código utilizado na programação do *site* foi extraído no próprio navegador de Internet, utilizando a função de visualização de código fonte. Os códigos CSS e Javascript também foram copiados e apenas adaptados para que funcionem da mesma maneira no servidor falso.

Como o número de páginas e serviços contidos no *website* da UNESC é elevado, apenas algumas páginas consideradas importantes e que contém sistema de autenticação foram implementadas, são elas: capa do *site* (www.unesc.net); *webmail* (webmail.unesc.net); educação a distância (www.ead.unesc.net); diário *on-line* (www.unesc.net/diario).

6.4.1 Capa do *site*

A capa do *site* é a página de abertura acessada no endereço www.unesc.net. Esta página não contém nenhum sistema que possibilite a inserção de informações sigilosas e posteriormente o envio ao fraudador, porém o seu desenvolvimento é

importante, já que o usuário iria desconfiar da fraude ao acessar o endereço principal do *site* e notar que nada seria mostrado.

6.4.2 *Webmail*

No *webmail* é possível adquirir os dados de nome de usuário e senha da pessoa fraudada. Esta informação é submetida por meio de uma aplicação PHP, que será comentada a seguir, logo após o usuário inserir as informações. Como a navegação está sendo feita no servidor falso, o acesso aos *e-mails* não é completado, e o usuário visualiza um alerta falso informando que existe uma incompatibilidade com o navegador utilizado.

6.4.3 Educação a distância

A página de educação a distância possui uma autenticação para que os usuários possam acessar o sistema. Estes dados de nome de usuário e senha, mesmo utilizado no sistema de matrícula, são também enviados ao fraudador no momento que a autenticação é feita. O mesmo alerta de incompatibilidade é mostrado nesta página após a tentativa de acesso.

6.4.4 Diário *on-line*

A página do diário *on-line* da UNESC também apresenta um sistema de autenticação de usuário, que é utilizado por professores, onde inserem o seu código e uma senha no momento da autenticação. Estas informações são absolutamente restritas,

já que o acesso aos dados possibilita a visualização e manipulação de informações importantes.

O envio do código de usuário e senha deste *site* ocorre da mesma forma dos outros. Ao tentar acessar o sistema, o usuário visualiza uma mensagem de alerta falso de incompatibilidade de navegador, e no mesmo instante o fraudador recebe os dados inseridos.

6.4.5 Aplicação que envia as informações por *e-mail*

Para que as informações inseridas no *site* fossem enviadas ao fraudador, foi implementado um sistema em linguagem PHP para tal necessidade.

Este sistema utiliza uma função de envio de *e-mail*, para submeter os dados ao fraudador. Este recebe as informações de nome de usuário e senha da pessoa fraudada, o respectivo *site* utilizado e a data e hora da operação.

6.5 DESENVOLVIMENTO DO CARTÃO ANIMADO

O cartão animado foi desenvolvido utilizando o *software* Macromedia Flash, da Adobe. Animações do Flash são muito comuns de serem encontradas na Internet, e podem ser interpretadas pela grande maioria dos navegadores.

Este tipo de arquivo também pode ser executado sem o auxílio de nenhum outro *software*, o que necessita que ele seja publicado em formato de aplicativo (.exe), já que assim o arquivo leva anexo o *plugin*[12] necessário para execução da animação.

---

[12] Tipo de aplicativo auxiliar que adiciona novas capacidades ao programa. Neste caso a capacidade de reproduzir arquivos do Macromedia Flash.

É neste arquivo executável que vai inserido o *pharming* com auxílio de um *Joiner*, ou seja, um cavalo de tróia com dois arquivos executáveis.

6.6 DESENVOLVIMENTO DO *E-MAIL* PARA ENVIO DO CARTÃO

O *e-mail* enviado ao usuário fraudado é um *phishing* e tem semelhança com *e-mails* comuns de cartões virtuais utilizados na Internet.

A identidade visual do *e-mail* é bastante parecida com a de uma empresa conhecida, e só não foi desenvolvido igual porque seria necessário a autorização jurídica da empresa, o que é bastante difícil de conseguir. Normalmente fraudes como esta utilizam a mesma identidade visual, para tornar ainda mais difícil sua identificação.

O *e-mail* informa que existe um cartão virtual enviado para a pessoa que está recebendo a mensagem, e mostra um *link* para que o usuário faça o *download* do arquivo do cartão.

Para que o usuário desconfie ainda menos de que está sendo fraudado, o *link* mostrado em forma de texto no *e-mail* não é o mesmo que o apontado no momento que o usuário clica.

A mensagem é enviada em formato HTML, com o auxílio do *software* gratuito Vallen e-Mailer, desenvolvido pela empresa Vallen-Systeme GmbH, que é capaz de enviar *e-mails* em massa para uma lista pré-definida.

6.7 DESENVOLVIMENTO DO CAVALO DE TRÓIA

O Cavalo de Tróia é a união do arquivo do cartão virtual, que é o executável que contém a animação, com o *pharming*.

Este tipo de união de arquivos executáveis pode ser feito por intermédio de um *software* chamado *Joiner*, que pode ser encontrado para *download* na Internet.

Neste caso foi utilizado o *Joiner* chamado Juntador Beta, desenvolvido por um programador brasileiro em Delphi.

O *software* permite que além da junção dos dois arquivos executáveis, seja editado o ícone que é mostrado no aplicativo, o que possibilita a configuração do ícone padrão dos arquivos de animação do Flash.

6.8 EXECUÇÃO DA SIMULAÇÃO

A execução da fraude inicia com o envio do *e-mail* falso para uma lista de *e-mails* que pode ser definida em um arquivo de texto, com o auxílio do *software* gratuito Vallen e-Mailer, que faz o envio para inúmeros destinatários ao mesmo tempo.

Ao receber o *e-mail* falso, o usuário faz o *download* do cartão virtual e o executa. No momento da execução o arquivo de *hosts* do Windows é modificado.

Quando o acesso ao *site* da UNESC for feito, o usuário irá navegar no *site* falso, e os dados inseridos na autenticação dos sistemas serão submetidos por *e-mail* ao fraudador, enquanto ele visualiza uma mensagem de erro.

O esquema da Figura 20 mostra o funcionamento da fraude.

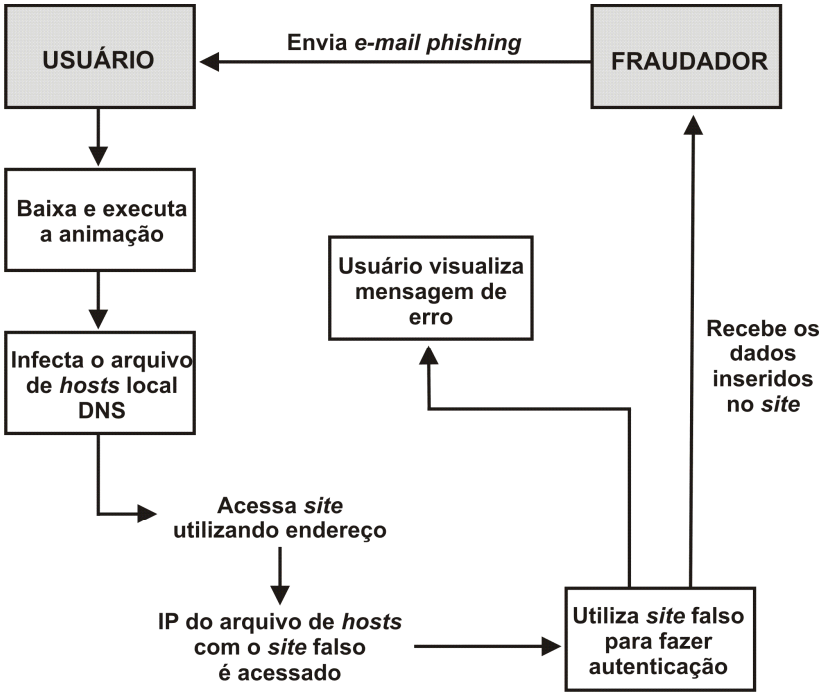

Figura 21. Esquema do funcionamento da fraude

6.9 FORMAS DE PROTEÇÃO

Como já mencionado neste trabalho, boa parte das ações criminosas praticadas na Internet podem ser evitadas com um pouco de conhecimento e cuidado por parte dos usuários, o que não é diferente na fraude aqui aplicada.

A seguir são listadas algumas ações que o usuário pode fazer para se defender desta ameaça:

a) ao receber o *e-mail*, identificar a veracidade da existência da empresa que fez o envio, que neste caso não existe. Uma simples procura pela palavra “boxcards” em um sistema de busca na Internet seria suficiente para esta identificação.

b) verificar também no *e-mail*, se a pessoa que fez o envio é conhecida. Neste caso o *e-mail* não traz esta informação, o que normalmente não ocorre com cartões virtuais verdadeiros.

c) o endereço existente no *e-mail* para visualização do cartão (http://boxcards.id.com.br/dc/6A0CEC1134924D02832ABAA0D86C63AC) não é o mesmo que é apontado no momento que o usuário clica. Isso pode ser identificado tanto em *softwares* de visualização de *e-mail* como o Outlook da Microsoft, como também em navegadores de Internet, simplesmente passando o *mouse* sobre o *link*, sem clicar. O endereço real é mostrado na barra de *status* no canto inferior esquerdo.

d) normalmente *e-mails* de cartão virtual são mostrados no navegador de Internet, e não solicitam que seja feito o *download* do arquivo. Neste caso além do *download* solicitado, o arquivo é um executável, o que possibilita a execução simultânea de códigos maliciosos.

e) um bom antivírus instalado no computador acusaria o vírus Juntador-D contido no aplicativo. Este vírus é reconhecido após a utilização do *Joiner* que faz o Cavalo de Tróia.

Se mesmo após todas estas etapas o usuário não identificar a fraude, ainda é possível fazer isso no momento que o acesso ao *site* falso é feito, fazendo as seguintes observações:

a) verificar se o *site* visitado apresenta todas as suas funcionalidades normais. Neste caso uma simples navegação pela capa do *site* "www.unesc.net" seria suficiente para identificar que as páginas internas não abrem normalmente.

b) no caso do Diário *On-line*, verificar se o navegador de Internet apresenta o ícone de um cadeado fechado, que identifica o certificado de segurança. O *site* falso não apresenta este item.

c) após a mensagem de erro de incompatibilidade ser mostrada na tentativa de autenticação de acesso, entrar em contato imediatamente com os responsáveis pelo *site*, informando o problema. Como esta mensagem de erro não existe, a troca da senha de acesso seria feita imediatamente, uma vez que a tentativa de fraude seria reconhecida.

Apesar da técnica de fraude utilizada ser bastante completa e muito bem desenvolvida, qualquer uma destas dicas de ações poderia identificá-la. Isso mostra que o conhecimento e as ações executadas pelo usuário no momento da utilização da Internet são fundamentais para sua segurança.

6.10 TESTES DE FUNCIONAMENTO EM DIFERENTES REDES

O funcionamento da fraude foi testado em diferentes redes, e também em diferentes versões do sistema operacional Windows. Foram consideradas configurações padrão tanto para o *link* de Internet como para o sistema operacional. Para o sistema operacional os testes foram efetuados com *login* de usuário administrador. A Figura 22 mostra o resultado dos testes em diferentes redes.

Local/Rede/Link	**Funcionamento**	**Descrição**
UNESC / Rede interna / ATM	Não	Utiliza *proxy*[13] transparente.
ADSL doméstica Brasil Telecom	Sim	Perfeito funcionamento.
ADSL empresarial Brasil Telecom	Sim	Perfeito funcionamento.
ADSL empresarial GVT	Sim	Perfeito funcionamento.
Link dedicado Embratel	Sim	Perfeito funcionamento.
Conexão discada IG / POP	Sim	Perfeito funcionamento.
Conexão discada UNESC	Sim	Perfeito funcionamento.

Figura 22. Resultado dos testes em diferentes redes

[13] Servidor que atua como um intermediário entre a estação de trabalho e a Internet.

A Figura 23 mostra o resultado dos testes com diferentes versões do sistema operacional Windows.

Sistema operacional	Funcionamento	Descrição
Microsoft Windows 98	Sim	Perfeito funcionamento.
Microsoft Windows XP SP1	Sim	Perfeito funcionamento.
Microsoft Windows XP SP2	Sim	Perfeito funcionamento.
Microsoft Windows Vista	Não.	O sistema não permite a edição do arquivo de *hosts* pelo usuário.

Figura 23. Resultado dos testes em diferentes versões do Windows

6.11 RESULTADOS OBTIDOS

Para demonstração dos resultados obtidos foi considerada a execução da simulação de fraude já comentada.

Após o envio do *e-mail* falso para lista de *e-mails* que foi definida no arquivo de texto, o usuário recebe o *e-mail* com o *link* mascarado para fazer o *download* do cartão virtual. A Figura 24 mostra a tela com o e-mail e o *link* mascarado.

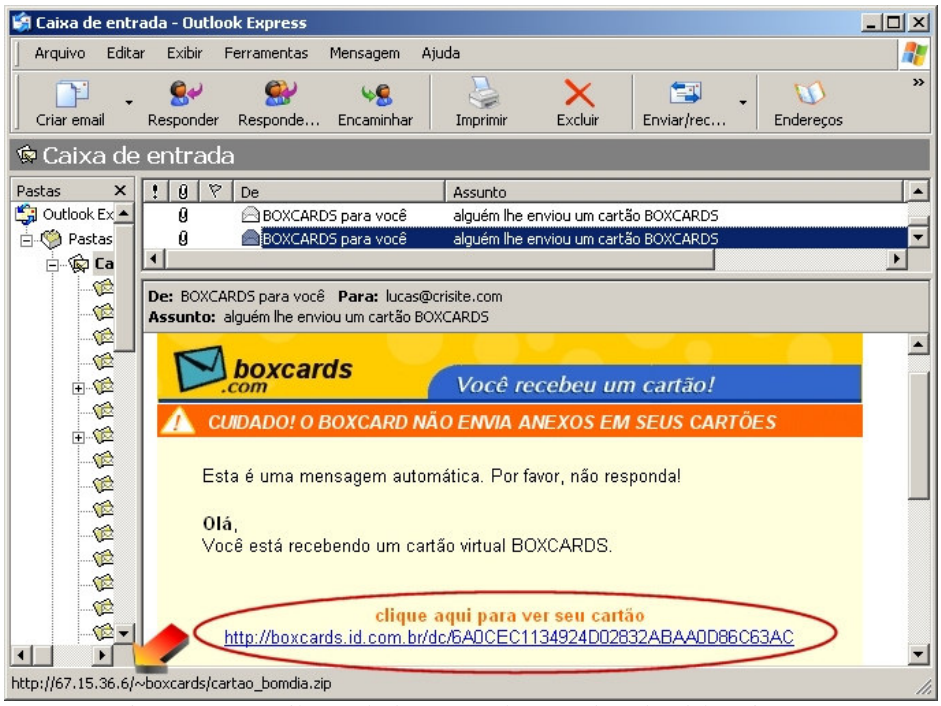

Figura 24. E-mail com *link* mascarado para *download* da animação
Fonte: Microsoft Outlook Express (2007).

Após a execução da animação do cartão virtual, conforme mostra a Figura 25, o arquivo de *hosts* do Windows é editado e novas linhas são inseridas. A Figura 25 também mostra o arquivo depois de modificado.

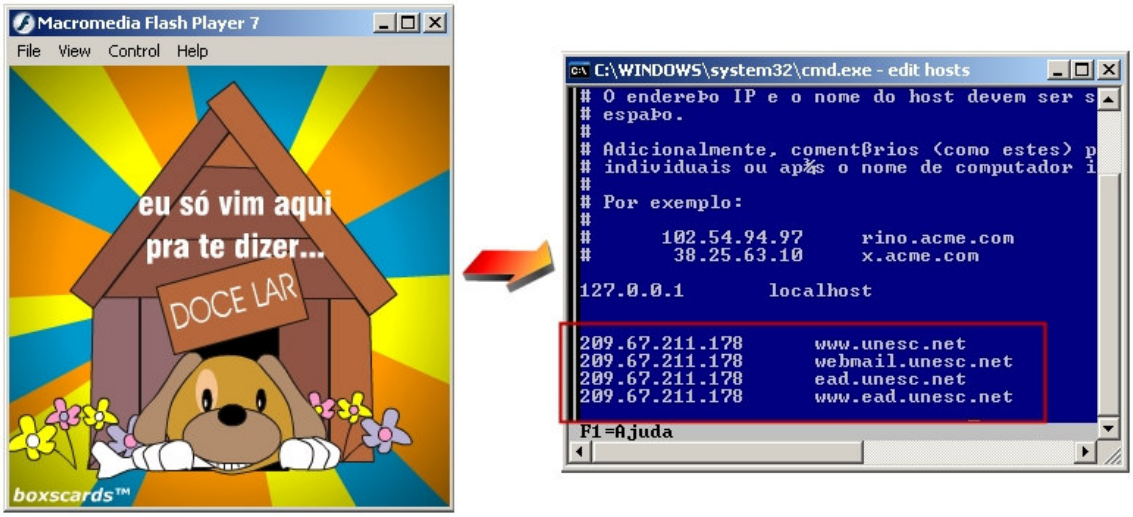

Figura 25. Animação que executa o *pharming* e linhas do arquivo de *hosts* inseridas

Quando o acesso ao *site* da UNESC é feito, o usuário navega no *site* que está no servidor falso, e os dados inseridos na autenticação dos sistemas são submetidos por *e-mail* ao fraudador, enquanto o usuário visualiza uma mensagem de erro. A figura 26 mostra os dados enviados após a execução da simulação.

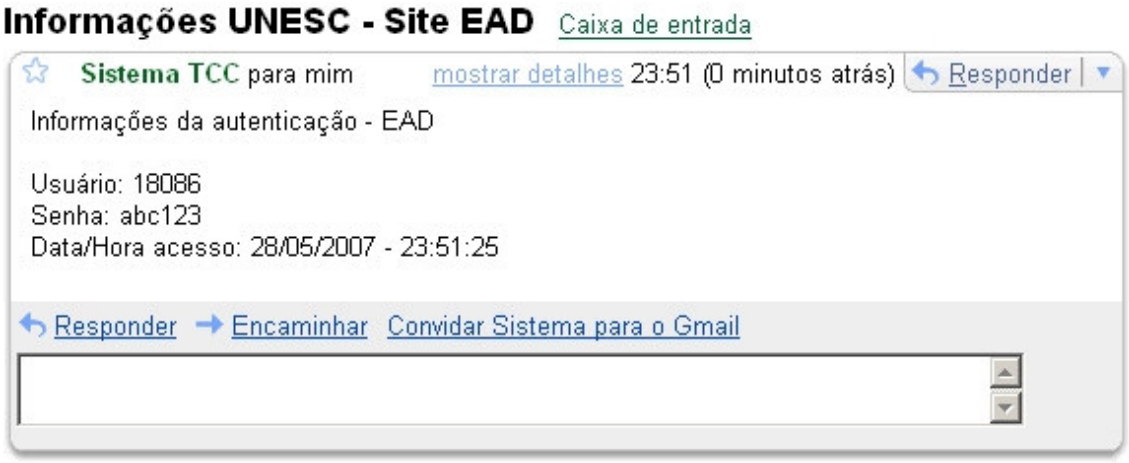

Figura 26. E-mail com os dados enviado ao fraudador
Fonte: Gmail – Google (2007).

A execução da simulação da fraude, quando não identificada pelo usuário ou por algum *software* de proteção como um antivírus, obteve sucesso nos testes efetuados.

CONCLUSÃO

Esta pesquisa demonstrou os principais perigos existentes na Internet, que colocam em risco a segurança da informação e podem desencadear uma série de problemas que envolvem principalmente questões financeiras.

O estudo das principais ameaças digitais foi fundamental para mostrar a necessidade de conhecer as ações mais importantes na busca pela proteção, uma vez que a grande maioria das fraudes digitais podem ser evitadas com simples ações durante a navegação.

A observação dos sintomas durante a utilização do computador é primordial para que possíveis pragas instaladas no sistema sejam identificadas, evitando problemas com a confidencialidade, integridade e disponibilidade das informações.

A pesquisa de campo mostrou que o número de pessoas que estão vulneráveis as ameaças digitais e possíveis fraudes é relativamente grande, já que na maioria dos questionamentos, os aspectos que tornariam a navegação mais segura não foram citados com grandes percentuais.

Algumas técnicas utilizadas para execução de fraudes digitais foram utilizadas no desenvolvimento da simulação implementada neste projeto, que também tornou possível a demonstração de procedimentos de defesa, principalmente no que diz respeito ao conhecimento e a forma de uso dos recursos disponíveis na Internet. A simulação também tornou possível a visualização prática de como é possível utilizar recursos computacionais objetivando ações ilícitas.

A descoberta de novas técnicas utilizadas na tentativa de executar com sucesso uma fraude na Internet é freqüente e em curto intervalo de tempo. Isso torna necessário o desenvolvimento de trabalhos futuros com materiais atuais relacionados a este assunto.

As justificativas que tornam importante o estudo de técnicas que permitam minimizar ao máximo o número de incidentes relacionados à segurança na Internet também são pontos importantes para serem abordados em novos estudos.

Por fim, aliado às técnicas e conhecimentos de ações que minimizem os problemas relacionados às ameaças digitais, está o desenvolvimento de aplicações que auxiliem no controle e identificação destas ameaças. Estas aplicações são algo que deve ser estudo e desenvolvido com velocidade para acompanhar o número crescente de técnicas utilizadas na execução de fraudes na Internet.

REFERÊNCIAS

Anti-Phishing Working Group (APWG) Research Partner. **Report Phishing.** Disponível em: <http://www.antiphishing.org>. Acesso em: nov. 2006.

BARBETTA, Pedro Alberto. **Estatística aplicada às ciências sociais**. Florianópolis: UFSC, 1998.

CERT - **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil.** Disponível em: <www.cert.br>. Acesso em: nov. 2006.

CETIC - **Centro de Estudos sobre as Tecnologias da Informação e da Comunicação.** Disponível em: <www.cetic.br>. Acesso em: mai. 2007.

CRONKHITE, Cathy; MCCULLOUGH, Jack. **Hackers, acesso negado :** o guia completo para a proteção dos seus negócios on-line. Rio de Janeiro: Campus, 2001

DIAS, Cláudia. **Segurança e auditoria da tecnologia da informação**. Rio de Janeiro: Axcel Books do Brasil, 2000.

E-BIT Web Shoppers - **Tecnologia em Marketing.** Disponível em: <http://www.ebitempresa.com.br/imprensa.htm>. Acesso em: mai. 2007.

FOINA, Paulo Rogério. **Tecnologia de informação:** planejamento e gestão. São Paulo: Altas, 2001.

GOMES, Olavo José Anchieschi. **Segurança total**. São Paulo: Makron Books, 2000.

HATCH, Brian et al. **Hackers linux expostos**. São Paulo: Makron Books, 2002.

LEMOS, Aline Morais de. **Política de Segurança da Informação.** Rio de Janeiro, 2001. Disponível em: <www.estacio.br/campus/millorfernandes/monografias/aline_morais.pdf> Acesso em: mai. 2007.

LIRA, Waleska Silveira. Fatores determinantes do uso dos serviços bancários via Internet segundo o método de avaliação SERVQUAL. **RNTI: Revista Negócios e Tecnologia da Informação.** Curitiba PR, 2006. . Disponível em:

<http://rnti.fesppr.br/include/getdoc.php?id=261&article=67&mode=pdf> Acesso em: mai. 2007.

MACHADO, André; FREIRE, Alexandre. **Como Blindar seu PC: aprenda transformar seu computador numa fortaleza digital**. Rio de Janeiro: Elsevier, 2006.

Microsoft Corporation. **Segurança em casa.** Disponível em: <http://www.microsoft.com/portugal/athome/security/privacy/pharming.mspx>. Acesso em: nov. 2006.

NBR/ISO/IEC 17799. **Tecnologia da Informação - Código de prática para a gestão da segurança da informação.** Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2001.

NIC – **Núcleo de Informação e Coordenação**. Disponível em: <www.nic.br>. Acesso em: set. 2006.

QUINTELLA, Heitor M et al. A segurança da informação e a geração de percepção de diferencial competitivo perante o mercado. **Relatórios de Pesquisa em Engenharia de Produção da UFF**. Rio de Janeiro, 2003. Disponível em: <http://www.producao.uff.br/rpep/relpesq303/relpesq_303_19.doc> Acesso em: nov. 2006.

SERRANO, Paulo. **Cuidados que se deve ter com seu computador.** Centro de Computação - UNICAMP. São Paulo, 2001. Disponível em: <ftp://ftp.unicamp.br/pub/apoio/treinamentos/tutoriais/virus.pdf>. Acesso em: mai. 2007

UOL. Linha Defensiva. **Antivírus e Anti-Spyware.** Disponível em: <http://linhadefensiva.uol.com.br/artigos/adwares/>. Acesso em: set. 2006.

Websense Security Labs. **Phishing and Crimeware Map**. Disponível em: <http://www.websense.com/securitylabs/charts/threatmap.php>. Acesso em: nov. 2006.

Wikimedia Commons. **Número de vírus conhecidos.** Disponível em: <http://pt.wikipedia.org/wiki/Imagem:Virus_N.PNG>. Acesso em: mar. 2007.

WIKIPEDIA a. **Vírus informático**. Disponível em: <http://pt.wikipedia.org/wiki/V%C3%ADrus_%28computador%29>. Acesso em: nov. 2006.

WIKIPEDIA b. **Exploit**. Disponível em: <http://pt.wikipedia.org/wiki/Exploit>. Acesso em: nov. 2006.

WIKIPEDIA c. **Spyware**. Disponível em: <http://pt.wikipedia.org/wiki/Spyware>. Acesso em: nov. 2006.

ZAPATER, Marcio; SUZUKI, Rodrigo. Segurança da Informação. Um diferencial determinante na competitividade das corporações. **Promon S.A. Promon Business & Technology Review**. São Paulo, 2005. . Disponível em: <http://www.promon.com.br/portugues/noticias/download/Seguranca_4Web.pdf> Acesso em: nov. 2006.

BIBLIOGRAFIA COMPLEMENTAR

CARUSO, Carlos A. A.; STEFFEN, Flávio Deny. **Segurança em informática e de informações**. 2.ed. São Paulo: SENAC, 1999.

FURMANKIEWICZ, Edson. **Segurança máxima: o guia de um hacker para proteger seu site na Internet e sua rede**. Rio de Janeiro: Campus, 2000.

MARQUES, Cláudia Lima**. Confiança no comércio eletrônico e a proteção do consumidor : (um estudo dos negócios jurídicos de consumo no comércio eletrônico)**. São Paulo: Revista dos Tribunais, 2004.

MCCLURE, Stuart; SCAMBRAY, Joel; KURTZ, George. **Hackers expostos**. São Paulo: Makron Books, 2000.

NORTHCUTT, Stephen et al. **Desvendando: segurança em redes.** Rio de Janeiro: Campus, 2002.

OLIVEIRA, Wilson José de. **Hacker:** invasão e proteção. Florianópolis: Visual Books, 2000.

PROSISE, Chris**. Hackers:** resposta e contra-ataque. Rio de Janeiro: Campus, 2001.

VOLPI NETO, Angelo. **Comércio eletrônico:** direito e segurança. Curitiba: Juruá, 2001.

APÊNDICE A – QUESTIONÁRIO APLICADO NA PESQUISA DE CAMPO

AMEAÇAS DIGITAIS: UM ESTUDO DOS RISCOS ENVOLVIDOS NO USO DA INTERNET, SEUS IMPACTOS E FORMAS DE PROTEÇÃO

QUESTIONÁRIO

Este questionário faz parte de uma pesquisa para o trabalho de conclusão do curso de Ciência da Computação da Universidade do Extremo Sul Catarinense UNESC.

Leia com atenção e responda de forma sincera.

Assinale um "x" na alternativa correspondente a sua resposta.

1) Curso: _____ Fase: ____ Idade: ____

Compras	**2) Você já fez compra por meio da Internet?** ( ) Sim ( ) Não Se não, porque? _____ **3) Você já deixou de fazer alguma compra na Internet por medo de expor seus dados pessoais (CPF, RG, Endereço)?** ( ) Sim ( ) Não ( ) Não, porém tive receio **4) Você já deixou de fazer alguma compra na Internet utilizando seu cartão de crédito por medo de ser fraudado?** ( ) Sim ( ) Não ( ) Não, porém tive receio ( ) Não uso cartão ( ) Nunca comprei na Internet

Bancos	**5) Você utiliza o site do seu banco para executar tarefas como, ver saldo, fazer pagamentos?** ( ) Sim, com freqüência ( ) Sim, poucas vezes ( ) Não **6) Em alguma vez deixou de fazer alguma transação financeira em seu banco utilizando a Internet por medo de ser fraudado?** ( ) Sim ( ) Não ( ) Não, porém tive receio ( ) Não utilizo meu banco na Internet

Empresa	**7) Você utiliza a Internet em seu local de trabalho?** ( ) Sim ( ) Não ( ) Não trabalho **8) Sua empresa costuma alertá-lo dos perigos existentes no uso da Internet?** ( ) Sim, muitas vezes ( ) Sim, poucas vezes ( ) Nunca ( ) Não utilizo Internet no trabalho

Segurança	**9) Você conhece alguma ferramenta para aumentar sua segurança na utilização da Internet?** ( ) Sim ( ) Não. Se sim, qual(is)? _____ **10) Você tem conhecimento das ações mais comuns que devem ser feitas para se proteger durante a navegação na Internet? Como por exemplo, não clicar em links (endereços) desconhecidos?** ( ) Sim, conheço várias ( ) Sim, conheço poucas ( ) Não **11) Você costuma verificar se, os sites que exigem maior grau de segurança que você utiliza, possuem certificado de segurança SSL (aquele ícone de cadeado fechado que é mostrado no navegador)?** ( ) Sim ( ) Não ( ) Não sei o que é isso **12) Você acha que utilizaria mais a Internet para fazer compras e executar transações financeiras se tivesse mais conhecimento sobre segurança?** ( ) Sim ( ) Não. Já me sinto seguro. **13) Alguma vez você parou para ler dicas de segurança, normalmente contidas em sites de bancos e lojas virtuais importantes?** ( ) Sim, varias vezes ( ) Sim, poucas vezes ( ) Nunca

14) Comente o que você acredita que seria interessante para diminuir o número de incidentes relacionados à segurança na Internet. (Opcional)

_____
_____
_____.

Muito obrigado!