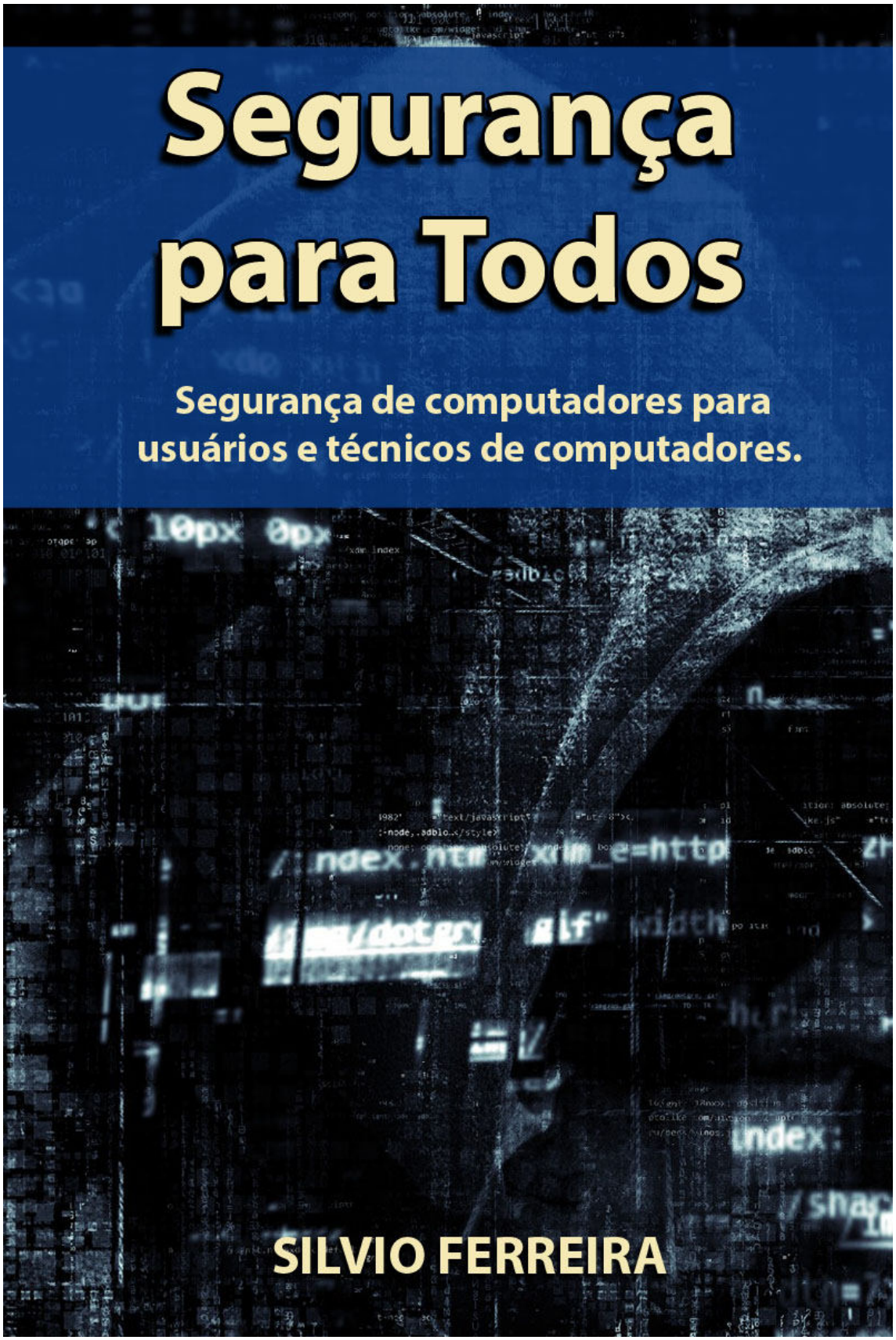

**Segurança para todos – Segurança de computadores para usuários e técnicos de computadores.**

Por Silvio Ferreira

# Capítulo 01 - Vírus

## Essencial saber

Um dos grandes problemas que todos os usuários de computadores enfrentam são os vírus de computadores. Eles contaminam milhões de computadores ao redor do mundo, apagam arquivos, causam problemas à sistemas operacionais, corrompem dados e provocam uma enorme quantidade de variados danos.

A cada dia que passa vários ou centenas de novos vírus surgem, se espalhando através de diversos meios e afetando uma grande quantidade de computadores, corrompendo ou apagando dados, alterando informações e por aí vai.

E por trás dos vírus há os seus criadores, *hackers* ou *crackers*, cada um com seu propósito, com seu objetivo. Nos noticiários da TV, na internet e nos jornais, sempre vemos e veremos notícias sobre invasões: web sites que foram invadidos, dados e informações que foram roubadas.

Por isso, todo usuário de computador, principalmente aqueles que usam a internet, deve ter conhecimentos mínimos de como evitar e eliminar vírus e como se proteger de invasões de computadores. É preciso ter conhecimentos mínimos de segurança de computadores locais e na internet.

Nos tempos atuais é exigido muito mais que um anti-vírus instalado. Devemos saber como evitar "contaminação" por vírus, evitar que eles venham a destruir informações de um computador, saber como eles surgem, como eles agem, como se multiplicam.

Em muitas empresas, a *base de dados* contidas em seus servidores é o motivo delas existirem, e se a base de dados é destruída, a empresa pode até não ser destruída, mas pode ter um prejuízo enorme.

Se você trabalha com suporte de computadores (montagem e manutenção) saiba que o fado do técnico dos novos tempos não é só montar computadores e/ou prestar suporte técnico. Mas, preservar para que os dados que lá estão tenham o máximo de segurança possível. Quando um usuário ou empresa contratar seus serviços para concertar um sistema que está muito lento, ele (o usuário ou a empresa) pode nem imaginar que a causa do problema são vírus. Mas, você deverá identificar e resolver o problema.

Se estivermos preparados saberemos eliminar os vírus sem problemas, saberemos que eles não são tão perigosos como muitos afirmam, como se eles fossem seres capazes de decidir por conta própria o que irão fazer com o computador infectado.

Não há mágica no que fazem, eles apenas se aproveitam de falhas na segurança do sistema operacional, falhas na segurança dos softwares usados no sistema e se aproveitam das piores falhas que existe: a humana.

Se um Disco Rígido é formato, não foi porque criaram um vírus com "poderes" "malignos", e sim que criaram um vírus capaz de enganar o homem, como os

famosos *trojans* que exibem uma charge enquanto prepara o sistema para ser formatado na próxima vez que iniciar.

Um vírus pode ser programado para agir de forma engenhosa, quase dotado de inteligência, porém, só irá infectar o computador da vítima se esta não estiver preparada.

Não somente os vírus são uma ameaça, mas também os criadores dos vírus, sejam eles hackers ou não.

Falar sobre hackers para muitos ainda é um tabu ou besteira, para outros, isso é pura indeliquência.

A grande verdade é que hacker é associado por muitos como aquele que invade computadores, que faz vírus entre outras coisas. Se isso é ser hacker, então estamos condenados, porque qualquer criança de 12 anos pode ir na banca mais próxima e comprar um livro contendo um CD demonstrando como fazer vírus, invadir computadores e trazem até todos os programas necessário e muita vezes códigos de vírus prontos.

É lógico que devemos nos prevenir (não posso entrar em qualquer site que encontrar e digitar o número do meu cartão de crédito), mas também não há motivos para pânico.

**O que são os Vírus?**

Vírus de computador são programas ou rotinas de programação dentro de outro programa, que ao infectar (se instalarem) um computador irá alterar o seu funcionamento normal.

Essa alteração pode ser de incontáveis formas (dependerá único e exclusivamente da imaginação de seu criador), como o computador ficar mais lento, travar, reiniciar do nada, imprimir caracteres que não foram digitados, abrir milhares de janelas de forma descontrolada tendo como única alternativa resetar o computador, apagar arquivos, exibir mensagens na tela (mensagens que podem ser engraçadas ou até mesmo grosseiras, racistas, etc), alterar o setor de boot, formatar o Disco Rígido, etc.


**Figura 01.1: vírus podem alterar o funcionamento normal do computador.**

Muitas vezes os vírus acabam sendo vistos como "pragas" destrutivas, que irão causar um evento negativo ao funcionamento do computador.

Mas saiba que nem sempre um vírus é feito para destruir arquivos. Por exemplo: imagine um programa que esteja instalado em seu computador, que monitora tudo que está sendo digitado no teclado e copia tudo que você digitar.

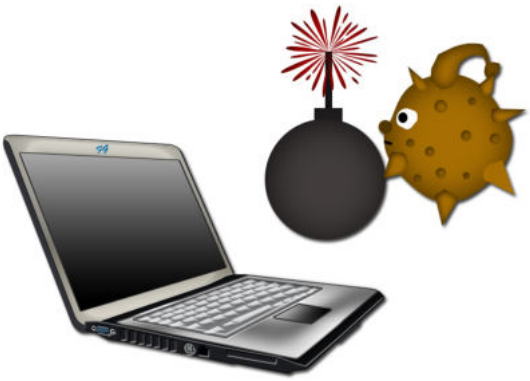

**Figura 01.2: nem sempre o objetivo de um vírus é destruir o seu sistema.**

Mas vamos um pouco mais longe: imagine agora que ao invés desse programa copiar tudo que você digitar, ele copia apenas coisas relacionada com "senha", "pass", "password", "key", "nome", "tel", "telefone", "end", "endereço", "CPF", etc.

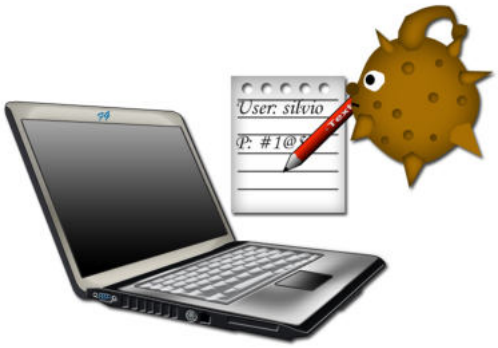


**Figura 01.3: vírus podem roubar informações.**

Ele não destroi nada, mas é um vírus. E quando por exemplo, você se conectar na internet, esse programa poderá enviar essas informações para algum e-mail pre-determinado, por exemplo.


**Figura 01.4: vírus podem enviar informações através da internet.**

Tudo isso é possível simplesmente porque o vírus nada mais é do que um "programinha", ou seja, um software que tem um código, e que pode fazer qualquer coisa que outros programas fazem, obviamente cada vírus só irá fazer aquilo que estiver programado em seu código.

Um tipo de linguagem que pode ser usada para programar vírus é a Assembly, pois é a linguagem "nativa" do computador, o que gera menos códigos para executar alguma tarefa, além de ficarem com tamanhos pequenos (variam de 20 bytes até aproximadamente 2MB).

Outras linguagens usadas podem ser o Pascal, C, Basic, entre outras. Alguns Pseudo Vírus são feitos usando comandos do DOS em arquivos de lot (BAT) ou até scripts (java scripts) em home pages.

Um grande mito é de os vírus poderiam danificar (quebrar) hardware, o que é mentira.

Hardware é a parte física, vírus é software, é parte lógica. Para danificar um hardware (literalmente) seria necessário provocar um super aquecimento, provocar um curto circuito, etc.

**Figura 01.5: hardware é a parte física de um computador.**

Alguns vírus, como o *Chernobyl* (que conheceremos um pouco sobre ele neste livro), conseguem reescrever a gravação da BIOS em alguns modelos de placas mães (entenda isso, não são em todas), apagando-a. Nesse caso, o vírus conseguiu inutiliza-la temporariamente, mas não quebrá-la, ela pode ser recuperada usando técnicas apropriadas.

Essas "pragas" virtuais podem ser classificados em três tipos principais: *vírus*, *worms* e *trojans*.

**Vírus**

Os vírus *precisam de um arquivo* ("hospedeiro"), de outro programa para que eles possam agir.

Eles se ocultam em programas executáveis (com extensão .EXE, .COM por exemplo) ou bibliotecas compartilhadas (com extensão .DLL).

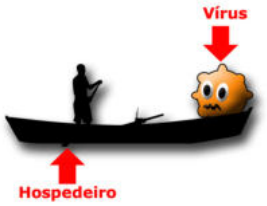


**Figura 01.6: Vírus necessitam um arquivo hospedeiro para agirem.**

Por causa dessa característica, são capazes também de infectar outros arquivos que sejam requisitados para a execução de algum programa, como os arquivos de extensão .SYS, .OVL, .OVY, .PRG, .MNU, .BIN ou .DRV.

São muito mais rápidos que os worms e atingem um grande número de dados rapidamente.

O vírus de macro (um tipo de vírus) por exemplo, se espalham através de documentos Word ou Excel, que são os aplicativos muitos usados em computadores.

Para que os vírus façam qualquer coisa, ele deve ser ativado pelo usuário. Isso é feito quando ativamos o programa que contém o *código viral*, em outras palavras, o vírus é ativado quando abrimos o programa que o contém.

Caso esse programa não seja ativado pelo usuário, o vírus não conseguirá fazer nada ao sistema, ele ficará apenas alojado.

Uma vez ativado, ou seja, o usuário executou o programa, o vírus passará a infectar outros arquivos. Aí começa a *replicação*: se o arquivo infectado for copiado para outro computador "limpo", ele estará lá novamente esperando para ser ativado pelo usuário. Se o usuário ativar o arquivo, o sistema também será infectado.

**Worms**

Fazendo uma recapitulação sobre os vírus, dissemos anteriormente que eles (os vírus) precisam de um arquivo para agirem, ou seja, necessitam de um "hospedeiro".

No caso dos worms (ou *vermes*, em Português), eles *não precisam de um "hospedeiro"* para agirem, são independentes.

O código do worm não necessita de outro arquivo para executar as funções que lhes foram programadas.


**Figura 01.7: Worms são totalmente independentes, não precisam de hospedeiros para agirem.**

O worm consegue se *auto duplicar*, fazer cópias de si mesmo, e isso é feito sem necessitar de interferência humana.

Outra característica do worm é a capacidade de enviar essas cópias através de e-mails (Vírus-mail).

Os worms também podem tentar desativar Anti- vírus e Firewall, gerar executáveis (muitas vezes pode ser trojans), gravar rotinas no registro, entre outras coisas.

**Trojans**

O Trojan horse (Cavalo de Tróia) também são programas que *não necessitam de um "hospedeiro",* sendo que eles tem uma particularidade: se disfarçam de um programa "inofensivo" mas que tem por trás um código malicioso.

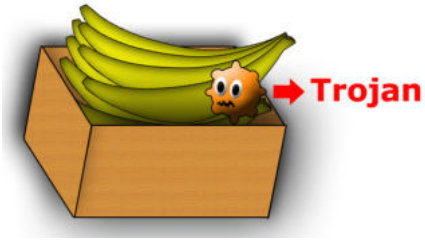


**Figura 01.8: O Trojan possui a particularidade de usar um programa inofensivo como disfarce para enganar sua vítima.**

Daí o seu nome ser *cavalo de Tróia*, uma analogia com a mitologia grega do livro "a Odisseia", onde um grande cavalo de madeira é deixado nas portas de Tróia. Os troianos imaginando que se tratava de um presente, levaram o cavalo para o centro da cidade, mas, o que eles não imaginavam é que dentro desse cavalo haviam soldados gregos, que aproveitaram a situação e os atacaram.

Os Trojan horse não se duplicam, mas são eles que podem, por exemplo, copiar informações que são digitadas pelo usuário e incluir *backdoors* no computador da vítima.

Os backdoors são programas que irão garantir que o hacker consiga retorno em um computador que ele invadiu, ou seja, ele abre "uma porta dos fundos", como muitos dizem.

Os trojans podem chegar em um computador através de inúmeros formas que os "disfarcem", fazendo os parecerem com programas benéficos.

Exemplo: aplicativos muito requisitados, como aplicativos para retirar bugs do sistema, retirar senhas, que dizem acelerar o computador ou até mesmo jogos e protetores de tela.

Alguns exibem algum tipo de animação ou se "disfarçam" de imagens BMP ou JPG por exemplo.

Um trojan que venha a se "disfarçar" de uma imagem, tipo jpg por exemplo, poderá ter o nome da seguinte forma: um_nome_qualquer.jpg.exe.

Uma configuração do Windows permite que não seja exibido as extensões dos arquivos (o que é sem dúvida uma falha), dessa forma o arquivo irá aparecer como: um_nome_qualquer.jpg (a extensão EXE fica oculta), o que mais cedo ou mais tarde acaba pegando um desavisado.

Alguns trojans se disfarçam de jogos famosos, como o trojan *Fintas.C*, que chegava por e-mail com um anexo chamado FF8.EXE e a mensagem: "the cool game about Final Fanstasy VIII :)". O campo Assunto geralmente vinha vazio.

Trata-se de um disfarce de uma prévia de um famoso jogo que foi lançado, o Final Fantasy 8. Quando o usuário executa o arquivo em anexo, ele substitui o

AUTOEXEC.BAT do Windows incluindo comandos para que o Disco Rígido fosse formatado na próxima vez que o computador fosse iniciado.

Ele formatava não só o disco C:\, mas sim todos os discos do computador que ele encontrasse, indo de C:\ à Z:\.

Para se espalhar pela internet ele usava a lista de e-mails do *Outlook Express* do computador contaminado.

O trojan *Fintas.C* é um trojan do passado e que ficou na história, principalmente pela sua "agressividade".

**Variações de vírus**

Os vírus também podem ser classificados quanto ao *modus operandi*, isto é, modo que eles operam, seu funcionamento e capacidades adicionais.

São eles: vírus de boot, Vírus Multipartite/ Vírus Múltiplos, vírus de macro, vírus polifómicos, vírus stealth, vírus-mail e duas variações de não-vírus, que são eles: pseudos vírus e Hoax Vírus.

**Vírus de arquivo**

São aqueles que infectam arquivos do Disco Rígido em especial arquivos executáveis (com extensão .EXE ou .COM por exemplo).

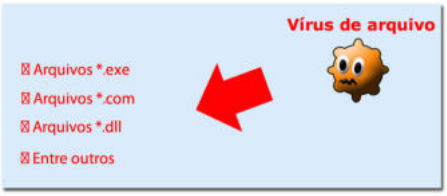


**Figura 01.9: vírus de arquivo e alguns tipos de arquivos que eles atacam.**

**Vírus de boot**

Conhecido também por *vírus de MBR*, eles se instalam no setor de inicialização do Disco Rígido.

Na verdade eles conseguem se instalar em setores de inicialização de qualquer meio de armazenamento, como o CDs, DVDs e Pen Drives.

No tempo em que se usava muitos os *disquetes de boot* (era necessário para instalar o sistema operacional ou fazer manutenções no sistema por exemplo), um disquete contaminado representa um grande risco, uma vez que inseridos podem contaminar o setor de boot do Disco Rígido. Caso a FAT seja corrompida, o acesso a arquivos e diretórios era perdido. E imagine se um técnico desenformado levasse esse disquete de computador em computador, cliente em cliente. Vários computadores seriam contaminados.

Hoje, um cuidado que devemos ter são com os Pen Drives contaminados. Pen Drive é um dispositivo muito comum, e se tiver contaminado poderá contaminar outros computadores (no leva e trás de arquivos).


**Figura 01.10: vírus de boot se instalam no setor de inicialização.**

**Vírus Multipartite/ Vírus Múltiplos**

São vírus capazes de infectar tanto o setor de boot (MBR) quanto arquivos de programas.

São uma combinação do vírus de boot com os Vírus de arquivo, fazendo com que eles se propaguem com muito mais rapidez.


**Figura 01.11: Vírus Multipartite infectam setor de boot e arquivos**

**Vírus de macro**

Os vírus de macro começaram a surgir por volta de 1995 e se espalharam a uma velocidade espantosa.

Os vírus de macro se espalham rapidamente graças a popularidade dos programas Word e Excel da Microsoft. Infectam os arquivos dos aplicativos do pacote Microsoft Office (doc - word, .xls - excel, .ppt - power point, .mdb - access.)

Um dos primeiros vírus de macro que se tem notícia foi o *CONCEPT*, que infectaram documentos do Microsoft Word (versões 6.x, 7.x e 97), nas plataformas Windows e Macintosh. Surgiram mais tarde o Concept (F, G, J, L e M), todos baseados no Concept.

Só para se ter uma idéia o Concept.F trocava as letras dos documentos do Word infectados, substituindo "." por ",", "a" por "e" e "and" por "not".

Além disso os vírus Concept.F, G e J exibem no 16° dia de cada mês a seguinte mensagem na tela do monitor:

*- / Parasite Virus 1.0 / X / Your computer is infected with the Parasite / Virus, version 1.0! / OK*


**Figura 01.12: Vírus de macro Infectam arquivos do Microsoft Office**

**Vírus Residente**

Quando executados pelo usuário esse vírus é colocado na memória e a parti daí passa a infectar outros arquivos que forem abertos, ampliando cada vez mais a quantidade de arquivos contaminados.

**Vírus polifómicos/ Vírus criptografados**

São vírus com capacidade de enganar os anti-vírus. Esses vírus são conhecidos também por mutantes.

Eles alteram o seu tamanho e formato de código, o que poderá dificultar (ou até impossibilitar) que o anti-vírus o detecte.

Para que o vírus seja *polifórmico*, o seu código deve ser randômico. Dessa forma, o vírus fará copias de si mesmo, porém, com formato de códigos diferentes. E como normalmente os anti-vírus usam como referencia pedaços do código virótico, ele poderá ser enganado.

Outra técnica usada é a criptografia do código viral com uma *chave não constante* com conjuntos aleatórios de comandos de *descriptografia*.

Geralmente envolve um laço ("loop") no qual o vírus é *encriptado* ou *desencriptado*, toda a vez que é executado.

Os vírus polifórmicos foram divididos em seis níveis de acordo com o seu poliformismo:

| Nível | Descrição |
|---|---|
| 1 | Compostos por descriptadores com código constante, que escolhe um deles durante a infecção. Conhecidos também por: "semipolimórficos" ou "oligomórficos". |
| 2 | Composto por descriptador com uma ou diversas instruções constantes e o restante pode ser modificado. |
| 3 | Compostos por um descriptador com funções não utilizadas como NOP, STI, etc. |

| | |
|---|---|
| 4 | Compostos por um descriptador que utiliza instruções intercambiáveis e modifica sua ordem, mantendo o algoritmo de descriptação inalterado. |
| 5 | Basicamente o algoritmo de descriptação é modificável e usa todas as técnicas mencionadas. |
| 6 | O código principal do vírus está sujeito a mudanças, é divido em blocos que são posicionados em ordem aleatória durante a infecção. Pode ser descriptografado. |

**Vírus Stealth**

São os vírus "invisíveis". São aqueles que usam algum tipo de técnica para se "esconder" dos anti-vírus e/ou do usuário.

São portanto vírus difíceis de localizar tanto pelos anti-vírus quanto pelo usuário.

Os polifôrmicos por exemplo mudam a sua forma e/ou usam criptografia. Os vírus de macros utilizam técnicas que impossibilitam que sejam encontrados como desabilitar ou redirecionar todos os comandos do Word ou excel (barra de ferramentas e menus) que possam exibir o seu código.

**Vírus-mail**

São vírus que se propagam anexados a E-mail. Geralmente são worms.

Esse tipo de vírus funciona da seguinte forma: ao abrir o arquivo anexado ao E-mail, ele contaminará o computador fazendo com que todas as mensagens que forem enviadas pelo usuário, levarão junto o vírus anexado.

O destinatário por receber um arquivo anexo de uma pessoa conhecida, muito provavelmente irá abrí-la.


**Figura 01.13: Vírus-mail se propagam anexados a E-mails.**

E para induzir a as vítimas a abrirem o arquivo anexo ao e-mail mais rapidamente, o vírus introduz no corpo do e-mail uma mensagem que faz parecer que o e-mail recebido é de alguém conhecido. Veja a seguir um exemplo de mensagem:

*Olá, a quanto tempo! Eu me mudei dai para os Estados Unidos, e faz um tempo que perdemos o contato e consegui seu email através de uma amiga sua. Vamos fazer assim, eu vou lhe mandar meu álbum de fotos se você me reconhecer, me retorna o email. Quero ver se você ainda lembra de mim. :)*

O vírus Worm.ExploreZip por exemplo envia a mensagem:

*"Recebi seu e-mail e estarei respondendo assim que possível. Até lá, dê uma olhada no arquivo .zip atachado".*

Se o arquivo anexo for aberto, o vírus modifica o arquivo WIN.INI e utiliza o programa de e-mail para se propagar. Além disso ele tenta apagar arquivos do Word, Excel e PowerPoint.

Tenha, sempre, cuidado ao receber mensagens de e-mails sobre acontecimentos atuais, avisos de bancos, sobre atualizações, tragédia, pessoas desaparecidas, terremotos, desabamentos entre outros.

É comum, chegando a ser normal, a exploração de assuntos atuais e de grande ascensão na disseminação de vírus.

Veja alguns assuntos que estão sendo explorados (no momento em que escrevo este livro) para a prática de vírus mails ou simplesmente para a prática de *hoax* (ver mais adiante):

- Cinegrafista morre em operação do Bope;
- Hacker divulga vídeos e fotos do arquivo pessoal do e-mail de Dilma;
- Bruno é morto na cadeia;
- Banco "X" Informa;
- Cliente "do banco X", comunicado importante;
- Recadastramento "banco x" de segurança;
- Seu nome foi citado na rede de vídeos Youtube;
- Tava te procurando;
- Recado de uma juíza federal;
- Extrato de multas online;
- Sua conta do Hotmail será desativada;
- Serasa: encontrei um protesto em seu nome e da sua mãe;
- Espero de alguma forma que eu esteja te ajudando;
- Módulo de proteção;
- Desculpe-me pela minha fraqueza;
- Aviso de bloqueio de conta;
- É você mesmo nessas fotos?
- Você recebeu um torpedo;
- Abra os olhos;
- Criança desaparecida;
- Seu cadastro foi inabilitado para negociar no Mercado Livre;
- CPF/RG suspensos;
- Alerta de compra;
- Vale presente;
- Você recebeu um vídeo torpedo;
- Seu e-mail será cancelado;

O ideal é não abrir mensagens desse tipo. E se abrir, não abra os anexos. E jamais reenvie essas mensagens em diante.

É preciso ter bom senso com mensagens recebidas. Mensagens desses tipos vitimam pessoas desenformadas, curiosas e às vezes até "inocentes" (que não percebem a maldade por trás do e-mail recebido).

O assunto "banco" é muito explorado. No geral, bancos não enviam mensagens pedindo dados, atualizações e afins. Além disso, você já recebeu mensagens de bancos ao qual você não é cliente. Atente-se.

Evite participar de *correntes* de mensagens, que são aquelas mensagens bonitinhas, com apelo religioso, que dizem que é para ajudar alguém, entre outras finalidades. Por mais bonito, nobre ou religioso que pareça ser, os objetivos, em muitos casos, em praticar correntes é capturar e-mails, e o próprio e-mail daquele que quer capturar e-mails vai estar na lista.

Por isso, ao receber mensagens desse tipo, apague-a, por mais apelativa que ela seja. Não passe para frente, não envie-a para sua lista de e-mails e nem para seu amigo ou parente.

**Hoax Vírus**

Na verdade não são vírus e sim boatos que se espalham pela Internet com o objetivo de provocar tumultos, capturar e-mails, fazer com que usuários menos experientes danifiquem os seus sistemas operacionais (como apagando arquivos importante), entre outras finalidades.

Como realmente começaram a surgir no Brasil, se vieram de fora ou começaram por aqui mesmo é incerto dizer. Mas até alguns anos atrás isso era um problema típico nos EUA.

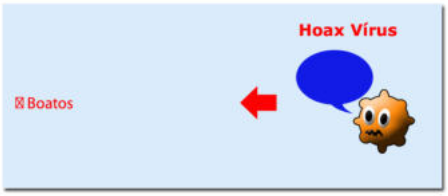


**Figura 01.14: Hoax Vírus - Boatos**

É importante entender, que apesar desse tipo se chamar Hoax Vírus (vírus boatos), ele não é um aplicativo, não é transportado por um "hospedeiro", não se multiplica automaticamente, portanto não são vírus.

Os Hoaxes se propagam através de E-mails e na maioria dos casos os motivos por trás de tais mensagens podem ser destrutivos (tentar convencer ao usuário a apagar algum arquivo do sistema), captuar e-mails, etc.

Muitos podem fingir que são mensagens enviadas (inclusive com assinatura) por pessoas da IBM, Microsoft, Unicamp, bancos, etc.

Além disso, a cada dia que passa, o número de Hoax aumenta, o que torna difícil distinguir o que é verdade do que é mentira.

Alguns Hoaxes como o "Garoto perdido do tsunami" traziam simplesmente uma foto de 1MB de um garotinho supostamente abandonado depois da tragédia na Ásia. Foi descoberto mais tarde que era mentira.

Já outros como o "jdbgmgr.exe" trazia uma mensagem dizendo que esse arquivo (jdbgmgr.exe) presente no System do Windows tratava-se de um vírus e que devia ser apagado imediatamente, ou seja, se o seu sistema tivesse esse arquivo ele estava "contaminado" por um vírus. Só que o arquivo jdbgmgr.exe é na verdade usado pelas versões atuais do Windows para interpretação do Java, que é uma linguagem multiplataforma.

Outros tentam provocar pânico e desordem com mensagens do tipo "pir vírus encontrado" ou "vírus mais perigoso do mundo" ou ainda "vírus que destrói hardware".

Alguns são em inglês e outros tem diversas variantes em diversas línguas. Veja a seguir uma mensagem do Hoax "A Virtual Card for You" que foi distribuída via e-mail (o original é em inglês). Vale lembrar que trata-se de um trote, ou seja, é mentira:

*Pior Vírus já encontrado.*
*POR FAVOR ENVIE ESTA MENSAGEM PARA TODOS OS CONTATOS DE SUA LISTA!!*
*Um novo vírus foi descoberto e classificado pela Microsoft como o mais destrutivo já existente. Este vírus foi descoberto ontem à tarde pela McAfee e ainda não existe vacina.*
*Este vírus simplesmente destrói a zero os setores do disco rígido, onde as informações vitais para funcionamento estão armazenadas. Este vírus atua da seguinte forma: Ele envia automaticamente para todos os contatos de sua lista com o título "A Virtual Card for you" ou "Um Cartão Virtual para você". E quando supostamente este cartão é aberto o computador congela de modo que o usuário tenha que religar o micro. Quando você pressiona a chave ctrl+alt+del ou pressiona o botão de reset, o vírus destrói o Setor Zero, deste modo destrói permanentemente o disco rígido.*
*Ontem por poucas horas este vírus causou pânico em Nova York, de acordo com as notícias do programa da CNN. Este alerta foi recebido pelos operadores da Microsoft. Por isso não abram o arquivo "A Virtual Card for you".*
*Caso receba este e-mail, Delete. Por favor passe este e-mail para todos os seus amigos. Envie este para todos de sua lista de endereços.*
*Além disso, a Intel anunciou que um novo e, muito destrutivo vírus foi descoberto recentemente. Se você receber um e-mail chamado "An Internet Flower For You", não abra. Delete assim que receber. Este vírus remove todos os arquivo ..dll (dynamic link libraries) do seu computador. Seu computador não poderá carregar os arquivos acima.*

**Pseudo vírus**

Esse tipo de "não-vírus" causam na verdade um grande incômodo, perda de tempo e irritação.

São feitos por pessoas com pouco conhecimento em programação ou por pessoas que desejam apenas dar um susto em um amigo.

Um Pseudo Vírus não provoca danos no sistema e nem contaminam automaticamente outros arquivos. Além disso só entram em ação quando são iniciados pelo usuário.

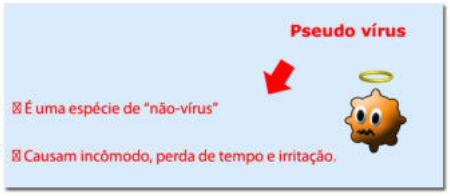


**Figura 01.15: Pseudo vírus**

Até um tempo atrás era comum encontrar Pseudo Vírus feitos em arquivos de lote do MS-DOS. Alguns "mais modernos" em JavaScripts. Mas, na prática podem ser construídos usando qualquer linguagem.

Algumas páginas da internet tem o que seus criadores chamam de "ísca" ou "armadilha", que são links que irão desencadear uma ação, que em alguns casos provocam uma desordem tamanha no sistema, que o que resta a fazer é resetar o computador.

Quando é usado JavaScript, por exemplo, essas iscas podem fazer com que o browser comece a abrir páginas infinitamente, ou abra janelas pou-up de forma descontrolada, exiba mensagens, entre outras ações.

Apesar desses tipos de códigos não necessariamente representarem um risco, parecerem muitas vezes até "bobos", se uma pessoa entrar na página que os contenha, possivelmente terá que resetar o computador, não adiantando apertar a tecla ESC e muito menos tentar fechar as janelas que se abrem.

Existem diversos outros tipos de scripts que provocam os mais variados efeitos.

Já os "vírus" feitos com arquivos de lote do MS-DOS (.BAT) usam os comandos do DOS, como DEL, FORMAT , DELTREE, COPY entre outros.

No geral são feitos para uma finalidade bem específica e restrita, por exemplo: um arquivo .BAT com a linha C:\DEL *.exe. Se esse arquivo for executado, ele irá apagar todos os arquivos com a extensão EXE que estiverem em C:\. Apesar de parecerem inofensivos, podem formatar um Disco Rígido inteiro.

Vejamos no exemplo, um pseudo vírus feito em um arquivo BAT.

```
:
@echo off
cls
echo Exemplo para o livro.
echo Responda a pergunta corretamente, ou seu HD será formatado.
Echo O que significa a sigla T.U.J.F.D???
echo ----------------------------------------------------
Echo [1] Nao sei..
Echo [2] Eu desisto...
Echo [3] Nao tenho nada importante no HD mesmo!...
choice /c123
echo ----------------------------------------------------
if errorlevel 3  dir
if errorlevel 2  cls
if errorlevel 1  vol
echo
echo
echo ----------------------------------------------------
```

echo Isso e apenas um teste, seu HD nao foi formatado!

Esse pseudo vírus não faz nada a não ser fazer uma pergunta ao usuário. Ele não formata o Disco Rígido. Observe que há três alternativas de respostas:

- Echo [1] Nao sei..: Escolhendo essa alternativa, o arquivo executa a linha "if errorlevel 1 vol", ou seja, mostra o volume do Disco Rígido (através do comando vol);
- Echo [2] Eu desisto...: Escolhendo essa alternativa, o arquivo executa a linha "if errorlevel 2 cls", ou seja, limpa a tela (através do comando CLS);
- Echo [3] Nao tenho nada importante no HD mesmo!...: Escolhendo essa alternativa, o arquivo executa a linha "if errorlevel 3 dir", ou seja, mostra os diretórios do Disco Rígido (através do comando dir).

Nesse exemplo não é causado nada de grave. O problema começa quando pessoas mau intencionadas trocam os comandos *dir, cls e vol* por outros comandos como por exemplo o Deltree/Y, que exclui pastas e arquivos sem pedir confirmação do usuário.

Esses sim poderiam ser perigosos e causarem sérios danos aos arquivos de um computador.

Nem todo vírus feito com arquivos BAT será um Pseudos vírus.

# Capítulo 02 – Os criadores

**Os criadores**

Vírus não surgem do nada nos computadores, eles são escritos por alguém e colocados em circulação.

O surgimento (a criação) de um vírus se dá de duas formas:

- **Intencional:** o criador desde o início queria fazer um vírus;
- **Acidental ou não-itencional:** apesar de parecer um absurdo que um vírus seja feito acidentalmente, imagine que um programador estava fazendo um aplicativo qualquer, descobre que ao inserir um determinado código ao seu aplicativo, este acabar reagindo de uma forma ao qual não era esperado, seja causando danos ao sistema ou não.

Mas quem pode fazer vírus? Ou melhor dizendo, quem consegue fazer vírus?

Qualquer pessoa com um mínimo de tempo e uma grande disposição para aprender.

Essa reposta pode assustar em um primeiro momento, mas é a pura realidade. Com o avanço e a disseminação da Internet que temos atualmente, encontrar informações de como fazer não é o problema.

Inclusive é possível encontrar livros ou revistas nas maiorias das bancas ou livrarias com tudo que é necessário para uma pessoa sem experiência nenhuma fazer vírus.

Ha vírus que são extremamente complexo de se fazer, outros são feitos com seis ou oito linhas de comandos.

Devido a isso tudo, quantidade de informação disponível e pessoas dispostas a fazer, a quantidade de vírus crescem aceleradamente.

Os motivos que podem levar uma pessoa a fazer um vírus são os mais variados possíveis.

Pode ser por frustração, desejo de vingança, curiosidade, como forma de punir aqueles que usam programas de computadores sem pagar por direitos autorias, para roubar informações, rebeldia (enquanto alguns picham muros, outros fazem vírus), etc.

É impossível determinar um motivo que justifiquem todos, mas algumas coisas são certas: vandalismo e desejo de destruir. Muitos vírus foram feitos para simplesmente "aniquilarem" com o sistema operacional, formatando o Disco Rígido e junto com ele todas as informações que estavam guardadas.

A criação dos vírus são na maioria das vezes associadas aos *Hackers*, jovens com muito tempo livre e muita vontade de aprender mais e mais sobre computadores, em especial, a programação.

**Hackers: mito ou realidade?**

Mas o que são os Hackers, esses "seres" que ninguém vê, ou, quando vê é sendo presos acusados de crimes digitais.

A grande verdade é que um hacker de verdade nunca é preso, simplesmente porque ele não dá alarde de seus feitos e nem sai por aí dizendo que é um hacker (esse não é o objetivo dele).

O significado para o termo *Hacker de computadores* encontrado em qualquer livro sobre o assunto é um indivíduo que sabe muito sobre computadores, possui grande capacidade de análise, assimilação e compreensão.

É hábil na programação e por isso não fica perdendo tempo tentando derrubar os outros da net, o negócio dele é fazer programas novos, testar e corrigir falhas na segurança dos sistemas.

Os hackers possuem conhecimentos além da programação: conhecem perfeitamente sobre todo o hardware de computadores, dominam redes cabeadas e wireless, entendem muito sobre internet no geral e por aí vai.

O que fica evidente é que foi criado uma espécie de "submundo", de pessoas aficcionadas por computadores, onde a palavra de ordem é o conhecimento. Isso é levado tão a sério, que passam a levar uma rotina de vida quase que esotérica, estudando e aprendendo cada vez mais, principalmente novas linguagens de programação.

Algumas dessas pessoas acabam trabalhando para grandes empresas, na área de segurança, programação ou outra relacionada com informática. Esses são os verdadeiros hackers.

Mas outros acabam usando os seus conhecimentos para invadir sistemas, roubar senhas, desviar alguns centavos de contas bancárias (ou roubar muito dinheiro mesmo), entre outras coisa erradas, e, muitos acabam, conseqüentemente atrás das grades. Esses são chamados de crakers.

Se você fizer uma rápida pesquisa no Google (www.google.com.br) irá descobrir vários nomes que ficaram conhecidos mundialmente pelos seus feitos: invasões de sistemas, sites e muito mais. Vejamos alguns:

- Adrian Lamo: invadiu o sistema do jornal *The New York Times* para incluir o próprio nome na lista de colaboradores;

- Albert Gonzalez: invadiu sistemas de lojas e se apoderou de milhares e milhares de números de cartões de créditos.;

- François Cousteix: invadiu  o Twiter e teve acesso à contas do Barack Obama, Britney Spears, entre outras;

- Auernheimer: desbloqueou um Ipad;

- Kevin Mitnick: considerado um dos hackers mais famosos de todos os tempos. Invadiu diversos computadores como de operadoras de telefonia, provedores de internet e empresas de tecnologia.

Se você se interessou pelo assunto, indicamos a leitura do artigo "Dez hackers famosos e seus feitos: http://www.terra.com.br/noticias/tecnologia/infograficos/hackers/

Não há como fechar os olhos e fingir que hackers não existem ou que isso é besteira. Realmente eles existem: pessoas que preferem trocar as "baladas" da noite por horas a fio em frente do computador.

E é preciso saber também que há muitas vezes um marketing exagerado sobre eles, atribuindo-lhes qualidades que muitas vezes não existem, como se eles tivesse controle de todos os computadores do mundo. Nem sempre um ataque hacker terá como ponto de partida um computador. Muitas vezes eles usam a engenharia social (leia o tópico a seguir).

Existe ainda uma divisão hierárquica que separa os indivíduos quanto ao seus conhecimentos. Somente com o objetivo de se fazer constar, vejamos o significado de alguns:

- **Hackers:** é um indivíduo que sabe muito sobre computadores, possui grande capacidade de análise, assimilação e compreensão. Prefere fazer novos programas, testar e corrigir falhas em sistemas;
- **Crakers:** Possui o mesmo conhecimento do hacker, com a diferença que para ele só invadir sistemas não basta. Eles precisam deixar um aviso que estiveram lá, através de mensagens ou até apagando arquivos. Usam seus conhecimentos para proveito pessoal e financeiro próprio;
- **Phreaker:** Fusão das palavras "freak, phone, free". É o especialista em telefonia
- **Lamer:** Novato. É aquele que aprendeu alguns truques, pegou algumas "receitas de bolo" (ferramentas que vão poupar-lhes seu trabalho intelectual, está relacionado com coisas prontas, já descobertas, algo fácil), e acha que é um hacker. Exatamente por saber pouco, corre o sério risco de ser preso.

Atualmente a palavra hacker é usada de forma "genérica" (quando você vê na TV a prisão de um endivido relacionado com o que falamos aqui, são chamados pela mídia de hacker, e não cracker, phreaker ou lamer), sem distinção de hacker ou Crakers, o que pode até fazer sentido, porque de forma resumida, hacker de computador é aquele que é "fera" na informática, não importando se ele é o mocinho ou o ladrão.

**Engenharia social**

Imagine a seguinte situação: você trabalha em uma grande empresa, e em um determinado dia, quando se encaminhava até a sua sala de trabalho encontra dentro de um elevador um DVD escrito "demonstrativo de salários da empresa".

Você mais que curioso corre para seu computador para ver quanto as pessoas estão ganhando.

Ao abrir o suposto documento é exibida a mensagem: "versão do sistema incompatível". Ou você tentaria novamente em outro computador, ou deixaria de lado.

Mas o que você não sabe, é que este DVD foi deixado por um hacker, e que ao executar o arquivo você instalou um vírus (um worm ou trojan) que dará acesso ao hacker. Esse é só um exemplo de uma prática criminosa que pode acontecer.

Veja alguns exemplos que aconteceram: uma pessoa liga para você dizendo que é da telefônica e que você acabou de ganhar um carro 0KM. Para retirar o prêmio será necessário você comprar três cartões de celulares pre-pagos e passar para eles as senhas dos créditos. Parece um absurdo mas isso aconteceu, e muitas pessoas desenformadas caíram no golpe.

Veja mais um exemplo: alguém te liga e diz que é o "suporte técnico" do provedor e que a sua conexão está com problema. Para resolver o problema ele precisa de sua senha de conexão. Se você passar a senha para esse suposto "técnico", ele poderá usar a sua conta de acesso para práticas maliciosas.

Tudo isso são exemplos de engenharia social, onde o Hacker consegue informações de sua vítima aproveitando da falta de informação da mesma. Eles procuram induzir as suas vítimas a fazer alguma tarefa, e o sucesso do ataque irá depender exclusivamente da decisão do usuário.

**Contaminação**

A contaminação de um computador com qualquer tipo de vírus pode se dar de várias formas.

Alguns anos atrás essa contaminação se dava basicamente através de disquetes. Com o advento da Internet, os vírus passaram a se alastrar via E-mail. Veja a seguir as diversas maneiras de ocorrer uma contaminação:

- Abrir arquivos anexados aos e-mails;
- Abrir arquivos armazenados em outros computadores, através do compartilhamento de recursos;
- Instalar ou copiar arquivos de CDs de procedência duvidosa;
- Instalar ou copiar arquivos de DVDs de procedência duvidosa;
- Instalar ou copiar arquivos de um disquete de procedência duvidosa;
- Instalar ou copiar arquivos de disco de Zip Drive, Pen Drives ou outros meios de armazenamento de procedência duvidosa.

A contaminação pode ocorrer em qualquer sistema que permita que de alguma forma um arquivo contaminado seja executado.

Isso quer dizer que novos meios de contaminação irão surgir acompanhando o avanço tecnológico.

E como vimos nas páginas anteriores, alguns tipos de vírus podem contaminar um sistema e ficar "invisível" sem que seja percebido, uma vez que, nem todos os vírus são feitos com a intenção de apagar arquivos.

**Sintomas de um PC contaminado**

Um computador contaminado pode apresentar os mais variados sintomas possíveis:

- **Arquivos deletados:** é comum surgir (principalmente quando se inicia o computador) mensagens do tipo "não foi possível encontrar o arquivo um_nome_qualquer.DLL", ou o computador nem conseguir iniciar, o computador retornar mensagens que não foi possível encontrar algum arquivo.

Outros arquivos podem simplesmente "sumir", como arquivos de textos, tabelas e na pior das hipótese, a formatação completa do disco;

- **Computador travando:** o computador pode travar por vários motivos, e um deles, pode ser vírus;
- **Lentidão:** ao abrir programas, ao fechar programas, ao conectar na internet, ao iniciar o computador ou até mesmo ao desligar o computador;
- **Imprimindo caracteres que não foram digitados:** acontece geralmente nos programas do Microsoft Office como o Word, provocados por vírus de macro;
- **Mensagens na tela:** Surgimento repentino de mensagens que nada tem a ver com algum programa ou erros do sistema operacional;

Vírus perigosos podem ser bem agressivos ao sistema, causando dentre outras coisas, a formatação do disco.

Mesmo que seus computador apresente algum desses sintomas, não significa necessariamente que ele está com vírus. Pode ser simplesmente a falta de uma boa manutenção no sistema, erro de algum aplicativo, falta de memória RAM, entre outros fatores.

# Capítulo 03 – Ataque: Como age um vírus

**Como os vírus atacam**

Vimos até agora o que são vírus e suas variantes, os meios de contaminação e os principais sintomas que o sistema geralmente apresenta.

Veremos agora um pouco sobre como alguns vírus atacam. Com isso iremos compreender melhor como eles chegam ao computador do usuário, como eles atacam e quais os reais riscos.

**Worms**

A principal especialidade do *worm* é fazer cópias de si mesmo e se propagar pela rede, sem necessitar da intervenção humana.

Por ter essa característica muitos são feito com o intuito principal de proliferarem o máximo possível.

Isso faz deles uma grande ferramenta para os hackers, que podem usá-lo para espalharem outros tipos de vírus.

É o caso dos *trojans*, que podem chegar em um computador através de um worm. Isso quer dizer, que se um ati-vírus detectar e eliminar um worm, não necessariamente o computador ficará "limpo", talvez há um trojan instalado no sistema.

Vale lembrar que o worm pode ser programado para fazer diversas outras coisas além de se propagar.

Vamos usar como exemplo o worm W32/BugBear@mm: uma vez ativo em memória, esse worm tentará enviar uma cópia de si mesmo para todos os endereços de e-mail do sistema infectado.

Além disso, ele tentará desabilitar os programas anti-vírus e Firewall ativos e instalará um trojan no computador com o objetivo de capturar o que for digitado no teclado.

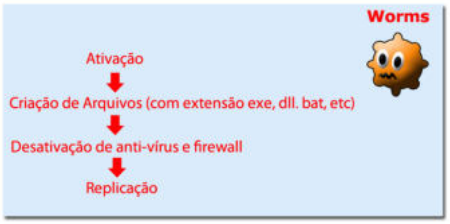


**Figura 3.1: Exemplo de como um Worm pode agir**

**Trojans**

Os trojans não se multiplicam e podem chegar ao computador da vítima anexo a E-mails ou podem ser instalados através de worms.

O objetivos deles geralmente são dois: coletar informações e incluir *backdoors*, para garantir que um hacker tenha acesso posterior ao computador.

Um trojan pode ser instalado manualmente pelo hacker ou pelo usuário.

Para que ele seja instalado pelo usuário, o hacker tentará convencê-lo a executar o trojan, e isso é feito disfarçando-o de uma aplicativo  que pode ser jogos, charges, proteções de tela, etc.

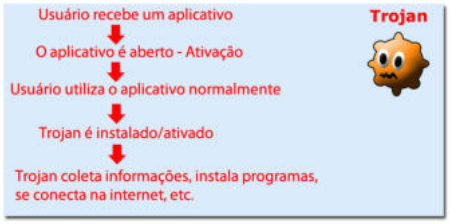


**Figura 03.2: como um trojan pode ser instalado em um computador.**

Na época do "apagão" (2001 e 2002) apareceu o Trojan "infectus" que exibia três tela fazendo uma alusão ao racionamento de energia.

A primeira tela vinha com a frase: "Com a onda do 'Apagão', o governo após vários estudos encontrou a tão esperada solução para os problemas referentes ao racionamento de energia. Ela é totalmente segura e não requer gastos e verbas".

A Segunda tela: "O Ministério do 'Apagão' adverte: perder tempo com esse tipo de e-mail é desperdício de energia :-)".

E por fim a terceira: "Seu computador já pode ser desligado com segurança".

Apesar de parecer engraçado, o trojan por "trás", se conectava a uma site da Bélgica e baixava um programa que iria dar acesso ao computador da vítima ao hacker.

**Vírus de Macro**

Macro é um conjunto de comandos que são armazenados em alguns aplicativos, como o Word e Excel, que visam diminuir as tarefas repetitivas executadas pelo usuário, como por exemplo substituir todos os "eh" por "é", em outras palavras, são rotinas personalizadas para serem feitas automaticamente pelo Word ou Excel ou qualquer programa que suporte scripts VBA (Visual Basic for Applications). O VBA é a linguagem das macros.

Utilizando macros é possível por exemplo acrescentar um cabeçalho automaticamente em um documento usando um conjunto de teclas, ou seja, é possível personalizar o processador de textos afim de otimizar o trabalho.

Todas essas facilidades chamaram a atenção de pessoas mau intencionadas que perceberam que podiam usar o scripts VBA para alterar o funcionamento normal dos aplicativos que suportem esses scripts, em especial o Word e Excel. Surgindo a parti daí os vírus de Macro.

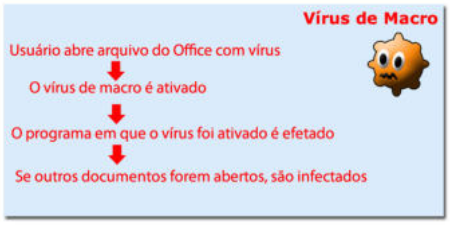


**Figura 03.3: como um vírus de macro pode ser ativado**

Os vírus de macro só funcionam dentro dos programas aos quais estão ligados, dessa forma, atacam exclusivamente documentos do Microsoft Office.

Para que  o vírus de macro contaminem outros documentos, este deve ser aberto. Geralmente o que o vírus de macro gostam de fazer é bagunçar os menus do Word.

O grande problema é que isso pode ser feito de forma simples. Só para se ter uma idéia, você pode ver quais menus do Word podem ser modificados através de scripts VBA:

1. Abra o aplicativo Word;
2. Pressione Alt+F8 para abrir a janela Macro;

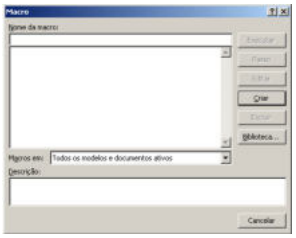

**Figura 03.4: janela Macro.**

3. Na caixa *Listagem de macros* escolha Comandos do Word.

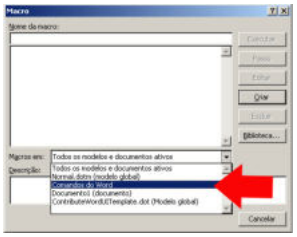

**Figura 03.5: escolha Comandos do Word.**

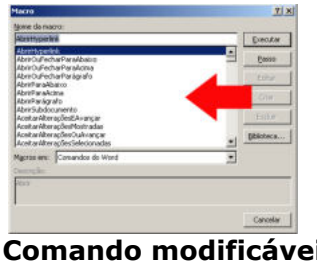

**Figura 3.6: Comando modificáveis do Word**

Para modificar qualquer comando, faça o seguinte:

1 - Na caixa *Listagem de macros* escolha Comandos do Word, como já foi dito;

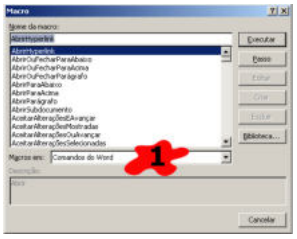


**Figura 03.7: escolha Comandos do Word.**

2 – Escolha o comando desejado na lista;

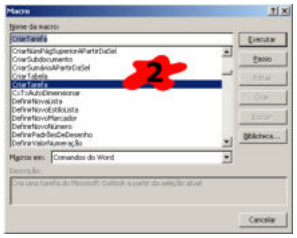


**Figura 03.8: escolha do comando.**

3 - Mude a categoria (na caixa de listagem) para o nome do documento em que será aplicada a macro;

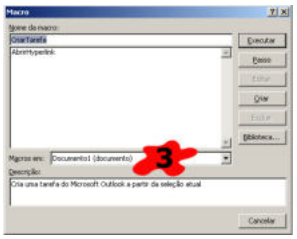


**Figura 03.9: escolha do documento.**

4 - Clique no botão Criar;

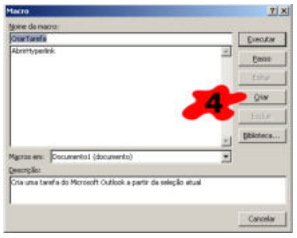


**Figura 03.10: clique no botão Criar.**

O editor do Visual Basic será aberto e com pouca linhas de códigos o comando pode ser mudado. Pode-se por exemplo redirecionar os comandos para exibir mensagens, ao invés de executar a rotina padrão do software.

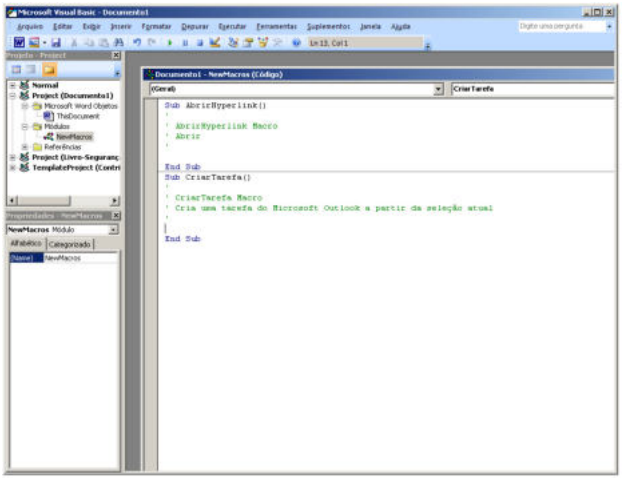

**Figura 03.11: a janela do Microsoft Visual Basic será aberta. Você deverá conhecer Visual Basic para trabalhar nessa janela.**

Comandos importante, como copiar texto ou formatar fonte (além de vários outros) podem ser mudados. E um detalhe é que os atalhos (Ctrl+C) também serão afetados.

A barra de ferramentas também pode ser mudada. Isso é conseguido através do *número ID* que identifica cada nome da barra de ferramentas, ou seja, cada nome (ou botão) que vemos na barra de ferramentas do Word tem um número que se trata da identificação "Visual Basic" correspondente.

Uma vez com posse desses números, é possível gerar instruções (macros) que podem por exemplo, desabilitar um determinado botão.

E para conseguir essas IDs não é necessário fazer nenhuma "mágica" e basta, seguir os passo a seguir:

1 - Abra o Word e acesse o Editor do Visual Basic (pressione Alt+F11);

2 - À esquerda no editor haverá janela escrito *Project* (visualizador de projetos).

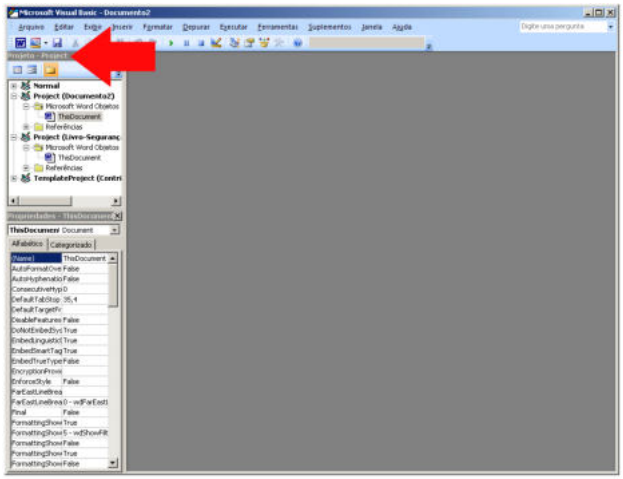

**Figura 03.12: Editor do Visual Basic – opção *Project.***

3 - Clique com o botão direito do mouse em uma área vazia dessa janela, e clique em *Inserir – Módulo*;

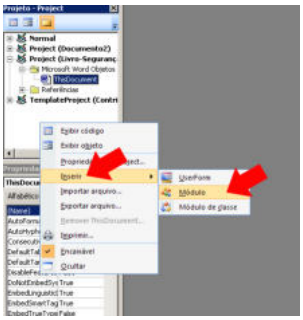

**Figura 03.13: Inserir Módulo.**

4 – Um módulo em branco será aberto;

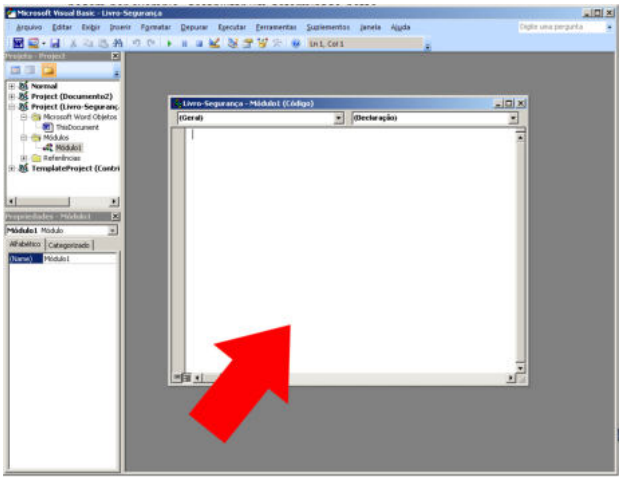

**Figura 03.14: Módulo em branco.**

5 - Para prosseguir, digite os códigos a seguir:

```
Sub ExibeBarraDeFerramentas()
Dim i As Integer
Dim j As Integer
Word.Documents.Add
For i = 1 To Word.CommandBars.Count
Selection.TypeText Word.CommandBars(i).Name & vbCrLf
For j = 1 To Word.CommandBars(i).Controls.Count
Selection.TypeText " ID= " & Word.CommandBars(i).Controls(j).ID & " --- " & "
Texto = " _
& Word.CommandBars(i).Controls(j).Caption & vbCrLf
Next j
Selection.TypeParagraph
Selection.TypeParagraph
Next i
End Sub
```

Observação: script extraído do livro Dossiê vírus – RENAN DE LIMA LIRA.

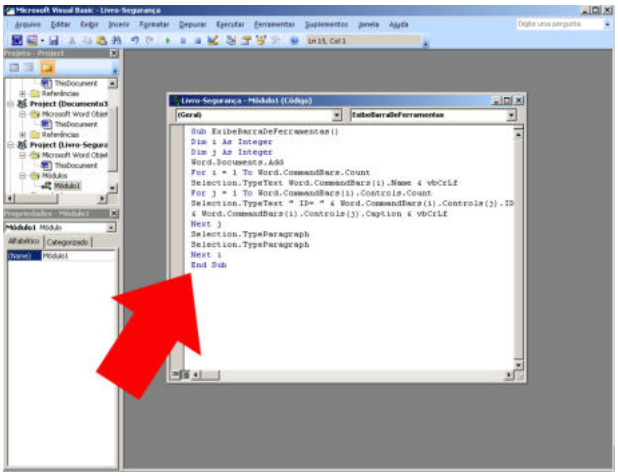

**Figura 03.15: código digitado.**

6 - Ao terminar clique no botão *Executar Sub/User/Form* (ou simplesmente pressione a tecla F5) do Editor;

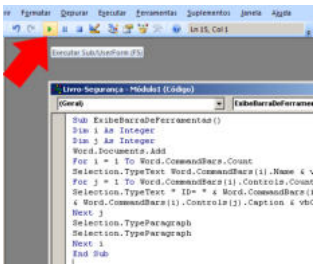

**Figura 03.16: botão Executar Sub/User/Form.**

7 - Será criado um novo documento do Word contendo uma lista com todas as barras de ferramentas e todos os botões do Word e seus respectivos IDs

Veja na lista a seguir alguns IDs gerados no Worn 2007. No nosso teste foi gerado um documento com mais de 80 páginas. Por isso, aqui dispomos apenas alguns IDs:

*Standard*
*ID= 2520 --- Texto = Novo documento em &branco*
*ID= 23 --- Texto = &Abrir...*
*ID= 3 --- Texto = &Salvar*
*ID= 9004 --- Texto = Permissão (Acesso Irrestrito)*
*ID= 3738 --- Texto = Destinatário do e&mail*
*ID= 2521 --- Texto = &Imprimir*
*ID= 109 --- Texto = Visualização de I&mpressão*
*ID= 2566 --- Texto = &Ortografia e Gramática...*
*ID= 7343 --- Texto = Pes&quisar...*
*ID= 21 --- Texto = R&ecortar*
*ID= 19 --- Texto = Copi&ar*
*ID= 22 --- Texto = C&olar*
*ID= 108 --- Texto = &Formatar Pincel*
*ID= 128 --- Texto = VBA-Selection.TypeText*
*ID= 129 --- Texto = Não é Possível &Refazer*
*ID= 9404 --- Texto = Inserir &Anotações à Tinta*

*ID= 1576 --- Texto = Hiperlin&k...*
*ID= 916 --- Texto = Barra de ferramentas &Tabelas e bordas*
*ID= 333 --- Texto = &Inserir tabela...*
*ID= 142 --- Texto = &Inserir Planilha do Excel*
*ID= 9 --- Texto = Co&lunas...*
*ID= 204 --- Texto = &Desenho*
*ID= 1714 --- Texto = Mapa do &Documento*
*ID= 119 --- Texto = &Mostrar Tudo*
*ID= 1733 --- Texto = &Zoom:*
*ID= 984 --- Texto = Aj&uda do Microsoft Office Word*
*ID= 7226 --- Texto = Le&r*

*Formatting*
*ID= 5757 --- Texto = Est&ilos...*
*ID= 1732 --- Texto = &Estilo:*
*ID= 1728 --- Texto = &Fonte:*
*ID= 1731 --- Texto = Taman&ho da Fonte:*
*ID= 3659 --- Texto = &Idioma do teclado*
*ID= 113 --- Texto = Ne&grito*
*ID= 114 --- Texto = &Itálico*
*ID= 115 --- Texto = S&ublinhado*
*ID= 120 --- Texto = Alinhar à &Esquerda*
*ID= 122 --- Texto = &Centralizar*
*ID= 121 --- Texto = A&linhar à Direita*
*ID= 123 --- Texto = &Justificar*
*ID= 2792 --- Texto = &Distribuído*
*ID= 5734 --- Texto = &Espaçamento entre linhas*
*ID= 1846 --- Texto = Da &Esquerda para a Direita*
*ID= 1847 --- Texto = Da Di&reita para a Esquerda*
*ID= 11 --- Texto = &Numeração*
*ID= 12 --- Texto = &Marcadores*
*ID= 3473 --- Texto = &Diminuir recuo*
*ID= 3472 --- Texto = &Aumentar recuo*
*ID= 203 --- Texto = &Bordas*
*ID= 340 --- Texto = &Realce*
*ID= 401 --- Texto = Cor d&a fonte*

*Tables and Borders*
*ID= 2059 --- Texto = De&senhar Tabela*
*ID= 2060 --- Texto = &Borracha*
*ID= 1724 --- Texto = &Estilo de Borda*
*ID= 2622 --- Texto = &Largura da Borda*
*ID= 2628 --- Texto = &Cor da Borda*
*ID= 203 --- Texto = &Bordas*
*ID= 2947 --- Texto = &Cor do Sombreamento*
*ID= 3693 --- Texto = &Inserir tabela*
*ID= 798 --- Texto = Mesclar Cél&ulas*
*ID= 800 --- Texto = Divi&dir Células...*
*ID= 30461 --- Texto = &Alinhamento de célula*
*ID= 2068 --- Texto = Distri&buir Linhas Uniformemente*

*ID= 2067 --- Texto = Distribuir Colu&nas Uniformemente*
*ID= 2872 --- Texto = &Alterar Direção do Texto*
*ID= 3157 --- Texto = &Classificação crescente*
*ID= 3158 --- Texto = Classificação &decrescente*
*ID= 226 --- Texto = &AutoSoma*

*Database*
*ID= 3272 --- Texto = &Formulário de dados*
*ID= 3124 --- Texto = &Gerenciar campos*
*ID= 213 --- Texto = &Adicionar registro*
*ID= 214 --- Texto = &Excluir registro*
*ID= 3157 --- Texto = &Classificação crescente*
*ID= 3158 --- Texto = Classificação &decrescente*
*ID= 216 --- Texto = &Banco de dados...*
*ID= 215 --- Texto = &Atualizar campo*
*ID= 183 --- Texto = &Localizar no campo*
*ID= 244 --- Texto = &Documento principal*

*Drawing*
*ID= 31333 --- Texto = &Desenhar*
*ID= 182 --- Texto = &Selecionar Objetos*
*ID= 30177 --- Texto = Aut&oFormas*
*ID= 130 --- Texto = &Linha*
*ID= 243 --- Texto = &Seta*
*ID= 1111 --- Texto = &Retângulo*
*ID= 1119 --- Texto = &Elipse*
*ID= 139 --- Texto = &Caixa de Texto*
*ID= 318 --- Texto = Desenhar Caixa de Texto &Vertical*
*ID= 1031 --- Texto = WordArt&...*
*ID= 1032 --- Texto = Diagrama&...*
*ID= 682 --- Texto = &Clip-art...*
*ID= 2619 --- Texto = &Imagem...*
*ID= 9405 --- Texto = &Desenho e Texto à Tinta*
*ID= 1691 --- Texto = Cor do &Preenchimento*
*ID= 1692 --- Texto = Cor da &Linha*
*ID= 401 --- Texto = Cor d&a fonte*
*ID= 692 --- Texto = &Estilo da linha*
*ID= 693 --- Texto = &Estilo do tracejado*
*ID= 694 --- Texto = &Estilo da seta*
*ID= 394 --- Texto = Estilo de &sombra*
*ID= 339 --- Texto = Estilo &3D*

*Forms*
*ID= 219 --- Texto = Caixa de &Edição*
*ID= 220 --- Texto = Caixa de &Seleção*
*ID= 221 --- Texto = Caixa de &Combinação*
*ID= 1607 --- Texto = &Propriedades*
*ID= 2059 --- Texto = De&senhar Tabela*
*ID= 333 --- Texto = &Inserir tabela...*
*ID= 3174 --- Texto = Q&uadro*

*ID= 223 --- Texto = &Mostrar sombreamento do campo*
*ID= 6678 --- Texto = &Redefinir campos de formulário*
*ID= 225 --- Texto = &Proteger Formulário*

*Full Screen*
*ID= 178 --- Texto = Fechar &tela inteira*

*Edit Picture*
*ID= 299 --- Texto = &Ajustar margens*
*ID= 922 --- Texto = Fec&har Imagem*

*Visual Basic*
*ID= 186 --- Texto = &Macros...*
*ID= 184 --- Texto = &Gravar Nova Macro...*
*ID= 3627 --- Texto = &Segurança...*
*ID= 1695 --- Texto = E&ditor do Visual Basic*
*ID= 548 --- Texto = Caixa de Ferramentas de C&ontrole*
*ID= 1605 --- Texto = Modo de &Design*

*Stop Recording*
*ID= 2186 --- Texto = &Parar gravação*
*ID= 185 --- Texto = &Pausar Gravação*

*Mail Merge*
*ID= 6926 --- Texto = Configuração do documento pri&ncipal*
*ID= 2246 --- Texto = &Abrir fonte de dados*
*ID= 6349 --- Texto = &Destinatários da Mala Direta*
*ID= 6346 --- Texto = &Inserir Bloco de Endereço*
*ID= 6347 --- Texto = &Inserir Linha de Saudação*
*ID= 6348 --- Texto = &Inserir Campos de Mesclagem*
*ID= 30077 --- Texto = Inserir campo do Word*
*ID= 163 --- Texto = &Mostrar Campos/Valores*
*ID= 6069 --- Texto = &Realçar Campos de Mesclagem*
*ID= 6345 --- Texto = &Coincidir Campos*
*ID= 6693 --- Texto = &Divulgar Etiquetas*
*ID= 154 --- Texto = &Primeiro*
*ID= 155 --- Texto = Ante&rior*
*ID= 1730 --- Texto = &Gravar:*
*ID= 156 --- Texto = Pró&ximo*
*ID= 157 --- Texto = Ú&ltimo*
*ID= 6539 --- Texto = &Localizar Entrada*
*ID= 161 --- Texto = Verificação de &Erros na Mesclagem*
*ID= 159 --- Texto = &Mesclar ao Documento*
*ID= 160 --- Texto = &Mesclar para Impressora*
*ID= 5908 --- Texto = &Mesclar para Email*
*ID= 5909 --- Texto = &Mesclar para Fax*

*Master Document*

*Microsoft*
*ID= 263 --- Texto = Microsoft &Excel*
*ID= 267 --- Texto = Microsoft Office &PowerPoint*
*ID= 6225 --- Texto = &Microsoft Outlook*
*ID= 264 --- Texto = Microsoft &Access*
*ID= 266 --- Texto = Microsoft Visual &FoxPro*
*ID= 269 --- Texto = Microsoft P&roject*
*ID= 265 --- Texto = &Microsoft Schedule+*
*ID= 268 --- Texto = Microsoft Pu&blisher*

Qualquer pessoa com um pouco de experiência em criar macros, que conheça as linhas de códigos, e que tenha posse dos IDs, pode fazer coisas como alterar as funções dos botões e/ou menus, remover os menus da barra de tarefa, etc.

Isso é conseguido usando o número do controle (exemplo: 798) e poucas linhas de código.

Vejamos um exemplo:

```
Sub DeletaVBE()
    Word.CommandBars("Visual Basic").FindControl(, 798).Delete
End Sub
```

Essa macro usa o comando Delete para excluir o controle 798, removendo-o da barra de ferramentas.

Observação: script extraído do livro Dossiê vírus - RENAN DE LIMA LIRA.

Alguns vírus de macro usam exatamente essa técnica para se tornar invisível (stealth), onde eles apagam todos os menus da barra de ferramentas que poderiam exibir o seu código, como por exemplo apagando o menu que abre o editor do Visual Basic.

Isso pode complicar a vida de muitos, uma vez que alguns vírus de macro devem ser apagados manualmente de um computador contaminado.

Além disso, se o vírus for executado, ele poderá contaminar o arquivo normal.dot (modelo geral de arquivos do Word), e a partir desse ponto todos o outros arquivos que forem abertos passarão a ser contaminados.

Aí vem aquela dúvida: vírus de macro pode iniciar automaticamente, sem a intervenção do usuário? Sim. A resposta é tão direta que talvez até assunta. Os vírus de macro podem ser iniciados automaticamente graças as Automacros, que são macros que iniciam automaticamente em determinadas circunstâncias. As principais são:

- AutoExec: Executada quando iniciamos o Word;
- AutoNew: Executada quando criamos um novo documento no Word;
- AutoOpen: Executada quando abrimos um documento;
- AutoClose: Executada quando fechamos um documento;

- AutoExit: Executada quando saímos do Word.

Usando-se dessas automacros, surgem vírus que são ativados de várias formas, dependendo apenas das ações do usuário.

Por isso que a simples abertura de um documento Word pode ativar o vírus de macro. Neste caso o vírus estaria usando por exemplo o módulo AutoOpen(), que abriria algum rotina.

# Capítulo 04 – Contra ataque : Eliminando Vírus

**Sintomas**

Os sintomas de um computador com vírus de  macro são típicos: a começar pela exibição de uma janela avisando sobre a presença de macros sempre que iniciamos um arquivo (caso a proteção contra vírus de macro esteja ativada).

Menus e botões faltando, imprimindo caracteres que não foram digitados, textos sendo apagados sem comando do usuário entre outros.

**Como proteger o computador de vírus de Macro**

As versões atuais do Office possuem um recurso chamado "Central de Confiabilidade", que possui configurações de segurança e privacidade.

Nessa Central podemos alterar as configurações de macro. Quando alteramos as configurações na Central de Confiabilidade, as modificações valem apenas para o programa em questão. Isso significa se alteramos as configurações no Word, as alterações na valem para o Excel, PowerPoint ou Access.

Vejamos como acessar a Central de Confiabilidade no Microsoft Word 2007 (pode ser feito no Word, Excel, PowerPoint ou Access):

1 – Clique no botão Office. É o botão redondo que fica no canto superior esquerdo;

**Figura 04.1: botão Office.**

2 – Clique em opções do Word;

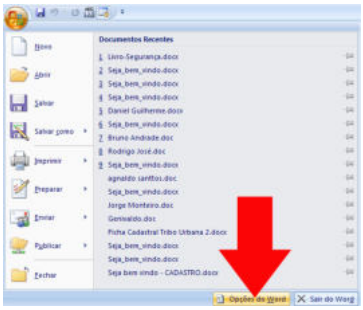

**Figura 04.2: botão opções do Word.**

3 – Na janela que se abre, clique em Central de Confiabilidade;

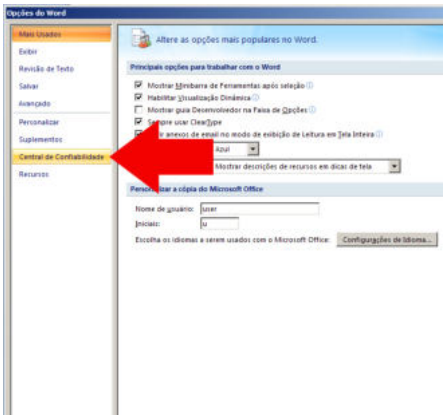


**Figura 04.3: botão Central de Confiabilidade.**

4 – Agora clique no botão Configurações da Central de Confiabilidade;

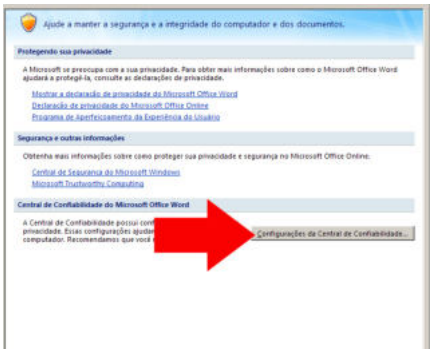


**Figura 04.4: botão Configurações da Central de Confiabilidade.**

5 – Veremos a opção Configurações de Macro onde há as seguintes opções:

5.1 - Desabilitar todas as macros sem notificação: se você não confia em macros, marque essa opção. Todas as macros existentes nos documentos são desabilitadas e não será exibido nenhuma notificação;

5.2 - Desabilitar todas as macros com notificação: Todas as macros existentes nos documentos são desabilitadas, mas, sempre que for detectado alguma macro no documento será exibido alertas.

5.3 - Desabilitar todas as macros, exceto as digitalmente assinadas: esta opção equivale à Desabilitar todas as macros com notificação. A diferença é que neste caso, quando a macro for assinada de forma digital por um editor confiável ela poderá ser executada e caso contrário você será sempre notificado;

5.4: Habilitar todas as macros: se marcar essa opção não haverá proteção. Todas as macros serão executadas, inclusive os vírus de macro caso haja algum, sem nenhuma notificação.

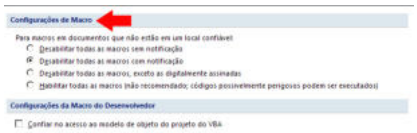


**Figura 04.5: opção Configurações de Macro.**

6 – Para que haja proteção contra vírus de macro, marque a opção Desabilitar todas as macros com notificação ou Desabilitar todas as macros, exceto as digitalmente assinadas. Caso não use macros, pode marcar inclusive a primeira opção: Desabilitar todas as macros sem notificação.


**Figura 04.6: marque uma dessas opções.**

**Como Eliminar vírus de macro manualmente**

Funciona somente com vírus mais simples. Os vírus de macro podem ser encontrados nos componentes VBA do arquivo, lá no Explorador de projetos. Quando criamos uma macro em um arquivo para nosso uso, ela vai estar lá, e quando ela não for mais necessária, podemos simplesmente exclui-la. O mesmo pode ser feito com vírus de macros simples.

1. Vá ao Editor do Visual Basic (Alt+F11);
2. Na janela do editor, à esquerda, estará o Explorador de projetos. Procure por componentes (dentro de pastas chamadas módulos) que deseja excluir. Clique com o botão direito do mouse sobre o componente, no menu que se abre, clique em Remover.

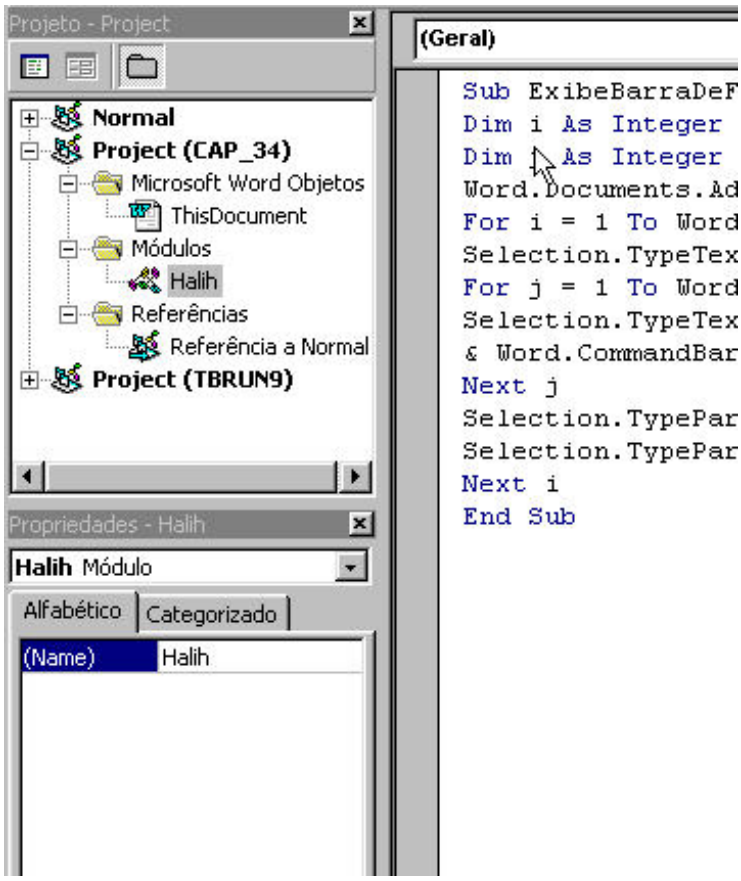


**Figura 4.7: Excluindo componentes pelo Editor do Visual Basic**

**Como eliminar seqüelas**

Os vírus de macro mesmo depois de removidos podem deixar seqüelas no Word, como menus faltando ou botões a menos.

A solução mais eficiente é instalar novamente o os aplicativos do Microsoft Office com a instalação completa. Mas ante de fazer isso, tenha a certeza que não há mais vírus de macro instalado em nenhum documento, caso contrário pode acontecer uma recontaminação.

**Prevenção**

Instale um anti-vírus e mantenha-o sempre atualizado. A freqüência com que deve ocorrer essa atualização, vai depender da freqüência com que você expõem o computador a situações que podem permitir a entrada de um vírus. Exemplo: Receber e-mails.

O ideal é que seja feita uma atualização pelo menos uma vez por semana.

Além disso é preciso tomar cuidado com arquivos anexo a e-mails e com arquivos de origem duvidosa.

**Como remover vírus de um HD contaminado**

Imagine a seguinte situação: você trabalha como técnico em manutenção de computadores e um cliente leva para sua oficina um computador contaminado por vírus.

O cliente muitas vezes não pode perder os dados que estão no disco, aí é o papel do técnico em fazer de tudo para salvar as informações que estão no disco e eliminar os vírus.

A melhor forma de livrar o computador totalmente de vírus é formatando o Disco Rígido. Mas como nem sempre isso é possível, o que resta a fazer é retirar o Disco Rígido que está contaminado do computador, instalá-lo como em outro computador e rodar um anti-virus.

Para isso siga as orientações que se seguem:

1- Prepare o seu computador: antes de instalar o HD do cliente em seu computador, certifique-se que o Anti-vírus está atualizado. Atualize-o no mesmo dia, para garantir;
2- Não deixe dados importantes em seu computador: não ponha em risco os seus próprio dados. O ideal é usar um computador de trabalho, ou seja, não use o seu computador pessoal, a não ser que você não tenha dois;
3- Configure o anti-vírus para iniciar quando ligar o computador;
4- Com seu computador desligado, instale o Disco Rígido do cliente. Se for um HD IDE ele deverá ser ligado como slave. Se for SATA, conecte-o na porta SATA2, por exemplo;
5- Ao iniciar o computador, rode o anti-vírus imediatamente.

Para resolver casos extremos:
Em alguns casos o ideal é formatar o Disco Rígido, pois, talvez o sistema operacional ficou comprometido (faltando arquivos, com erros aleatórios, etc). Neste caso:

1- Instale o Disco Rígido em seu computador;
2- Rode um anti-vírus atualizado;
3- Copie todos os Dados importantes do cliente em um CD-R ou DVD-R;
4- Formate o Disco Rígido e reinstale o sistema operacional.

**Vírus famoso**

Alguns vírus ficaram famosos (se é que podemos dizer assim) pelo seus atos, se tornando vírus perigosos, que tiveram uma disseminação muito rápida.

O ideal é que essas pragas digitais nunca tivessem existidos, como infelizmente isso não foi possível, veremos resumidamente como dois deles agiram: o Melissa e o Chernobyl.

**Messila**

O Melissa chegou aos computadores das vítimas através de um trojan dentro de uma macro do Word, chamada Document_Open, que é executada automaticamente quando um documento é aberto.

Assim que executada, a primeira ação do vírus era desabilitar os recursos de segurança de macro (isso faz com que qualquer outra macro seja executada sem a notificação do usuário).

Em seguida o Melissa trata de garantir a sua replicação usando o address book do MS Outlook e enviando uma cópia de si mesma para os 50 primeiros nomes em cada lista de endereços encontrados.

Para garantir que os E-mails sejam abertos, o melissa coloca o nome do usuário retirado do Outlook e colocava no corpo da mensagem a frase:

Here is the document you asked for .. don´t show anyone else.

Nas próximas etapas o Melissa tentava contaminar outros documentos do Word no computador da vítima se propagando cada vez mais, através de documentos e e-mails criados pelo próprio usuário. Isso vez com que ele se alastrasse rapidamente pela internet.

**Chernobyl**

O chernobyl é um vírus polifórmico e encriptografado, residente da memória RAM e que infecta arquivos executáveis.

Ele era disparado por data, ou seja, em uma determinada data ele entra em ação.

É um vírus perigoso que dependendo da versão ataca no dia 26 de qualquer mês (ou apenas em meses específicos). Geralmente a forma de ataque é a seguinte:

1. Ele apaga o primeiro megabyte de informações da principal unidade de disco rígido, o que causa perda completa das informações no Disco Rígido;
2. Tenta reescrever a gravação da BIOS. Quando ele consegue, o computador fica temporariamente inutilizável.

# Capítulo 05 – Segurança: todos devemos ter

**Essencial saber**

Nas páginas anteriores deste livro tivemos um importante embasamento sobre vírus, onde podemos constatar os principais tipos de vírus que podem contaminar um computador, desde os *pseudos vírus* aos mais perigosos *worms*.

Vimos também que os vírus podem ser construídos de forma simples, muita vezes até "bobas" usando técnicas nem um pouco tecnológica mas que se o usuário não estiver preparado, principalmente se o usuário estiver mau informado, poderá perder dados, entre outros problemas e chateações.

Vimos também que muitos vírus são mais perigosos, onde usam técnicas de propagação pela rede e até pelos e-mail, se replicam, instalam trojans entre outras coisas.

Então de nada adianta dizer: "isso nunca irá acontecer comigo", "o meu computador nunca irá pegar vírus", o "meu computador nunca será invadido", etc.

O que deve ser feito é tomarmos algumas medidas simples, que na maioria das vezes são eficazes.

A partir deste ponto deste livro estaremos vendo como se proteger de vírus e hackers, quais os reais riscos, as medidas de segurança elementares que podemos aplicar em nossos computadores, etc.

Vamos conhecer um modelo de segurança que visa:

- Trabalhar com segurança física e lógica;
- Conhecer os principais tipos de vírus e combaté-los com antí-vírus;
- Preservar a privacidade do usuário e a segurança dos dados usando firewalls e anti-trojans;
- Cultivar atitudes seguras, o que inclui: conscientização do uso correto de senhas, e-mail, identificação de sites seguros e por fim identificação de informações idôneas.

**O que é segurança**

Podemos definir a segurança como a restrição dos recursos de um computador para um ou um grupo usuários definidos e a proteção dos dados.

Temos a segurança quando haver a gestão de tais restrições, constituindo assim uma *política de segurança*.

Não adianta usar os melhores softwares e hardwares se haver falhas humanas, se as pessoas não souberem gerenciar tais recursos. Isso nos leva a concluir que segurança é antes de tudo uma questão humana e não técnica.

Os elementos que compõem a segurança lógica são:

- Integridade: evitar problemas causados por vírus (pois eles podem apagar dados, abrir brechas para um invasor, etc;
- confidencialidade: as informações estão disponíveis somente ao usuário devidamente autorizado;
- Disponibilidade: os recursos estão disponíveis sempre que necessário.

O computador não está protegido ou há falhas na segurança quando:

- É contaminado por vírus. São instalados aplicativos não autorizados;
- Informações são acessadas/lidas/copiadas por pessoas não autorizada, seja remotamente ou não;
- Informações são alteradas por pessoas não autorizada;

A segurança não se limita somente ao meio lógico, ela é dividida em: *segurança lógica* e *segurança física*.

De nada adianta instalar em um computador o melhor sistema de segurança no sistema operacional, se alguém não autorizada conseguir sentar na frente do computador e obter acesso as informações.

Todos os usuários (ou pelo menos grande partes deles) cuidam da segurança física do computador, muita vezes sem perceber que a faz. Por exemplo: com a instalação de *nobreaks*, evitando colocar o computador em locais onde há risco de queda de objetos sobre o mesmo (debaixo de prateleiras), etc.

**Segurança física**

Há segurança física quando:

- O acesso ao computador é restringindo (e controlado) a um grupo pessoas;
- É garantida o funcionamento do computador durante um determinado tempo caso ocorra queda de energia elétrica (através de nobreaks);
- É tomada todas as precauções para que problemas na rede elétricos ( excesso de tensão, tensão insuficiente ou ruídos), relacionados a fenômenos da natureza (raios) ou curtos circuitos na rede não interfiram no funcionamento do computador. Isso é feito com filtros de linhas, estabilizadores e nobreaks.
- A instalação do computador é feita em locais apropriados (onde não há risco de queda de objetos sobre o PC, onde não há infiltrações de água, etc) em tomadas apropriadas e com uso de aterramento.
- A entrada e saída dispositivos de armazenamento (disquetes, CDs, DVDs, Pen Drives, etc.) é controlado.

A segurança física em determinadas empresas é mais importante que a segurança lógica. Um grande exemplo disso, e que todos nós já estamos acostumados a ver, são em lojas de suprimentos para informática. É claro que em casos como esse, a segurança física conta com muito mais recursos, incluindo: serviços de guarda, treinamento adequado dos funcionários, instalação de câmaras, etc.

Devemos estar atentos quanto a segurança física do computador, com atenção à instalação de filtros de linha, nobreak, uso de tomadas adequadas (o que evita possíveis curto circuitos) etc.

São importantes práticas: instalação de tomadas adequadas, aterramentos, ventilação de ambientes, proteção e eliminação de poeiras, mesas ideais e umidade (entre outros). Tudo isso faz parte da segurança física do computador.

**Segurança lógica**

Ela visa a proteção dos dados de um computador para que não sejam apagados ou copiados dados indevidamente, para que o sistema esteja sempre acessível quando necessário, etc.

Com um bom trabalho de segurança lógica iremos obter os seguintes benefícios:

- Evitar que um computador seja invadido localmente ou em rede;
- Impedir que informações sejam roubadas;

- Manter a integridade dos dados;
- Evitar vírus e suas variações;
- Manter o sistema operacional e demais programas funcionando sem problemas;
- Entre muitos outros.

**Quais os reais riscos?**

Esse tipo de dúvida é muito comum: quais os reais riscos? Os ricos reais são os vírus que podem chegar através de anexos de e-mails, vírus disfarçados de programas benignos (trojans) baixados pelo próprio usuário em sites desconhecidos, boatos (que induzam o usuário a apagar algum arquivo, por exemplo) e o acesso ao sistema por pessoas não autorizadas (exemplo: hackers).

Mas é preciso esclarecer que os computadores domésticos são de longe, muito mais atacados por vírus do que por hackers.

O que pode levar um hacker a invadir um computador doméstico é quando o usuário instala (sem saber que fez isso) um trojan.

Em outras palavras, o usuário é quem facilitou a entrada do hacker. Logicamente um hacker pode tentar invadir um computador de outras formas que não seja usando um vírus, o que nesse caso, pode não ser tão simples se o sistema estiver com todas as atualizações.

Dessa forma, os principais riscos que afetam um computador doméstico são:

- **Vírus:** de todos os tipos. Podem apagar, modificar ou corromper dados. Podem permitir a entrada de um hacker;
- **Boatos:** Apesar de parecer ridículo, pode acontecer do usuário receber uma mensagem com textos do tipo "pior vírus do mundo", pedido para o usuário deletar um arquivo específico o mais rápido possível, pois trata-se de um vírus capaz das piores "malvadezas" que se possa imaginar. Nesse item se encaixa também informações provenientes de sites não confiáveis;
- **Hackers:** Como dissemos anteriormente, os hackers representam um risco menor do que os próprios vírus aos computadores domésticos. Se os hackers atacassem os computadores na mesma proporção que os vírus os contaminam, seria o mesmo que dizer que praticamente todos os computadores que acessam internet estão sendo invadidos por hackers, o que não acontece. Ressaltamos também que nem sempre uma pessoa que obtém acesso (seja remotamente ou não) não autorizado a um computador, será um hacker. Por isso é preciso sempre se prevenir. Se um hacker invadir um computador, ele pode roubar dados sigilos do mesmo, instalar vírus, apagar dados, ou na pior das hipóteses, iniciar um ataque a parti do computador invadido.

**Por que se preocupar com segurança?**

Para proteger nossas informações confidenciais. Imagine se uma fotografia pessoal, ou uma carta escrita para alguém, ou até mesmo um livro como este, seja copiado por uma pessoa não autorizada.

E pior, imagine se essa pessoa coloque o que ele pegou disponível na Internet. Para evitar isso é preciso segurança.

Com certeza você já fez alguma comprar pela internet (ou conhece alguém que fez). Durante essa compra foi digitado o número do CPF, endereço, telefone, e talvez até o número do cartão de crédito. É preciso haver segurança para que transações desse tipo possam ocorrer sem problemas.

É preciso haver segurança para que pessoas não autorizadas não usem a sua conta de acesso à internet. É preciso haver segurança para que pessoas não autorizadas não acessem aos seus e-mail. É preciso segurança para que pessoas não autorizadas não acessem o seu computador.

A integridade das informações contidas em um computador depende do quão seguro ele é.

Além disso, um ponto importante a saber: em uma rede doméstica, todos os computadores devem estar protegidos. Se apenas um deles estiver desprotegidos, o esquema de segurança está deficiente, pois, possui um ponto vulnerável. E à partir deste ponto vírus podem se propagar, hackers podem iniciar ataques, o que irá comprometer a integridade das informações que circulam pela empresa.

Além disso, como dissemos, a segurança não se restringe somente aos dados. A segurança é necessária para que nas lojas não haja furtos e para que os equipamentos que lá estão não sejam danificados. E tudo isso vale plenamente para qualquer Computador pessoal.

**Segurança mínima**

As regras para manter um mínimo de segurança possível são:

1. Tenha sempre um anti-vírus atualizado instalado no computador. Não adianta instalar um antí-vírus e não atualizá-lo com freqüência, pois, novos vírus surgem a todo momento. A tabela a seguir contém o endereço eletrônico de alguns anti-vírus:

| **Anti-vírus** | **Endereço eletrônico** |
|---|---|
| Norton Anti-Vírus | http://www.symantec.com/ |
| Mcafee Visruscan | http://mcafee.com/ |
| Panda Anti-Vírus | http://www.pandasoftware.com/ |
| Kapersky Anti-Vírus | http://www.kapersky.com/ |
| AVG Anti-Vírus | http://www.grisoft.com/ |
| AntiVir Personal Edition | http://www.free-av.com/ |

| | |
|---|---|
| Avast! Home edition | http://www.avast.com/ |
| Bit Defender free | http://www.bitdefender.com/ |

2. Use um Firewall, que é um programa que auxilia na proteção das informações contidas em um computador. Através do firewall é possível bloquear tentativas de instruções (como a tentativa de instalar ou apagar algum arquivo) bem como o tráfego não autorizados no computador. A tabela a seguir contém o endereço eletrônico de alguns Firewall:

| Firewall | **Endereço eletrônico** |
|---|---|
| Norton Personal Firewall | http://www.symantec.com/ |
| Mcafee Personal Firewall | http://mcafee.com/ |
| Tiny Personal Firewall | http://tinysoftware.com/ |
| Zone Alarm Free | http://www.zonelabs.com/ |
| Outpost Firewall | http://www.agnitum.com/ |
| Sygate Personal Firewall | http://www.sygate.com/ |

3. Use um programa Anti-trojans. Os trojans, como sabemos, são um tipo de vírus que podem entre outras coisas, copiar o que se está digitando no teclado. A tabela a seguir contém o endereço eletrônico de alguns Anti-trojans:

| Anti-trojans | **Endereço eletrônico** |
|---|---|
| Ad-Aware SE Personal Edition | http://www.lavasoft.com/ |
| Trojan Guarder | http://www.anti-viruses.net/ |
| PestPatrol | http://www.pestpatrol.com/ |
| Trojan Remover | http://www.simplysup.com/ |
| Anti-Trojan Shield | http://www.atshield.com/ |
| Microsoft Windows Antispyware 2005 Beta | http://www.microsoft.com/ |
| TDS: Trojan Defense Suite | http://tds.diamondcs.com.au/ |
| The Cleaner | http://www.moosoft.com/ |

Além disso é necessário fazer uso correto de senhas, atualizar constantemente os programas e o sistema operacional através de *Patches* do fabricantes e ficar sempre alerta com os conteúdos que chegam através de e-mails, principalmente no anexos.

Os *Patches* são arquivos para aplicar correções, atualizações de seguranças, entre outras coisas, em sistemas operacionais e programas. Quando um fabricante de um determinado software disponibiliza *Patches,* significa que o objetivo é exatamente esse: aplicar ao software alguma atualização que irá melhorar e/ou corrigir algo, seja na segurança, corrigindo bugs ou simplesmente atualizado.

**Senhas**

Neste tópico vamos falar de um dos principais pontos em se tratando de segurança de computadores pessoais, que são as senhas.

Existem diversas técnicas para se descobrir senhas de acesso (tais como senhas de acesso à conta de e-mails ou FTP), tais como:

- **Brute force:** são softwares programados para testar senhas até descobrir uma que dê acesso. Esses softwares podem testar milhares de senhas por hora (depende da velocidade de conexão do invasor). É um método que pode ser barrado, pois, muitos sistemas atuais bloqueiam o acesso do usuário se ele errar a senha por mais de três vezes seguidas;

- **Uso de listas de palavras chaves:** também usa-se softwares para essa finalidade, porém, ao invés dele ficar gerando as senhas, usa-se uma lista de palavras pré-selecionadas;

- **Vírus:** worms ou trojans, por exemplo, podem capturar o que você digitar no teclado e enviar isso para o seu criador;

- **Por adivinhação:** o invasor irá tentar adivinhar a senha. Para obter sucesso, a engenharia social poderá ser usada. Muitas fontes importantes de pesquisa para um hacker experiente são: Twiter, Orkut, blogs, etc. Por isso, muito cuidado com o que escreve em redes sociais, com seu perfil que está digitado, etc. Um exemplo típico de "um hacker" que descobriu a senha de e-mail de sua vítima, foi simplesmente lendo o seu perfil no Orkut, que tinha uma foto do Homem-Aranha. E no e-mail, a pergunta secreta para ter acesso à uma nova senha era: "Qual o seu super herói favorito?". A resposta mais do que óbvia era homem-aranha. E dessa forma, o "hacker" conseguiu a senha do e-mail. Por isso, muito cuidado (muito cuidado mesmo) com o que escreve em redes sociais, blogs e afins.

Senhas fáceis de deduzir são as principais causas com problemas na segurança. Devemos evitar a qualquer custo formular senhas tomando como base datas de nascimento, número da placa do carro, número de um telefone, nome de pessoas, etc.

Tudo isso é o que chamamos de *pistas*. Então a senha segura é aquela que não deixa nenhuma pista, não importando em que situação está sendo criado a senha:

- Para abrir E-mails;
- Para obter acesso ao computador;
- Para abrir arquivos;
- Para efetuar algum login, etc;

E ao criar senhas em sistemas (conta de e-mails, por exemplo) que lhe exigem criar uma "pergunta secreta" (que serve para te dar uma nova senha caso você se esqueça da sua senha original), não formule perguntas cuja resposta é fácil (pelo menos se pesquisarem um pouco sobre você) de descobrir.

Perguntas como "qual o nome de sua mãe", "qual sua data de nascimento", "qual o seu super herói favorito", entre outros exemplos, são fáceis de descobrir a resposta. Um hacker pode simplesmente ligar para sua casa, e poderá obter facilmente essas respostas (principalmente se quem atender o telefone for alguém mais inocente, como uma criança de dez anos por exemplo). Por isso não se pode passar quaisquer informações via telefone se você não tiver certeza absoluta de quem está lhe solicitando.

Se algum dia alguém te ligar, lhe dizendo que é do banco, dos correios, do seu provedor de internet, entre outros exemplos, e você ficar desconfiado que tem algo errado, faça o seguinte: desligue o telefone e ligue novamente para o número oficial (do banco, dos correios, do seu provedor de internet, etc) e pergunte se a entidade em questão te ligou. Se a entidade em questão te informar que não (eles não te ligaram), saiba que você quase caiu em um golpe. Mas, se "safou" porque estava preparado para lidar com esse tipo de situação.

**Como formular senhas segura**

Uma senha para ser segura deve descartar palavras óbvias (pass, abrir, password, senha, etc), em branco ou mesmo nome do login.

Nunca use: datas de nascimento, número de casa ou apartamento, número de telefones, nome da esposa ou marido, seu próprio nome ou segundo nome, apelido, nome da empresa, nome de objetos ou ferramentas com que você trabalha, sua profissão, números consecutivos (12345), nomes de personagens favoritos, time do coração, etc.

Além disso a senha não deve ser pequena (palavras com menos de seis caracteres), nunca dever ser a mesma para um grupo de usuários (cada usuário deve ter uma senha individual) e usuários não devem acessar o computador com a senha do administrador.

A senha segura é aquela formulada seguindo três regras fundamentais:

- Ela é composta por números, letras e símbolos especiais (@ # $ % * +, etc);
- Fácil de digitar, para que não seja necessário olhar para o teclado enquanto digitamos;
- Fácil de lembrar e difícil de deduzir.

Exemplo de uma boa senha: ompcsscel.

Mas como lembrar uma senhas dessas? É simples. A primeira coisa a fazer é criar uma frase que você se lembre facilmente. Pode ser um fato que aconteceu, um sonho, algo que deseja comprar, etc. Em seguida basta usar as iniciais de cada palavra.

Como exemplo da senha anterior, temos a frase:

**O**s **M**aiores **P**roblemas **C**om **S**enha **S**ão: **C**riar **E** **l**embrar

Observe que usamos as iniciais de todas as palavras, inclusive as letras "O" (os) e "E" para formar a senha ompcsscel. Mas lembre-se que tem que ser uma frase de fácil memorização, algo que será lembrado sem problemas.

Usando a mesma frase podemos chegar a uma nova senha mais segurara, veja:

**O**s **M**aiores **P**roblemas **C**om **S**enha **S**ão 2: 1- **C**riar **E** 2- **l**embrar

A senha agora ganha números em sua composição, ficando mais segura ainda: ompcss21ce2l.

E para tornar a senha ainda mais segura, você pode desenvolver uma regra particular, tipo: acrescentar o caractere "#" sempre no início de cada senha. Nesse caso a nova senha será: #ompcss21ce2l.

Não se esqueça que a senha deve ser de fácil e rápida digitação. E nunca anote senhas em um pedaço de papel.

Um ponto importante é que as palavras não podem ser muito repetidas, caso contrário podem ser facilmente descobertas através de softwares especiais usados para *brute force*. Exemplo: aaabccc. Senhas como essas são o equivalente a senha com números consecutivas.

***Senha segura = Fácil de lembrar, difícil de deduzir***

Sugestões para manter uma senha segura:

- **Cuidado ao digitar:** pessoas podem ver o que você digita;
- **Leitura labial:** não adianta ter uma boa senha se você a ler (mesmo que muito baixo, apenas mexendo com os lábios) a cada vez que a digita. Alguém que estiver perto de você pode acabar descobrindo-a apenas lendo os seus lábios;
- **Troque as senhas:** troque as senhas de período em período (a cada dois ou três meses);
- **Uma senha para cada situação:** Nunca use a mesma senha em lugares diferentes (para E-mails, documentos, etc). Se uma for descoberta, todas serão;
- Nunca passe a sua senha por telefone ou E-mail para ninguém. A senha é pessoal e intransferível.

**Vulnerabilidades**

A Vulnerabilidade nada mais é que falhas na segurança, são erros (bugs) que atingem tanto os programas instalados quanto os sistemas operacionais.

Esses bugs podem surgir na criação ou na implementação do programa/ou sistema operacional.

As patches (atualizações) lançadas pelas empresas são feitas para corrigir erros, conforme vão sendo descobertos.

O problema desses erros é que são uma porta de entrada para muitos hackers.

Normalmente há três situações que designam vulnerabilidades:

- **Disponibilidade:** esses tipos de erros podem afetar a disponibilidade do computador (tirá-lo do "ar"). Isso geralmente é feito (não é a única forma) através da negação de serviço (DdoS - Distributed Denial of Service), que ocorre quando um conjunto de computadores são utilizados para tirar do ar um ou mais computadores conectados à internet. Os computadores não são invadidos, eles apenas ficam fora do ar;

- **Acesso limitado:** é a invasão propriamente dita, ou seja, essa falhas (que podem ser de softwares ou de configurações humanas) permitem que um hacker acesse o sistema. No caso dos erros humanos, acontece por exemplo quando o administrador se esquece de trocar as senhas padrões do sistema;

- **Execução de códigos arbitrários:** são falhas que permitem que seja executado de um código arbitrário no computador;

**Qual o perigo de um sistema vulnerável?**

São uma porta de entrada para hackers, que usam programas chamados "scanners" que "varrem" a internet em busca de vulnerabilidades remotas, ou seja, em busca de computadores vulneráveis ligados na internet naquele momento.

Os scanners não são ferramentas exclusivas de hackers, são usadas também por administradores de sistemas para varrer e encontrar possíveis vulnerabilidade seja em redes, sistemas operacionais, bancos de dados entre outros.

Hackers que usam esses programas geralmente não tem um objetivo específico (e geralmente são iniciantes), nem querem tentar invadir uma empresa "x" ou o banco "y". Eles apenas vasculham a internet, usando os scanner que fornecem a eles um conjunto de máquinas que estão vulneráveis.

Esses scanners geralmente "varrem" tanto provedores que tenham conexão com fibras óticas ou a backbones rápidos, quanto computador ligados a rede telefônica através de uma grande quantidade de números telefônicos por sinais Carrier ou através de uma faixa de IPs. Exemplo: endereços entre 64.x.x.1e 64.y.y.254, o que dá 252 máquinas na internet pública.

O scanner pode ainda trabalhar com um banco de dados de Ips pré-definidos, onde quanto maior o banco de dados, maior será a probabilidade do objetivo (encontrar sistemas vulneráveis) ser alcançado.

Ao invés de procurar por vulnerabilidades remotas, o hacker pode tentar também procurar somente por uma falhas específica (e se nossos computadores não tiverem essa falha, não estarão na lista do hacker), e isso pode acontecer quando por exemplo o hacker tem uma ferramenta que foi feita para explorar uma determinada falha. Aí ele sai a procura de um computador remoto que tenham essa falha para usar a ferramenta.

**Qual a solução?**

Visite regularmente os websites das empresas de software para obter os patches de segurança e atualizações disponíveis.

**Melhore a segurança**

- Instale Patches: instale patches somente de sites oficiais (ou de sites que você já conhece);
- Instale Um anti-virus e um anti-trojan: e atualize regurlamente;
- Instale um firerwall: prefira sempre as versões completas, nunca use demos, prefira as freeware;
- Sempre alerta: Em uma rede, um alerta de vírus encontrado em um computador, vale para todos ou outros computadores, ou seja, todos devem passar por uma "limpeza geral" do sistema, para evitar que um computador recentemente descontaminado, seja contaminado novamente.

**Segurança em E-mail**

Os e-mails são as maiores porta de entrada dos vírus, dessa forma é preciso tomar muito cuidado com os arquivos anexo.

Mesmo que você esteja recebendo um e-mail de alguém conhecido é preciso tomar cuidado. Não que algum amigo seu resolveu te "sabotar", enviando vírus para você. O problema é que esse seu amigo pode nem saber que vírus estão sendo anexados aos e-mails que ele envia.

Por isso é preciso desconfiar de tudo. Comece pela mensagem que vem no corpo do e-mail. Vamos usar como exemplo a mensagem a seguir:

*Olá, a quanto tempo! Eu me mudei dai para os Estados Unidos, e faz um tempo que perdemos o contato e consegui seu email através de uma amiga sua. Vamos fazer assim, eu vou lhe mandar meu álbum de fotos se você me reconhecer, me retorna o email. Quero ver se você ainda lembra de mim. :)*

A mensagem que vem no corpo do texto de alguma forma pedirá a você que abra ao anexo. E ela é escrita de tal forma que dará a impressão que você já conhece a pessoa.

Se você receber um e-mail desse tipo de alguém que nunca viu falar e a mensagem não é de muita importância, não tenha dúvida e exclua-a.

Vale lembrar que a mensagem anterior é apenas uma em várias outras, então o texto sempre irá variar.

Um cuidado especial é quanto as mensagem em outros idiomas. Se você não sabe ler em inglês, e recebe uma mensagem com um anexo, encare da mesma forma, pois, muitos vírus que se propagam por e-mails, são de origens internacionais.

A extensão do arquivo não importa muito, pois alguns vírus tem dupla extensão, tipo um_nome_qualquer.jpg.exe. Mas o que você vê é somente um_nome_qualquer.jpg, o que pode acabar passando por despercebido.

Por isso é importante configurar o Windows para mostrar todas as extensões dos arquivos (veja isso mais adiante).

Já explicamos também sobre os hoaxes, que são os boatos que se propagam através de e-mails com intenções maldosas.

Sempre verifique a veracidade das informações que circulam na internet. Se uma dada informação diz que a Microsoft descobriu um arquivo maligno no Windows, e este deve ser apagado, verifique antes de fazer qualquer coisa, no site da Microsoft, lógico.

E nunca passe a informação para frente. É comum esse e-mail virem com frases do tipo: *POR FAVOR ENVIE ESTA MENSAGEM PARA TODOS OS CONTATOS DE SUA LISTA!!*

**Segurança em sites**

Há sites que são seguros e há sites que não são seguros. É preciso antes de tudo que o usuário do computador tenha um bom senso.

Não é em qualquer site que entrar que ele pode baixar aqueles "programinhas" que tanto procurava.

Da mesma forma não se deve levar a sério informações de qualquer site antes de averiguar a veracidade da informação.

Fazer compras pela internet é seguro, desde que você esteja em um site seguro. Para realizar compras ou qualquer tipo de transação, verifique antes a procedência do site, se realmente são instituições que dizem ser e através de informações de usuários que já compraram no site.

A seguir listamos importantes dicas para garantir segurança em sites:

1. Identifique o endereço físico da empresa, seus dados cadastrais, como CNPJ, telefone, etc. você pode fazer isso acessando www.registro.br;
2. Muitos sites são realmente seguros (como os sites de bancos), mas sempre certifique-se de estar no endereço eletrônico correto. O endereço pode conter pequenas modificações;
3. O sufixo do domínio é importante. Através dele você saberá em qual país o site está hospedado;
4. Ao comprar qualquer produto, verifique se haverá despesas de envio, prazo de entrega e se há garantia do produto em estoque. Caso haja dúvida em ter ou não o produto em estoque, envie um e-mail (ou ligue pelo telefone) antes para confirmar;

5. Verifique a política adotada pela empresa para a troca ou devoluções de produtos, a garantia;
6. Ao digitar dados pessoais como RG, CPF, entre outros, verifique se você está em uma área segura (representada por um ícone de um cadeado bem na parte inferior do browser);
7. Ao confirmar a compra, sempre guarde todos os dados, inclusive o número do pedido;
8. Exija a nota fiscal;
9. Compre de preferência produtos originais;
10. Sempre certifique se o produto é novo ou usado. Em sites de compra e venda, é comum haver muitos produtos usados. Nesse caso, sempre pergunte (através de e-mails ou outros formas permitidas no site) sobre a conservação do produto.

Dicas específicas para sites de compra e venda:

1. O produto é novo ou usado?
2. Qual o estado de conservação do produto?
3. Verifique as qualificações (atributos, comentários) do vendedor (se você for comprador) ou do comprador (se você for vendedor). Verifique quantos pontos positivos e negativos ele tem. Verifique a quanto tempo ele é cadastrado no site;
4. O produto é original? Em casos de CDs e DVDs, verifique se é gravação caseira (feita pelo próprio vendedor);
5. Por fim, verifique o preço (sempre compare antes, faça uma pesquisa no próprio site), formas de pagamento, prazo de entrega e garantia.

**O sufixo é importante**

O Sufixo encontrado no final de cada endereço eletrônico nos dá importantes dicas do tipo de site e em qual país o mesmo está hospedado.

| **Sufixos** | **Significado** |
|---|---|
| COM | Empresas comerciais |
| EDU | Instituições educacionais (escolas e universidades) |
| GOV | Entidade do governo |
| INT | Instituições internacionais, como a OTAN |
| MIL | Instalações militares |
| NET | ***Companhias ou organizações que administram grandes redes*** |
| ORG | Organizações sem fins lucrativos e outras que não se enquadram em nenhum dos outros casos, como as ONGs |

**Sufixo de alguns países:**

| **Sufixo** | **País** | **Sufixo** | **País** |
|---|---|---|---|
| AE | Emirados Árabes Unidos | GT | Guatemala |
| AF | Afeganistão | GW | Guiné-Bissau |
| AL | Albânia | GY | Guiana |
| AR | Argentina | HK | Hong Kong |
| AT | Áustria | HN | Honduras |
| AU | Austrália | HT | Haiti |

| | | | |
|---|---|---|---|
| AW | Aruba | HU | Hungria |
| **BE** | **Bélgica** | ID | Indonésia |
| BG | Bulgária | IE | Irlanda |
| BO | Bolívia | IL | Israel |
| BR | Brasil | IN | Índia |
| BS | Bahamas | IQ | Iraque |
| CA | Canadá | IR | Irã |
| CF | República Centro-Africana | JP | Japão |
| CH | Suíça | KP | Coréia do Norte |
| CI | Costa do Marfim | KR | Coréia do Sul |
| CL | Chile | MX | México |
| CM | Camarões | MY | Malásia |
| CN | China | MZ | Moçambique |
| CO | Colômbia | NG | Nigéria |
| CR | Costa Rica | NL | Holanda |
| CS | Tchecoslováquia | NO | Noruega |
| CU | Cuba | NZ | Nova Zelândia |
| CV | Cabo Verde | PA | Panamá |
| DE | Alemanha | PE | Peru |
| DK | Dinamarca | PT | Portugal |
| DM | Dominica | PR | Porto Rico (US) |
| DO | República Dominicana | PY | Paraguai |
| DZ | Argélia | RU | Federação Russa |
| EC | Equador | SA | Arábia Saudita |
| EG | Egito | SB | Ilhas Salomão |
| ES | Espanha | SE | Suécia |
| ET | Etiópia | TH | Tailândia |
| FI | Finlândia | TR | Turquia |
| FR | França | US | Estados Unidos |
| GR | Grécia | UY | Uruguai |

**Ajustes "finos" para Windows**

Alguns ajustes quando feitos no Windows garante uma maior privacidade das informações, individualidade e principalmente, maior segurança. Nos tópicos a seguir listamos alguns mais importantes.

**Definição de usuários no Windows 9X**

Definindo as configurações pessoais para cada usuário, fará com que ao iniciar o PC seja pedido o nome do usuário e senha, que quando digitados corretamente, as configurações pessoais como ícones da área de trabalho e do menu iniciar serão carregadas. Veja a seguir como configurar corretamente cada perfil de usuários:

1. Vá ao painel de controle. Localize e acesse o ícone *Senhas*. Na tela que se abre, clique na guia *Perfis de usuários*;
2. Na guia *Perfis de usuários*, marque a opção: *Os usuários podem personalizar suas preferências e configurações para ...*;

3. Ainda na guia *Perfis de usuários*, marque logo abaixo a opção: *Incluir menu iniciar e os grupos de programas na configuração do usuário*

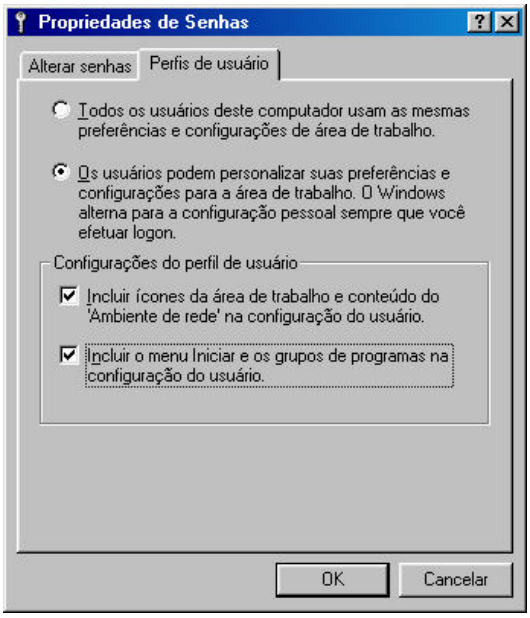


**Figura 5.1: Definindo as propriedades de senhas**

4. Clique em OK. Uma janela avisando que é necessário reiniciar o Windows para as novas configurações tenham efeito irá aparecer. Clique em não.
5. Localize  e acesse o ícone usuários. Clique em *novo usuário*.


**Figura 5.2: Criando um novo usuário**

6. Na janela novo usuário, clique em avançar. Na próxima janela, insira um nome para o usuário e clique em avançar. Na seqüência, insira uma senha para esse usuário e clique em avançar;
7. A próxima janela defini os itens que serão personalizados e a forma com que serão criados. Cada item marcado significa que será personalizado para este usuário. Por exemplo: se você selecionar o item *Menu Iniciar*, os item que aparece no menu iniciar serão personalizados. Clique em avançar para prosseguir. Para finalizar, clique em concluir e em reinicie o Windows.


**Figura 5.3: Definindo os itens personalizados**

**Cuidados com o recurso salvar senha**

Em determinadas situações em que digitamos uma senha em uma caixa, iremos encontrar uma opção denominada "salvar senha".

Esse recurso visa facilitar o trabalho do usuário, uma vez que ele não precisará digitar a senha novamente, pois, o sistema irá "memorizá-la". Sempre que ele entrar nessa caixa, a senha já estará lá (em forma de asteriscos).

O problema em marcar essa opção é que a senha estará disponível para qualquer pessoa que tenha acesso ao computador, e se for uma senha para conexão com a internet, qualquer pessoa poderá se conectar desse computador usando a mesma senha.

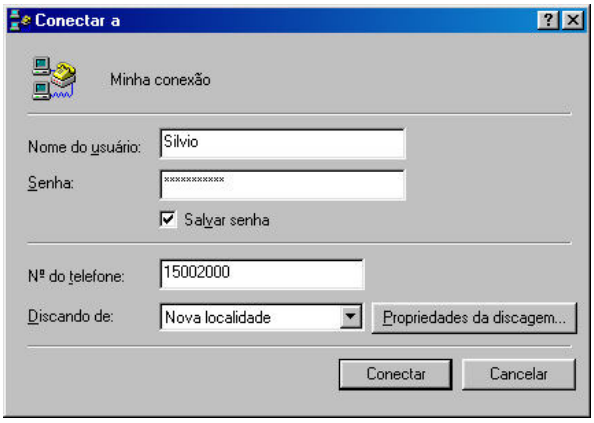


**Figura 5.4: recurso salvar senha**

O uso indiscriminado desse recurso coloca em risco a segurança do sistema, pois uma pessoa mau intencionada pode facilmente descobrir qual é senha por trás dos asteriscos.

Somente para usar como exemplo, vamos simular uma conexão com a internet usando a rede dial-up do Windows XP. A senha que iremos usar é Hjldodbet3#. Ao digitá-la, ela aparecerá somente como asteriscos (**********). Selecionando o

recurso memorizar senha, sempre que abrirmos a janela da conexão dial-up a senha já estará digitada.

Agora será que uma pessoa mau intencionada, uma vez tendo acesso físico a esse computador pode descobrir a senha por traz dos asterisco? Sim. Essa pessoa poderia por exemplo usar algum aplicativo, que ao passar o mouse sobre o asterisco, a senha é revelada.

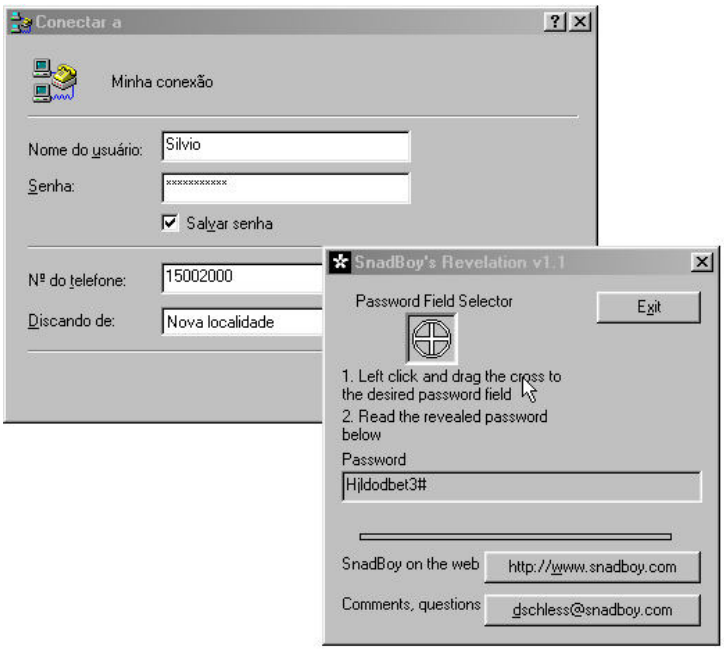


**Figura 5.5: alguns programas específicos revelam a senha por trás dos asteriscos**

### Mostrar todas as extensões

Por defaut, o Windows oculta todas as extensões dos arquivos. Para desativar esse recurso é simples, veja:

No Windows XP
1- Vá ao *Meu computador*. Na janela Meu Computador, Clique *em Ferramentas, Opções de pastas*;
2- Clique na guia *Modo de Exibição*;
3- Procure e desmarque a opção *Ocultar as extensões dos tipos de arquivos conhecidos*.

### Contas de usuários no Windows XP

Vamos usar como exemplo para dar sequencia a este livro o Windows XP simplesmente por dois motivos:

1 – Essa versão ainda é muito utilizada no mundo inteiro. E provavelmente ainda levará um bom tempo para ser totalmente "abandonada" e substituída;

2 – E é justamente a versão mais vulnerável em relação às versões lançadas mais recentemente: Windows Vista e Windows 7.

Dessa forma, vamos ao que interessa. Contas de usuário é um meio que defini as ações que um usuário pode executar em um sistema.

Em um computador autônomo ou em um computador membro de um grupo de trabalho, uma conta de usuário estabelece os privilégios atribuídos a cada usuário.

Em um computador membro de um domínio da rede, um usuário deve ser membro de, no mínimo, um grupo. As permissões e os direitos concedidos a um grupo são atribuídos a seus membros.

O sistema de contas de usuários do Windows XP são bem mais funcionais e seguros do que as versões anteriores. Temos dois tipos de contas:

- Administrador: permite ao usuário alterar as configurações do computador. Ele pode instalar programas e hardware, fazer alterações que abranjam todo o sistema, acessa e lê todos os arquivos que não sejam particulares, pode criar ou excluir outros usuários, alterar contas de outras pessoas e alterar seus próprios dados;
- Limitadas: o usuário pode mudar apenas algumas configurações, como sua imagem e senha.

**Criar um novo usuário (limitado)**

Para adicionar um novo usuário você deve ter uma conta de administrador do computador para adicionar um novo usuário;

1. Vá ao *Painel de Controle – Contas de usuário*;
2. Na janela que se abre, clique em *Criar uma Nova Conta*;
3. Dê um nome para a nova conta e clique em *avançar*;
4. Em seguida escolha o tipo de conta. Atenção: se você escolher *administrador* como tipo de conta, ele terá todos os direitos que o atual administrador tem. Se for apenas um usuário, escolha *Limitada* e clique em Criar conta;

**Criar uma senha para o novo usuário**

Da mesma forma que o administrador tem uma senha e só ele acessa com a sua conta, o usuário também pode ter uma senha:

1. Vá ao *Painel de Controle – Contas de usuário*;
2. Clique na imagem que representa o usuário que você deseja criar uma senha;
3. Clique em *criar senha*;
4. Na janela que se abre digite a senha escolhida e uma palavra ou frase para ser usada como dica de senha. Clique em *criar senha* para finalizar.

**Criar uma imagem para o usuário**

Sempre que iniciamos o computador, uma imagem (que pode ser um desenho ou foto ou até texto) é mostrada na tela de boas vindas ao lado do nome de cada conta.

Essa imagem serve tão somente para representar (ilustrar) o usuário. A mesma pode ser mudada de acordo com o gosto de cada usuário, ele pode inclusive colocar no lugar uma fotografia escaneada.

1. Vá ao *Painel de Controle – Contas de usuário*;
2. Clique na imagem que representa o usuário que você deseja alterar a imagem;
3. Clique em *alterar imagem*;
4. Irá abrir uma janela com várias opções de imagens. Se você desejar, pode usar uma outra imagem que não esteja na lista, bastando para isso clicar em *procurar imagens*. Essa imagem pode ser BMP, JPG, GIF ou PNG.

**Excluir uma conta**

Da mesma forma que para adicionar um novo usuário, para excluir você deve ter uma conta de administrador do computador.

1. Vá ao *Painel de Controle – Contas de usuário*;
2. Clique na imagem que representa o usuário que você deseja excluir;
3. Na janela que se abre clique em excluir a conta;
4. Na próxima janela, escolha *Manter arquivos* (dessa forma será criado uma pasta na área de trabalho do administrador contendo os arquivos da pasta meus documentos e da área de trabalho desse usuário) ou excluir arquivos;
5. Na próxima janela clique me *Excluir conta*.

**Criar um novo administrador**

O processo para criar um novo administrador é idêntico ao usado para criar um novo usuário limitado, com a diferença que no passo número 4, você escolhe *administrador* como tipo de conta. Não se esqueça em que o administrador deve ter uma senha. Para criar a senha basta seguir os mesmos passo usado para criar uma senha para o usuário que descrevemos anteriormente.

**Instalando um Firewall pessoal**

Firewall (que em inglês é porta de fogo), com já explicamos é um programa que auxilia na proteção das informações contidas em um computador. Nesse caso trata-se de um Firewall pessoal, para um computador.

Em algumas Redes, o Firewall são elementos que combinam hardware e software, construídos usando roteadores, servidores e uma variedade de softwares sendo que são instalados nos pontos mais vulneráveis.

**Norton Personal Firewall**

Para um Firewall pessoal basta utilizar um programa, que nesse tópico será o Norton Personal Firewall (http://www.symantec.com/).

A instalação é simples e intuitiva, a primeira janela dá as boas vindas a instalação do Norton Personal Firewall e a segunda trata-se dos termos de licença. Obviamente você poderá instalar uma versão diferente da que usamos como referência neste livro. Mas, mesmo que a versão seja diferente e as janelas de instalação seja levemente diferente a instalação será simples e fácil.

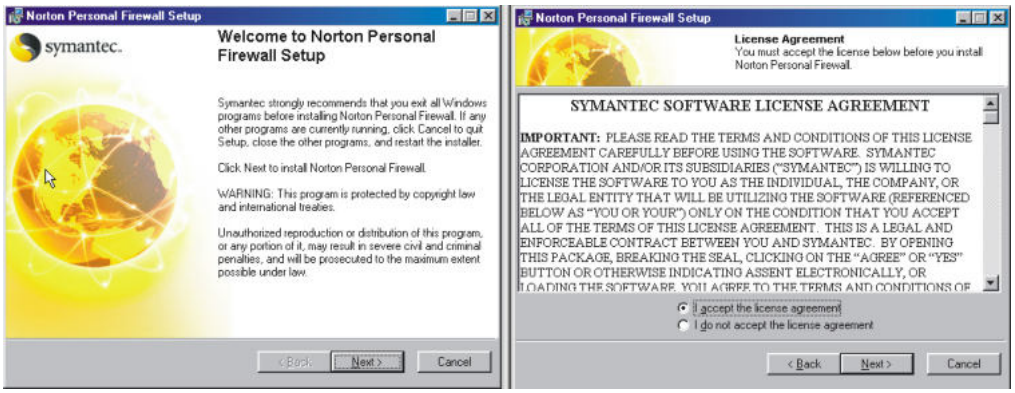


**Figura 5.6: Norton Personal Firewall - Janelas iniciais da instalação**

Na próxima janela configuramos se o LiveUpdate será executado assim que a instalação terminar. Basta escolher "yes" ou "no" e clicar em *Next*. Na seqüência devemos informar em qual unidade e pasta será feita a instalação. O defaut é *Arquivos de programas\Norton Personal Firewall*.

Só instale em outra unidade se haver problemas com falta de espaço no Disco Rígido. Para prosseguir, clique em *Next* e novamente em *Next* na janela seguinte. Será dado início ao processo de instalação,

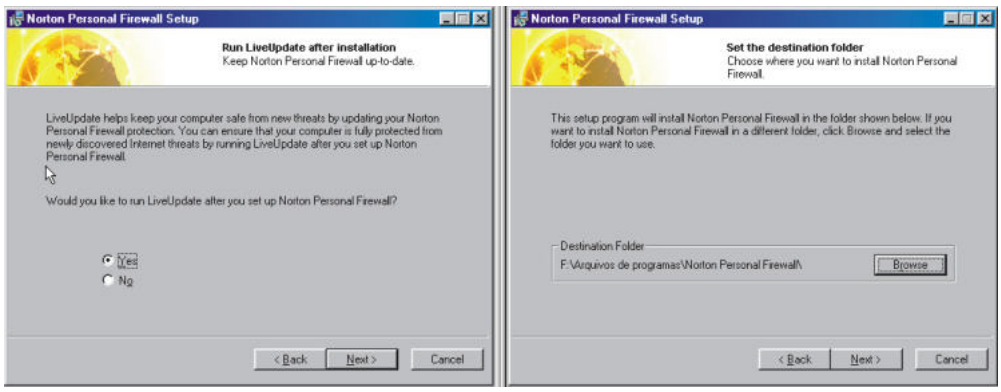


**Figura 5.7: LiveUpdate e diretório de instalação**

Ao terminar o processo de instalação, irá abrir uma janela de registro do produto. Basta clicar em *Avançar* para preencher os dados para o registro ou clicar em *Registrar mais tarde* para efetuar essa operação em outro momento.

Em seguida o Readme será aberto, basta clicar em *Next* e na tela em *Finish.* Clique em Yes na próxima janela para reiniciar o computador.

Ao reiniciar o computador, um ícone do Norton Personal Firewall terá sido criado na área de trabalho. Um assistente de segurança irá iniciar automaticamente. Para fechá-lo clique em *Close*.

Para verificar se o Firewall está ativado, abra o Norton Personal Firewall (pela área de trabalho ou pelo menu iniciar – Programas - Norton Personal Firewall). A janela que se abre é mostrada na figura seguinte.

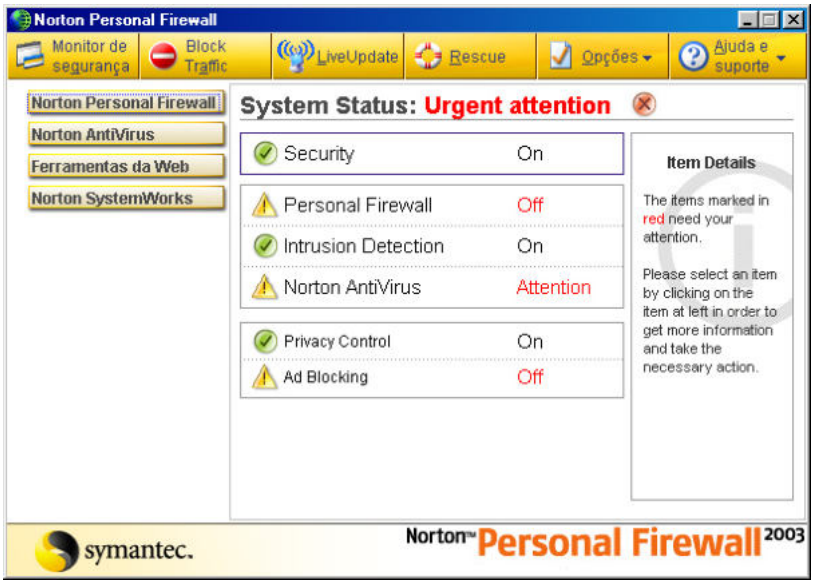


**Figura 5.8: Janela Principal do Norton Personal Firewall**

Para ativar o Firewall, clique uma vez com o mouse em *Personal Firewall*. Uma janela irá abrir na direita com duas opções: *Turn ON* e *Configure*.

Clique em *Turn ON* para ativar. Alguns ajustes podem ser feitos clicando em *Opções, Firewall*.

**Firewall do Windows XP**

O Windows XP tem um firewall próprio. Você pode habilita-lo (se não estiver usando nenhum outro) ou desabilita-lo (se estiver usando algum outro), bastando para isso seguir os passo a seguir:

1. Vá ao Painel de Controle. Clique em Conexões de Rede. Na janela que se abre, clique com o botão direito do mouse sobre a conexão (ou conexões) que estiver disponível e, clique na guia *Avançado;*
2. Marque ou desmarque a opção referente ao firewall. O firewall do Windows limita ou impede o acesso ao computador, ou seja, controla apenas a entrada de dados, e não a saída. Portanto o ideal é optar pela instalação de um firewall de terceiros.

**ZoneAlarm - Free**

O ZoneAlarm (http://www.zonelabs.com/) inclui quatro ferramentas:

- Firewall: para controle da porta do PC e possibilita somente o tráfego que o usuário permitir e/ou iniciar;
- Application Control: permite ao usuário decidir quais aplicativos podem ou não usar a internet;
- Internet Lock: serve para bloquear o tráfego quando o PC ou a internet não está sendo usada;
- Zones: usado para monitorar as atividades do PC e alerta quando um novo aplicativp tentar usar a internet.

O ZoneAlarm é freeware, dessa forma, basta realizar o download no site do fabricante, e instalar no computador.

A instalação é simples, bastando seguir as orientações das janelas. Ao término da cópia dos arquivos, irá abrir uma janela como mostrada na figura seguinte.

Responda às duas primeiras questões (as duas últimas podem ficar em branco): tipo de conexão usada pelo computador (Modem/Dial-Up, DSL, ISDN, Cable Modem, T1 LAN, Other) e tipo de plano (Personal Use, Business Use).

Para finalizar, clique em *finish* e na próxima janela, clique novamente em *finish.*

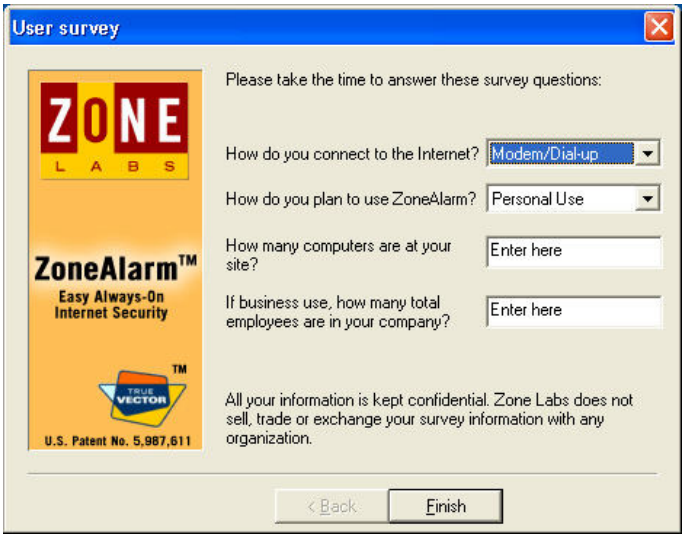


***Figura 5.9: ZoneAlarm – Configure o tipo de conexão e plano.***


**Figura 5.10: janela principal do ZoneAlarm**

**Back Orifice e NetBus**

São programas que permitem o controle remotamente de um computador. É importante entender que ambos não são vírus de nenhum tipo.

Apesar de suas origens (o Back Orifice por exemplo, foi desenvolvido por *Sir Dystic* que era membro de uma organização hacker americana), são programas para propósitos sérios. Eles não foram criados para ser um trojan muito menos um worm, porém, alguns trojans podem instalá-lo no computador da vítima.

O Back Orifice (não confundir com o software servidor da Microsoft chamado Back Office), ou simplesmente BO, é um programa que foi desenvolvido para ser uma ferramenta de administração remota, ou seja, que permite que uma pessoa possa operar o computador remotamente.

Ele funciona com uma arquitetura cliente-servidor, dessa forma, para que um computador possa ser controlado remotamente, este deve estar com o programa servidor instalado e será controlado pelo computador que tiver o programa cliente.

O NetBus foi desenvolvido para fazer manutenção de computadores a longa distância. Da mesma forma que o Back Orifice, o NetBus consiste de duas partes: um cliente e um servidor. O computador que tiver o servidor instalado poderá ser gerenciado remotamente.

Ambos os programas chamaram a atenção de aspirantes a hackers que passaram a usá-los para invadir computador. Mas para isso acontecer, o computador da vítima deve ter o programa servidor instalado.

E é o próprio usuário que instala esse programa. Como isso é possível? Principalmente através de trojans.

O usuário quando instala algum programa desse tipo, evidentemente ele não sabe o que realmente está instalando. Se o usuário conhecer o que é e o que faz esse programas, ele jamais o instalaria em seu computador.

Por isso, os hackers podem usar artifícios, como: um arquivo que diz ser um anti-Back Orifice ou algum outro programa qualquer (repare que nesse caso nem se trata de um trojan, o hacker apenas renomeia o arquivo do BO e envia para vitima) ou através de um trojan que instala "por trás" o BO.

E uma vez que o hacker se conecte ao computador da vítima ele pode por exemplo:

- Criar, deletar, procurar arquivos ou pastas;
- Acessar funções no registro;

- Travar ou reiniciar o computador;
- Mostrar senhas do sistema;
- Formatar o Disco Rígido;
- Abrir ou fechar o leito óptico;
- Inverter os botões do mouse;
- Monitorar tudo que a vítima está digitando.

**Como eliminar o Back Orifice**

1. Reinicie o seu computador em modo ms-dos.
2. Digite o seguinte comando "dir c:\windows\system\exe*.* /a".
3. Caso apareça o arquivo exe~1 você está infectado.
4. Digite "Attrib c:\windows\system\exe~1 -r -a -s -h".
5. Digite "Del c:\windows\system\exe~1".

**Como eliminar o Netbus:**

O Netbus normalmente utiliza o nome patch.exe (mas pode usar qualquer nome). Para verificar se ele está em execução você pode tentar da seguinte maneira:

1. Abra o MS-DOS (executar - cmd) e utilize o seguinte comando: *netstat - an | find "1234".* O DOS responderá algo do gênero: *TCP 127.0.0.1:12345 0.0.0.0 LISTENING;*
2. Em seguida é necessário verificar qual serviço está utilizando o endereço que o DOS forneceu. Para isso digite: *telnet 127.0.0.1 12345;*
3. *Caso o* Netbus esteja instaldo no PC, a resposta será algo do tipo: "NetBus 1.53" ou "NetBus 1.60" etc.

Para remover o Netbus, tente uma das opções a seguir:

**Opção 1**- Utilize o cliente do Netbus para fazer essa desinstalacão, indo na opção "Server Admin" e depois "Remove Server".

**Opção 2**- Tente pelo registro. Localize a chave e remova os valores: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run[Nome do
NetBus] HKEY_CURRENT_USER\Patch\Settings\ServerPwd.

**Instalando Anti-vírus**

Em se tratando de antí-virus, não podemos poupar recurso. Qualquer computador, por menos que use a internet, deve ter uma versão de anti-vírus instalado.

Use somente versões comerciais completas (nunca use demos ou versão que só funcionam durante 30 dias) ou versões freeware.

Os anti-vírus comerciais que tem se destacado podemos citar: o Norton Anti-Vírus (http://www.symantec.com/), Mcafee Visruscan (http://mcafee.com/) e Panda Anti-Vírus (http://www.pandasoftware.com/), entre outros.

Os anti-vírus freeware citamos: Avast! Home edition (http://www.avast.com/).

A instalação de qualquer anti-vírus é simples e intuitiva, basta seguir as orientação das janelas. Sempre ative as auto-proteções (auto-protect) ao instalar o anti-vírus,

dessa forma, assim que reiniciar o sistema, o computador estará sendo monitorado, e, caso algum arquivo com vírus seja aberto e detectado, o anti-vírus entra em ação.

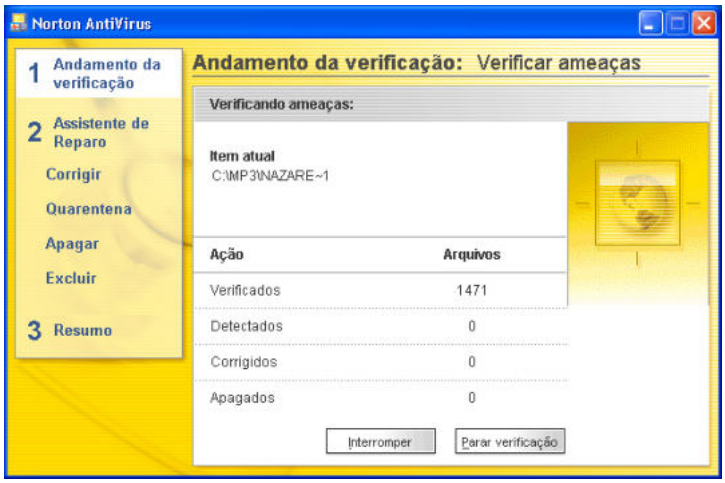


**Figura 5.11: Norton Anti-Vírus – Opção comercial**

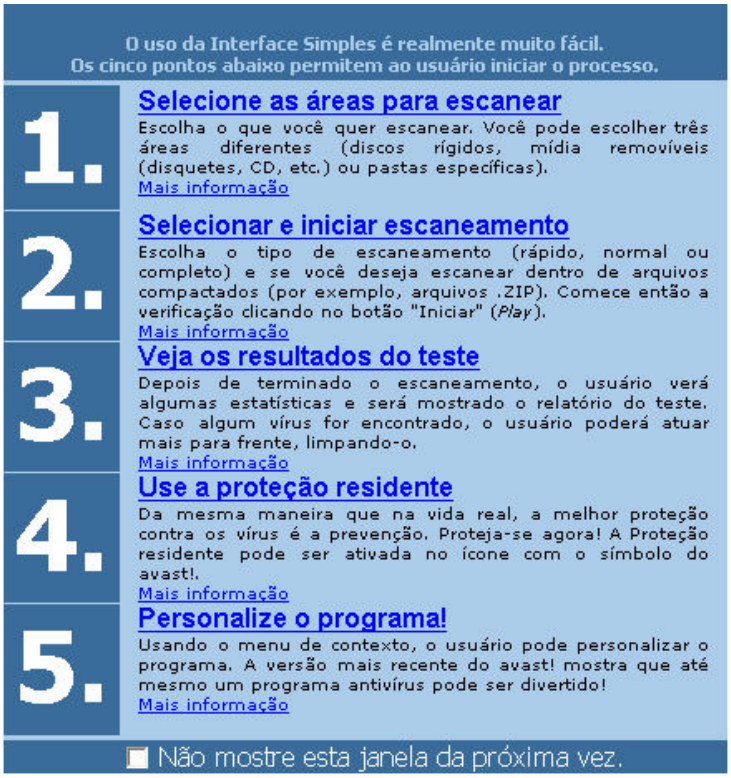


**Figura 5.12: Avast!– Opção freeware**

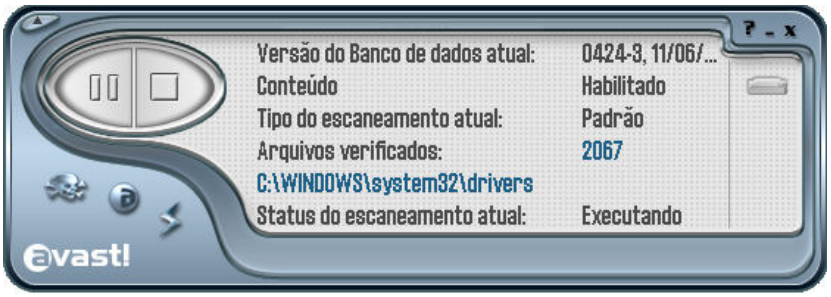


**Figura 05.13: Avast!- Guia rápido**

Ao instalar qualquer anti-vírus, sempre atualize o banco de dados de vírus pelo site do fabricante.

**Ativar o recurso comprimento mínimo de senha e requisitos de complexidade obrigatórios para senha no Windows XP**

No Windows XP podemos criar o que chamamos de contas de usuário, onde cada usuário ao iniciar o Windows digita o seu nome e senha e a partir daí entra em uma área personalizada, com seus ícones, programas instalados, papel de parede, etc.

A vantagem disso é as permissões de usuário, onde temos o administrador (consegue acessar e modificar qualquer coisa no Windows) e as contas limitadas (como o próprio nome sugere, o seu acesso é limitado a determinadas funções).

Por questões de segurança, um usuário com conta limitada não deve acessar a conta de um administrador, e por questões de privacidade, um usuário não deve acessar a conta de outro usuário. Neste panorama temos a seguinte situação: um computador que é usado por várias pessoas com contas limitadas (típico em escolas) e todas usam suas próprias senhas de usuário.

É típico muitos  usuários (principalmente iniciantes) fazerem suas senhas com um quantidade de número muito pequena (as famosas 123).

O administrador do sistema pode configurar o Windows para exigir que as senhas tenham um comprimento mínimo (6 caracteres no mínimo é o ideal) e que atendam aos requisitos de complexidade (para evitar as também famosa 123456).

A segurança também irá melhorar de forma considerável. Veja a seguir o que se trata os recursos que citamos anteriormente:

- Comprimento mínimo para senha: Determina o menor número de caracteres que uma senha de uma conta de usuário pode conter. Você pode definir um valor entre 1 e 14 caracteres, ou pode estabelecer que não é necessário senha definindo o número de caracteres como 0;

- Requisitos de Complexidade: Determina se as senhas devem satisfazer a requisitos de complexidade. Se esta diretiva estiver ativada, as senhas precisarão atender aos seguintes requisitos mínimos:
    1. Não conter todo ou parte do nome da conta do usuário;
    2. Ter pelo menos seis caracteres de comprimento;

3. Conter caracteres de três das quatro categorias a seguir:
4. Caracteres maiúsculos do inglês (A-Z);
5. Caracteres minúsculos do inglês (a-z) ;
6. 10 dígitos básicos (0-9) ;
7. Caracteres não alfanuméricos (por exemplo, !, $, #, %).

Para configurar ambos os itens, faça como se segue (não se esqueça que você deve ser o administrador do sistema):

1. Vá ao menu *Iniciar*, Painel de *Controle*;
2. Clique duas vezes no ícone ferramentas administrativas;
3. Clique duas vezes em *Diretiva de segurança local*;

*Outra forma de se chegar até em Diretiva de segurança local é digitando em Executar o comando secpol.msc e teclando Enter.*

4. Irá abrir uma janela como mostra na figura 05.14, onde, no lado esquerdo teremos uma lista com várias diretivas: Diretivas de conta, Diretivas locais, Diretivas de chave pública, Diretivas de restrição de software, Diretivas de segurança IP em Computador local;


**Figura 05.14: Janela principal das configurações locais de segurança**

5. Clicando no sinal de "+" ao lado de cada item, surge novos itens. O que nos interessa é a Diretiva de conta. Clique no sinal de "+" e surgirá no lado esquerdo duas novas diretivas: *Diretivas de senha e Diretiva de bloqueio de conta*. Acesse então *a Diretivas de senha* e no lado direito da janela surgirá várias diretivas: *A senha deve satisfazer a requisitos de complexidade, Aplicar histórico de senhas, Armazena senhas usando criptografia reversível para todos usuários no domínio, Comprimento mínimo da senha, Tempo de vida máximo da senha e Tempo de vida mínimo da senha*;

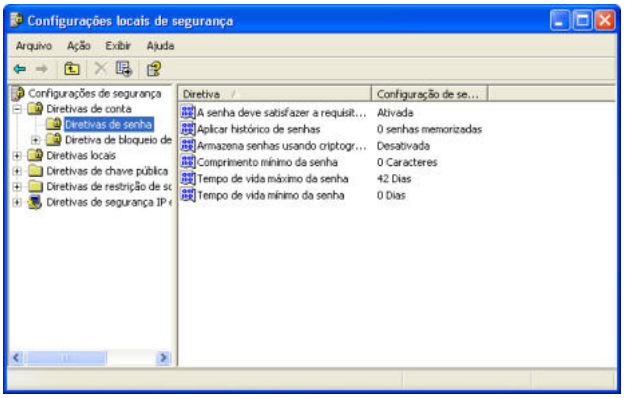


**Figura 05.15: Diretiva de senhas**

6. Você pode trabalhar todas as diretivas de acordo com a necessidade. Para alterar somente a diretiva *A senha deve satisfazer a requisitos de complexidade* e *, Comprimento mínimo da senha,* basta clicar duas vezes sobre cada uma e configurar. Vamos começar com a diretiva *A senha deve satisfazer a requisitos de complexidade.* Clique dias vezes sobre ela;

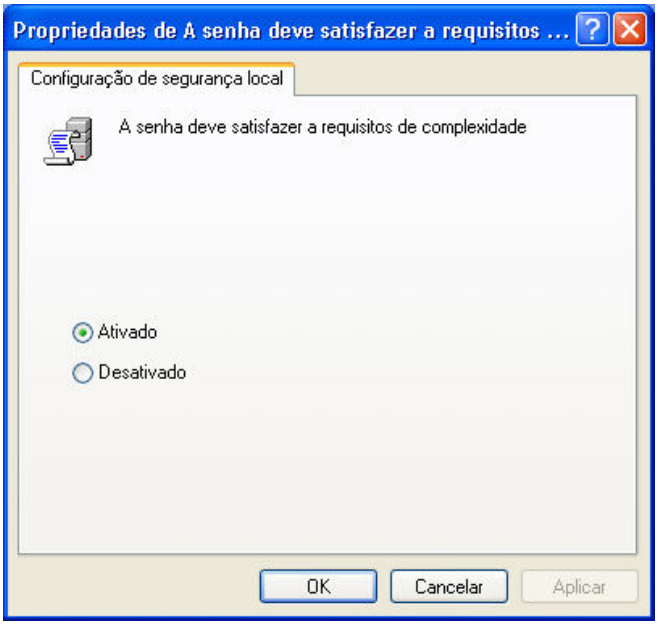


**Figura 05.16: Propriedades de *A senha deve satisfazer a requisitos de complexidade***

7. Marque a opção *ativado*, clique em *aplicar* e em *OK* para finalizar;
8. Clique duas vezes agora em *Comprimento mínimo da senha*;

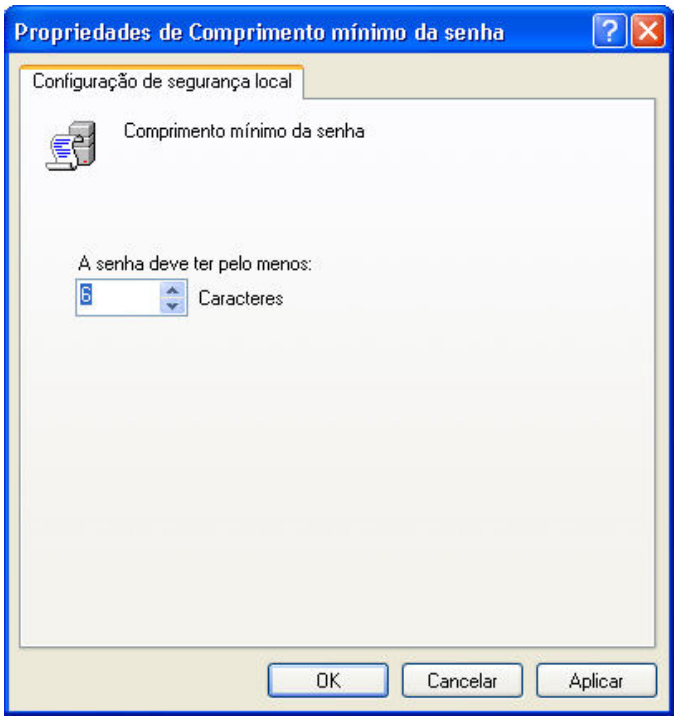


**Figura 05.17: Propriedades de *Comprimento mínimo da senha***

9. Em "A senha deve ter pelo menos" coloque o numero mínimo de caracteres desejado, lembre-se: o número ideal é 6. Clique em *Aplicar* e em *OK* para finalizar.

**Manutenção preventiva**

Uma dúvida que deve ser comum em técnicos iniciantes é o que fazer? Quais são os procedimentos que devo tomar para realizar manutenção preventivas em computadores?

Existe dezenas de resposta para essas perguntas. Vamos chamar todos os procedimento que são feitos de "plana de ação". Dessa forma, o técnico deve entender que para cada computador teremos um "plano de ação".

Um "plano de ação" de um computador doméstico é diferente do "plano de ação" para uma pequena rede. Como esse livro não é sobre redes, não iremos comentar sobre esse assunto aqui.

Em geral, o que deve ser feito, ou seja, um bom plano de ação, consiste no seguinte:

- **Inspeção Interna:** verificar o estado de todos os componentes, o aquecimento interno, a organização e a segurança física do mesmo;
- **Liberar espaço em disco:** eliminar os arquivos temporários, eliminar programas e outros arquivos desnecessário;

- **Otimização:** eliminar programas desnecessários que são executados ao iniciar o PC, corrigir erros no disco e desfragmentar os arquivos, limpar o registro, verificar o drivers;

- **Eliminar vírus:** usar programas antivírus para procurar e eliminar vírus;

- **Segurança:** Instalar softwares que impeçam a ação de vírus e hackers;

- **Backup:** realizar cópias de segurança dos arquivos mais importantes.

**A prevenção parte do usuário**

A manutenção preventiva começa pelo usuário, que a deve fazer diariamente. Um computador usado corretamente será um computador mais "saudável" e que funcionará por muito mais tempo sem apresentar problemas. Os hábitos considerados "saudáveis" ao computador são:

- **Sempre usar proteção de tela:** isso evita que os pontos de fósforo da tela do monitor venha a se queimar. A proteção de tela deve ter o maior número de movimentos possíveis, proteções de tela com pouco movimento (principalmente aquelas com uma frase que se movimenta em um fundo preto) não são boas;

- **Não instale softwares desordenadamente:** é comum o usuário, motivado pela curiosidade, instalar todo tipo de softwares no computador. Isso é errado. Instale um softwares, se não gostou, desinstale-o;

- **Execute o scandisk:** para corrigir possíveis erros no disco;

- **Desfragmente o disco:** pela menos uma vez por semana, deixe o computador ligado com o Desfragmentador do Windows rodando;

- **Cuidado com os vírus:** mantenha um software antivírus atualizado no computador.

**Preventiva física**

Realizar uma preventiva no hardware do computador consiste em:

- **Verificar se há oxidação:** verifique todos os contatos, trilhas impressas das placas e demais componentes eletrônicos;

- **Poeira:** todo computador tem, por menor que seja, um nível de poeira acumulada em seu interior. Realize uma limpeza do computador;

- **Umidade:** todo computador (e qualquer outro equipamento eletrônico) pode sofrer com a umidade, principalmente quando se ele ficar desligado por um período prolongado. Tome todas as providência para evitar que a umidade venha a danificar algum componente do computador;

- **Montagem do** computador**:** verifique se todos os componentes estão bem encaixados (procure por mau contato entre placas);

- **Circulação de ar:** verifique se o cooler está funcionando perfeitamente, se está havendo uma boa circulação de ar;

- **Organização:** organize todos os cabos internos do computador;

- **Segurança física:** instale nobreaks, verifique a fiação e a tomada usada pelo PC.

**Roteiro para preventiva lógica**

Os tópicos a seguir trata-se de um roteiro completo que você pode usar visando uma melhor performance, organização e estabilidade.

**Arquivos temporários**

O Windows e vários outros aplicativos geram arquivos temporários no Disco Rígido que são imprescindíveis ao seu funcionamento. Ao desligar o sistema operacional, todos esse arquivos são excluídos.

O problema ocorre quando há um desligamento anormal (pelo botão reset ou queda na energia) provocados por travamento (ou outros fatores), esse arquivos não são excluídos, e passam a ocupar espaço em disco.

O Windows guarda os seus arquivos temporários geralmente em C:\WINDOWS\Temp. Outros aplicativos podem usar a mesma pasta ou outra qualquer (no pior dos casos, alguns aplicativos infestam a raiz do Disco Rígido de arquivos temporários). Alguns aplicativos geram arquivos temporários ocultos, por isso é importante configurar o Windows para exibir todos os arquivos ocultos:

1. Na área de trabalho, acesse o ícone Meu Computador;
2. Na barra de ferramentas, clique em Ferramentas – Opções de pasta;
3. Clique na guia Modo de exibição;
4. Marque a opção Mostrar pastas e arquivos ocultos;
5. Clique em Aplicar e em OK para finalizar.

É gerado no Windows pelo menos dois tipos de arquivos que podem ser apagados:

- TMP: arquivos temporários do Windows, geralmente são apagados automaticamente;

- CHK: são dados perdidos no disco (não estão relacionados a nenhum arquivo), e que foram convertidos em arquivos pelo Scandisk. Por ser tratar de dados perdidos, dificilmente você conseguirá identificar o que eram estes arquivos perdidos, e eles só servirão para ocupar espaço em disco. Em alguns casos é possível recuperar esse dados. Faça assim: pegue o arquivo CHK e renomei-o para outro tipo de extensão (que você usa muito no computador), tipo DOC (documentos do Word), BMP (imagens Bitimap), etc. Em seguida tente abrir o arquivo. Se ele for aberto sem problemas, parabéns! Você conseguir recuperar o arquivo. Caso não consiga abri-lo em nenhum programa, exclua-o.

Todos esse arquivos podem ser excluídos do disco. Para isso vá ao Menu iniciar – Pesquisar (ou Procurar). No Windows XP selecione Todos os arquivos e Pasta. Digite .tmp e tecle Enter. A quantidade de arquivos com extensão TMP que será encontrada irá variar de sistema para sistema. É comum encontrar arquivos com nomes iniciando com o acento til (~), o que é normal. Exemplo: ~GLF2125.TMP. Todos podem ser excluídos. Não se esqueça de procurar pelos arquivos CHK (*.CHK) também.

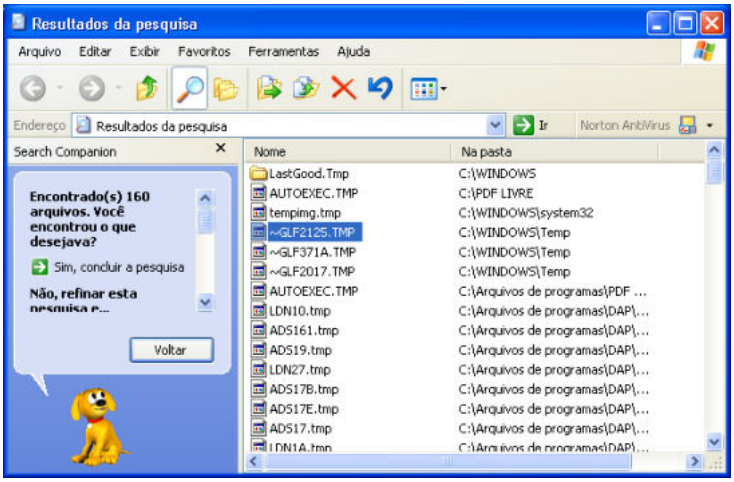


**Figura 05.18: resultados de uma pesquisa de arquivos "TMP" em um Disco Rígido**

Você pode configurar o Windows para que ele exclua os arquivos temporários sempre que iniciar. Faça o seguinte procedimento:

1. Acesse Iniciar / Executar e digite sysedit. Irá abrir um programa com várias;
2. Selecione a janela C:\AUTOEXEC.BAT (geralmente ela estará em primeiro plano) e adicione a seguinte linha: deltree/y c:\windows\Temp, e tecle Enter (para pular para a linha de baixo);
3. Na linha de abaixo da qual você digitou o comando anterior, digite: md c:\windows\temp;
4. Clique em Arquivo – Salvar, para finalizar.

Dessa forma, sempre que iniciar o Windows, os arquivos da pasta temp serão excluídos.

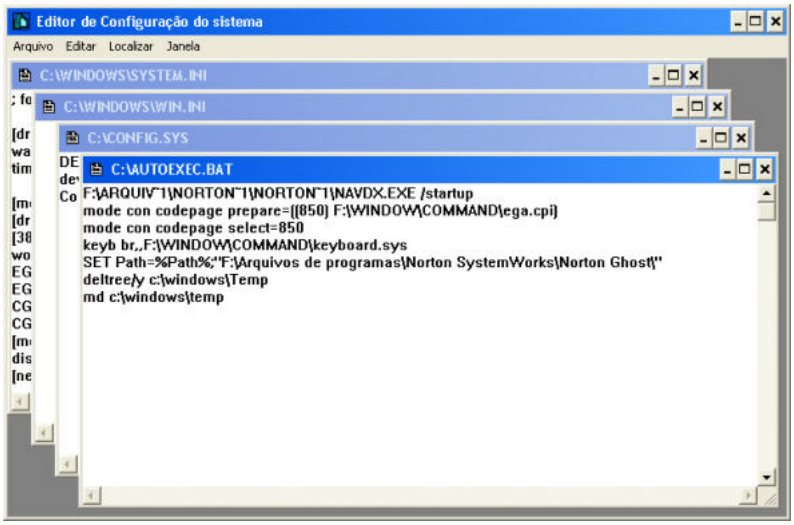


**Figura 05.19: Editor de configuração do sistema**

**Programas**

Após excluir todos os arquivos temporário, o técnico deve verificar todos os programas instalados no computador, e desinstalar aqueles que:

- **Forem versões demos (demonstrações):** as demonstrações são programas com seus recursos limitados (são incompletos). São encontrados principalmente em jogos, e representam uma versão mais curta do mesmo, com uma ou duas fases apenas. Muitos usuários instalam demonstrações em seus computadores que nem estão usando (na maioria dos casos porque a versão não apresenta todos os recursos se comparada a versão registrada);

- **Shareware**: são programas que o usuário pode instalar no computador, testar e somente se quiser continuar a utilizá-lo, irá comprar a licença de uso do mesmo e torna-se um usuário registrado, recebendo um número serial que destrava o software, deixando-o totalmente funcional. O problema é que nem sempre a compra desse registro ocorre. Muitas vezes o programa fica instalado ocupando espaço em disco e de tempo em tempo exibindo mensagens referente ao registro;

- **Trials:** funcionam de forma semelhante aos demos, e geralmente não salvam nem exportam os trabalhos realizados.

Verifique também se não há duas versões do mesmo programa instalado no computador. Exemplo: Show do milhão 1 e 2.

Desinstale aquela que não estiver funcionando, ou caso as duas funcionem, a versão mais antiga. Verifique todo o menu iniciar (Em algumas situações o menu iniciar do Windows pode conter pastas vazias, atalhos de programas que não estão mais instalados e atalhos repetidos) e o os diretórios do disco, principalmente em C:\Arquivos de programas.

Antes de desinstalar qualquer programa, mesmo sendo um Demo problemático, pergunte ao cliente se ele necessita dele ou não.

Use o recurso Adicionar ou remover programas do Windows (painel de controle - Adicionar ou remover programas) para verificar os programas que estão instalados e excluir aqueles que forem desnecessário.

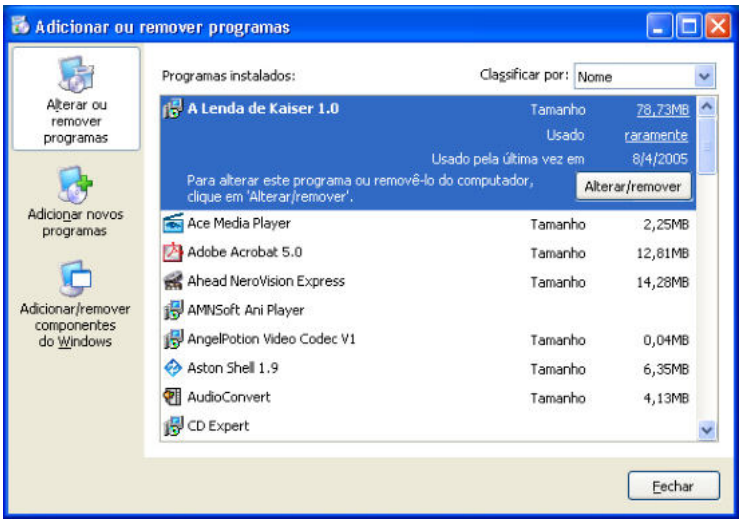


**Figura 05.20: Adicionar ou remover programas do Windows**

**Raiz das unidades**

Faça uma inspeção minuciosa de todos os arquivos que estão nas raízes de cada unidade de disco.

Muitos arquivos são criados por programas na raiz da unidade e podem ser excluídos. Cuidado para não excluir arquivos do sistema. Como regra, não exclua nada que tenha extensão SYS, COM, BAT, DOS e EXE.

Essas extensões são de arquivos necessário ao funcionamento do Windows. O técnico deve ser cauteloso, uma vez que, poderá haver arquivos importantes com outros tipos de extensão, vai depender do sistema operacional em questão.

Exclua arquivos com a extensão BAK, FFA, FFO, arquivos com nomes estranhos, tipo $LDR$ ou $DRVLTR$.~_~ e arquivos com nome image.

Sempre copie todos os arquivos em um disquete antes de excluí-los, dessa forma, caso o Windows apresente algum problema ao iniciar, basta repô-los.

**Programas que são executados automaticamente na inicialização do Windows**

Ao iniciar o Windows, vários programas podem ser executados automaticamente. Alguns são necessários como Antivírus, por exemplo.

Outros programas podem ser desabilitados para que não seja executado automaticamente. Verifique primeiramente o grupo Iniciar (Iniciar / Programas / Iniciar), ou inicializar caso use o XP.

Alguns programas indesejáveis podem ser facilmente retirados por esse menu.

A maioria desse programas entretanto ficam localizados no Registro. Vejamos como acessar o registro:

1. Vá ao menu Iniciar – Executar;
2. Digite Regedit, e tecle Enter;
3. No Editor de registro, localize a chave: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run;
4. Iremos encontrar várias entradas correspondentes aos programas que são executados na inicialização do Windows. Observe na direita da janela que nos é informado onde está instalado cada programa referentes as entradas. Para excluir alguma, basta clicar nela com o botão direito do mouse e escolher a opção Excluir.

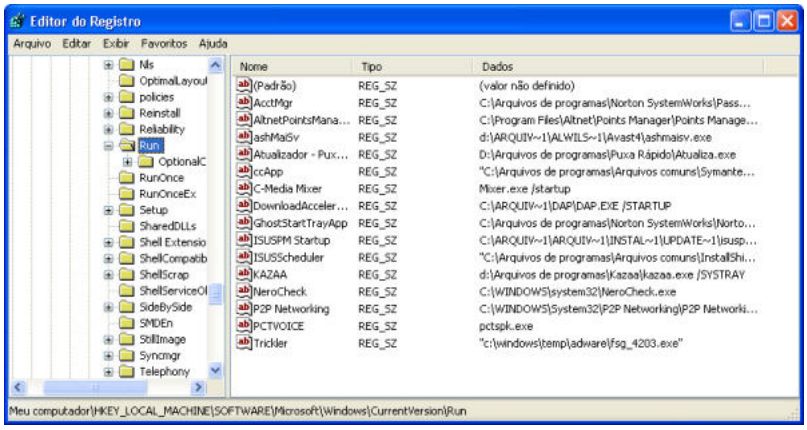


**Figura 05.21: Editor de registro do Windows: Programas que são executados na inicialização do Windows.**

Outra forma fácil de desabilitar os programas que estão sendo executados ao iniciar é rodando o aplicativo Msconfig.exe do Windows. Nele, encontramos uma lista de todos os aplicativos que são executados ao iniciar, não importando onde eles estão relacionados no registro. Veja:

1. Vá ao menu Iniciar – Executar;
2. Digite Msconfig e tecle Enter;
3. Na janela que se abre, clique na guia Inicializar;
4. Em seguida basta desabilitar os programas que são executados ao iniciar o Windows. Clique em aplicar para confirmar as configurações e em OK para finalizar.

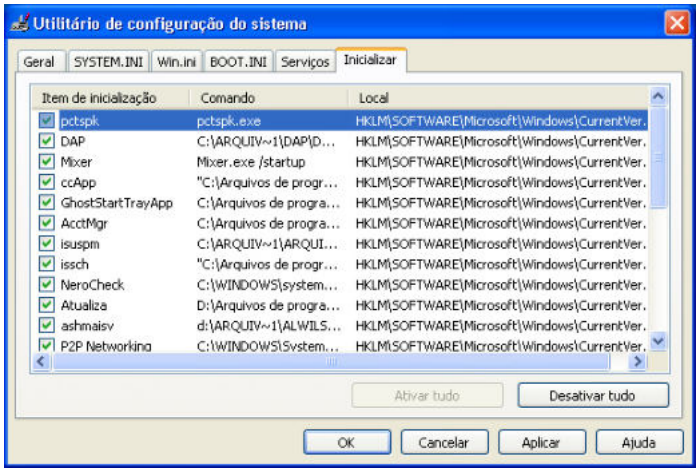


**Figura 05.22: Utilitário de configuração do sistema**