Vírus

Cuidados que se deve ter com o seu computador

Paulo Serrano

28/08/2001

Introdução:

A Tecnologia de Informação mudou totalmente a vida das pessoas. Hoje quase tudo é informatizado. A cada semana ouve-se notícias de lançamentos de novas tecnologias que vão substituindo as atuais numa velocidade espetacular.

Num ritmo mais acelerado, tecnologias da mesma área, vão se multiplicando a cada dia, e infelizmente não são desenvolvidas para auxiliar na melhoria das tecnologias atuais, pelo contrário, são ameaças suficientemente poderosas e com um notório poder de destruição, conhecidas como: **vírus de computador**.

Os vírus de computador podem ser inofensivos como uma simples brincadeira de criança, como também podem ser o fim de todo um trabalho.

Essas ameaças do mundo da informação eletrônica, são frutos de mentes doentias que se privilegiam de conhecimentos em linguagens de programação, e a partir delas, criam códigos que fazem de nossos vulneráveis computadores, verdadeiros bonecos de marionetes.

Mas esse alto conhecimento em programação já não é tanto assim um pré-requisito. Hoje existem programas que criam vírus ao gosto do usuário.

É preciso estar atento e preparado para identificar o inimigo e poder combatê-lo de forma eficaz.

Vírus de computador: o que é isso?

É um programa como outro qualquer, mas com um único diferencial: seu código é nocivo aos sistemas operacionais e respectivos aplicativos.

Gerados como arquivos executáveis, têm como característica principal a possibilidade de auto replicação, ou seja, uma vez executado, ele passa a ficar ativo na memória do computador e é feita uma cópia de seu código para dentro da unidade de armazenamento (disquete ou disco rígido) onde serão rodadas suas instruções nocivas no sistema infectado.

As finalidades desses programas nocivos não são outras senão a de alterar, corromper e ou destruir as informações acondicionadas em disquetes e discos rígidos de microcomputadores.

Histórico: a evolução do vírus de computador

1983 – O pesquisador Fred Cohen (doutorando de engª. elétrica da Univ. da Califórnia do Sul), entre suas análises, batizou os programas de códigos nocivos como "Vírus de Computador".

1987 - Surge o **Brain**, o primeiro vírus de computador de que se tem notícia.
Ele infecta o setor de boot de disquetes (na época de 360 Kb), e utiliza técnicas para passar despercebido pelo sistema.
Stoned (primeiro vírus a infectar o registro mestre de boot, MBR) é liberado.
Ele danifica o MBR da unidade de disco rígido, corrompendo ou até mesmo impedindo a inicialização do sistema operacional.

1988 – O primeiro software antivírus é oferecido por um programador da Indonésia. Depois de detectar o vírus **Brain**, ele o extrai do computador e imuniza o sistema contra outros ataques da mesma praga.
O **Internet Worm** é liberado na ainda emergente Internet e atinge cerca de 6.000 computadores.

1989 – Aparece o **Dark Avenger**, que contamina programas rapidamente, mas o estrago subseqüente acontece devagar, permitindo que o vírus passe despercebido por muito tempo.
A IBM fornece o primeiro antivírus comercial e é iniciada uma pesquisa intensiva contra as pragas eletrônicas.
No início do ano, apenas 9% das empresas pesquisadas sofreram um ataque de vírus. No final do ano, esse número saltou para 63%.

1992 – **Michelangelo**, o primeiro vírus a causar agitação na mídia. É programado para sobregravar partes das unidades de disco rígido em 6 de março, dia do nascimento do artista da Renascença. As vendas de software antivírus disparam, embora apenas alguns casos de infecção real sejam reportados.

1994 – O autor de um vírus chamado **Pathogen**, na Inglaterra, é rastreado pela Scotland Yard e condenado a 18 meses de prisão. É a primeira vez que o autor de um vírus é processado por disseminar código destruidor.

1995 – Surge o **Concept**, o primeiro vírus de macro. Escrito na linguagem Word Basic da Microsoft, pode ser executado em qualquer plataforma com Word - PC ou Macintosh.
O Concept desencadeia uma explosão no número de vírus de macro, pois são muito fáceis de criar e se disseminar.

1999 – O vírus **Chernobyl,** que deixa a unidade de disco rígido e os dados do usuário inacessíveis, chega em abril. Embora tenha contaminado poucos computadores nos Estados Unidos, provocou danos difundidos no exterior. A China sofre prejuízos de mais de US$ 291 milhões. Turquia e Coréia do Sul também foram duramente atingidas.

2000 – O vírus **LoveLetter**, liberado nas Filipinas, varre a Europa e os Estados Unidos em seis horas. Infecta cerca de 2,5 milhões a 3 milhões de máquinas, causando danos estimados em US$ 8,7 bilhões.

2001 – A “moda” são os códigos nocivos do tipo **Worm** (proliferam-se por páginas da Internet e principalmente por e-mail).
São descobertos programas que criam vírus. Um deles é o VBSWorms Generator, que foi desenvolvido por um programador argentino de apenas 18 anos.

Infecção: como acontece ?

- Vírus por disquete

Para que um programa de código destrutivo(vírus) possa proliferar-se, é necessário uma forma de transporte. Como os vírus biológicos, é preciso um "hospedeiro" para entrar em contato com outro corpo e assim poder disseminar o vírus.

Uma das formas mais usadas por muito tempo e até hoje é o uso de disquetes. O criador do vírus grava seu código destrutivo em disquete, e posteriormente, executa-o em máquinas que são usadas por várias pessoas, como computadores de salas de treinamento ou de empresas. O próximo usuário a utilizar o computador infectado, entrará com seu disquete e o vírus que já está carregado na memória, se auto copiará ocultamente para o disquete, gerando assim mais um "hospedeiro".

- Vírus por e-mail

Outra forma, que hoje é a mais focada pelos criadores de vírus, é o correio eletrônico.

É a forma mais eficiente de se disseminar um vírus, pois praticamente todas as pessoas que usam computadores, possuem um e-mail.

Ao abrir uma mensagem que contenha em anexo um arquivo de código nocivo, nada de anormal acontecerá, isso porque o conteúdo da mensagem não pode ser executado, por se tratar de texto que não utiliza linguagens de programação como recurso. Mas ao executar o arquivo anexado, será iniciado o processo de execução das instruções contidas em seu código.

As principais instruções desses vírus são a de se auto copiar para o disco rígido, buscar a lista de endereços eletrônicos do gerenciador de e-mail utilizado (Outlook Express, Netscape Messenger, Eudora, etc.) e se auto enviar para todos os nomes da lista.

Quais os tipos de vírus ?

Existem vários tipos de vírus, que veremos a seguir, mas entre esses vários tipos, existem duas formas de ação que são comuns entre todos, que é a alteração do setor de boot e, ou a inserção do código nocivo ao código de arquivos executáveis do sistema operacional ou dos programas aplicativos.

Principais tipos de Vírus:

- Vírus de Boot:

A característica desses tipos de vírus é a infecção de códigos executáveis localizados no setor de inicialização das unidades de armazenamento, tanto disquetes, quanto discos rígidos.
As unidades de armazenamento reservam uma parte de seu espaço para informações relacionadas à formatação do disco, diretórios e arquivos armazenados, além de um pequeno programa chamado "Bootstrap", que é responsável por carregar o sistema operacional na memória do computador.
O Bootstrap é o principal alvo dos vírus de boot. Eles alteram seu código, que por sua vez altera a seqüência de boot do computador, passando a carregar após o BIOS, o setor de boot infectado e as instruções do código do vírus de boot para a memória da máquina e posteriormente o sistema operacional.
Exemplos de alguns vírus de boot: Stoned; Ping-Pong; Leandro&Kelly; AntiEXE.

- Vírus de Arquivo:

Esses tipos de vírus têm como principal missão a infecção de arquivos executáveis, geralmente os arquivos de extensão EXE e COM. Podem também infectar arquivos importantes como os de extensão: SYS; OVL; OVY; PRG; MNU; BIN; DRV; DLL, etc. Um dos arquivos mais visados é o COMMAND.COM, que é um dos arquivos do sistema operacional com maior índice de execução.
Quando um programa é executado, ele fica carregado na memória do computador para que seja lido pelo processador. Estando esse programa

infectado, as instruções do código do vírus também serão executadas pelo processador, e uma das instruções é a de copiar o código nocivo para dentro dos demais arquivos executáveis "saudáveis", gerando assim uma infecção generalizada.
Alguns vírus de arquivos: Dark Avenger; MaTriX; Freddy Kruegger, Chernobyl, dentre tantos outros.

- Vírus de Macro:

Este é um tipo de vírus relativamente novo. O primeiro vírus de macro, o Concept, surgiu em 1995.
A criação desse tipo de vírus se dá a partir da linguagem de programação Word Basic, que é responsável por criar e executar macros(automatização de textos) no processador de textos Microsoft Word e também no Microsoft Excel.
O principal alvo dos vírus de macro é o arquivo NORMAL.DOT, que é responsável pela configuração do Word. A partir de sua contaminação, se torna ultra rápida a infecção de outros documentos, pois a cada vez que se abre ou se cria um novo documento, o NORMAL.DOT é executado.
As avarias causadas pelos vírus de macro vão desde a alteração dos menus do Microsoft Word, da fragmentação de textos, até a alteração de arquivos de lote como o AUTOEXEC.BAT, que pode receber uma linha de comando do DOS, como por exemplo: DELTREE, que apagará parcial ou totalmente o conteúdo do disco rígido, assim que o computador for inicializado.
Exemplos de vírus de macro: Wazzu, CAP.A, Melissa.

Prevenção: a batalha contra as "pragas"

Hoje não existe computador imune a vírus. A cada dia surgem novos vírus, e os pesquisadores das empresas desenvolvedoras de programas antivírus levarão um certo tempo para detectar que o código de um determinado arquivo é destrutivo e seja considerado vírus.
Até que seja desenvolvida uma atualização de antivírus para detectar a nova praga, poderá ter ocorrido sérios danos em decorrência de sua rápida

disseminação. Isso quer dizer que não existe programa que ofereça total proteção.
Uma estratégia de prevenção deve ser adotada, para não viver na vulnerabilidade.

- Prevenindo a infecção:

A seguir veremos alguns procedimentos que devem ser seguidos para manter a integridade dos dados de seu computador caso ocorra uma possível tentativa de infecção. Lembrando que é de vital importância ter um programa antivírus atualizado em seu sistema operacional. (veremos a instalação posteriormente)

- Executar o antivírus em todo o disco rígido, nos disquetes mais utilizados e também nos disquetes que não possuam nenhum conteúdo. O antivírus deve estar configurado para checar o MBR(Registro Mestre de Boot), setores de boot e principalmente a memória do computador. Lembre-se que muitas vezes, sequer é necessário abrir arquivos ou rodar um programa a partir de um disquete contaminado para infectar o seu computador. Pelo fato de todos os discos e disquetes possuírem uma região de boot (mesmo os não inicializáveis), basta o computador inicializar ou tentar a inicialização com um disquete contaminado no seu drive para abrir caminho para a contaminação. Normalmente, o modo padrão de checagem de um antivírus contém todos esses itens, incluindo outros tipos de arquivos além dos *.COM e *.EXE.

- Ajustar o antivírus para checar os setores de boot, MBR e memória do computador em toda inicialização é uma boa medida preventiva, para bloquear vírus de sistema que venham a infectar algum arquivo de inicialização. Ao instalar um antivírus, geralmente, ele já vem ajustado para executar esse procedimento.

- O antivírus, se possuir um checksummer (vacinador), deve ser habilitado para tirar a "impressão digital" ou "vacinar" todos os tipos de arquivos visados pelos vírus. É desnecessário vacinar todos os arquivos do disco, basta vacinar apenas os arquivos visados pelos vírus (arquivos de dados simples, como txt, html, som e imagem, por exemplo, não são infectáveis).

- O antivírus deverá ser utilizado toda vez que um disquete não checado for ser aberto pelo seu computador. Não permita a leitura de disquetes

suspeitos antes de checá-los com o antivírus e só os abra se eles estiverem "limpos".

- Trave fisicamente contra gravação todos os seus disquetes com programas de instalação, backups e drivers.

- Se existir, habilite a checagem automática de arquivos copiados(download) pela Internet.

- Se não possuir checagem automática de arquivos copiados pela Internet, cheque sempre os arquivos potencialmente infectáveis que forem copiados, principalmente os arquivos *.DOC, *.XLS e *.EXE (arquivos de imagem jpg, gif, etc, e texto simples não precisam ser checados).

- Jamais abra ou execute arquivos suspeitos ou de origem não confiável obtidos via Internet. Jamais abra ou execute arquivos “attachados” em e-mails sem checagem contra vírus. Contudo, pode ficar relativamente tranqüilo quanto aos e-mails propriamente ditos, eles em si são inofensivos, ao contrário dos boatos comuns indicando o contrário.

- Atualize constantemente seu antivírus. Usualmente são disponibilizados na Internet em atualizações mensais que podem ser copiadas na forma de arquivos executáveis ou acessadas diretamente na forma de smart-updates pelo seu antivírus.

- Após uma atualização, cheque todo seu HD conforme a etapa inicial.

Um monitor residente em memória (os antivírus possuem esse acessório), permite que o usuário, caso um vírus ultrapasse a primeira linha de defesa e tente infectar o PC, seja alertado, o que possibilita que barremos a disseminação. Mas essa segunda linha de defesa não substitui a primeira, apenas aumenta a segurança do conjunto para eventuais "furos" de procedimento (por exemplo, ao esquecermos de verificar um disquete).

- Prevenindo danos provocados por vírus

Evitar a contaminação é importante, mas devemos ficar atentos para a possibilidade do computador ser contaminado (que normalmente ocorre por descuido nos procedimentos de prevenção de infecção ou por falta de atualização dos antivírus). Nesse caso, o mais importante é detectar o vírus rapidamente, antes que ele provoque danos ao seu sistema, além de ter à mão os disquetes de emergência do seu antivírus ou pelo menos um disquete de inicialização (boot) "limpo" e travado contra gravação. Note que um vírus pode ser residente em memória e, ou atacar o programa de antivírus instalado no seu computador, por isso é tão importante ter sempre à mão um disquete "limpo" de boot com a inicialização do seu sistema operacional e, ou um antivírus que possa ser rodado a partir dele.

Os disquetes de emergência são feitos pelos antivírus e não devem ser dispensados. Durante a instalação eles se oferecem para criá-los. Caso não os tenha feito, procure a opção do seu antivírus para isso e faça-os. Lembre-se de atualizar periodicamente seus disquetes de emergência conforme o conteúdo do seu computador for se alterando.

Caso não disponha de um antivírus completo ou não tenha nenhum, precisará no mínimo de um disquete de inicialização para o caso de emergência. Um disquete de sistema pode ser feito pelo gerenciador de arquivos ou explorer do Windows ou com o comando FORMAT/S do DOS.

Um antivírus ajustado para escanear os setores de boot, MBR e memória do computador em toda inicialização garantirá que um vírus detectado não se dissemine caso ele consiga atingir alguma dessas áreas do computador. O monitor residente em memória também alerta imediatamente tentativas de residência em memória por vírus ou alteração de arquivos protegidos.

Lembre-se que o principal objetivo do vírus é disseminar-se o máximo possível até ser descoberto ou deflagrar um evento fatal para o qual foi construído, como, por exemplo, apagar todo disco rígido. Entretanto, é comum o aparecimento de alguns sintomas perceptíveis, mesmo sem o uso de antivírus, quando o computador está infectado. Geralmente, tais sintomas são alterações na performance do sistema e, principalmente, alteração no tamanho dos arquivos infectados. Uma redução na quantidade de memória disponível pode também ser um importante indicador de virose. Atividades demoradas no

disco rígido e outros comportamentos suspeitos do seu hardware podem ser causados por vírus, mas também podem ser causadas por softwares genuínos, por programas inofensivos destinados à brincadeiras ou por falhas e panes do próprio hardware.

Ainda que os sintomas descritos não sejam provas ou evidências da existência de vírus, deve-se prestar atenção à alterações do seu sistema nesse sentido. Para um nível maior de certeza é essencial ter um antivírus com atualização recente.

Outros sintomas de contaminação são propositalmente incluídos na programação dos vírus pelos próprios criadores, como: mensagens, músicas, ruídos ou figuras e desenhos. Tais sintomas podem ser as provas definitivas de infecção, mas podem se tornar evidentes apenas quando a infecção já está alastrada pelo PC ou no caso de alguns vírus destrutivos, surgirem na forma de danificação de dados ou sobregravação/formatação do disco rígido, o que seria, muito tarde.

Quando constatado que um PC está infectado ou que possui alta suspeita de infecção, antes de mais nada, ele deve ser desligado (não apenas reinicializado) e inicializado com um disquete de boot "limpo" ou o disco de emergência do seu antivírus.

Caso disponha dos disquetes de emergência criado pelo antivírus, eles praticamente serão suficientes para remediar qualquer problema no seu computador (desde que estejam atualizados). Siga as instruções do seu antivírus.

Caso disponha apenas de um disquete de inicialização simples do seu sistema operacional, utilize-o para inicializar o computador para permitir a instalação de um scanner antivírus, que em último caso pode ser um de versão DOS (mas lembre-se que utilizar um antivírus DOS para reparar arquivos do Windows 95 não é o procedimento mais seguro). Varra todo o seu HD e, se possível, solicite o reparo dos arquivos infectados.

É importante saber que os antivírus são produzidos para reparar os arquivos contaminados, entretanto nem sempre isso é possível. Além disso, o arquivo pode não ser corretamente reparado. Assim, recuperações realizadas sem nenhum procedimento preventivo são de alto risco. Arquivos de sistema corrompidos ou apagados de forma inadvertida durante a desinfecção muitas

vezes impedem o computador de funcionar, mesmo que antes da limpeza ele estivesse funcionando. Recuperações com discos de emergência criados por softwares antivírus costumam ser personalizados e conter backups de arquivos importantes do seu computador. Por isso, reparos realizados com tais discos são muito mais seguros do que aqueles realizados sem esses discos.

Quando um arquivo não pode ser reparado ou é mal reparado, ele pode e deve ser substituído por um mesmo arquivo "limpo" do software original ou de outro computador com programas e sistema operacional idênticos ao infectado. Mas saiba que muitas vezes, dependendo do vírus, da extensão dos danos ocasionados pela virose e a existência ou não de backups e discos de emergência, apenas alguém que realmente compreenda do assunto poderá desinfectar o seu computador e tentar recuperar os arquivos. No processo de descontaminação do computador é importante checar todos os seus disquetes, mesmo aqueles com programas e drivers originais a fim de evitar uma recontaminação.

Para quem não possui nenhum tipo de procedimento de prevenção contra infecção é vital ter, além do disquete de inicialização do sistema, um conjunto de back-ups contendo:

- Arquivos e documentos importantes e, indispensavelmente, aqueles visados por macrovírus como os do MS Word (*.DOC e *.DOT) e MS Excel (*.XLS e *.XLT);
- Programas de instalação dos aplicativos e do sistema operacional.

Opcionalmente, para quem entende mais do assunto, podem ser feitos backups dos seguintes arquivos:

- Arquivos executáveis (*.EXE e *.COM);
- Arquivos de sistema (*.SYS, *.BIN, *.DRV etc.);
- Arquivos *.INI e *.BAT;

Mesmo quem possui antivírus e os disquetes de emergência poderá se sentir mais seguro com backups desse tipo, ainda que raramente venha a necessitar deles (muitos ítens desses backups já são feitos nos disquetes de emergência).
Mas para quem não possui disquetes de emergência e nem antivírus, esse pequeno conjunto de backups e o disquete de inicialização permitirão, desde que se possua um mínimo de domínio no assunto, reparos de muitos danos, podendo ser a única salvação no caso de não termos nenhuma estratégia

preventiva contra infecção. Com alguma experiência pode-se eliminar boa parte dos vírus mesmo sem um antivírus completo à mão. Mas de qualquer forma, é altamente recomendável fazer a remoção e reparos com pelo menos um scanner antivírus (mesmo que seja um que rode em DOS).

Existem muitos programas antivírus que podem ser adquiridos no formato shareware (versões de uso limitado e gratuito) em sites de pesquisadores e empresas. Alguns produtores fornecem gratuitamente versões shareware que possuem apenas o scanner e, ou algum outro acessório, sem a opção de reparo ou remoção. Outros fornecem sharewares com todas as funções do produto completo para um período pré-determinado e não renovável, a título de "test drive" (não adianta tentar reinstalar o programa para "ganhar" mais um período de uso).

Veja no endereço abaixo, o resultado de um estudo técnico desenvolvido pelo CCUEC/Unicamp, sobre os principais programas antivírus do mercado bem como os endereços para acesso às informações dos fabricantes:

http://www.ccuec.unicamp.br/solucoes/antivirus/antivirus.html

Antivírus: instalando o guardião

A seguir veremos passo a passo como instalar o programa antivírus AVG Antivírus - Free Edition da Grisoft Inc..
Este antivírus foi escolhido para exemplo, por se tratar de um programa freeware (software gratuito) para uso pessoal, o que o torna atrativo, por não ser controlado por data de expiração do uso. Basta apenas registrar a cópia no site da desenvolvedora, em:

http://www.grisoft.com/

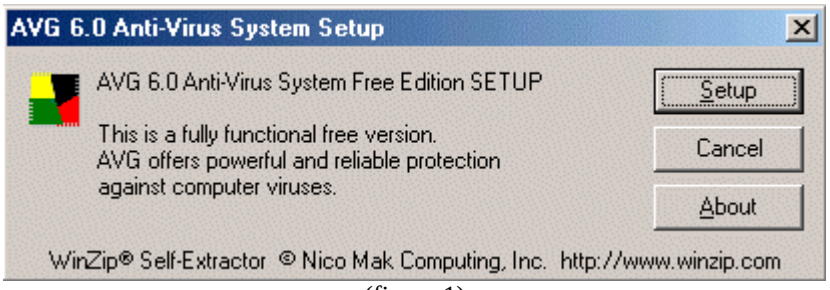
- Mãos à obra

Faça download do arquivo de instalação (avg6265fu.exe) que está disponível no repositório do CCUEC, em:

ftp://ftp2.unicamp.br/pub2/apoio/windows9x/antivirus/

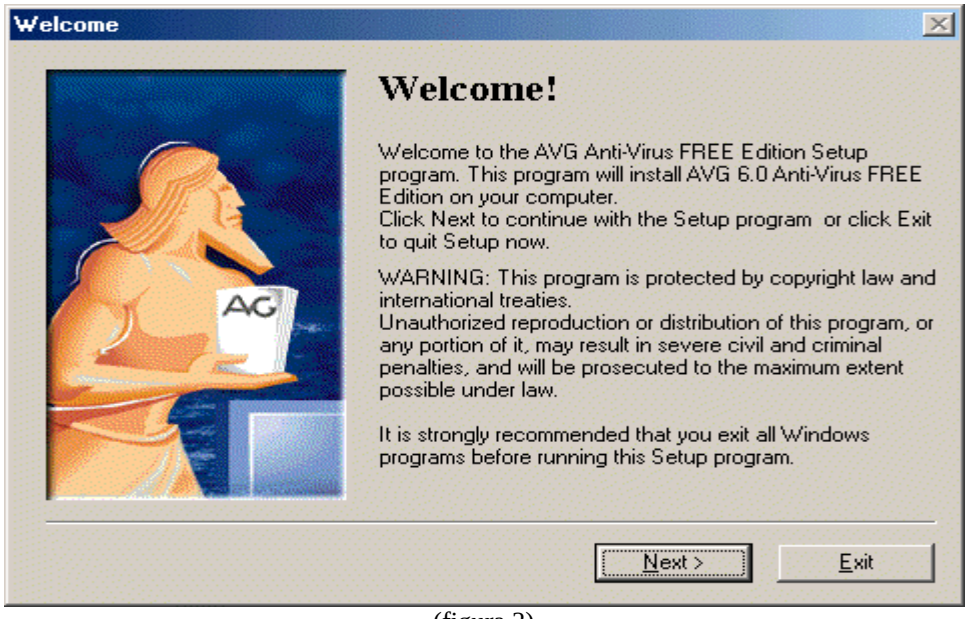
Para usuários externos, basta tirar o número 2 do endereço ftp2.unicamp.br .

Execute o arquivo de instalação. Aparecerá a tela de instalação com a janela de apresentação. (figura 1)



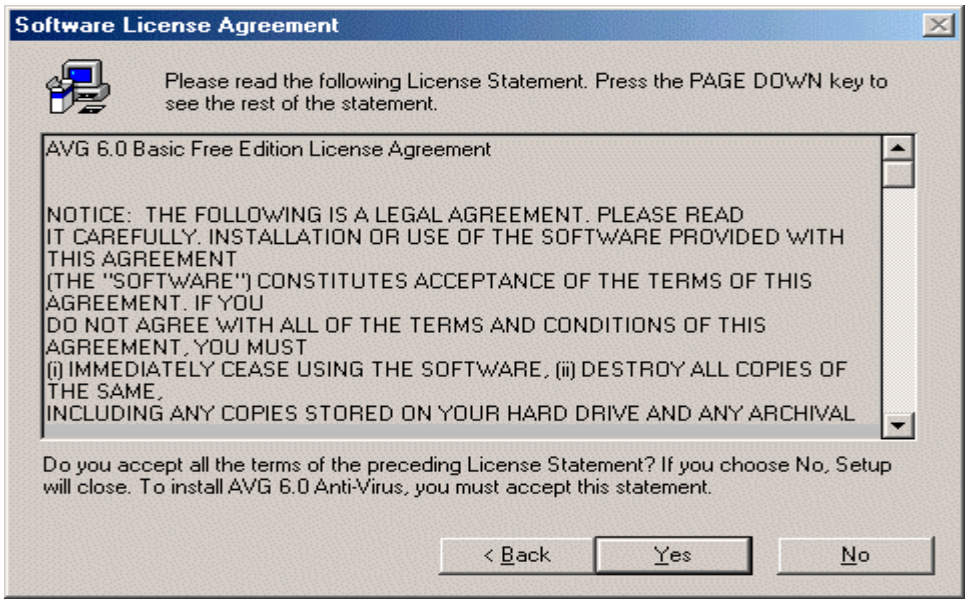
(figura 1)

Clique em “Setup” para seguir para a janela de primeiras informações sobre o produto(figura2):



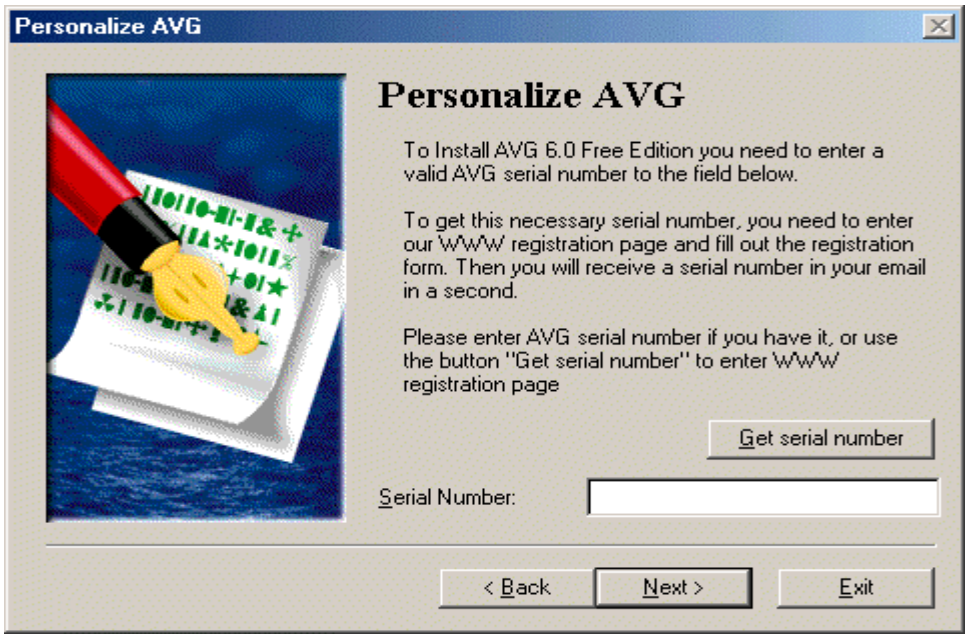
(figura 2)

Clique em “Next” para seguir para janela Software License Agreement (figura 3), que contém o termo de licença de uso do produto e clique no botão “Yes”.



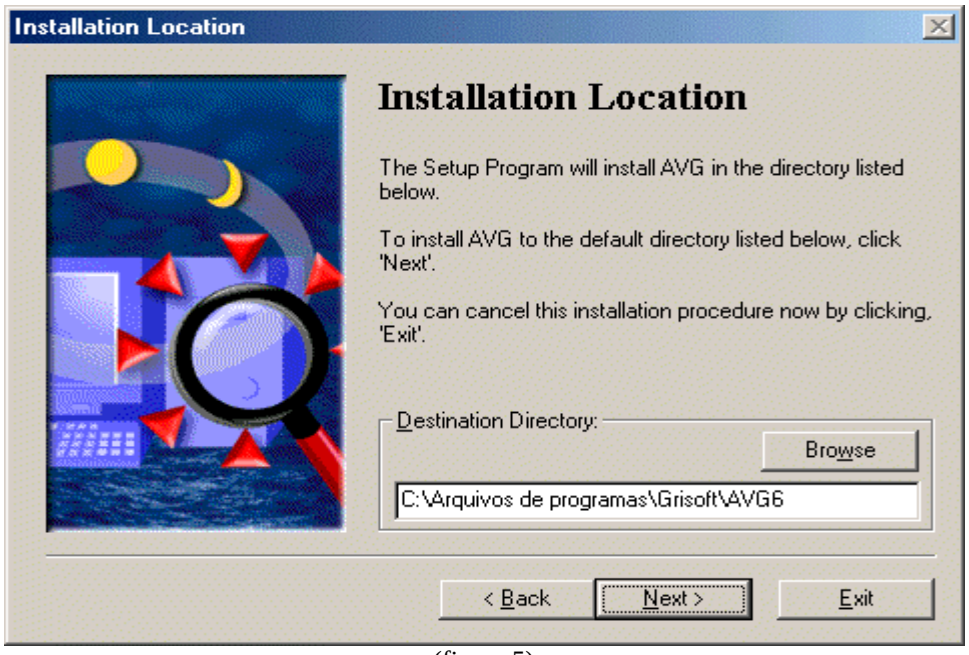
(figura 3)

Na janela Personalize AVG (figura 4) será necessário informar o Serial Number para dar continuidade à instalação do antivírus. Para obter o número de licença basta clicar no botão **Get serial number** que abrirá um navegador diretamente na página da Grisoft. Depois de feito o cadastro, será enviado o número de licença para o e-mail que você informou.



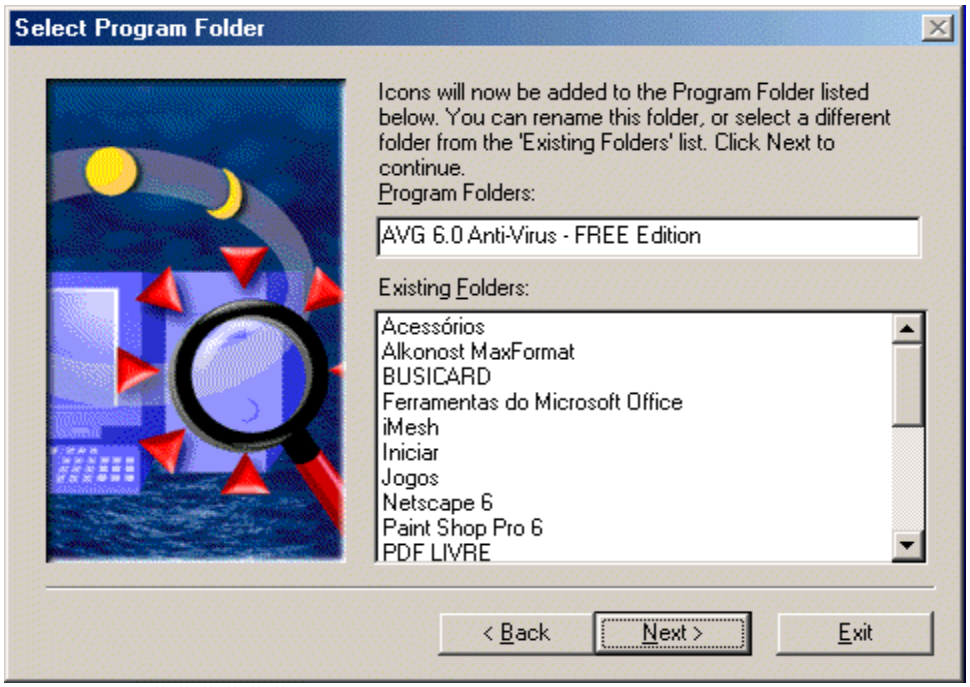
(figura 4)

A figura 5 mostra a janela Installation Location que informa o local onde serão instalados os arquivos do programa antivírus.



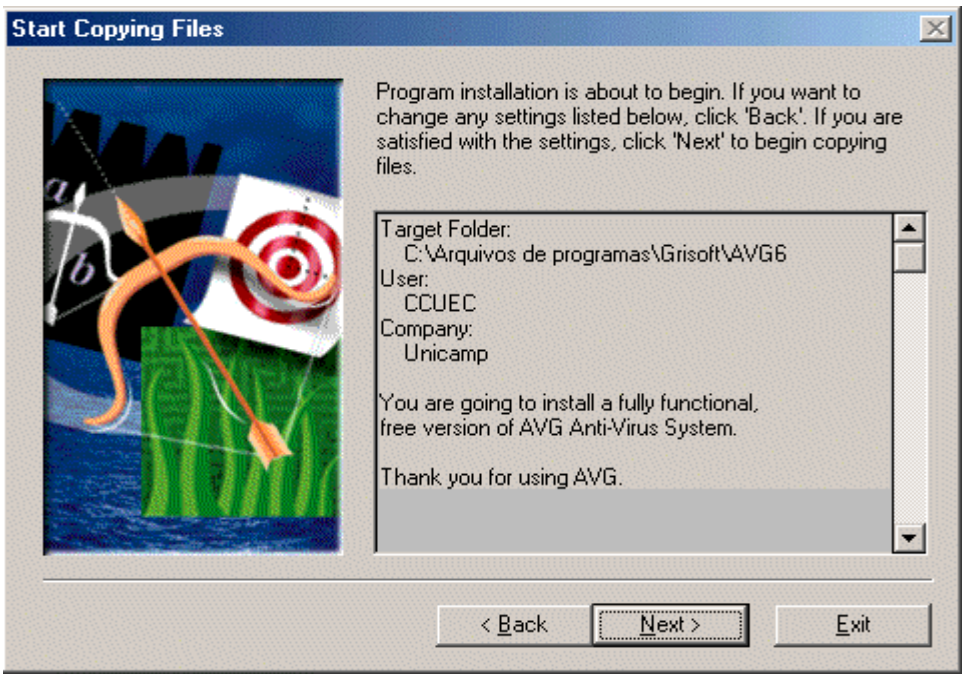
(figura 5)

Na tela Select Program Folder (figura 6), o programa de instalação informa onde serão adicionados os ícones e sua respectiva pasta dentro do menu Iniciar/Programas.



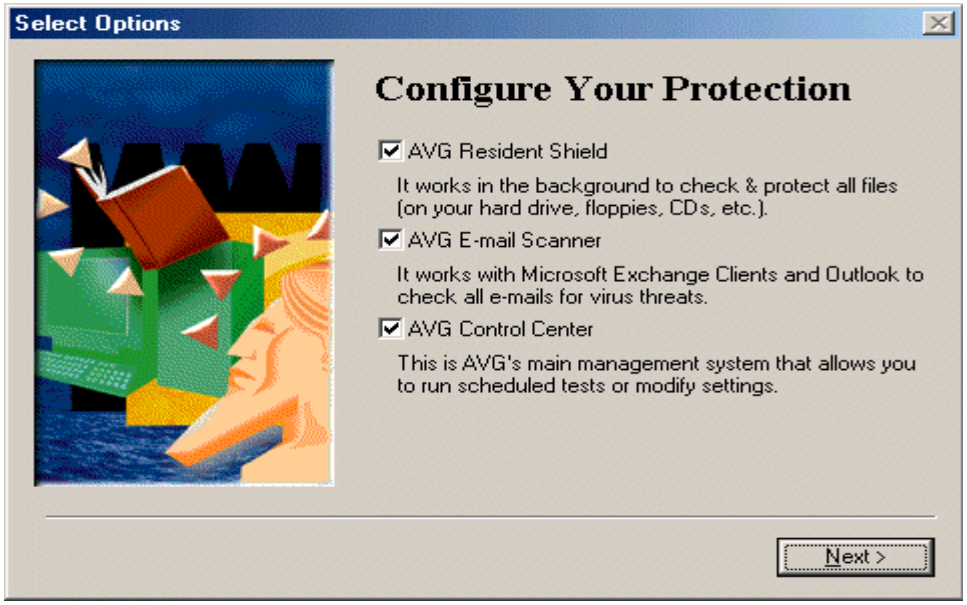
(figura 6)

Na figura 7, janela “Start Copying Files”, o programa de instalação dispõe informações gerais sobre o local de instalação de seus arquivos e identificação do usuário antes de iniciar a instalação propriamente dita.



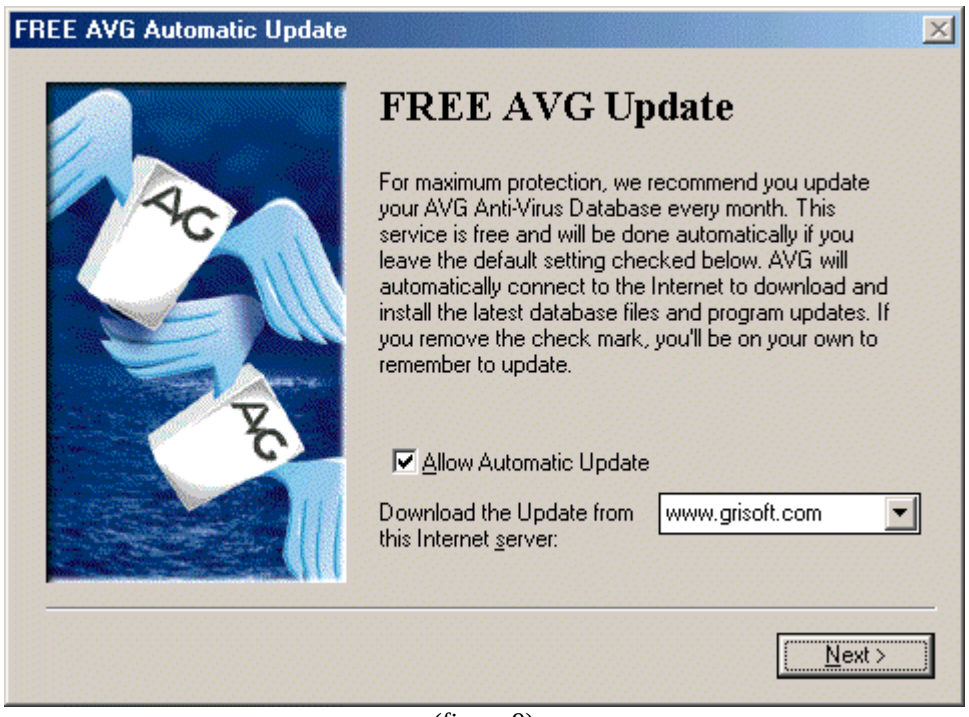
(figura 7)

Na janela Select Options (figura 8) o programa de instalação informa quais serviços de proteção podem ser configurados. Todos devem ficar ativos como proposto pelo programa de instalação.



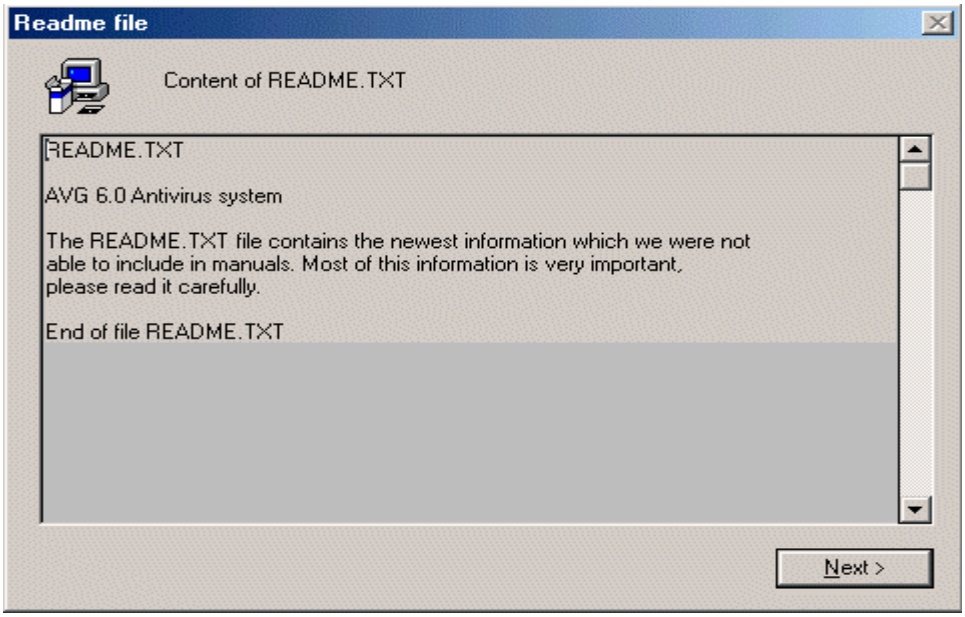
(figura 8)

O antivírus AVG dispõe de um serviço automático de atualização, o FREE AVG Automatic Update (figura 9). Clique em Next para aceitar esse importante recurso.



(figura 9)

A janela Readme File (figura 10), cita o arquivo de informações sobre o antivírus e o manual do usuário.

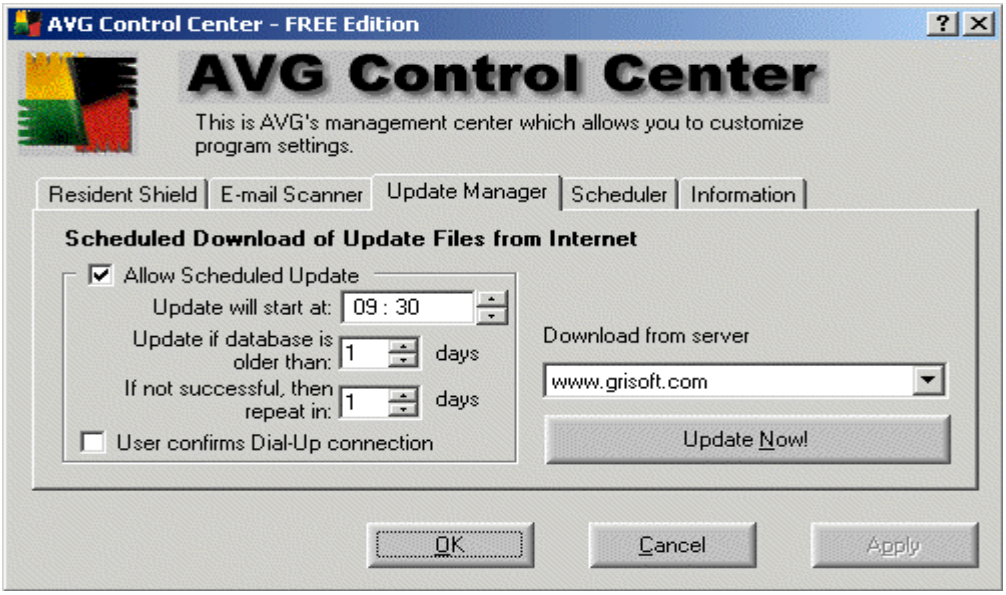


(figura 10)

Após a conclusão da instalação do AVG, será solicitada a reinicialização do Windows para que seu registro seja atualizado com as informações do novo programa antivírus (figura 11). Clique em OK.

(figura 11)

O AVG possui a característica de atualização automática. É um sistema que permite indicar um horário para que seja feita conexão com o servidor da desenvolvedora e possibilite o download das últimas versões de atualização. Pode-se optar ainda por atualizar o antivírus manualmente, basta clicar no botão Update Now, da guia Update Manager do AVG Control Center. (figura 12)



(figura 12)

Sites Relacionados:

- Grisoft Inc. – AVG Antivírus System
  - http://www.grisoft.com

- Network Associates – Mcafee VirusScan
  - http://www.nai.com/international/brazil

- Symantec – Norton Antivírus
  - http://www.symantec.com.br

- SplitNet
  - http://www.splitnet.com

CCUEC / Help Desk :

Atendimento: de 2ª à 6ª, das 14:00 às 17:00
Ramal: 82216 - **Direto**: 37882216
e-mail: apoio@ccuec.unicamp.br