Dicas sobre vírus

Dez mandamentos antivírus

Primeiro - sempre use antivírus residente na memória.

O fato de termos arquivos de antivírus armazenados no disco rígido nada significa em termos de proteção. Como os programas só podem realizar alguma coisa no computador quando cópias deles são carregadas para a memória, torna-se compreensível que, se desejamos que um vírus não chegue à memória, que outro programa específico esteja lá de guarda, na memória.
Nos programas de antivírus é opcional ao instalador habilitar ou não o antivírus na memória automaticamente, sempre que se liga o computador. Recomenda-se que esta opção seja sempre a selecionada.

Segundo - nunca use dois antivírus ao mesmo tempo.

Nunca use mais de um antivírus residente na memória, embora se possa ter outros apenas armazenados no disco rígido. Esta recomendação decorre do fato de um antivírus instalado na memória ocupar sempre as mesmas áreas críticas para controle da invasão de um vírus. Fatalmente ocorrerá conflitos, e mensagens falsas da presença de vírus podem ser exibidas na tela. Sempre desinstale o anterior antes de instalar um novo ou nova versão do mesmo antivírus.

Terceiro - Nunca Use Antivírus Desconhecido.

Ao procurar um antivírus, selecione um que seja tradicional no mercado. Nunca tente um novo antivírus sem aconselhamento adequado. Softwares antivírus residentes têm que ser de muito boa qualidade a fim de poupar "recursos" e ser compatível com os requisitos do sistema, do contrário eles podem ser responsáveis por freqüentes congelamentos.

Quarto - sempre mantenha o antivírus atualizado.

O principal em um aplicativo antivírus é a sua atualização. De nada adianta instalar um programa antivírus, sem ter os arquivos de assinaturas dos vírus atualizados, o mais freqüentemente possível. Recomenda-se que os sites dos fornecedores sejam visitados pelo menos uma vez por semana para:

- efetuar download dos arquivos de assinaturas de vírus; e
- verificar se a versão mais atual da "engine" de software coincide com a instalada. Caso contrário, efetuar também o download da "engine".

NOTA: Os arquivos de assinaturas de vírus requerem a versão correta da "engine" de software.

Normalmente os sistemas de download instalam automaticamente as atualizações necessárias, quando o micro estiver conectado ao seu site, sem grande envolvimento do usuário. Para usuários que não tenham suficiente conhecimento desta operações, recomenda-se consultar uma pessoa familiarizada com o processo. Lembre-se que, a cada 30 dias, surgem cerca de 200 novos vírus (sempre de ocorrência mais freqüente que os mais antigos) contra os quais não se dispõe de proteção.

Quinto - sempre faça verificação de vírus.

Como os vírus e worms (vermes) podem invadir o sistema de um usuário num momento de distração, torna-se crucial que verificações sejam efetuadas periodicamente. Uma verificação total é recomendada toda vez que se atualiza o antivírus ou seus arquivos de assinaturas de vírus.

Sexto - nunca execute programas desconhecidos.

A maior ameaça aos dados de um usuário é o próprio usuário. Afinal, é ele quem mais lida com seus dados. Inadvertidamente o usuário deleta arquivos válidos, salva novos dados apagando os anteriores ainda válidos, salva trabalhos sem verificar qual a pasta para onde está salvando e depois acha que o computador é temperamental, isto é "ora salva ora não salva".
O maior cuidado refere-se à "irresistível" curiosidade quanto à execução de programas e arquivos desconhecidos recebidos. É deste humano ponto fraco que se valem os desumanos hackers criadores de vírus e principalmente de Cavalos-de-Tróia.

Sétimo - sempre fiscalize comportamentos anormais.

Há muitos vírus mal feitos que apresentam bugs (pequenos defeitos). Estes defeitos, às vezes, deixam o computador mais lento, ou interferem com o ponteiro do mouse na tela, ou causam resultados inesperados a certos comandos normais ou trancamentos muito freqüentes do Sistema Operacional (Windows). Os sintomas de falha de hardware e de software muitas vezes podem indicar um sinal de que arquivos normais que controlam hardware e software básico (Windows) foram contaminados por vírus que os corromperam no ato da contaminação sendo ou não, esta corrupção, a intenção principal do hacker fazedor do vírus.

Recomenda-se, quando falhas, inicialmente supostas como de hardware e/ou de software, permitirem operar o computador, executar uma varredura (scan) para verificação de vírus.
Não confundir com comportamentos anormais devido a insuficiência de "recursos" do Windows ou à programas honestos também mal feitos ou mal comportados.

Oitavo - sempre feche selo proteção de disquetes.

O selo deslizante que os disquetes de 3 1/2" possuem, quando na posição "fechado", impede fisicamente a gravação de qualquer coisa no mesmo. Atua como uma segurança contra ações inadvertidas do próprio usuário ou de terceiros ao manipular dados importantes em certo número de disquetes.
Este selo está na posição "FECHADO" quando paradoxalmente, se vê aberto o vazado do orifício quadrado, que o selo esconde no disquete, quando está na posição "ABERTO".

ATENÇÃO: Para se ler ou copiar um arquivo do disquete ou todo um disquete NÃO é necessário que o selo de proteção-contra-gravação esteja na posição "ABERTO". O selo é para impedir gravação mas, não a leitura.

Nono - sempre tenha backups e um disco "boot".

Considerando que o trabalho, que o usuário realiza num computador, está sendo feito na MEMÓRIA, que apaga quando se desliga a corrente elétrica ou é limpa quando se reinicia o computador, a rotina mais recomendável é a de se SALVAR A CADA 5 A 10 MINUTOS o trabalho que se está realizando, pois assim uma cópia atualizada será transferida para meios magnéticos que não apagam na ausência de eletricidade.
Para trabalhos mais complexos ou nas fases em que ele é mais complexo, recomenda-se SALVAR A CADA 3 A 5 MINUTOS. Exemplo: montagem de uma complexa tabela num editor de texto ou uma complicada fórmula numa planilha. Neste caso a cada fase concluída deve-se salvar o trabalho, independentemente do tempo transcorrido desde o último salvamento. O mesmo ocorre para outros aplicativos.

Décimo - nunca trabalhe com micro infectado.

Nunca continue a trabalhar com um computador infectado, pois além dos vírus poderem causar freqüentes trancamentos, mais cedo ou mais tarde, fatalmente causarão perda ou corrupção de arquivos vitais no disco rígido, tornando o computador inoperante, dificultando a operação de limpeza.
Com o computador infectado, isto é, com o vírus na MEMÓRIA, cada disquete, que esteja com o selo de proteção-contra-gravação ABERTO, que for inserido no drive (A:) para se copiar um arquivo dele para o disco rígido, ou deste para o disquete, será infectado em seu setor de boot e/ou em certos arquivos executáveis nele contidos.
Assim, quanto mais tempo se levar para se limpar um computador infectado, maior número de disquetes serão provavelmente infectados, aumentando em muito o trabalho de limpeza.