Como manter seu computador saudável

Frente às inúmeras ameaças, problemas e possibilidades existentes, é impossível manter um computador conectado à rede 100% seguro. O que se pode fazer é minimizar o risco desses problemas acontecerem, utilizando para isso medidas objetivas e desenvolvendo bons hábitos no uso do computador e da internet. Seguem algumas orientações que podem ajudar nesse processo. Apesar de serem mais voltadas ao Windows, a maioria dessas orientações são genéricas o suficiente para serem aplicadas também a quaisquer outros sistemas operacionais.

Cuidados essenciais (críticos)

- ***Mantenha o seu sistema operacional sempre atualizado***, preferencialmente de forma automática. Um sistema desatualizado é receita certa para que o computador seja infectado ou invadido, tendo ou não anti-vírus e firewall instalado.
- ***Não use conta com privilégios de administrador nas tarefas do dia a dia***. Utilize essa conta apenas onde for necessário, tais como nas instalações de programas, etc. Crie uma conta pessoal, com privilégios limitados e use essa para navegar, ler seus e-mails, etc. *Apenas essa simples medida pode reduzir drasticamente as possibilidades de infecção !*
- ***Utilize um bom anti-vírus e mantenha-o sempre atualizado***. Ele irá checar a navegação web,mensagens instantâneas (MSN & cia), recebimento e envio de e-mails, etc. Existem muitos *anti-vírus falsos* que, na verdade, são programas maliciosos que irão infectar o seu computador. Use sempre um anti-vírus de empresas confiável e conhecidas. *Em computadores da UFRGS, use preferencialmente o* ***F-secure*** *, que é licenciado.*
- ***Habilite o firewall do sistema ou instale um de terceiros***. O firewall efetua a filtragem de tráfego indesejado. Existem bons firewalls grátis para uso pessoal.
- ***Desabilite o AutoRun no sistema***. O AutoRun é aquela função que faz com que programas de instalação, músicas, etc, sejam executados quando uma mídia removível é inserida no drive (pendrive, etc). Esse mecanismo é muito utilizado por malwares para infectar computadores. Uma das atualização da Microsoft desabilitou por default esse recurso para os dispositivos USB. De qualquer forma, verifique se o AutoRun está mesmo desabilitado no seu computador.
- ***BONS HÁBITOS de navegação e no uso do computador***. Bons hábitos são adquiridos através de informação e uso do bom senso. O processo de adquirir bons hábitos ajuda a desenvolver o senso crítico, nos deixando mais "antenados" para reconhecer as possíveis ameaças e saber o que é razoável fazer (ou não fazer) para manter o nosso computador e os nossos dados mais seguros.

Cuidados importantes

- ***Proteja o seu computador com uma boa senha***, tanto na conta pessoal quanto na de administrador.
- ***Mantenha seus programas aplicativos sempre atualizados***. Não basta apenas o sistema operacional ser atualizado. Seu navegador, pdf reader, flash player, etc, podem ter vulnerabilidades tão sérias quanto as do sistema, e podem colocar seu computador em risco.
- ***Leia (e entenda!) os avisos que aparecem na tela do computador***. Não clique em alguma opção de uma janela que surgiu apenas pra se livrar dela e poder continuar o seu

trabalho.

- ***Instale um bom programa anti-spyware e mantenha-o sempre atualizado***. Sua atuação é complementar à do anti-vírus. Alguns podem bloquear acesso a sites maliciosos ou ameaças que o anti-vírus não detectou.

- ***Faça backups periódicos dos seus dados***. É o que vai garantir que seus dados não sejam perdidos para sempre se o pior acontecer com o seu computador.

- ***Compartilhe pastas na rede apenas se for absolutamente necessário*** e, mesmo assim, sempre com uma boa senha, e com as permissões adequadas. Se não for para ninguém incluir ou alterar dados na pasta, coloque atributos apenas para leitura. Nunca compartilhe a raiz de uma partição, especialmente a do sistema (C:\). Muitos vírus utilizam pastas compartilhadas para se propagar.

- ***Faça varreduras periódicas do sistema com o anti-vírus***, de preferência de forma automática, selecionando todos os drives e todos os tipos de arquivos (escolha uma hora de pouco uso do computador).

Cuidados Desejáveis

- ***Se possível, não utilize o Internet Explorer***. Historicamente, sempre foi fonte de problemas. Existem excelentes alternativas de navegadores, grátis para uso pessoal, tais como o *Firefox*, o *Chrome*, etc.

- ***Configure o Windows Explorer para mostrar todas as extensões dos arquivos***, facilitando assim reconhecer arquivos com extensões maliciosas, tipo ".txt.scr", por exemplo.

- ***Deixe desabilitados o java e javascript no seu navegador*** e habilite-os apenas quando necessário, desabilitando-os novamente depois. Alguns navegadores tem addons que permitem o controle da execução de java/javascript (por ex, o Firefox e o addon NoScript).

- ***Use o serviço do Proxy de Segurança da UFRGS para navegar***. Esse serviço pode bloquear o acesso a sites maliciosos, pornografia, pirataria, etc, permitindo uma navegação mais segura. *Dentro da UFRGS, esse serviço também pode ser usado diretamente, bastando para isso configurar o proxy no seu navegador:*

  Proxy: *proxyfilter.ufrgs.br* Porta: *3128*

- ***Mantenha no seu computador apenas os programas que você usa de fato***.

Bons hábitos

- ***Use sempre uma boa senha, para acessar suas contas***. Use senhas diferentes para contas diferentes.

- ***Fique atento às mensagens falsas*** (phishing & cia), recebidas por e-mail, mensagens intantâneas, SMS, etc.

- ***Não clique em links em mensagens de e-mails, mensagens instantâneas, etc***. Se for o caso, escreva a url do link à mão (não copie e cole!) no seu navegador.

- ***Não instale ou clique em arquivos recebidos via e-mails, mensagens instantâneas, etc***, sem ter certeza absoluta do que está fazendo. Mesmo arquivos tipo pdf, doc, flash e outros, podem conter código malicioso que podem causar danos aos seus dados ou ao sistema.

- ***Não aceite arquivos via e-mail ou mensagens instantâneas, sem estar explícito no texto seu envio*** , ou faça parte do contexto. Na dúvida, pergunte antes a quem enviou a mensagem. Da mesma forma, avise no texto que você está enviando que há um arquivo em anexo.

- ***Faça downloads de arquivos ou software apenas de sites conhecidos e confiáveis***. Não instale programas, plugins ou addons de origem duvidosa no seu computador. Se algum conhecido indicou algum programa, procure na internet um site confiável e baixe dali.

- ***Não acesse sites considerados de risco***, como por exemplo, sites de programas piratas, hackers, servidores piratas de jogos on-line, etc. É muito comum esses sites conterem páginas maliciosas e arquivos infectados.
- ***Evite usar programas de compartilhamento de arquivos***. São os programas do tipo eMule, Limewire, kazaa, etc. *Por motivos de segurança, a UFRGS* ***não permite*** *o uso desses programas !* Entretando, muitos usuários utilizam eles em casa. O uso desses programs é fonte muito comum de infecções, seja devido a falhas do próprio programa ou pela possibilidade de baixar arquivos infectados. Lembre que esse arquivos geralmente são baixados de computadores de outros usuários, que podem estar infectados.

- ***Acostume-se a verificar se a conexão é segura*** quando for efetuar determinadas operações na web (login, ler e-mails, acesso a sites bancários, etc). O ícone do *cadeado fechado deve estar na barra do navegador (e não na página!)* e a url deve começar por "https:" (note o "s" ali)

- ***Verifique sempre as mídias removíveis, tais como pendrives, mp3 players, etc***, quando forem conectadas no seu computador, para ver se não estão infectadas.

- ***Habilite a proteção de tela com senha, quando precisar se afastar do computador***.
- ***Feche a sua sessão, se não for mais utilizar o computador***.

- ***Desligue o seu computador, se não for usá-lo por um longo tempo***.

- ***Não permita que pessoas desconhecidas utilizem seu computador***. Tendo acesso físico, é muito fácil acessar o sistema e as demais contas.

- ***Evite utilizar o recurso de "lembrar a senha"***, existente em navegadores e outros aplicativos. Esse recurso facilita as coisas tanto para você quanto para quem quer acessar seus dados.
- ***MEU COMPUTADOR FOI INFECTADO !!!*** Apesar de todos os cuidados, isso é uma coisa que pode acontecer. Nesse caso, é importante tomar as seguintes medidas:
    - *Remova o cabo de rede (ou desconecte a interface wireless)* para que outros computadores da rede da UFRGS não sejam infectados também.
    - *Entre em contato com o administrador da rede ou com o bolsista responsável da sua Unidade.*
    - *Faça varredura no seu computador com anti-vírus on-line (use mais de um!). Você pode escolher um desses anti-vírus relacionados em ferramentas. Lembre que o anti-vírus instalado no computador infectado não é mais confiável !*
    - Se não houver ninguém que possa ajudar na sua Unidade, *entre em contato com a* **Central de Atendimento**, pelo fone **3308-5333** ou pelo e-mail "**central@cpd.ufrgs.br**", *e solicite orientação.*