Hackers e Crackers na internet: as duas faces da moeda

Glenio Leitão Marques Filho[1]

Resumo

O desenvolvimento das tecnologias digitais e a consequente criação da internet como espaço de interatividade comunicacional trouxe inúmeros benefícios ao mundo globalizado, mas também algumas preocupações consideráveis. Dentre elas, o fim da privacidade e as práticas invasivas de sites, e-mails, entre outros. Nesse contexto está a atuação dos Hackers e Crackers, dois grupos sociais que influenciam diretamente a dinâmica da grande rede. O primeiro tem a intenção de ajudar nessa construção coletiva do ciberespaço. Já o segundo, distribui uma cultura ilícita no meio. O presente trabalho tem como principal objetivo compreender as ações desses grupos, visto que elas podem desencadear diversos danos aos usuários da internet. Para isto é necessário conhecer os motivos pelos quais esses grupos atuam, além de esclarecer as principais diferenças entre os Hackers e Crackers, expondo suas características, facilitando o processo de identificação de seus ataques. Ao final de uma pesquisa exploratória, pode-se constatar que apesar da contribuição dos Hackers para a evolução dos sistemas de segurança, os danos que podem ser causados pelos Crackers são imensos e que, sendo assim, deveriam ser desenvolvidas penas mais rígidas contra esses grupos, além de um maior esclarecimento para a população sobre conceitos básicos de informática.

Introdução

Com o desenvolvimento e a evolução das tecnologias digitais, principalmente da Internet, um tema que vem sendo bastante discutido em todas as esferas da sociedade, especialmente nos ambientes midiáticos, é a invasão dos Hackers (ou Crackers, como veremos adiante) no Ciberespaço. Seja nas conversas cotidianas, em reuniões familiares ou no ambiente de trabalho, é comum ouvir experiências de alguém que já sofreu algum tipo de ataque ou dano proveniente da ação dos "Hackers".

A utilização do computador e da internet vem crescendo a cada dia em todas as faixas etárias e camadas sociais da população. Não existe mais o antigo pensamento de que o uso

[1] Graduado do Curso de Comunicação Social, habilitação Radialismo, da UFPB.

desta tecnologia é algo exclusivo de adolescentes aficionados por jogos virtuais que perdem seu tempo no ciberespaço ao invés de estudar ou realizar programas culturais.

De acordo com o Ibope Nielsen Online[2], em Junho de 2009, 33,1 milhões de usuários acessam regularmente a internet, seja em casa ou no trabalho. Desse total, 38% das pessoas acessam a *web* diariamente; 10% de quatro a seis vezes por semana; 21% de duas a três vezes por semana; 18% uma vez por semana. Somando, 87% dos internautas brasileiros entram na internet semanalmente

Com este avanço do acesso à internet, o poder de armazenamento de dados tende a ser cada vez maior. Se acrescentarmos a este fator o aumento constante da velocidade da conexão, o espaço virtual passa a ser utilizado com maior freqüência, fazendo parte, de vez, do dia-a-dia das pessoas.

Destarte, infinitas tarefas que antes necessitavam do deslocamento do indivíduo para que pudessem ser realizadas, hoje podem ser feitas a partir de sua própria residência através de um computador conectado à grande rede. Sendo assim, com a maior utilização do computador para tarefas simples, é que surge um problema de nível mundial que movimenta diversas reflexões acerca do mundo virtual: os Crackers.

Antes de tudo, é de extrema importância explicar e destrinçar uma questão que já perdura por vários anos e é inclusive objeto de análise de diversos estudiosos do assunto: a má utilização dos termos Hacker e Cracker nos estudos acadêmicos e sua veiculação através dos grandes meios de comunicação.

Originalmente, o termo Hacker é aplicado para aqueles indivíduos que possuem um conhecimento superior aos outros em determinada área e, ao contrário do que muitas pessoas imaginam, utilizam essa virtude para ajudar e não para destruir, como comumente é veiculado nas mídias. Desde o início da década de 90, este termo tem sido utilizado na área tecnológica, mais precisamente na área da informática.

Os Crackers, termo utilizado para identificar aqueles indivíduos que também possuem um conhecimento elevado relacionado à tecnologia, mas que não a utilizam de maneira

[2] O IBOPE Nielsen Online é uma joint-venture entre o IBOPE e a Nielsen, líder mundial em medição de audiência de Internet. Com o auxílio de um software proprietário, instalado em um painel de internautas representativo da população domiciliar brasileira com acesso à Web, a empresa detalha o comportamento dos usuários do meio digital. Disponível em: http://www.tobeguarany.com/internet_no_brasil.php Acesso em: 25 jul 2009.

positiva, são os que invadem sistemas e promovem ações com a intenção de prejudicar os outros, como desfigurar páginas da Internet ou promover a invasão de PCs (Computadores Pessoais) de usuários leigos. O problema existente quanto à diferenciação entre os termos é tanta, que existem casos de livros e filmes em que o termo "Cracker" é substituído por "Hacker" pelo tradutor, sem a menor preocupação.

Diferenciações devidamente feitas, os Crackers constantemente são alvos de matérias, tanto em revistas quanto nos jornais. No Brasil, nos últimos cinco anos, o aumento de notificações relacionadas a fraudes, furtos, vírus destruidores, invasões e tentativas de invasão de computador quadruplicou.

Isto é decorrente da maior utilização do computador pelos indivíduos para executar tarefas que antes não necessitavam deste meio, o que acarreta maior vulnerabilidade, especialmente entre os mais leigos no mundo virtual. Ou seja, se há alguns anos o indivíduo saía de casa para pagar uma conta ou realizar uma transferência bancária, hoje em dia, dentro da própria residência, no conforto do seu lar, esta tarefa pode ser feita.

Enquanto isso, os Hackers utilizam seus conhecimentos exatamente para barrar os Crackers. É uma espécie de "polícia-e-ladrão". Por onde os Crackers passam, os Hackers tentam rastreá-los para evitar que os problemas sejam mais catastróficos. A preocupação está tão evidente que, no ano de 2008, foi gasto 1,5 bilhão de reais em segurança digital, segundo a Federação Brasileira de Bancos[3].

A partir dessa realidade, existem duas hipóteses com relação ao futuro dos crimes virtuais, uma positiva e outra, de certa forma, negativa. A primeira é que com o tempo as pessoas saberão lidar com mais propriedade sobre a utilização da internet e, consequentemente, ficará mais difícil enganá-las. Porém, de acordo com Kevin Mitnick, o ex-cracker mais famoso do mundo, "A polícia vai pegar alguns tipos de fraude e os criminosos vão inventar outros, e assim por diante"[4], tornando esta problemática um ciclo-vicioso, onde a "polícia" sempre estará atrasada com relação ao "ladrão".

O estudo de temas atuais como os Hackers e Crackers podem possibilitar um desenvolvimento científico na área de segurança e possibilitar um avanço na área da informática. Visto que a comunicação virtual é cada vez mais freqüente, a segurança de dados que tramitam na rede é essencial para todos. Além do mais, é de extrema importância

[3] Retirado da revista Veja Ed. 2113, 2009, p. 90
[4] Retirado da revista Veja Ed. 2113, 2009, p. 92

compreender as ações de um Cracker assim como suas motivações, entendendo o porquê de se invadir um sistema, destacando os pontos positivos e os pontos negativos da ação destes indivíduos.

Ao realizar este estudo monográfico pretende-se esclarecer as principais diferenças entre os Hackers e Crackers, expondo suas características; apresentar os tipos mais conhecidos de Hackers e Crackers, facilitando o processo de identificação dos ataques; e entender o porquê da ação destes indivíduos, apresentando as possíveis soluções para os problemas causados por estes grupos, através de dicas sobre segurança virtual na internet.

A pesquisa que fizemos foi primeiramente exploratória para levantamento de dados e conhecimento do assunto em questão, consistindo assim, no reconhecimento de um tema que ainda está em fase de estudos. De acordo com Mattar (2001, p.18), tal pesquisa "visa promover ao pesquisador o maior conhecimento sobre o tema ou problema de pesquisa em perspectiva". Nesse caso, fizemos também uma pesquisa bibliográfica junto a autores e obras que tratam do assunto, bem como em fontes seguras da internet.

Depois foi realizada uma pesquisa explicativa que, conforme Gil (2002) afirma, "é aquela que identifica os fatores que determinam ou contribuem para a ocorrência dos fenômenos". Foi nessa parte que citamos as motivações que os Hackers e Crackers possuem para realizarem suas ações, concluindo assim o processo de elaboração da presente monografia.

Este trabalho está estruturado em três partes. Na parte um será apresentado um breve histórico sobre o desenvolvimento da *Web*. Abordaremos o surgimento da Internet tanto a nível nacional quanto global, a criação da WWW (*World Wibe Web*) e de alguns programas que surgiram através da ampliação do uso de computadores pessoais. Também será feita uma reflexão acerca da Cibercultura tratando um pouco sobre as tecnologias presentes na cultura contemporânea e, concluindo a parte um, abriremos um tópico sobre a recente dinâmica do mundo virtual: a Computação em Nuvem, onde serão apresentadas as formas pelas quais ela é utilizada, enfatizando também os problemas de segurança que essa nova tendência virtual possa vir a ter.

Na segunda parte será enfocada a questão da Cultura Hacker em si, explicando desde sua origem, passando por sua expansão a redor do planeta, destrinchando tanto as diferenças quanto os diversos tipos existentes entre os Hackers e os Crackers.

Por fim, na terceira parte será mostrada a ética virtual utilizada pelos Hackers, suas motivações e ações no ciberespaço e a apresentação de um manual com algumas dicas importantes sobre a utilização da internet de modo geral, especialmente, com a intenção de se prevenir contra possíveis ataques virtuais.

1 Desenvolvimento da Web

Ao contrário do que se possa imaginar, a internet nunca foi algo planejado. Ela surgiu diante da necessidade da comunicação entre as bases militares dos Estados Unidos durante a Guerra Fria (1945 – 1991). Inicialmente com o nome de ARPANET, derivado da empresa que a desenvolveu (*Advanced Research and Projects Agency*), ela afirmava que mesmo que o Pentágono fosse atingido pela então Ex-União Soviética, o contato entre os próprios americanos seria garantido.

Acreditando que a ameaça da Guerra Fria teria chegado ao fim e que a ARPANET não teria mais tanta utilidade, os militares cederam suas atividades à participação de cientistas. Em seguida, as universidades puderam ter o privilégio de conhecer a nova tecnologia. Com o passar dos anos, novos pontos nos Estados Unidos tiveram a possibilidade de conhecê-la, marcando a década de 70 com a expansão da grande rede. De acordo com Pierre Lévy (2000, p.31):

> Já nessa época era previsível que o desempenho do hardware[5] aumentaria constantemente. Mas que haveria um movimento geral de virtualização da informação e da comunicação, afetando profundamente os dados elementares da vida social, ninguém, com a exceção de alguns visionários, poderia prever naquele momento.

A linguagem inicial dos computadores era extremamente complexa, até mesmo para os cientistas da época. Até que um dia um dos membros do MIT (*Massachusetts Institute of Technology*), que é um dos maiores centros de pesquisa em ciência e tecnologia do mundo e onde se reuniam os maiores intelectuais da informática na época, sugeriu a idéia de fazer um

[5] O hardware, circuitaria, material ou ferramental é a parte física do computador, ou seja, é o conjunto de componentes eletrônicos, circuitos integrados e placas, que se comunicam através de barramentos.

programa que convertesse uma linguagem mais humana em linguagem de máquina. Era o início dos compiladores, que seriam uma espécie de decodificador das linguagens computacionais, utilizados até hoje.

Foi nessa época que surgiram os primeiros "mestres" da computação. Eram os chamados Hackers, que depois serão detalhados com maior ênfase. Esses gênios eram muito admirados. Foram eles que aprimoraram as linguagens de programação, criaram os compiladores, desenvolveram os *debuggers* (que servem para descobrir onde está o erro de uma programação) e iniciaram o trabalho dos sistemas operacionais. Ou seja, criaram os pilares do que hoje é conhecido como Computação.

Assim, aos poucos, o computador foi tomando a estrutura que nós conhecemos hoje. Foi em 1981 que a computação foi completamente redefinida. A partir deste ano, com o lançamento do PC da IBM, o usuário doméstico pôde ter alcance aos recursos e ferramentas que só os Centros de Processamento de Dados (CPD) das empresas tinham domínio. Não era uma transformação só na área da informática, mas sim, o início de uma transformação nas relações sociais que, posteriormente, viriam a ter um grande impacto mundial.

Em 1991, insatisfeitos com a lentidão e dificuldade para se utilizar a internet, visto que apenas programadores e operadores tinham conhecimento suficiente para utilizar a grande rede, um grupo de cientistas do CERN - *Laboratoire Européen pour la Physique des Particules* – decidiu criar a WWW (*World Wide Web*).

A internet e a WWW não são sinônimos, como muitas pessoas ainda acreditam e utilizam os termos desta maneira. Na verdade, a WWW é um espaço que permite que se troquem informações multimídias através da estrutura da internet. A WWW é apenas uma das formas de utilização da rede, assim como um programa que compartilhe arquivos, por exemplo, ou um comunicador instatâneo.

Com design simples, visualização mais clara e rápida, a navegação na internet pôde ser assim ampliada. O que antes era restrito apenas a especialistas, agora podia ser utilizado por pessoas comuns. Através de um novo tipo de *software* conhecido como *browser* ou navegador[6], facilitou-se a explosão que é o acesso à internet.

[6] É o navegador, o software que interpreta a linguagem html, permitindo assim explorar textos, fotos, gráficos, sons e vídeos na Internet e pular de uma página para outra com um simples clique nos links.

No Brasil, o desenvolvimento da internet teve seu pontapé inicial em 1988, quando Oscar Sala, professor da Universidade de São Paulo (USP) e conselheiro da Fundação de Amparo à Pesquisa no Estado de São Paulo (FAPESP), percebeu que poderia se comunicar e manter contato com outras instituições de outros países através de uma rede de computadores.

Foi só em 1991, mesmo ano da criação da WWW, que o acesso à internet foi permitido às instituições educacionais e de pesquisa e a órgãos do governo, porém tudo era destinado a um seleto grupo de indivíduos. Em 1992, o uso da internet foi liberado para Ong´s, mas apenas em 1993 que ocorreu, de fato, a primeira conexão à longa distância possibilitando, em 1994, a criação de diversos *sites* na grande rede.

Os primeiros endereços virtuais criados na Web foram relacionados a notícias. Posteriormente, foram criados os *sites* destinados a compras e entretenimento. A partir daí a internet foi sendo observada realmente como um meio comunicacional.

O surgimento das salas de bate-papo, que abriu portas para novos programas da mesma linha como o *mIrc*[7], foram muito utilizados pelos milhares de adolescentes mundo afora dando indícios do fenômeno global que a Internet viria a ser.

Atualmente o *Messenger* atrai, além dos adolescentes, tradicionais usuários desse meio de se comunicar, cada vez mais adultos e crianças para a comunicação virtual, especialmente devido aos seus recursos como as conversas através da *webcam* e do microfone.

A popularização do *e-mail* foi um fator marcante também para a expansão da internet. Não era mais necessário esperar dias para enviar uma mensagem a um destinatário. Qualquer que fosse o assunto, inclusive com fotos ou outros tipos de arquivos anexados, poderia ser enviado em questão de segundos para alguém do outro lado do planeta. Sem contar que, através dos diversos recursos de tratamentos textuais, a facilidade e a praticidade que se adquiriu para escrever, aumenta vertiginosamente, como afirma Dominique Wolton (2007, p.87):

[7] mIRC é um cliente de IRC, shareware, para o sistema operacional Microsoft Windows, criado em 1995 e desenvolvido por Khaled Mardam-Bey com a finalidade principal de ser um programa chat utilizando o protocolo IRC, onde é possível conversar com milhões de pessoas de diferentes partes do mundo.

> Sem dúvida são o correio eletrônico e as funções anexas de tratamento de texto as aplicações mais sedutoras. Escrever, se corresponder, arquivar, apagar, sem limite, sem esforço, continuamente, fora das pressões de tempo e espaço, constituem o principal trunfo dos sistemas automatizados.

Atualmente, mesmo diante dos problemas relacionados à inclusão digital, a internet é uma realidade global e representa um grande marco no processo comunicacional. Ela está completamente incrustada na sociedade, como afirma Manuel Castells (2003, p.286-287):

> Internet é sociedade, expressa os processo sociais (...) ela constitui a base material e tecnológica da sociedade em rede. (...) Esta é a sociedade (...) cuja estrutura social foi construída em torno de redes de informação a partir de tecnologia de informação microeletrônica estruturada na internet. Nesse sentido, a internet não é simplesmente uma tecnologia; é o meio de comunicação que constitui a forma organizativa de nossas sociedades; é o equivalente ao que foi a fábrica ou a grande corporação na era industrial.

Não existem fronteiras geográficas para limitar sua utilização. Seu acesso é feito a partir do seu próprio lar, através de *lan-houses* ou em lugares que ofereçam o sistema *wi-fi* de acesso à internet, onde qualquer indivíduo que tiver um *notebook* equipado com as ferramentas necessárias poderá utilizar a grande rede com enorme facilidade.

Através do uso de textos, sons, imagens e vídeos, pode-se acessar vários recursos culturais e educativos. A educação das crianças e o aprendizado na Academia vêm sendo modificado através do uso da *web*. O material disponível ao estudante, além de imenso, é sempre atualizado.

O mundo da internet, como em qualquer outra situação, também apresenta situações de riscos. Talvez por ela ser um reflexo da sociedade, existem aspectos positivos e aspectos negativos também. Há gente boa e há gente má. Porém, a utilização dessas novas tecnologias tem vindo mais a somar do que a diminuir na construção de uma sociedade mais informada e esclarecida.

2 Cibercultura

A humanidade há pouco tempo tem vivenciado um momento ímpar na sua história. É uma transformação significativa nos modos de encarar o cotidiano, que poucos poderiam

prever a algumas décadas atrás. A sociedade está conectada. Os limites territoriais não são capazes de impedir que a comunicação flua com uma velocidade antes inimaginável.

Lentamente as culturas nacionais tendem a tornar-se globalizadas e cibernéticas. A língua inglesa já domina grandes regiões do planeta. Não é do nosso interesse entrar no mérito da discussão sobre o que é certo ou errado nesse movimento expansionista da cultura americana pelo mundo. Porém, é de extrema importância citar que esse tipo de ação é um exemplo claro da homogeneidade que o mundo, gradualmente, vai adquirindo.

O desenvolvimento e a evolução constante das tecnologias digitais têm transformado e levado a humanidade a experimentar diferentes sensações e novas experiências sociais. E o ciberespaço se torna termo evidente neste contexto. Ele "especifica não apenas a infra-estrutura material da comunicação digital, mas também o universo oceânico de informações que ela abriga, assim como os seres humanos que navegam e alimentam esse universo" (LÉVY: 2000).

A interatividade, capacidade de um equipamento, sistema de comunicação ou de computação, etc. de interagir ou permitir interação mútua entre duas ou mais coisas, tem sido um ponto fundamental desta realidade. Essa relação que advém das trocas e relações entre a sociedade e as novas formas de tecnologia, especialmente aquelas que englobam as convergências midiáticas através da informática, aliadas à comunicação, é que é conhecida como Cibercultura. É a cultura contemporânea. É a cultura tecnológica que está incrustada em nossa sociedade. O modo de vida "*online"* passa a ser mais presente a cada dia.

O termo, apesar de parecer atual e futurístico, de certa forma, já vem sendo estudado há algumas décadas. O que pode ser considerado o marco ou o momento de transição desta nova era é a criação do computador digital, na época da Segunda Guerra Mundial, pelos americanos. Com o passar dos anos, o computador digital foi se aperfeiçoando, ganhando novas funcionalidades e adquirindo o formato que é utilizado atualmente no dia-a-dia da população. Sua utilidade, dentre os meios digitais utilizados com maior freqüência, com certeza é o de maior importância.

É importante compreender que a cibercultura não é uma cultura que é guiada pelas inovações tecnológicas. De acordo com André Lemos (2007, p.184):

> Por cultura entende-se um conjunto de valores e crenças que formam o comportamento; padrões repetitivos de comportamentos geram costumes que

> são repetidos por instituições, bem como por organizações sociais informais. Cultura é diferente de ideologia, psicologia ou representações individuais. Embora explícita, a cultura é uma construção coletiva que transcende preferências individuais, ao mesmo tempo em que influencia as práticas das pessoas no seu âmbito.

Sendo assim, o que existe de fato, é o estabelecimento de uma ligação profunda entre a sociedade pós-moderna e a tecnologia, marcando a cibercultura como a cultura contemporânea extremamente marcada pelas novas formas de tecnologias digitais.

Nomes como *palm tops*, *notebooks*, *iphone*, *mp4 player*, *playstation* ou *webcam* já fazem parte do nosso cotidiano. Por mais que tente resistir, o indivíduo é cercado de todos os lados por inovações tecnológicas e, na maioria das vezes, com nomes estrangeiros, exemplificando a tendência da globalização cultural que nós vivemos. Sendo assim, não deve-se confundir a cibercultura com uma subcultura particular. Pierre Lévy (2007, p.11), ao analisar o livro Cibercultura de André Lemos, afirma que:

> (...)a cibercultura é a nova forma da cultura. Entramos hoje na era da cibercultura como penetramos na cultura alfabética há alguns séculos. Entretanto, a cibercultura não eh uma negação da oralidade ou da escrita, ela eh o prolongamento destas; a flor, a germinação.

Os meios digitais não só fazem parte, como tomam conta das nossas vidas. Segundo dados da União Internacional de Telecomunicações (UIT)[8], ainda em 2006, os meios de comunicação digitais já eram mais utilizados pela população mundial do que a televisão, o rádio, os jornais impressos e o cinema. Essa tendência vem crescendo consideravelmente.

Se formos analisar este dado, pode-se compreender claramente a "substituição" de determinadas mídias e a dedicação quase que inteiramente ao PC.

Já existem *softwares* vinculados à Internet, onde é possível assistir a determinados programas televisivos ao mesmo tempo em que ele está sendo veiculado pela emissora. Existe ainda a possibilidade de acessar somente os trechos ou partes de uma entrevista, por exemplo, através de *sites* como o *YouTube*, que armazena uma infinidade de vídeos, por vezes, disponibilizados pela própria emissora de televisão. Sem contar que já está no ar uma nova

[8] *Site* do Terra (*online*, acesso em: 15 de Julho de 2009)

versão do *YouTube* só para vídeos com alta definição, que são mais lentos de serem acessados devido à sua qualidade.

O rádio e a nova dinâmica dos arquivos em *mp3* vêm despertando a reflexão de diversos autores que analisam se o rádio está, de fato, dando lugar às novas tecnologias. Os *mp3 players* e *mp4 players* (o segundo, que permite a exibição de vídeos também) possibilitam que o indivíduo leve para onde quiser suas músicas preferidas, sem a necessidade de ligar o rádio. Com a ampliação da banda larga, o *download* de álbuns inteiros é feito em questão de minutos, deixando o usuário livre para montar suas próprias *playlists* em seu computador pessoal.

O jornal impresso é outro meio que vem enfrentando problemas relacionados às suas vendagens. Não é mais novidade ouvir notícias de que determinado jornal ou tem que demitir funcionários ou está perto de fechar as portas. As notícias *online* acabam atraindo mais os leitores, seja pela praticidade de se ler, pelo apelo da imagem que ela pode conter ou pela velocidade de informações que chegam aos grandes portais de notícias.

Com a velocidade cada vez maior da Internet, devido à utilização da banda larga, "baixar" filmes através da grande rede tornou-se um hábito para a maioria dos internautas, que preferem assistir a seus filmes prediletos no próprio computador ou gravá-los em um DVD e visualizá-los em seus *Homes Theaters*, que, aliados às recentes televisões de LCD de alta-definição, praticamente transformam a própria sala de casa em um cinema.

Desta forma, as relações entre o homem, as novas tecnologias da informação e a comunicação são, a cada dia, mais intrínsecas. Com o desenvolvimento tecnológico os indivíduos têm a possibilidade de se libertar do limite espaço/tempo, visto que, através da internet, pode-se navegar e "viajar" para novos lugares com um simples clique de um mouse. Isso só é possível graças às tecnologias da cibercultura.

Apesar de ser mais cômodo para alguns usuários, determinadas práticas virtuais acarretam diversos problemas. O *download* ilegal e a venda de cópias de músicas e filmes já superam, em alguns casos, a receita obtida pelas respectivas indústrias. No Brasil, o faturamento do mercado informal chega a igualar com o do mercado formal em um bilhão de dólares. Com as músicas, os dados são bem mais surpreendentes, já que 82% do faturamento total é destinado ao mercado informal contra apenas 18% do mercado formal[9].

[9] Retirado da revista Veja, Ed. 2126, p. 102

Até o fim do século XX, aproximadamente, o processo de distribuição de informações nunca esteve ao alcance de cidadãos comuns, de modo geral. Essa funcionalidade estava restrita, como sempre esteve, nas mãos de poucos, normalmente da elite, que detinha o poder do controle dos veículos de comunicação de massa, o que facilitava o processo de manipulação das informações.

Com a modernidade, as novas formas de comunicação se tornam mais flexíveis. Nas mídias tradicionais como televisão, rádio e jornal impresso, a hierarquia da produção e distribuição de informações segue o modelo um-todos, característico da comunicação de massa, onde um ou apenas poucas pessoas são os responsáveis pela disseminação da informação para o resto da sociedade. Já com a cibercultura, essa tendência vai sendo diminuída, visto que essa relação de produção é baseada no modelo todos-todos, onde qualquer indivíduo tem o poder de expressar suas idéias e transmitir para qualquer lugar do mundo através do diversos meios que a internet pode oferecer. De acordo com a afirmação de Manuel Castells (2003, p.8):

> A internet é um meio de comunicação que permite, pela primeira vez, a comunicação de muitos com muitos, num momento escolhido, em escala global. Assim como a difusão da máquina impressora no Ocidente criou o que MacLuhan chamou de a "Galáxia de Gutenberg", ingressamos agora num novo mundo de comunicação: A "Galáxia da Internet".

Desta forma, o grande fantasma da censura se torna cada vez mais difícil de ocorrer, na medida em que as informações podem ser provenientes de diversas fontes. O que a princípio aparenta ser uma evolução positiva, pode ser encarado de forma negativa também, como afirma Pierre Lévy (1999, p.188):

> Antes da popularização da internet, o espaço público de comunicação era controlado através de intermediários institucionais que preenchiam uma função de filtragem entre os autores e os consumidores de informação. Hoje, com a internet, quase todo mundo pode publicar um texto sem passar por uma editora nem pela redação de um jornal. No entanto, essa liberdade de publicações que a internet oferece acarreta no problema da veracidade e da garantia quanto à qualidade da informação. A cada minuto novas pessoas assinam a internet, novos computadores se interconectam e novas informações são injetadas na rede. Quanto mais o ciberespaço se estende, mais universal se torna. Novas maneiras de pensar e de conviver estão sendo elaboradas no mundo das telecomunicações e da informática.

A quantidade de notícias oferecidas ao usuário é imensa. Teoricamente isso é muito interessante, pois amplia o conhecimento do internauta. Porém, o que ocorre é que, na maioria das vezes, o indivíduo limita-se a apenas ler a manchete ou aquelas notícias com o texto que não passe de três parágrafos. No fim das contas, pelo desejo de saber de tudo que a página principal oferece, o navegante termina por não investigar nada a fundo e capta apenas algumas pequenas informações do fato. Isto, quando não se esquece delas, como diria Umberto Eco, em entrevista à Folha de São Paulo (2008):

> Sim, parece que tudo é certo, que você dispõe de toda a informação, mas não sabe qual é confiável e qual é equivocada. Essa velocidade vai provocar a perda de memória. E isso já acontece com as gerações jovens, que já não recordam nem quem foram Franco ou Mussolini. A abundância de informações sobre o presente não lhe permite refletir sobre o passado. Quando eu era criança, chegavam à livraria talvez três livros novos por mês; hoje chegam mil. E você já não sabe que livro importante foi publicado há seis meses. Isso também é uma perda de memória. A abundância de informações sobre o presente é uma perda, e não um ganho.

Destarte, observando as novas tecnologias digitais, não nos cabe tachá-las de boas ou ruins. O que se deve compreender é que elas existem e são ativas dentro da sociedade, transformando-a e moldando-a de acordo com novas criações. Pierre Lévy (2000, p.11) resume perfeitamente o que estamos vivenciando:

> Consiste apenas em reconhecer dois fatos. Em primeiros lugar, que o crescimento do ciberespaço resulta de um movimento internacional de jovens ávidos para experimentar, coletivamente, formas de comunicação diferentes daquelas que as mídias clássicas nos propõem. Em segundo lugar, que estamos vivenciando a abertura de um novo espaço de comunicação, e cabe apenas a nós explorar a s potencialidades mais positivas deste espaço nos planos econômico, político, cultural e humano.

E a cada dia a internet evolui, cresce e nos envolve. Existe uma nova tendência de desenvolvimento de seu futuro, não tão distante, que será abordado em seguida: a Computação em Nuvem. Se trata da nova dinâmica de armazenamento de dados na internet que tem despertado o interesse de estudos na área da segurança, haja vista que os dados que irão tramitar na rede ficarão muitos mais suscetíveis a invasões do que se forem armazenados

no próprio disco rígido. Em seguida será abordado um pouco mais dessa tendência e da problemática envolvendo a segurança virtual inserida em tal contexto.

2.1 Computação em Nuvem

A Computação em Nuvem ou *Cloud Computing*, como é mais conhecida internacionalmente, é um novo sistema de compartilhamento de ferramentas e armazenamento de dados no ciberespaço. Através da interligação de sistemas, semelhante às nuvens do céu, onde nada existe ligando-as a alguma coisa fixa, nessa nova tendência também não será necessário que uma máquina dependa de outros equipamentos para que o processo passe a existir.

Não haverá mais a necessidade de alocar os arquivos em unidades físicas, pois a Computação em Nuvem cuida deles, mesmo que o indivíduo esteja com o PC desligado. Isto só é possível graças aos grandes centros de computação espalhados ao redor do mundo, conectados entre si, que processam e armazenam as informações digitais produzidas desde os simples usuários domésticos a grandes corporações. A informação estará "livre" da memória de um computador.

Ou seja, a capacidade de armazenar e de processar dados está se deslocando dos computadores pessoais para a internet em si. Os usuários poderão acessar suas vidas digitais através de computadores, *netbooks*[10] ou telefones celulares em qualquer lugar do mundo.

Muitos usuários já estão vivenciando essa realidade das nuvens, mas ainda não se deram conta, conforme matéria da Veja:

> Quem mantém fotos no Flickr[11], ou salva textos e planilhas no Google Docs, recorre a serviços de armazenamento de dados que operam na nuvem. A vantagem é poder

[10] Termo usado para descrever uma classe de computadores portáteis tipo subnotebook, com dimensão pequena ou média, peso-leve, de baixo custo e geralmente utilizados apenas em serviços baseados na internet, tais como navegação na web e e-mails.

[11] O Flickr é um site da web de hospedagem e partilha de imagens fotográficas (e eventualmente de outros tipos de documentos gráficos, como desenhos e ilustrações), caracterizado também como rede social.

> acessar os arquivos de qualquer lugar: a informação não está "trancada" na memória de um computador.[12]

Outro fator importante é a questão relativa aos programas instalados em um computador. Também não será mais necessário realizar o *download* dos *softwares*, já que eles serão acessíveis gratuitamente e com a possibilidade de serem acessados em qualquer lugar que se esteja, com a vantagem ainda de estar livre dos direitos de propriedade.

As empresas também lucram com esse novo sistema, haja vista que elas não irão precisar mais instalar sistemas próprios de computação, já que agora elas podem comprar, sob demanda específica, com espaço para arquivar e processar seus dados na nuvem.

Desde 2002 que o Google já iniciou essa tendência tecnológica, através da disponibilização de programas como editores de textos, correio eletrônico e criação de agendas, para que pudessem ser utilizados online, sem custo nenhum do usuário.

Outro grande benefício que pode ser aplicado a este novo rumo que a computação vem tomando é a idéia de que não se tem mais a necessidade de serem adquiridos super-computadores, que custam uma fortuna, nem existirá a preocupação com o sistema operacional que está sendo utilizado, visto que tudo estará inserido na "Nuvem Computacional".

Como todas as revoluções tecnológicas, a criação da nuvem também instiga preocupação e apreensão de determinadas pessoas. Normalmente, esses temores estão ligados a segurança e a privacidade (ou, a falta dela) que pode vir a acontecer com essas mudanças na estrutura virtual. Com tudo arquivado na nuvem, acredita-se que seja mais fácil, de certa forma, para um criminoso virtual realizar deus delitos, pois o acesso à nuvem será mais direto e em cima do alvo, não precisando penetrar na máquina de um usuário.

Desta maneira, através do poder de armazenamento da Nuvem, muitos indivíduos terminam se tornando vulneráveis a determinados tipos de ataques. Por exemplo, é muito comum o armazenamento de fotos no próprio e-mail, algumas delas com conteúdos muito pessoais. Mas pelo fato de estarem sendo guardadas na Nuvem e não no próprio disco rígido, basta que seja descoberta uma senha, a do e-mail, para que aquele material possa vazar por toda a internet, sem existir a necessidade de se invadir o computador pessoal da vítima.

[12] Retirado da revista Veja, ed. 2126, p. 81.

A falta de segurança e a privacidade são assuntos bem próximos um do outro. O exemplo dito acima foi só um dos diversos que podem ser citados que acabam interferindo na segurança do usuário. Se um grupo musical lança um novo álbum e o armazena na Nuvem, ele pode ter suas músicas divulgadas sem a devida autorização. Isto serve também para um filme.

Portanto, esse novo caminho que a internet vem se direcionando continua a ter situações de risco que, apesar de todo o conhecimento moderno empregado no desenvolvimento das novas tecnologias, ainda devem provocar diversas discussões sobre como guiar este processo sem que o internauta seja prejudicado.

3 Cultura Hacker

3.1 A Origem

Como já foi dito, os primeiros Hackers, ou melhor, as primeiras vezes em que o nome apareceu, ele foi atribuído aos cientistas e estudiosos que freqüentavam o MIT. Foram eles que fizeram os computadores saírem dos laboratórios e irem para as universidades. E das universidades, posteriormente, para as nossas casas.

O termo Hacker, literalmente, significa “cortador”. Se formos analisar por outro prisma, realmente, pode-se entender Hacker como aquele que corta e derruba barreiras e fronteiras. Porém, no dito popular, muitos interpretam e associam o termo à pirataria digital e ao vandalismo.

Hacker, inicialmente, era o nome atribuído a qualquer indivíduo que fosse especialista em determinada área. Qualquer que fosse o assunto, se alguém fosse considerado bom naquilo, não necessariamente em algo ligado à informática, poderia ser chamado de Hacker. Eric Steven Raymond[13], em seu popular texto amplamente divulgado pela internet, “How to become a Hacker", diz que:

[13] Eric S. Raymond é um antropologista da cultura hacker da Internet. Sua pesquisa ajudou a explicar o modelo descentralizado open source para o desenvolvimento de software - e que provou ser efetivo na evolução da Internet. Disponível em: http://www.linhadefensiva.org/2005/05/hacker/ Acesso: 28 jul 2009.

> Há pessoas que aplicam a atitude hacker em outras coisas, como eletrônica ou música -- na verdade, você pode encontrá-la nos níveis mais altos de qualquer ciência ou arte. Hackers de software reconhecem esses espíritos aparentados de outros lugares e podem chamá-los de "hackers" também -- e alguns alegam que a natureza hacker é realmente independente da mídia particular em que o hacker trabalha.

No início, a internet era ligada ao sistema de defesa dos Estados Unidos. Porém, com o tempo, o governo abriu seu acesso às universidades. Consequentemente, os Hackers do MIT puderam ter acesso à nova tecnologia e, através dos protocolos de rede, começaram a interligar os microcomputadores e as universidades. Ou seja, aos poucos, os gênios do país inteiro estavam conectados entre si.

Com a proliferação dos computadores e do acesso à internet, os Hackers já não eram mais um grupo restrito de *experts* em programação. Alguns especialistas em internet também começaram a integrar este time. Logo, a denominação Hacker começava a ganhar certa heterogeneidade, visto que o termo abrangia desde superprogramadores até especialistas em redes e protocolos.

O grande problema dessa heterogeneidade foi o fato de alguns indivíduos se sentirem no poder de agir sem ética, apenas pelo fato de ter mais conhecimentos que outros. Como conseqüência, foi a partir daí que o nome Hacker começou a ser mal-visto pelas pessoas. As ações dos pseudo-hackers começaram a causar prejuízos.

Dessa forma, os Hackers "de verdade" criaram a expressão "Cracker", advindo de *Criminal Hacker*, para representar todos aqueles que vinham causando problemas no sistema, a fim de salvar a própria reputação. Porém, a mídia ignorou isso e tachava todos que utilizavam internet e tinham um conhecimento mais avançado sobre computadores de Hacker, sem se importar se o que eles estavam fazendo era algo positivo ou negativo.

3.1.1 Expansão da Cultura Hacker

Com o maior uso do termo Hacker, visto que novos especialistas eram agregados à nomenclatura, e com a nova categoria, os Crackers, a utilização desses termos foi se tornando mais freqüente entre estudantes e pessoas comuns.

Em 1983 um filme teve uma repercussão muito grande em toda a sociedade, especialmente entre os adolescentes da época. *Wargames* contava a história de um

adolescente apaixonado por computadores que, brincando com seu modem, consegue ter acesso ao NORAD, que era o computador responsável pela segurança de guerra dos Estados Unidos. Ele, sem querer, deu uma ordem de ataque que poderia causar a Terceira Guerra Mundial. Claro que o garoto não sabia do perigo que estava se envolvendo, mas as pesquisas e técnicas feitas por ele para descobrir a senha do suposto "jogo" eram próprias de Hackers.

Na época, este filme fez quadruplicar a venda de *modems* e inspirou diversos adolescentes a iniciarem o desejo de invadir o sistema de defesa dos Estados Unidos ou qualquer outra coisa, a partir de seu próprio quarto. Isso não quer dizer que o filme foi o pontapé inicial para que a Cultura Hacker fosse disseminada pelo mundo, mas com certeza influenciou o pensamento de muitos que hoje são, ou foram, Hackers.

Naquele período, o mercado americano colocou a disposição de quem quisesse livros com temáticas *Cyberpunk*, que é um termo utilizado para denominar indivíduos estudiosos da internet que usam seus conhecimentos para se manifestar na rede, seja invadindo computadores pessoais ou empresariais, com a finalidade de promover o divertimento próprio ou adquirir algo lucrativo. Tudo que era relacionado a invasões de sistemas ou crimes virtuais referentes ao mundo Hacker, ganhava enorme notoriedade na mídia.

No entanto, a juventude aficionada pela nova tecnologia, percebeu que se tornar um Hacker não era algo tão simples como num filme. Era preciso muito estudo e horas de dedicação. E assim, diversos jovens em busca de fama ou apenas conhecimento adentraram no *hacking*[14] e contribuíram para a difusão do mundo Hacker. Muitos dos que se aventuraram neste mundo e seguiram os caminhos contra a lei, hoje estão presos. Outros ganham fortunas como chefes de segurança em grandes corporações.

3.2 Hackers e Crackers: conhecendo suas principais diferenças

A diferenciação básica entre Hacker e Cracker já foi feita anteriormente. Hackers constroem e Crackers destroem. Porém, é necessária uma análise mais aprofundada da origem dos termos e como eles são aplicados, erroneamente, pelas mídias e pelo resto da população até os dias de hoje.

[14] Ato de penetrar em sistemas de computadores para ganhar mais conhecimento e entender como é o seu funcionamento.

As primeiras tentativas de diferenciação dos termos ocorreram na década de 80 pelos próprios Hackers, que estavam insatisfeitos com as atitudes anti-éticas dos Crackers. O grande entrave para maior disseminação dessa diferenciação do nome foi a própria mídia que apregoava e criava uma energia negativa acerca dos Hackers, fazendo com que o senso comum os tachassem de criminosos.

Vários foram os termos criados para designar as atitudes de cada grupo no ciberespaço. Entre os próprios Hackers e Crackers existem sub-grupos mais específicos que poderiam nos orientar sobre suas ações, mas apenas aqueles que lêem e pesquisam sobre o assunto são cientes disso. Estes termos são praticamente inexistentes na grande imprensa e nos portais virtuais. Em seguida, no próximo tópico, serão detalhadas essas sub-divisões.

Os Hackers defendem a idéia de que acesso à rede deve ser ilimitado e total, porém, com a condição de buscar apenas o auto-conhecimento. Desde os primeiros Hackers, a intenção principal daquela categoria era liberar as informações e os computadores do poder militar e industrial. De acordo com André Lemos (2007, p.204):

> (...)a microinformática foi, por si só, uma espécie de rebelião contra o peso da primeira informática (grandes computadores ligados à pesquisa militar). Para eles (os Hackers), todas as informações devem ser livres, as redes devem ser democráticas e os computadores acessíveis a todos e utilizados como ferramenta de sobrevivência na sociedade pós-industrial.

Mas, na prática não é isso que ocorre. Os Crackers se valem destas ideologias para cometer crimes, como furtar ou destruir dados. Ainda existem aqueles que se auto-denominam Hackers, apoiados também pela mídia, que têm o hábito de promover invasões a computadores pessoais, infectando-os de vírus[15] e alterando o sistema. Normalmente eles gostam de deixar seus *nicknames* ou codinomes, que são os apelidos que os identificam.

Vale salientar que o fato de invadir um computador apenas para "olhar" e não danificar nada, não implica dizer que é uma atitude correta, condizente com a lei. Determinadas atitudes dos Hackers, mesmo que não venham a causar nenhum prejuízo, pode vir a ser considerado um crime virtual.

[15] É um programa malicioso desenvolvido por programadores que, tal como um vírus biológico, infecta o sistema, faz cópias de si mesmo e tenta se espalhar para outros computadores, utilizando-se de diversos meios.

Apesar de serem tachados de bandidos por alguns, é graças aos Hackers que podemos usufruir de alguns benefícios na internet como as possibilidades de compras seguras em *sites* de comércio eletrônico, já que foi através das "olhadas" dos Hackers e das descobertas de falhas de seguranças, que pôde-se criar um sistema mais seguro e confiável para que os clientes pudessem realizar suas operações com tranqüilidade. Um Cracker olharia as falhas do sistema e se aproveitaria delas para lucrar ou causar prejuízos ao *site*. Já o Hacker, faz o contrário; corrige as falhas. Em síntese, as empresas contratam os Hackers para garantir que seu sistema fique seguro contra a ação dos Crackers.

3.3 Os diversos tipos de Hackers e Crackers

Apesar da utilização do termo Hacker ainda ser designado a todos aqueles que promovem qualquer atitude no mundo do *hacking* – desde indivíduos que invadem sistemas ou redes, desenvolvendo a criação de vírus para computador, até chefes de segurança na internet de grandes corporações – existem alguns outros termos que são usados na segurança da informação para diferenciar os tipos de Hackers/Crackers:

a) White Hat:

White Hats são os Hackers do "bem". É a categoria que os Hackers "de verdade" se enquadram. São aqueles especializados em explorar os sistemas de segurança, em busca de falhas ou possíveis problemas, a fim de solucioná-los e não de buscar proveitos próprios. Eles procuram detectar os erros, atuando dentro da lei.

Os White Hats utilizam seus conhecimentos sobre invasão de sistemas com o propósito de ajudar empresas, governos ou qualquer outro tipo de órgão para o qual eles trabalhem, com a intenção de evitar possíveis problemas relacionados às invasões. Ou seja, ele é apenas um profissional de segurança, que, vale salientar, estudou por muitos anos e que se dedica a proteger sistemas.

Normalmente, das ações dos White Hats, ao encontrar problemas no sistema de segurança do órgão para o qual trabalham, a primeira atitude dos mesmos é entrar em contato

com os donos ou responsáveis pelo sistema e avisá-los dos problemas, a fim de que medidas sejam providenciadas.

A maioria dos White Hats trabalha junto a auditorias de sistemas, redes e banco de dados. Mesmo que hoje esse Hacker Ético – ou de "Chapéu Branco", como são conhecidos os membros dessa categoria – preste um serviço do bem à comunidade, boa parcela destes indivíduos já foram Black Hats (categoria que veremos em seguida, constituída por elementos que utilizam seus conhecimentos para propósitos contra a lei). Afinal de contas, se tornar um White Hat pode ser considerado uma evolução.

Numa analogia ao filme "Prenda-me se For Capaz", que narra a história de um falsário que aplicava golpes em companhias aéreas, bancos, hospitais e enganava qualquer um quando lhe fosse útil, mas que no fim do filme, após ser capturado, é contratado pela polícia para trabalhar no departamento de segurança para combater exatamente os tipos de crime que ele cometia, passando a ter uma vida correta, longe das perseguições que sofria enquanto fugitivo.

É óbvio que não é uma regra geral, nem todos eles já foram vilões, nem é necessário que tenha sido para que se torne um "segurança" melhor. Mas muitos dos White Hats já fizeram coisas ilegais e hoje aplicam seus conhecimentos em uma atividade profissional, em prol de uma maior segurança para os usuários da internet.

Encontram-se também White Hats na função de pesquisadores acadêmicos dentro das universidades e nas escolas ministrando palestras sobre segurança na internet e computação em geral.

Devido ao sentido negativo com que a imprensa costuma estigmatizar os Hackers, julgando-os de Crackers, os Chapéus Brancos normalmente são classificados pela mídia como especialistas em tecnologia de informações, analistas de sistemas ou qualquer outra função na área da informática. Porém, o que eles são na verdade, é puro e simplesmente Hackers, no sentido mais original da terminologia.

O exemplo real mais claro relacionado à "conversão" do Black Hat em White Hat é o caso do ex-Cracker mais famoso do mundo: Kevin Mitnik. Após a explicação de todos os tipos de Hackers e Crackers será abordado um sub-tópico contando um pouco de sua história.

b) Black Hat:

Os Black Hats, que seriam os “Hackers” do lado negro, compõem exatamente os tipos de indivíduos que é comum se associar quando o termo Hacker é utilizado pela população em geral. Como já foi dito, tal termo é erroneamente associado, especialmente pela mídia, aos criminosos virtuais. Na verdade, a maioria das ações que prejudicam sistemas e usuários da internet e é atribuído aos “Hackers”, são ações promovidas pelos Black Hats, ou seja, os Crackers.

São pessoas com um bom nível de conhecimento sobre programação, sistemas operacionais e redes de computadores. Eles costumam investigar as falhas dos sistemas operacionais, das redes ou banco de dados para, através dessas deficiências, invadi-los e desenvolver ações ilícitas, em busca de benefício próprio.

São capazes de desenvolver seus próprios *softwares* a fim de encontrar vulnerabilidades para, posteriormente, modificar valores de um banco de dados, furtar informações, assim como derrubar servidores e sistemas e descobrir informações sigilosas e importantes em busca de ganho próprio.

A metodologia de trabalho desse grupo normalmente é feita de forma individual, cada Black Hat trabalhando sozinho em busca de informações. Porém, também existe uma parcela que costuma participar de comunidades restritas com a intenção de trocar informações técnicas sobre invasões, criação de programas, entre outros.

É através do controle de programas e aplicativos que espalham códigos maliciosos, ou seja, dos vírus, que esses Crackers, normalmente, agem, provocando os mais diversos danos aos usuários.

É importante perceber que os White Hats e os Black Hats formam uma espécie de dois separadores entre as categorias Hackers/Crackers. Indivíduos com grande conhecimento podem fazer parte tanto de um grupo quanto do outro, variando apenas de acordo com suas atitudes.

As especificidades aparecem como sub-divisões desses grupos em alguns casos. Defacers também podem ser Black Hats, mas nem todo Black Hat é um Defacer. Assim como um Phreaker pode ser um White Hat, mas nem todo White Hat é um Phreaker. Com o entendimento das próximas categorias, essa divisão ficará mais clara.

c) Gray Hat:

Essa categoria é a junção dos White Hats com os Black Hats. Por isso são conhecidos como os "Hackers" de Chapéu Cinza. Eles se tornam muito perigosos pelo fato de não ser possível discernir se esses indivíduos estão atuando de maneira positiva ou de maneira negativa. Eles podem tanto ser do "bem" quanto do "mal".

Esse status vai variar de acordo com o tipo de serviço que lhes é encomendado. Eles normalmente exigem retribuição financeira para compensar a missão que lhes é dada. São conhecidos por serem mercenários e tem como objetivo primordial a obtenção de lucro financeiro através de seus conhecimentos, mesmo que para isso tenha que realizar alguma tarefa ilícita.

De acordo com sua ética, dizem ser aceitável que se invada algum sistema, com acessos não prejudiciais, sem que seja cometido algum furto, configurando-se, segundo eles, com ações que não envolvem propriamente vandalismo ou destruição.

Em contra-partida, confiar num Hacker que não tem sua ética bem definida, que hora pode agir para o mal, hora para o bem, é arriscado. Por mais que afirmem que irão adentrar num sistema e não prejudicar nada, o fato de invadir uma "propriedade" por si só, já se torna uma atitude, de certa maneira, anti-ética.

d) Phreaker:

Eles são alucinados por telefonia. É a melhor forma de tentar defini-los. O termo Phreaker advém do inglês *freak*, que significa "maluco". Por terem um imenso conhecimento sobre telefonia (móvel e fixa), através de programas e equipamentos, eles são capazes de invadir centrais telefônicas e realizar ligações internacionais sem pagar nenhuma taxa – a partir de ataques a servidores que estão localizados em outros países – por exemplo. Normalmente, os Phreakers são ex-funcionários de companhias e, que por "n" motivos, tentam prejudicar tais empresas através de seus conhecimentos.

O primeiro Phreaker foi o americano John Draper, mais conhecido como Capitão Crunch. Ele foi o responsável por descobrir que um pequeno apito de plástico que era encontrado nas caixas de um cereal – contendo um mascote chamado *Cap'n Crunch* (daí

advém seu apelido) –, emitia fielmente a mesma freqüência de 2600hz dos orelhões da AT&T, permitindo que o usuário pudesse realizar ligações gratuitas.

No ano de 1972, John Draper foi preso por fraude e condenado a cinco anos de estágio. No início da década de 70, ele havia ensinado algumas técnicas das suas habilidades com o phreaking a Steve Jobs e a Steve Wosniak. Eles dois foram elementos importantíssimos na computação daquela época. Equipados de um Fusca e uma calculadora científica, foram os responsáveis pela criação do primeiro microcomputador realmente popular. Com a venda de alguns bens, em seguida, eles criaram a *Apple*.

Na época, tentaram vender seu projeto pra a *HP*, porém o mesmo foi recusado com a justificativa de que ambos ainda não tinham nem terminado a faculdade, o que levou Jobs e Wosniak a desenvolverem o projeto sozinhos.

Atualmente, John faz *softwares* de segurança e é o responsável por desenvolver o *KanTalk* (*VoIP software* para cantores adolescentes), além de organizar também um programa de TV na internet, o *TV Crunch*.

Um programa comum que é muito utilizado pelos Phreakers é o *Blue Box*, que possibilita gerar tons de 2600hz pela placa de som, fazendo com que a companhia telefônica não identifique a chamada.

Existe ainda uma outra técnica, muito utilizada no Brasil, que consiste na utilização de diodo e resistor em telefones públicos. Cobrir o cartão telefônico com papel alumínio para que os créditos não terminem também já foi muito usado entre os Phreakers brasileiros, porém a técnica só servia nos antigos orelhões. Nos novos a possibilidade é maior de tomar um choque do que conseguir uma ligação. Vale dizer que essas técnicas são utilizadas no mundo inteiro.

No Brasil, existem alguns Phreakers que conseguem ter acesso direto à algumas centrais de telefonia. Dessa forma, eles podem tanto ligar quanto desligar telefones, além de ter o poder de apagar contas. Um dos programas mais utilizados por eles é o *Ozterm*, que não é nada fácil de se encontrar pela internet.

f) Script Kiddie:

O Script Kiddie é o nome dado aos indivíduos que não tem um grande poder de conhecimento e de domínio sobre programação. Alguns consideram que são uma espécie de

Crackers inexperientes, normalmente adolescentes, e outros afirmam que nem isso são, configurando-se apenas como pessoas que tentam se passar por Crackers a fim de conseguir fama e outras formas de lucros pessoais, provocando a ira e a repulsa dos Hackers.

A grande maioria dos ataques virtuais são feitas por Script Kiddies, através da utilização de programas como *exploits*[16], *trojans*[17] e outras ferramentas de *cracking* para auferir seus objetivos.

Esse grupo procura por alvos fáceis, tendo como objetivo principal obter acesso à conta do administrador de uma máquina, seja lá qual ela for. Não existe a procura por informações ou companhias específicas. Sendo assim, suas ações consistem em buscar um pequeno número de falhas pela internet inteira, até que se consiga achar uma máquina que tenha uma boa vulnerabilidade.

Mesmo que cada Script Kiddie possua o conhecimento diferente um do outro, quando entram em ação, todos seguem basicamente o mesmo raciocínio ou plano de estratégia; procurar, de forma alternada, por falhas específicas, para que, mais a frente, elas possam vir a ser exploradas.

Ou seja, sua metodologia consiste em realizar um rastreamento pela internet em busca de uma falha específica. Quando encontrada, começam a explorá-la através de ferramentas, muitas delas automáticas, requerendo uma intervenção mínima do Script Kiddie. Pode-se ainda executar tal ferrramenta e retornar até alguns dias depois para observar o resultado.

Eles podem atacar a qualquer hora do dia, assim como também podem rastrear uma máquina por 24 horas diárias. Não existe como adivinhar a que horas ou quando esse rastreamento poderá ocorrer, pois eles podem vir de qualquer parte do mundo. Seu ataque pode ser lançado ao meio-dia do seu país de origem, mas no país atacado pode ser outro horário, por exemplo.

Existem algumas maneiras para evitar problemas com os Script Kiddies. Por procurarem falhas comuns, é de praxe que eles busquem invasões mais simplificadas, menos

[16] Um exploit, em segurança da informação, é um programa de computador, uma porção de dados ou uma sequência de comandos que se aproveita das vulnerabilidades de um sistema computacional.

[17] Trojan Horse ou Cavalo de Troia é um programa que age como a lenda do Cavalo de Troia, entrando no computador e liberando uma porta para um possível invasão e é fácil de ser enviado, é só clicar no ID do computador e enviar para qualquer outro computador.

complexas. Se o sistema e sua rede estiverem protegidas contra as vulnerabilidades mais conhecidas, já é um grande avanço contra o ataque deste grupo.

Sendo assim, tendo conhecimento que os Script Kiddies podem atacar qualquer sistema, independentemente de sua importância, a melhor forma de se proteger é entender a maneira como eles atacam, como os sistemas funcionam, assim como suas falhas e vulnerabilidades.

g) Lammer:

Lammers, que traduzido do inglês significa "otário", são os indivíduos que se auto-promovem, tentando transformar sua imagem pessoal semelhante a de um Hacker. São pessoas que não conhecem aspectos técnicos do computador, mas fazem-se passar por especialistas. Na maioria das vezes, os Lammers gostam de utilizar (quando conseguem) programas pré-fabricados disponíveis na internet para executar suas ações.

Esse grupo, apesar de possuir um conhecimento pífio, por vezes conseguem algumas façanhas, por pura sorte, de compreender algum sistema e conseguir conectar-se a um computador remoto por exemplo. O que se torna um motivo ainda maior de auto-gabação. Um Lammer, na verdade, é definido por suas atitudes e não por seu conhecimento.

Uma boa maneira de reconhecer um Lammer é quando algum indivíduo deste aparecer se vangloriando e contando alguma história relacionada a um programa que o mesmo "criou", questioná-lo sobre a linguagem do tal programa. Com certeza a maioria irá responder "inglês"; afirmando não a linguagem de programação, mas sim o idioma.

Desta forma, o Lammer normalmente recebe o título de preguiçoso por não gostar de se dedicar a leituras sobre computação, diferentemente dos Hackers, que passam anos lendo e se dedicando muito para adquirirem o conhecimento que possuem. Se assemelham aos Script Kiddies, porém, são ainda mais inferiores que eles. O Lammer, devido às suas atitudes é, normalmente, execrado pelos Hackers.

h) Newbie:

Newbies, de cara, remete logo a "novo", advindo do *new* e, na verdade, é a melhor definição a ser aplicada para este grupo: novatos. Eles são os novatos na rede, os aprendizes do mundo *hacking*, afoitos por colher novas informações, descobrir novos conhecimentos e por vezes, de tão apressados, querem saber mais do que a capacidade intelectual atual permite.

Normalmente são muito questionadores, perguntando sobre coisas que às vezes não são necessárias ou apropriadas no momento, o que provoca a raiva nos Hackers, que os escanteiam e os ignoram, em determinados casos.

Pode-se se tentar confundi-los com os Lammers, porém a diferença primordial entre ambos está no fato de que os Newbies não tentam passar por cima de outra pessoa para obter a fama, característica fortíssima dos Lammers; na maioria das vezes, os "novatos" são garotos simples, ingênuos e muito inexperientes.

Existem pessoas que usam essa terminologia para ofender aqueles usuários que não aparentam ter determinadas aptidões ou grande domínio sobre a informática, especialmente no que se trata de comunicação virtual, como em jogos on-line, por exemplo. Newbie normalmente é o apelido do pior jogador da equipe, aquele que não consegue produzir muito e não consegue ajudar seu próprio time.

Em contrapartida, os próprios Newbies se defendem afirmando que eles são apenas novatos em busca de aprendizado. Este seria o motivo de, por muitas vezes, questionarem os Hackers mais experientes. Simplesmente para obter mais conhecimento; e não para deixá-los furiosos. Segundo eles, com o tempo, também virão a se tornar Hackers.

i) Defacer:

Defacers sãos os Crackers que se especializam em alterar *websites* na internet. Não é sempre que esse Defacer é um especialista. Apesar de poder ser um usuário com muito conhecimento, ele também pode ser um Script Kiddie, utilizando apenas programas pré-fabricados (nunca por eles) e executáveis.

Normalmente esses indivíduos são jovens, visto que é necessário dedicar grande parte do tempo ao dia procurando *sites* com o sistema de segurança baixo.

O Brasil já é conhecido no mundo inteiro por ter a maior porcentagem de páginas modificadas pelos Defacers. Essa medição é feita através de *sites* que servem para contabilizar esses ataques, como uma espécie de ranking. São milhares de indivíduos que dedicam várias horas do seu dia a procura de *sites* com grande potencial de vulnerabilidade a fim de criar um *deface* neles.

A maioria deles ataca apenas a página principal do *site*, alterando-a e inserindo uma desenvolvida por ele. As mensagens costumam atacar o administrador do *site* com xingamentos e palavrões e, muito habitualmente, costumam chamá-lo de "burro"; ou seja, querem evidenciar que o criador ou o responsável pelo sistema de segurança da empresa ou do *site* não é capaz de deixá-lo seguro.

Quase todos os Hackers, no início da sua "carreira", já foram um Defacer. São os chamados "quinze minutos de fama", que realmente, em *sites* mais importantes e acessados, duram tais minutos, pois é o tempo suficiente que o administrador perceba o erro e tome as providências necessárias para corrigi-lo. Porém, há casos de *sites* que passam dias com a página principal alterada por grupos Defacers.

As motivações que levam os grupos a praticarem este tipo de *hacking* são um pouco variadas, mas perpassam, em grande parte, pelo prazer. Este prazer dura algo em torno de 10 a 20 minutos. Após horas de busca, encontrar o *bug*[18], ou seja, a falha do sistema, pode ser considerado o clímax para os Defacers. É por esse *bug* que eles podem invadir e, desta forma, enviar seu aquivo HTML e postar no *site*, confirmando que, agora sim, ele conseguiu completar sua "missão". O gol foi feito e agora o jogador pode comemorar.

O grande objetivo dos Defacers, ao contrário do que muitos possam imaginar, não é simplesmente se divertir, roubar dados, colher informações ou furtar dinheiro dos *sites*, já que, através das invasões, os Defacers têm acesso a números de contas e cartões de crédito.

Para eles, o grande barato desse "jogo" é a fama. Os "quinze minutos de fama" que foi dito mais acima é o que interessa para a maioria deles. Sendo assim, quanto mais famoso e reconhecido for o *site*, com mais prestígio determinado grupo invasor irá se tornar.

Logo, o valor de uma invasão para os Defacers está na relevância que a página invadida tem no ciberespaço. De nada adiantará a invasão de um *site* desconhecido, que não

[18] Bug é um erro no funcionamento comum de um software, também chamado de falha na lógica programacional de um programa de computador, e pode causar discrepâncias no objetivo, ou impossibilidade de realização, de uma ação na utilização de um programa de computador.

seja acessado com muita freqüência; porque, desta maneira, ninguém poderá visualizar suas "pixações".

Um dos grandes problemas decorrentes dos pixadores virtuais, é a falta de credibilidade que os Hackers brasileiros tem fora do país. Devido a imensa quantidade de Defacers e Script Kiddies que atuam no Brasil, aliados à errônea interpretação da mídia, ao denominar praticamente todos os indivíduos que tem o conhecimento mais avançado na área computacional, de Hackers, sem distingui-los quanto às suas ações, os especialistas de outros países tem a impressão que aqui só existem adolescentes que não estudam programação e só utilizam o computador para se divertir com os programas criados, em grande parte, por eles.

j) Carder:

Este é o termo utilizado para denominar todos os Crackers que se especializaram nas, tão comentadas atualmente, fraudes aos cartões de crédito e boletos bancários. Eles têm o poder de conseguir vários números de cartões de créditos, válidos em *sites* que fazem o uso dos mesmos, como *sites* de comércio eletrônico, salas de bate-papo virtuais que são pagas, *sites* pornográficos, que é necessário ser feito um pagamento para receber a senha, entre outros.

Estas ações podem ser realizadas através de *trojans*, que é uma espécie de programa executável que, uma vez acionado, permite que o invasor possa ter acesso aos dados da vítima, roubando-lhe todas as senhas pessoais, por exemplo; ou por meio dos *keyloggers*, que é um programa capaz de gravar as senhas digitadas pelo usuário e, posteriormente, podem ser utilizadas para comprar em *sites* de vendas ou qualquer outra utilidade que seja necessário o cartão de crédito.

Outro método muito utilizado pelos Carders, que em sua maioria, também são *webdesigners* e *webmasters*, é a aplicação do golpe denominado *phishing scam*, que se caracteriza pela criação ou clonagem de *sites* falsos, para "pescar" as senhas dos usuários que, ingenuamente, acreditam em tais *sites* e realizam operações neles.

Normalmente, quando um Cracker possui as informações da conta bancária de algum usuário ou ele usa para si mesmo, para um bem próprio; ou vende essas informações a preços muito altos, lucrando muito com esse tipo de crime virtual.

Ainda existe a ilusão de que uma transação feita pela *web* é totalmente segura. Porém, isto não passa de propaganda da empresa para vender mais. Claro, que a cada dia os *sites* evoluem suas formas de segurança e diminuem o risco de serem invadidos e o cliente ter sua conta prejudicada. Mas nada é garantido, nada é 100% seguro.

Existem até *sites* que explicam como *cardear* sem ser pego pela polícia, o que acaba por incentivar que algumas pessoas tenham a esperança de obter lucros pessoais em cima de outros usuários.

A grande maioria dos Carders concentram-se no *Irc* (sim, o *Irc* não acabou) para a troca de senhas e informações.

Aqui na Paraíba, em fevereiro de 2006, foi muito divulgada a prisão de uma quadrilha de adolescentes, em sua maioria, especializada em desviar dinheiro de contas bancárias por meio de transferências fraudulentas e pagamentos realizados através da internet. Estima-se que os Crackers foram responsáveis pela movimentação de mais de 10 milhões de reais.

k) Warez:

Os Warez são os conhecidos "Piratas" da Internet. De acordo com o Dicionário Priberam da Língua Portuguesa, "Piratear" significa "reproduzir ilegalmente conteúdos protegidos por direitos autorais". Já o Aurélio denomina de "Pirata", a "pessoa que enriquece a custa de outrem". Em síntese, pode-se definir esse grupo *hacking* como: indivíduos que se utilizam do comércio ilegal de produtos com direitos autorais, para hospedá-los na internet visando compartilhá-los entre os usuários. É importante não confundir Warez com a pirataria normal que estamos acostumados a observar nas ruas.

As modalidades mais comuns de pirataria, atualmente, são de filmes em DVD e CDs musicais. Porém, sempre existiu, ainda que em menor número de vendas no comércio ilegal, a pirataria entre *softwares* e *hardwares* também.

O boom da pirataria ocorreu no início dessa década com a popularização dos gravadores de CD. Inicialmente, pelo preço ser muito elevado, poucas pessoas tinham condições de adquirir um equipamento deste porte. Porém, muitos indivíduos pensaram na possibilidade de juntar um capital e investir no gravador a fim de comercializar CDs piratas.

Na época, a prática mais comum era a de se alugar um CD musical em lojas especializadas, ripar para o computador e depois copiar para um CD-R (*compact disc* virgem). Ou ainda, comprar um CD de algum *game*, já pirateado, e, a partir dele, produzir várias cópias e iniciar as vendas entre amigos e conhecidos. As pessoas perceberam que poderiam lucrar muito dinheiro com este "comércio" e pequenas "mini-empresas" ilegais foram criadas para copiar esses CDs, tanto musicais, quanto de jogos e programas, e começaram a produzir para vender em massa nos camelôs ou nos tradicionais "carrinhos de CD".

Aos poucos, os gravadores de CDs se tornaram acessíveis à população e iniciou-se a moda da venda de DVDs que, um dia, também já tiveram um valor alto e eram difíceis de ser adquiridos. Sendo assim, com a comercialização dos gravadores de DVDs, iniciou-se o boom da venda de filmes piratas.

Muitos problemas foram apresentados com relação a esta prática, já que muitos filmes não eram somente copiados e distribuídos ilegalmente; vários deles, mesmo antes de serem lançados nos cinemas, já tinham a sua cópia ilegal sendo vendida livremente nas ruas.

E esta é uma problemática que também envolve os *softwares*, visto que é muito raro encontrar alguém que compre os programas originais nas lojas (que quase nunca tem programas originais à venda, exatamente pela falta de demanda).

Agora, a nova tendência é que a venda de DVDs piratas comece a ter uma relativa queda. Com o aumento da velocidade da internet e das tecnologias que permitem a conexão de uma televisão de LCD a um *notebook* e diante da diminuição dos valores dos preços dos monitores LCD, muitos usuários preferem assistir aos filmes nos próprios computadores, pela praticidade e economia tanto financeira, quanto de tempo.

E isto só é possível graças aos Warez, que disponibilizam esses filmes e programas, além de jogos e todos os outros tipos de materiais na grande rede.

Um pequeno resumo de como acontece a distribuição dos Warez pode ser descrito logo abaixo.

Um grupo de piratas adquire, através de algum contato interno, na produtora, uma cópia do material a ser distribuído, antes do lançamento do mesmo, seja ele filme, CD musical, *software* ou qualquer outro.

Outras formas de se conseguir o produto pode ser através do roubo de uma cópia do CD (o que facilita a divulgação do produto antes mesmo do seu lançamento oficial) ou

comprando normalmente uma cópia original autorizada, para posteriormente, reproduzir, sem nenhum empecilho.

A partir daí, se o produto adquirido for o original, esses Crackers recompilam o material a fim de infringir as licenças de uso e sistemas de proteção contra cópias não autorizadas, abrindo espaço para que eles possam distribuir o programa tanto fisicamente quanto virtualmente.

Se o material obtido já for o pirata, não precisam ter nem esse trabalho, porque o conteúdo já está pronto pra ser entregue em mãos ou enviado para *sites* de programas *warez*, que os hospedam em servidores privados, facilitando a distribuição entre os usuários.

Após serem hospedados, o "serviço" está praticamente terminado. Depois que os outros usuários iniciam os *downloads* do material, ele se multiplica e se espalha muito velozmente, seja através de *blogs*, das comunidades virtuais, fóruns ou outros meios de compartilhamento de arquivos.

Apesar de alguns não os classificarem como piratas, pois o Warez seria um método de compartilhamento de arquivos sem fins lucrativos - ao contrário da "pirataria de rua", onde os produtos são vendidos em troca de valores financeiros - os grupos *warez*, embora atuem com maior ênfase na própria internet - com a hospedagem de arquivos -, também contribuem para a prática da "pirataria de rua". A seguir serão apresentados os tipos mais conhecidos de Warez.

a) *Keygen*: Um *software* capaz de gerar números seriais para destravar programas ou jogos.

b) Serial: É uma combinação advinda do *Keygen*, de letras e/ou números que servem para destravar *softwares*.

c) *Patch*: É um programa que contém uma cópia já modificada dentro dele e substitui o arquivo original pelo alterado.

d) *Crack*: Uma versão alterada do programa original, que roda uma cópia como se fosse completa.

É através desses programas, que o Warez, ou, a "pirataria virtual", pode ser difundido. Jogos, Filmes, Séries de Televisão, *Mp3*, *E-Books* e *Softwares* só puderam chegar sem custo nenhum aos nossos computadores através destes programas. E, consequentemente, eles só puderam ser desenvolvidos graças ao intermédio dos Hackers e Crackers. Sem eles, talvez nunca tivéssemos acesso a todo esse conteúdo.

3.3.1 Kevin Mitnick

Kevin David Mitnick foi um Cracker americano mundialmente conhecido na década de 90. É considerado pelos próprios Estados Unidos como o maior Cracker da sua história.

Ele começou suas ações ainda na década de 70, no início da sua adolescência, alterando notas na sua escola e trapaceando o sistema de cartões de passagens de ônibus, conseguindo viajar de graça pra diversos lugares.

Legalmente falando, Kevin Mitnick teve seu primeiro grande problema quando, aos 17 anos, invadiu o sistema de informática da Defesa Aérea Norte Americana do Colorado, porém, devido a sua pouca idade, não pôde ser condenado.

Depois, Mitnick entrou no mundo dos Pheakers, desorganizando e alterando os sistemas telefônicos. Na época, conseguiu invadir ainda as instalações da *Pacific Bell* em busca de manuais técnicos.

Em seguida, o Cracker adentrou no, na época, recém mundo da informática e aprimorou suas técnicas para poder continuar a realizar seus crimes. Com o passar dos anos, ele iniciou uma série de viagens pelos Estados Unidos, buscando novas máquinas e sistemas que pudessem ser invadidos, instigando sua "fome" de conhecimentos e desenvolvimento de suas habilidades, tirando a paciência do governo nacional.

Nessa época, continuou a invadir vários computadores de grandes empresas, redes e ainda alterou a segurança dos sistemas de departamentos essenciais do governo dos Estados Unidos. Essa insistência fez com que o mesmo fosse, finalmente, preso aos 32 anos de idade e teve em sua pena a condenação de um ano de prisão por invasão de sistema e furto de *software* da DEC (*Digital Equipment Corporation*), que foi a companhia americana pioneira na indústria de computadores.

Após cumprir a setença, Mitnick resolveu viajar para Israel para encontrar-se com amigos Crackers, violando sua condicional e, sabendo que a polícia iria procurá-lo, pois continuava a invadir sistemas, resolveu desaparecer utilizando identidades falsas, se passando por outro indivíduo.

Sendo assim, por ser um fugitivo, continuar praticando seus delitos e nunca ser pego, o Cracker começou a ser considerado como um indivíduo perigoso e sua fama percorreu o mundo. Nos tempos de hoje, seria uma espécie de Osama Bin Laden da informática.

Mitnick cometeu seu primeiro grande erro em 1995. Na época Tsutomu Shimomura era um famoso especialista em segurança do Centro Nacional de Supercomputacão em San Diego, na Califórnia. Enquanto estava de férias, seu computador pessoal foi invadido por Mitnick. Indignado, com a credibilidade em baixa por ser quem era e ter o próprio computador invadido, Shimomura não poupou esforços para capturar o invasor.

Após algumas armadilhas envolvendo rastreamento de ligações, com a ajuda do FBI e da *National Security Agency*, finalmente Kevin foi pego e foi condenado a passar cinco anos na prisão. Foi libertado em 2000 condicionado a distanciar-se de qualquer tipo de computador, celular ou telefones portáteis durante três anos.

Depois de algum tempo, o Cracker decidiu encerrar sua carreira criminosa e resolveu trocar a vida ilícita que levava para utilizar seus conhecimentos e habilidades de forma positiva. Abriu uma empresa de proteção a informações pessoais, ministrando palestras sobre o tema, inclusive visitou o Brasil numa dessas palestras em 2006. Além disso, escreve livros e artigos sobre segurança de informações na rede e trabalha como consultor de segurança de sistemas.

Apesar de ter sido um criminoso, Mitnick afirma que distorceram muito do que realmente acontecia. Tudo, para que ele fosse pego o mais rápido possível. Segundo o mesmo, o tratavam como terrorista e retiraram vários de seus direitos legais. No relato abaixo, feito pelo próprio ex-Cracker, retirado do "Kevin Mitnick's Story" de Thomas C. Green, publicado em 2003, ele conta um pouco como foi a repercussão e o que ele sofreu na época em que ele se tornou uma pessoa conhecida mundialmente.

"Alguns Hackers destroem arquivos das pessoas ou discos rígidos inteiros - são chamados de Crackers ou vândalos. Alguns Hackers iniciantes não se preocupam em aprender a

tecnologia, simplesmente baixam ferramentas hacker para invadir sistemas de computadores - são chamados de Script Kiddies. Hackers mais experientes com conhecimento de programação criam programas hacker e os colocam na web e em bulletin boards. E depois há os indivíduos que não têm nenhum interesse na tecnologia, mas que usam o computador apenas como uma ferramenta para roubar dinheiro, bens ou serviços. Apesar do mito Kevin Mitnick criado pela mídia, não sou um Hacker mal-intencionado. O que eu fiz não era ilegal quando comecei, mas se tornou um crime depois que uma nova legislação foi criada. Eu continuei assim mesmo e fui flagrado.O tratamento que recebi do governo federal não foi devido aos crimes, mas para me transformar num exemplo. Eu não merecia ser tratado como um terrorista ou como um criminoso violento: minha casa foi vasculhada sem um mandado de busca; fui colocado na solitária durante meses; meus direitos constitucionais fundamentais, garantidos para qualquer acusado de crime, foram negados; minha fiança foi negada, assim como uma audiência de fiança; e fui forçado a gastar vários anos lutando para obter do governo as evidências para que meu advogado indicado pela Justiça pudesse preparar minha defesa.E sobre meu direito a um julgamento rápido? Durante anos, a cada seis meses me forçavam a escolher: assinar um documento abrindo mão dos meus direitos constitucionais de ter um julgamento rápido ou ir a um julgamento onde seria defendido por um advogado despreparado. Resolvi assinar."

4 Hacker: uma ética virtual

Ética Hacker é uma nova ética iniciada a partir de comunidades virtuais e através dos próprios Hackers e estudiosos do tema. Um dos seus grandes criadores foi o finlandês Pekka Himanen, que é um filósofo conhecido por sua obra *The Hacker Ethic and de Spirit of the Information* (2001).

A ética é essencial em qualquer que seja a atividade humana. De acordo com o sociólogo e professor Sérgio Amadeu (2009: *online*):

> Os grupos sociais acabam construindo finalidades para sua existência e para as suas ações. Estar de acordo com esses objetivos finais é atuar com ética. A cultura hacker é essencialmente baseada em atitudes éticas e no tripé: liberdade, colaboração e conhecimento.

De acordo com a Ética Hacker, as informações são essenciais para a sociedade trazendo-lhes benefícios em todos os quesitos. Sendo assim, é necessário que as informações sejam compartilhadas. É a partir desta idéia, que os Hackers trocam experiências e desenvolvem o *software* livre, que facilita o acesso às informações para todos.

A frase que diz "Toda informação deve ser livre" é seguida com muita veemência por eles. O acesso a computadores - e qualquer outro meio que seja capaz de ensinar algo sobre como o mundo funciona - deve ser ilimitado e total.

Esses ideais advêm do pensamento de Buckminster Fuller, grande visionário, designer, arquiteto, inventor e escritor estadunidense, que afirmava que "A verdadeira riqueza é a informação, se o indivíduo souber como aproveitá-la".

Acreditam que invadir sistemas por pura diversão e exploração, sem fins prejudiciais como roubos ou destruição de dados, mesmo com as quebras de confidencialidade, pode ser aceitável. Porém, esta idéia não é aderida por todos. Como já vimos, alguns especialistas acreditam que só o fato de se invadir, tira a privacidade do usuário, tornando-se uma ação antiética.

Na sociedade de consumo atual, quase tudo é modificado e transforma-se em mercadoria, tendo o poder de ser vendido. E a informação é incluída como produto também. Porém, os Hackers afirmam que a informação não existe enquanto mercadoria física. Ela só existe nas mentes das pessoas e, sendo assim, por não ter o poder de possuir a mente de outro indivíduo, não faz sentido ter o direito de comercializar essas informações.

O Hacker deve ser aquele que trabalha com grande paixão e entusiasmo pelo que faz. Destarte, ele procura por novas informações diariamente e acreditando que todos devem ter acesso a essa informação, sente prazer em transmiti-la para qualquer um que deseje "pensar" e "criar" novas coisas.

Outra característica da Ética Hacker é o fato deles não aceitarem o poder "ilimitado" das autoridades, especialmente com relação à censura. Também não acreditam que a centralização seja a melhor maneira de organizar a sociedade, pois assim a informação ficaria retida a uma pequena parcela da sociedade.

Para os Hackers, o que prevalece como base é a idéia da meritocracia. De acordo com o Aurélio, meritocracia significa "s.f. Sistema (p. ex., educacional ou administrativo) em que

os mais dotados ou aptos são escolhidos e promovidos conforme seus progressos e consecuções; sistema onde o mérito pessoal determina a hierarquia."

E é assim que eles acham que devem ser julgados; de acordo com o seu *hacking*. "Faça o que você sabe que o respeito virá como conseqüência". Não é necessário diplomas ou certificados para provar o que você conhece. Critérios como graus acadêmicos, raça, cor, religião ou posição social não dizem nada no mundo Hacker.

Segundo os Hackers, através do computador, também pode se criar arte e beleza. Uma programação bem feita seria uma arte única, que detém a assinatura e o estilo do Hacker.

Os Hackers também tem um código de ética de acordo com as invasões realizadas em um *site*. Existe uma postura moral ao serem realizados estes tipos de ações. As atitudes de um Hacker são bem diferentes daquelas desenvolvidas por um Script kiddie, um Lammer ou qualquer outro tipo de Cracker.

Existe um respeito pelos computadores invadidos. Abaixo serão listadas algumas das regras do código de ética dos Hackers:

- Nunca delete propositalmente ou danifique qualquer que seja o arquivo em um computador que você tenha invadido.
- Trate os sistemas que você invade como você trataria seu próprio computador.
- Notifique os administradores de sistemas sobre qualquer brecha de segurança que você possa vir a encontrar.
- Não invada para roubar ou desviar dinheiro.
- Não invada para roubar informações, especialmente se elas forem sigilosas.
- Não distribua ou colecione *software* pirateado.
- Nunca corra riscos estúpidos. É importante ter consciência de sua habilidade.
- Sempre esteja disposto a compartilhar e repassar seu conhecimento e os métodos que utiliza no mundo *hacking*.
- Respeite quem está aprendendo. Humildade é um ponto fundamental, até porque você também já foi iniciante.

5 Ações e motivações dos Hackers

Há vários anos tem-se escutado falar sobre jovens "viciados" em computação que viram a noite em busca de invadir sistemas computacionais. E não é de hoje também que a lei atua contra esses invasores. Os primeiros casos de *hacking* que resultaram em processos penais remetem à década de 80.

O primeiro caso aconteceu em 1983 e envolveu um grupo de adolescentes, entre 15 e 17 anos, que invadiram o banco de dados da Ciments Lafarge, localizada no Canadá. No mesmo ano, em solo americano, nos Estados Unidos, a banda dos 414, grupo formado por diversos estudantes de Milwauke, estavam sendo procurados pela polícia. Um dos adolescentes, com 17 anos, chegou a afirmar que o que mais surpreendeu o grupo foi a facilidade encontrada para realizar a invasão na maioria dos bancos de dados. Segundo ele, as senhas utilizadas eram simplesmente palavras como "teste", "demo" ou "sistema".

A partir daí vários casos foram sendo encontrados ao redor do planeta. Em 1988, um belga conseguiu ter acesso a caixa postal de todos os ministros do país através da invasão na rede telemática Bistel. Já no Reino Unido, um outro pirata penetrou no sistema Prestel, que era também uma espécie de sistema telemático.

A maioria dos piratas virtuais que são pegos, normalmente não são realmente os Crackers perigosos. Os que ganham a mídia são os que não possuem o conhecimento necessário para que consigam se manter ocultos. Talvez até por inexperiência, por onde passam deixam marcas de sua "visita", dando motivos para serem capturados posteriormente.

Os Crackers perigosos, que nem sempre estão nesse mundo pra brincadeira, especialmente os Black Hats, aí sim são difíceis de se capturar. Eles são profissionais e tem o conhecimento necessário para permanecerem desconhecidos.

Independentemente do tipo de Hacker ou Cracker que existam, as motivações que os levam a cometer suas invasões e seus crimes são as mais variadas possíveis. Isso varia com a idade, conhecimento, situação ocorrida, educação, classe social, entre outros milhões de fatores. Porém, existem alguns grandes grupos em que provavelmente a maioria destes indivíduos se encaixa.

a) Espionagem Industrial:

Ocorre quando uma empresa contrata um Cracker para que este invada o sistema de sua concorrente, a fim de furtar informações como planos de investimentos, políticas de parcerias ou até mesmo com a intenção de furtar programas essenciais pro funcionamento da concorrência.

b) Proveito Próprio:

Piratas virtuais podem penetrar em sistemas com o intuito de roubar dinheiro, transferir bens, cancelar dívidas ou até burlarem concursos.

c) Vingança:

Ex-Funcionários ou pesquisadores que tenham seus contratos cancelados e que possuem conhecimentos acerca dos sistemas de segurança da empresa podem provocar alguns danos. Sendo assim, o chefe de segurança deve proibir todo e qualquer tipo de acesso a empregados que deixem de atuar junto à empresa.

d) Status ou Necessidade de Aceitação:

A competitividade e a vontade de se mostrar superior não é nenhuma novidade entre os seres humanos. O mundo *hacking* também não foge à regra. Então, com essas intenções muitos indivíduos buscam superar seus limites penetrando em *sites* considerados difíceis de se invadir com o intuito de obter status e aceitação diante de determinados grupos.

f) Curiosidade e Aprendizado:

Invasões relacionadas a este tipo de motivação são as menos criticadas pelos especialistas na área. Penetrar em um sistema para estudar seu funcionamento, testar o esquema de segurança e procurar por falhas, com a intenção de aprender sobre elas, ainda é

aceitável por parte das pessoas. Ainda existem aqueles que invadem para denunciar o erro aos chefes de segurança do *site*, como fazem os White Hats.

g) Busca de Aventuras:

O perigo é motivador de diversos Crackers. O fato de saber que algo é proibido, já os fascina e, quando esse desafio é difícil, aí é que mexe com a mente do invasor. Sistemas de segurança muito avançados os motivam a superar seus conhecimentos em busca daquele objetivo.

h) Maldade:

Esse talvez seja a pior motivação que se existe. Simplesmente pelo desejo de ver outras pessoas serem destruídas, Crackers invadem e destroem tudo do seu "inimigo".

Sendo assim, é muito importante manter seu sistema sempre protegido e atualizado. Os Crackers atuam por todos os lados, em diversas categorias, por diversas maneiras e motivações. Infelizmente, os sistemas de segurança ainda são bem falhos; tanto, que existem Crackers não muito experientes que podem causar danos em diversas máquinas. No próximo tópico serão abordadas dicas de segurança na internet para que o uso do computador não seja mais "um problema do que uma solução".

6 Segurança na internet: o que dizem os manuais sobre proteção na internet

Iniciar a "viagem" e navegar através da internet pode ser perigoso, como temos compreendido. Sendo assim, é importante que o usuário perceba que a maioria dos problemas envolvendo segurança na internet pode ser evitado através de algumas medidas preventivas básicas. As dicas que virão em seguida não livrarão o internauta completamente de todos os problemas, mas servirão para dificultar que grande parte deles apareça.

O texto abaixo foi retirado do *site* InfoWester. Na seção "Dicas" existe um *link* chamado "Dicas de Segurança na Internet", o qual é exposto na íntegra logo abaixo:

Quando você sai de casa, certamente toma alguns cuidados para se proteger de assaltos e outros perigos existentes nas ruas. Na internet, é igualmente importante pôr em prática alguns procedimentos de segurança, já que golpes, espionagem e roubo de arquivos e senhas são apenas alguns dos problemas que as pessoas podem ter na web. É para ajudá-lo a lidar com isso que o InfoWester apresenta a seguir, quinze dicas importantes para você manter sua segurança na internet e em seu computador:

1) Saia usando *Logout*, Sair ou equivalente

Ao acessar seu *webmail*, sua conta em um *site* de comércio eletrônico, sua página no *Orkut*, seu *home banking* ou qualquer outro serviço que exige que você forneça um nome de usuário e uma senha, clique em um botão/*link* de nome *Logout*, *Logoff*, Sair, Desconectar ou equivalente para sair do *site*. Pode parecer óbvio, mas muita gente simplesmente sai do *site* fechando a janela do navegador de internet ou entrando em outro endereço. Isso é arriscado, pois o *site* não recebeu a instrução de encerrar seu acesso naquele momento e alguém mal-intencionado pode abrir o navegador de internet e acessar as informações de sua conta, caso esta realmente não tenha sido fechada devidamente.

2) Crie senhas difíceis de serem descobertas

Não utilize senhas fáceis de serem descobertas, como nome de parentes, data de aniversário, placa do carro, etc. Dê preferência a seqüências que misturam letras e números. Além disso, não use como senha uma combinação que tenha menos que 6 caracteres. O mais importante: não guarde suas senhas em arquivos do *Word* ou de qualquer outro programa. Se necessitar guardar uma senha em papel (em casos extremos), destrua-o assim que decorar a seqüência. Além disso, evite usar a mesma senha para vários serviços.

3) Mude a sua senha periodicamente

Além de criar senhas difíceis de serem descobertas, é essencial mudá-las periodicamente, a cada três meses, pelo menos. Isso porque, se alguém conseguir descobrir a

senha do seu *e-mail*, por exemplo, poderá acessar as suas mensagens sem que você saiba, apenas para espioná-lo. Ao alterar sua senha, o tal espião não vai mais conseguir acessar as suas informações.

4) Use navegadores diferentes

Se você é usuário do sistema operacional *Windows*, talvez tenha o hábito de utilizar apenas o navegador *Internet Explorer*. O problema é que existe uma infinidade de pragas digitais (*spywares*, vírus, etc) que exploram falhas desse navegador. Por isso, uma dica importante é usar também navegadores de outras empresas, como o *Opera* e o *Firefox*, pois embora estes também possam ser explorados por pragas, isso ocorre com uma freqüência menor neles. Se ainda assim preferir utilizar o *Internet Explorer*, use um navegador alternativo nos *sites* que você considerar suspeitos (páginas que abrem muitas janelas, por exemplo).

5) Cuidado com *downloads*

Se você usa programas de compartilhamento de arquivos, como *eMule*, ou costuma obter arquivos de *sites* especializados em *downloads*, fique atento ao que baixar. Ao término do *download*, verifique se o arquivo não possui alguma coisa estranha, por exemplo, mais de uma extensão (como *cazuza.mp3.exe*), tamanho muito pequeno ou informações de descrição suspeitas, pois muitos vírus e outras pragas se passam por arquivos de áudio, vídeo e outros para enganar o usuário. Além disso, sempre examine o arquivo baixado com um antivírus. Também tome cuidado com *sites* que pedem para você instalar programas para continuar a navegar ou para usufruir de algum serviço. Ainda, desconfie de ofertas de programas milagrosos, capazes de dobrar a velocidade de seu computador ou de melhorar sua performance, por exemplo.

6) Atente-se ao usar *Windows Live Messenger*, *Google Talk*, *Yahoo Messenger*, entre outros.

É comum encontrar vírus que exploram serviços de mensagens instantâneas, tais como o *Windows Live Messenger* (antigo *MSN Messenger*), *AOL Instant Messenger* (AIM), *Yahoo! Messenger*, entre outros. Essas pragas são capazes de, durante uma conversa com um contato, emitir mensagens automáticas que contém links para vírus ou outros programas maliciosos. Nessa situação, é natural que a parte que recebeu a mensagem pense que seu contato é que a enviou e clica no *link* com a maior boa vontade:

Mesmo durante uma conversa, se receber um *link* que não estava esperando, pergunte ao contato se, de fato, ele o enviou. Se ele negar, não clique no *link* e avise-o de que seu computador pode estar com um vírus.

7) Cuidado com *e-mails* falsos

Recebeu um e-mail dizendo que você tem uma dívida com uma empresa de telefonia ou afirmando que um de seus documentos está ilegal, como mostra a imagem abaixo?

Ou, ainda, a mensagem te oferece prêmios ou cartões virtuais de amor? Te intima para uma audiência judicial? Contém uma suposta notícia importante sobre uma personalidade famosa? É provável que se trate de um *phishing scam*, ou seja, um *e-mail* falso. Se a mensagem tiver textos com erros ortográficos e gramaticais, fizer ofertas tentadoras ou tem um *link* diferente do indicado (para verificar o *link* verdadeiro, basta passar o mouse por cima dele, mas sem clicar), desconfie imediatamente. Na dúvida, entre em contato com a empresa cujo nome foi envolvido no *e-mail*.

8) Evite *sites* de conteúdo duvidoso

Muitos *sites* contêm em suas páginas *scripts* capazes de explorar falhas do navegador de internet, principalmente do *Internet Explorer*. Por isso, evite navegar em *sites* pornográficos, de conteúdo hacker ou que tenham qualquer conteúdo duvidoso.

9) Cuidado com anexos de *e-mail*

Essa é uma das instruções mais antigas, mesmo assim, o *e-mail* ainda é uma das principais formas de disseminação de vírus. Tome cuidado ao receber mensagens que te

pedem para abrir o arquivo anexo, principalmente se o *e-mail* veio de alguém que você não conhece. Para aumentar sua segurança, você pode checar o arquivo anexo com um antivírus, mesmo quando estiver esperando recebê-lo.

10) Atualize seu antivírus e seu *antispyware*

Muita gente pensa que basta instalar um antivírus para o seu computador estar protegido, mas não é bem assim. É necessário atualizá-lo regularmente, do contrário, o antivírus não saberá da existência de vírus novos. Praticamente todos os antivírus disponíveis permitem configurar uma atualização automática. Além disso, use um *antispyware* com freqüência para tirar arquivos e programas maliciosos de seu computador. Uma boa opção é o *Spybot*. Assim como o antivírus, o *antispyware* também deve ser atualizado para que este conheça pragas novas.

11) Cuidado ao fazer compras na internet ou usar *sites* de bancos

Fazer compras pela internet é uma grande comodidade, mas só o faça em *sites* de venda reconhecidos. Caso esteja interessado em um produto vendido em um *site* desconhecido, faça uma pesquisa na internet para descobrir se existe reclamações contra a empresa. Ao acessar sua conta bancária através da internet, também tenha cuidado. Evite fazer isso em computadores públicos, verifique sempre se o endereço do *link* é mesmo o do serviço bancário e siga todas as normas de segurança recomendadas pelo banco.

12) Atualize seu sistema operacional

O *Windows* é o sistema operacional mais usado no mundo e quando uma falha de segurança é descoberta nele, uma série de pragas digitais são desenvolvidas para explorá-la. Por isso, vá em Iniciar / *Windows Update* e siga as orientações no *site* que abrir para atualizar seu sistema operacional. Fazer isso uma vez ao mês é suficiente para manter seu sistema operacional atualizado. Se for usuário de outro sistema operacional, como o *Mac OS* ou alguma distribuição *Linux*, saiba que essa dica também é válida. Falhas de segurança existem

em qualquer sistema operacional, por isso, é importante aplicar as atualizações disponibilizadas pelo desenvolvedor.

13) Atualize também os seus programas

Também é importante manter seus programas atualizados. Muita gente pensa que as versões novas apenas adicionam recursos, mas a verdade é que elas contam também com correções para falhas de segurança. Por isso, sempre utilize a última versão dos seus programas, especialmente os que acessam a internet (navegadores de internet, clientes de *e-mail*, etc). Muitos aplicativos contam com uma funcionalidade que atualiza o programa automaticamente ou avisa do lançamento de novas versões. É um bom hábito deixar esse recurso ativado.

14) Não revele informações importantes sobre você

Em serviços de bate-papo (*chat*), no Orkut, em *fotologs* ou em qualquer serviço onde um desconhecido pode acessar suas informações, evite dar detalhes da escola ou da faculdade que você estuda, do lugar onde você trabalha e principalmente de onde você mora. Evite também disponibilizar dados ou fotos que forneçam qualquer detalhe relevante sobre você, por exemplo, fotos em que aparecem a fachada da sua casa ou a placa do seu carro. Nunca divulgue seu número de telefone por esses meios, tampouco informe o local em que você

estará nas próximas horas ou um lugar que você freqüenta regularmente. Caso esses dados sejam direcionados aos seus amigos, avise-os de maneira particular, pois toda e qualquer informação relevante sobre você pode ser usada indevidamente por pessoas má-intencionadas, inclusive para te localizarem.

15) Cuidado ao fazer cadastros

Muitos *sites* exigem que você faça cadastro para usufruir de seus serviços, mas isso pode ser uma cilada. Por exemplo, se um *site* pede o número do seu cartão de crédito sem ao menos ser uma página de vendas, as chances de ser um golpe são grandes. Além disso, suas informações podem ser entregues a empresas que vendem assinaturas de revistas ou produtos por telefone. Ainda, seu e-mail pode ser inserido em listas de spams. Por isso, antes de se cadastrar em *sites*, faça uma pesquisa na internet para verificar se aquele endereço tem registro de alguma atividade ilegal. Avalie também se você tem mesmo necessidade de usar os serviços oferecidos pelo *site*.

Existem diversos manuais espalhados em sites e cartilhas com dicas e "mandamentos" para utilização da internet de forma segura. Este é apenas um deles, que por ser mais completo, foi descrito no trabalho monográfico.

O conhecimento é uma boa maneira de se evitar danos pessoais ao se utilizar a grande rede, porém, o nível que os Crackers estão, em determinados casos, é muito elevado e não há como impedir suas ações. Isto pode até gerar um certo receio do computador, pois utilizá-lo sabendo que a qualquer momento pode-se ser atacado realmente é decepcionante. Sendo assim, é importante que o usuário se informe cada vez mais e fique atento a qualquer reação estranha que o computador possa vir a ter. Talvez, só assim, será possível conectar-se com a certeza de se estar preparado para qualquer invasão.

Considerações Finais

Após todo este apanhado acerca da Cibercultura, das novas tecnologias e da explicação das diferenças existentes no mundo Hacker, pôde-se observar que a internet ainda tem muito a evoluir e acrescentar na vida das pessoas.

Desde a década de 50 que as tecnologias têm sido desenvolvidas com muita rapidez. É até possível arriscar algumas previsões do que virá no futuro com relação ao mundo virtual. Porém, é um exercício difícil de se realizar, diante de tantas novidades que nos são apresentadas diariamente e das possibilidades que podem ser empreendidas na área.

Vale salientar que o Brasil não é um país de primeiro mundo e tudo que nos é trazido, já chega com atraso em relação aos países desenvolvidos. Existem muitas tecnologias que, mesmo com a globalização crescente da informação, ainda é desconhecido por grande parte dos brasileiros.

A exclusão digital é uma realidade social e conseguir reverter essa situação não é algo que é realizado do dia para a noite. As políticas públicas de investimento na educação computacional sempre foram fracas e continuam a ser. Bem que se tenta criar postos de informática em comunidades humildes, onde o acesso ao computador e a internet é reduzido, mas mais complexo ainda é tentar fazer com que essas pessoas consigam acompanhar o desenvolvimento tecnológico diariamente.

Assim, ter conhecimento dos Hackers e Crackers se torna ainda mais difícil. A generalização do termo, como foi apresentada neste trabalho, é muito ampla ainda. Não se tem a devida noção do perigo que estes elementos representam pra sociedade. Eles são invasores, alguns menos perigosos, porém em algumas categorias de Crackers, estes indivíduos podem fazer estragos irreparáveis.

Existe o lado positivo deste processo. O desenvolvimento das indústrias de segurança tem evoluído bastante. O conhecimento que os White Hats oferecem na construção dos sistemas computacionais são primordiais, mas existem os vilões. Os Crackers necessitariam talvez de uma fiscalização maior por parte do governo, com uma pena mais rígida com relação a esse tipo de atitude. A população precisa saber quem são esses sujeitos, precisa conhecer suas ações e ter noção do risco que correm ao ligarem os próprios computadores.

Talvez por essa falta de "cultura computacional" que o país é submetido é que exista tanta falta de informação com relação a termos e ações simples dentro informática. Muitas pessoas ainda não sabem ligar um computador sozinhas, não conhecem conceitos básicos de *hardware* e muito menos conseguem resolver problemas básicos no próprio PC, que nem sempre necessita da ajuda de um técnico.

Com uma sociedade assim, é até compreensível, de certa forma, a ignorância presente nos próprios meios de comunicação ao veicularem que qualquer indivíduo que possua o conhecimento mais evoluído na área da informática – não importando se suas ações são positivas ou atitudes menos nobres – seja caracterizado como um Hacker.

Apesar do conhecimento dos Crackers ser avançado também, se fossem estimulados o desenvolvimento de programas de educação que visassem a inclusão digital desde cedo das pessoas, diversos problemas relacionados aos crimes virtuais e problemas virtuais em geral, seriam diminuídos. Óbvio que anular estes problemas nunca vai ser 100% possível. Mas, muitas das situações em que os usuários são prejudicados podem ser evitadas com passos simples. O básico do ensino da informática já faria uma enorme diferença.

E isso vale para todas as classes sociais. Existem muitos cidadãos que são "incluídos digitalmente" mas que não faz nem idéia de como utilizar um computador para realizar determinadas tarefas simples, necessitando sempre do auxílio de outra pessoa.

Por isso que fica tão fácil, em determinados casos, para os Crackers agirem. Muitos percebem que não é preciso grande esforço para se conseguir prejudicar um internauta e obter o lucro desejado, seja ele financeiro ou de outra natureza. Como analisamos, suas motivações para agir no mundo virtual são diversas. E para impedir essas ações, a melhor solução é o conhecimento.

É fácil exemplificar a situação acima. Diversos usuários são infectados por, ingenuamente, abrirem *e-mails* de desconhecidos, ou até de conhecidos, com extensões estranhas. Um caso deste é muito simples de se resolver. Basta que esse indivíduo aprenda um pouco sobre o funcionamento dos vírus e da ação dos Crackers, possibilitando que, assim, ele possa se defender e não repetir este erro novamente.

As políticas públicas têm um papel fundamental, não só na "inclusão digital" da população, mas também na inclusão de conhecimentos sobre a área a todos, mesmo aqueles que já têm o acesso ao computador diariamente. A aplicação de cursos gratuitos ensinando

medidas preventivas ao se utilizar um PC e propagandas mais eficientes alertando a sociedade quanto a determinadas atitudes simples, como instalar um antivírus na máquina também já resolveria uma parte dos problemas.

Enfim, o que é preciso ser feito para que diminua o risco do usuário ter sua privacidade roubada, seus dados e bens financeiros furtados e conseguir ter uma vida tranquila ao se utilizar a internet é apenas produzir reflexões na população em seu próprio cotidiano sobre o mundo virtual, com diálogos abertos, diretos e objetivos, sem o mito de que mexer em computador é algo difícil e que só os jovens conseguem aprender. Todos podem ter acesso à internet com segurança e, assim, usufruir de tudo de positivo que este meio pode oferecer.

Referências

ANIVERSÁRIO da internet. **Geração Arroba**. Disponível em: http://www.pime.org.br/missaojovem/mjcomungeracao.htm. Acesso em 12 de junho de 2009

ANOS 90: o desenvolvimento da internet no Brasil. **Tecnologia do site Terra**. Disponível em: http://tecnologia.terra.com.br/internet10anos/interna/0,,OI541825-EI5026,00.html. Acesso em 15 de junho de 2009.

BAUDRILLARD, Jean. **Tela Total**. Porto Alegre: Ed. Sulina, 1997.

BRETON, Philippe. **História da Informática**. Editora da Unesp, 1991.

CASTELLS, Manuel. **A galáxia da Internet**. Jorge Zahar Editor, 2003

CRACKER e Hacker: experts trabalhando em sentidos opostos. **Sisnema Informática**, 2005. Disponível em: http://www.sisnema.com.br/Materias/idmat014717.htm. Acesso em 17 de junho de 2009

DINIZ, Laura. Mãos ao Alto!. In: **Revista Veja**. ed. 2113, 2009.

DOM, Rodnei. Hackers - Quem são eles?. **Sacrahome**, 2003. Disponível em: http://www.sacrahome.net/v2/node/120. Acesso em: 12 de julho de 2009.

GIL, Antônio Carlos. **Como laborar Projetos de Pesquisa**. 4. ed. São Paulo: Atlas, 2002.

HACKERS e Crackers famosos. **Hackerteen**. Disponível em: http://www.hackerteen.com/pt-br/enjoy-it/hackers-crackers-famosos.html. Acesso em 18 de junho de 2009.

HACKERS: entre a ideologia libertária e o crime. **Comciência**. Disponível em http://www.comciencia.br/reportagens/internet/net10.htm. Acesso em 16 de junho de 2009.

HIMANEM, Pekka. **A ética dos Hackers e o espírito da era da Informação**. ed. Campus. 2001.

HISTÓRIA dos Hackers. **Fórum HardMOB**, 2003. Disponível em: http://www.hardmob.com.br/archive/index.php/t-66873.html. Acesso em 16 de junho de 2009.

INTERNET: dependência versus utilidade. **Saúde do Homem**, 2009. Disponível em: http://www.clicrbs.com.br/blog/jsp/default.jsp?source=DYNAMIC,blog.BlogDataServer,getBlog&uf=1&local=1&template=3948.dwt&section=Blogs&post=137011&blog=591&coldir=1&topo=4254.dwt&espname=vidafeminina. Acesso em 14 de junho de 2009.

INVASORES e atacantes. **Fórum Oficial do Priston Tale Brasil**, 2009. Disponível em: http://forum.priston.com.br/archive/index.php/thread-57.html. Acesso em 03 de julho de 2009.

JOHN Draper, o rei. **Theusinho blog**, 2008. Disponível em http://theusinhorei.blogspot.com/2008/03/john-draper-o-rei.html. Acesso em 21 de junho de 2009.

LEÃO, Lúcia. **O labirinto da hipermídia: arquitetura e navegação no ciberespaço**. 2.ed. São Paulo: Iluminuras, 2001.

LEMOS, André. **Cibercultura: tecnologia e vida social na vida contemporânea**. Editoria Sulina.2007

LEMOS, André. **Cultura das Redes**. Salvador: EDUFBA, 2002.

LÉVY, Pierre. **Cibercultura**. Editora 34. 2000

LÉVY, Pierre. **A Inteligência Coletiva**. São Paulo: Editora 34, 2000.

LÉVY, Pierre. **O que é o Virtual?** São Paulo: Editora 34, 1996.

MATTAR, Fause N. **Pesquisa de Marketing**. 3 ed. São Paulo: Atlas, 2001.

MEIOS digitais são os mais consultados em todo o mundo. **Tecnologia do site Terra**, 2006. Disponível em: http://tecnologia.terra.com.br/interna/0,,OI1280639-EI4802,00.html. Acesso em 12 de junho de 2009

O QUE É ser um hacker?. **Roy1**. Disponível em: http://www.roy1.hpg.com.br/Entretenimento/7/interna_hpg1.html. Acesso em 16 de junho de 2009.

O QUE SÃO: Hacker, Cracker, Lammer, Newbie, Carder, Talvez vocês parem de achar que tem hackers no servidor. **TrakinasRO**, 2009. Disponível em: http://www.trakinasro.com/forum/index.php?showtopic=140. Acesso em: 15 de julho de 2009.

PONTE, Gabriella. O que a ética hacker tem a ver com a inclusão digital na sociedade?. **Sete Pontos**. Disponível em: http://www.comunicacao.pro.br/setepontos/7/etihack.htm. Acesso em: 02 de julho de 2009.

ROCHA, marcos. Benefícios da Internet. **Focus Consultoria**, 2009. Disponível em: http://www.focusconsultoria.com.br/blog/artigos/beneficios-da-internet. Acesso em 15 de junho de 2009.

RAYMOND, Eric Steven. Como se tornar um Hacker. **Hacker Friend**. Disponível em: http://www.rackerfriend.hpg.ig.com.br/comtorhacker.htm. Acesso em: 23 de julho de 2009.

RYDLEWSKI, Carlos. Computação sem Fronteiras. In: **Revista Veja**. ed. 2126, 2009.

SILVA, Antônio. Newbie não precisa ser burro. **Numclique**. Disponível em: http://www.numclique.net/newbie-nao-precisa-ser-burro/. Acesso em 04 de julho de 2009.

VASCONCELOS, Fernando Antonio de. **Internet: Responsabilidade do provedor pelos danos praticados**. Jaruá Editora (2003)

WOLTON, Dominique. **Internet, e depois?** Editora Sulina, 2007.

ZORDICK, Dreack. **Tipos de Hackers**. 2009. Disponível em: http://blog.clickgratis.com.br/dreackz/69747/Hackers+e+suas+Defini%E7%F5es.html. Acesso em 20 de junho de 2009.