# Guia de segurança do cardionauta

Nesta edição do Jornal SBC, continuamos a tratar dos diversos riscos envolvidos no uso da internet e seus métodos de prevenção. Comentaremos sobre Worms, vulnerabilidade, Backdoors, navegação na internet e salas de bate-papo.

## Worms:

São aplicativos que realizam uma série de atividades, incluindo sua propagação, sem que o usuário tenha conhecimento. Além de utilizar um bom antivírus, que permita detectar e até mesmo evitar a propagação de um worm, é importante que o sistema operacional e os softwares instalados em seu computador não possuam vulnerabilidades.

## Vulnerabilidade:

A melhor forma de evitar que o sistema operacional e os softwares instalados em um computador possuam vulnerabilidades é mantê-los sempre atualizados. Entretanto, fabricantes, em muitos casos, não disponibilizam novas versões de seus softwares quando é descoberta alguma vulnerabilidade, mas sim correções específicas (patches). Estes patches, em alguns casos também chamados de hot fixes ou service packs, têm por finalidade corrigir os problemas de segurança referentes às vulnerabilidades descobertas. Existem sites na internet que mantém listas atualizadas de vulnerabilidades em softwares e sistemas operacionais. Alguns destes sites são http://www.cert.org/ e http://cve.mitre.org/.

## Backdoors:

São entradas deixadas desprotegidas no seu computador. A maneira mais eficaz de preveni-los é sempre atualizar as versões do seu sistema operacional e evitar a instalação de programas como o Kazaa. É importante ressaltar que os antivírus não detectam backdoors. Use também um firewall para travar eventuais intromissões.

## Navegação na internet:

Os riscos envolvidos quando se navega pela internet podem estar relacionados a:

- execução de Javascript ou de programas Java hostis;
- execução de programas ou controles ActiveX hostis;
- obtenção e execução de programas hostis em sites não confiáveis.

Ao serem executados, esses programas podem fazer de tudo, desde enviar um arquivo qualquer pela internet, até instalar programas (que podem ter fins maliciosos) em seu computador.

**Algumas medidas preventivas para navegar na internet:**

- manter o seu navegador sempre atualizado;
- desativar a execução de programas Java na configuração de seu navegador. Se for absolutamente necessário o Java estar ativado para que as páginas de um site possam ser vistas, basta ativá-lo antes de entrar no site e, então, desativá-lo ao sair;
- desativar a execução de Javascripts antes de entrar em uma página desconhecida e, então, ativá-la ao sair. Caso você opte por desativar a execução de Javascripts na configuração de seu navegador, é provável que muitas páginas Web não possam ser visualizadas;
- permitir que programas ActiveX sejam executados em seu computador apenas quando vierem de sites conhecidos e confiáveis;
- manter maior controle sobre o uso de cookies, caso você queira ter maior privacidade ao navegar na Internet;
- certificar-se da procedência do site e da utilização de conexões seguras ao realizar transações via Web.

**Salas de bate-papo, comunicadores tipo ICQ, Odigo, Messanger:**

Tais programas podem fornecer o seu endereço na internet (endereço IP). Um atacante pode usar esta informação para, por exemplo, tentar explorar uma possível vulnerabilidade em seu computador. Algumas medidas preventivas para o uso de programas de troca de mensagens são:

- manter seu programa de troca de mensagens sempre atualizado;
- não aceitar arquivos de pessoas desconhecidas;
- evitar fornecer muita informação, principalmente a pessoas que você acabou de conhecer;
- não fornecer, em hipótese alguma, informações sensíveis, tais como senhas ou números de cartões de crédito;
- configurar o programa para ocultar o seu endereço IP.

Ainda temos outros temas importantes sobre segurança, como Comércio Eletrônico e internet Banking, que trataremos na próxima edição do Jornal SBC. Aguardem!

**Augusto Uchida**