PCWORLD
TECNOLOGIA+INOVAÇÃO+PRODUTIVIDADE
http://www.pcworld.com.br

**DICAS**

# Evite ser pego pelo malware

(http://pcworld.uol.com.br/dicas/2010/11/30/evite-ser-pego-pelo-malware)

**Justin Phelps, da PC World EUA**

30/11/2010

## Bastam alguns ajustes de comportamento e o software certo pra ficar mais protegido contra as ameaças que circulam pela internet.

Malware é um termo usado para descrever uma ampla categoria de software nocivo que inclui vírus, worms, cavalos de tróia, rootkits, spyware (software espião) e adware (software que enche seu PC de propaganda). Os efeitos do malware vão de um simples incômodo a panes frequentes no PC e roubo de identidade. É mais fácil evitar o malware do que removê-lo, e para isso é necessária uma estratégia em duas partes. Siga nossas dicas para se manter seguro.

### Fique atento e evite o malware

O principal fator na prevenção de uma infecção de seu PC por malware é você mesmo. Você não precisa ter treinamento ou conhecimento especializados, basta ficar de olho e evitar baixar e instalar qualquer coisa que você não entende ou na qual não confia, não importa quão tentadora seja a oferta, de fontes como estas:

*De um site na web:* se você não tem certeza, deixe o site e faça uma pesquisa sobre o software no Google. Se ele for inofensivo, basta voltar ao site e instalar. Se não, você terá evitado uma dor de cabeça.

*De um e-mail:* não confie em nada associado a uma mensagem de spam, e tenha cautela com e-mails de conhecidos que tenham links ou anexos. Se você suspeitar do que a mensagem quer lhe mostrar ou instalar, não clique nos links e apague-a.

*De mídia física:* seus amigos, familiares e conhecidos podem, sem perceber, lhe passar um disco ou pendrive contendo um arquivo infectado. Não abra nem execute nenhum arquivo sem antes analisá-lo com um software de segurança.

*De uma janela pop-up:* ao navegar na internet é comum encontrar janelas e avisos que tentam lhe empurrar um programa, prometendo corrigir ”erros críticos”, “falhas de segurança” ou “otimizar seu PC”. Estas mensagens geralmente tentam assustá-lo para fazer com que você aceite o que está sendo oferecido. Feche estas janelas imediatamente sem clicar em nada dentro delas, inclusive no X no canto da janela: use o atalho Alt+F4, ou clique com o botão direito do mouse no botão ou ícone correspondente a ela na barra de tarefas e clique em “Fechar janela”.

*De outros softwares:* alguns programas tentam colocar malware em seu computador como parte do processo de instalação. Ao instalar um programa, preste muita atenção na janela do instalador antes de clicar em botões como “Próximo”, “OK” ou “Eu Aceito”. Leia o contrato de licença em busca de menções a malware que possa ser parte da instalação. Se não tiver certeza cancele o processo, faça uma busca sobre o programa no Google e, se ele for mesmo seguro, instale-o novamente.

*De serviços de compartilhamento de arquivos:* se você se aventurar por aqui, estará sozinho. Não há controle de qualidade no mundo do software ilegal, e é fácil para um criminoso dar a um malware o nome de um filme, álbum ou programa popular para tentar fazer com que você o instale.

### Bloqueie o malware com o software certo

É provável que, não importa o quão cuidadoso você seja, um dia você será infectado. Isto acontece porque o malware é projetado para se infiltrar em seu computador de formas que você nem pode prever. Proteja-se com os seguintes programas:

*Um sistema operacional atualizado:* use o Windows Update e tire proveito de sua capacidade de avisá-lo automaticamente sobre novas atualizações. Melhor ainda, configure-o para baixá-las e instalá-las automaticamente e fique tranquilo.

*Um navegador atualizado:* não importa qual navegador você usa, mantê-lo em dia é vital para impedir uma infecção. Mozilla Firefox e Google Chrome são exemplos de browsers capazes de se atualizar automaticamente. Também aproveite recursos como bloqueio de pop-ups e varredura de downloads.

*Software antivírus:* se você quer se manter seguro, use um software antivírus. Mantenha-o atualizado, ligado e agendado para fazer uma varredura completa em sua máquina pelo menos uma vez por mês. Não rode dois antivírus na mesma máquina, ou pode acabar havendo conflito entre eles.

*Software anti-malware:* também conhecido como anti-spyware, é um componente comum de muitos pacotes de segurança no mercado, como o Norton Internet Security, Kaspersky Internet Security, Trend Micro Titanium Internet Security, Panda Internet

Security e Microsoft Security Essentials, entre muitos outros.. Se você não tem um, instale um anti-malware avulso que não entre em conflito com seu antivírus (veja os sites dos fabricantes) e mantenha-o atualizado.

*Firewall:* use ao menos o Windows Firewall, parte de versões recentes do Windows deste o XP SP 2, ou então um software dedicado para esta tarefa. Não rode dois firewalls simultâneamente, pois um pode interferir no outro.

*Filtro de SPAM:* se seu programa de e-mail não dá conta do recado na hora de filtrar as mensagens que chegam à sua caixa postal, considere o uso de um software especializado para esta tarefa. A maioria dos pacotes de segurança inclui um anti-spam, basta ativá-lo no painel de controle do software.