# Dicas de segurança na internet

## Introdução

Quando você sai de casa, certamente toma alguns cuidados para se proteger de assaltos e outros perigos existentes nas ruas. Na internet, é igualmente importante pôr em prática alguns procedimentos de segurança, já que golpes, espionagem e roubo de arquivos e senhas são apenas alguns dos problemas que as pessoas podem ter na Web. É para ajudá-lo a lidar com isso que o InfoWester apresenta a seguir, quinze dicas importantes para você manter sua segurança na internet e em seu computador.

### 1 - Saia usando Logout, Sair ou equivalente

Ao acessar seu webmail, sua conta em um site de comércio eletrônico, sua página no Orkut, seu *home banking* ou qualquer outro serviço que exige que você forneça um nome de usuário e uma senha, clique em um botão/link de nome **Logout**, **Logoff**, **Sair**, **Desconectar** ou equivalente para sair do site. Pode parecer óbvio, mas muita gente simplesmente sai do site fechando a janela do navegador de internet ou entrando em outro endereço. Isso é arriscado, pois o site não recebeu a instrução de encerrar seu acesso naquele momento e alguém mal-intencionado pode abrir o navegador de internet e acessar as informações de sua conta, caso esta realmente não tenha sido fechada devidamente.

### 2 - Crie senhas difíceis de serem descobertas

Não utilize senhas fáceis de serem descobertas, como nome de parentes, data de aniversário, placa do carro, etc. Dê preferência a seqüências que misturam letras e números. Além disso, não use como senha uma combinação que tenha menos que 6 caracteres. O mais importante: não guarde suas senhas em arquivos do Word ou de qualquer outro programa. Se necessitar guardar uma senha em papel (em casos extremos), destrua-o assim que decorar a seqüência. Além disso, evite usar a mesma senha para vários serviços. Mais orientações sobre senhas podem ser encontradas aqui.

### 3 - Mude a sua senha periodicamente

Além de criar senhas difíceis de serem descobertas, é essencial mudá-las periodicamente, a cada três meses, pelo menos. Isso porque, se alguém conseguir descobrir a senha do seu e-mail, por exemplo, poderá acessar as suas mensagens sem que você saiba, apenas para espioná-

lo. Ao alterar sua senha, o tal espião não vai mais conseguir acessar as suas informações.

**4 - Use navegadores diferentes**

Se você é usuário do sistema operacional Windows, talvez tenha o hábito de utilizar apenas o navegador Internet Explorer. O problema é que existe uma infinidade de pragas digitais (spywares, vírus, etc) que exploram falhas desse navegador. Por isso, uma dica importante é usar também navegadores de outras empresas, como o Opera e o Firefox, pois embora estes também possam ser explorados por pragas, isso ocorre com uma freqüência menor neles. Se ainda assim preferir utilizar o Internet Explorer, use um navegador alternativo nos sites que você considerar suspeitos (páginas que abrem muitas janelas, por exemplo).

**5 - Cuidado com downloads**

Se você usa programas de compartilhamento de arquivos, como *eMule*, ou costuma obter arquivos de sites especializados em downloads, fique atento ao que baixar. Ao término do download, verifique se o arquivo não possui alguma coisa estranha, por exemplo, mais de uma extensão (como *cazuza.mp3.exe*), tamanho muito pequeno ou informações de descrição suspeitas, pois muitos vírus e outras pragas se passam por arquivos de áudio, vídeo e outros para enganar o usuário. Além disso, sempre examine o arquivo baixado com um antivírus.

Também tome cuidado com sites que pedem para você instalar programas para continuar a navegar ou para usufruir de algum serviço. Ainda, desconfie de ofertas de programas milagrosos, capazes de dobrar a velocidade de seu computador ou de melhorar sua performance, por exemplo.

**6 - Atente-se ao usar Windows Live Messenger, Google Talk, AIM, Yahoo! Messenger, entre outros**

É comum encontrar vírus que exploram serviços de mensagens instantâneas, tais como o Windows Live Messenger (antigo MSN Messenger), AOL Instant Messenger (AIM), Yahoo! Messenger, entre outros. Essas pragas são capazes de, durante uma conversa com um contato, emitir mensagens automáticas que contém links para vírus ou outros programas maliciosos. Nessa situação, é natural que a parte que recebeu a mensagem pense que seu contato é que a enviou e clica no link com a maior boa vontade:


Mesmo durante uma conversa, se receber um link que não estava esperando, pergunte ao contato se, de fato, ele o enviou. Se ele negar, não clique no link e avise-o de que seu computador pode estar com um vírus.

**7 - Cuidado com e-mails falsos**

Recebeu um e-mail dizendo que você tem uma dívida com uma empresa de telefonia ou afirmando que um de seus documentos está ilegal, como mostra a imagem abaixo?


Bem-vindo ao
TRIBUNAL SUPERIOR ELEITORAL
Praça dos Tribunais Superiores - Bloco C
CEP: 70.096-900 Brasília/DF (61) 316-3000
Fax: (61)3322-0603/0630/0641/0642

Brasília, 05 de Fevereiro de 2006

Informamos que seu titulo eleitoral teve um **Cancelamento provisório**.

O motivo do cancelamento foi uma irregularidade em seu Cadastro de Pessoa Física (CPF) a qual motivou o cancelamento do mesmo, e também de seu título eleitoral.

Para saber mais detalhes sobre esta irregularidade, e quais providências tomar, leia o regulamento clicando no link abaixo.

Após clicar no link, será exibida uma janela, onde a opção "Abrir" deve ser clicada.

CLIQUE AQUI PARA ABRIR O REGULAMENTO

ou se não conseguir Clique Aqui

INFOWESTER.COM

Todos os direitos reservados ao Tribunal Superior Eleitoral

Ou, ainda, a mensagem te oferece prêmios ou cartões virtuais de amor? Te intima para uma audiência judicial? Contém uma suposta notícia importante sobre uma personalidade famosa? É provável que se trate de um **scam**, ou seja, um e-mail falso. Se a mensagem tiver textos com erros ortográficos e gramaticais, fizer ofertas tentadoras ou tem um link diferente do indicado (para verificar o link verdadeiro, basta passar o mouse por cima dele, mas sem clicar), desconfie imediatamente. Na dúvida, entre em contato com a empresa cujo nome foi envolvido no e-mail.

Acesse os seguintes links para saber como lidar com e-mails falsos:

- Dicas contra e-mails falsos;
- Fique atento: scams usam sustos para enganar internautas.

**8 - Evite sites de conteúdo duvidoso**

Muitos sites contêm em suas páginas scripts capazes de explorar falhas do navegador de internet, principalmente do Internet Explorer. Por isso, evite navegar em sites pornográficos, de conteúdo hacker ou que tenham qualquer conteúdo duvidoso.

**9 - Cuidado com anexos de e-mail**

Essa é uma das instruções mais antigas, mesmo assim, o e-mail ainda é uma das principais formas de disseminação de vírus. Tome cuidado ao

receber mensagens que te pedem para abrir o arquivo anexo, principalmente se o e-mail veio de alguém que você não conhece. Para aumentar sua segurança, você pode checar o arquivo anexo com um antivírus, mesmo quando estiver esperando recebê-lo.

**10 - Atualize seu antivírus e seu antispyware**

Muita gente pensa que basta instalar um antivírus para o seu computador estar protegido, mas não é bem assim. É necessário atualizá-lo regularmente, do contrário, o antivírus não saberá da existência de vírus novos. Praticamente todos os antivírus disponíveis permitem configurar uma atualização automática. Além disso, use um antispyware com freqüência para tirar arquivos e programas maliciosos de seu computador. Uma boa opção é o Spybot. Assim como o antivírus, o antispyware também deve ser atualizado para que este conheça pragas novas.

Em ambos os casos, verifique no manual do software ou no site do desenvolvedor, como realizar as atualizações.

**11 - Cuidado ao fazer compras na internet ou usar sites de bancos**

Fazer compras pela internet é uma grande comodidade, mas só o faça em sites de venda reconhecidos. Caso esteja interessado em um produto vendido em um site desconhecido, faça uma pesquisa na internet para descobrir se existe reclamações contra a empresa. Um bom serviço para isso é o site Reclame Aqui.

Ao acessar sua conta bancária através da internet, também tenha cuidado. Evite fazer isso em computadores públicos, verifique sempre se o endereço do link é mesmo o do serviço bancário e siga todas as normas de segurança recomendadas pelo banco.

**12 - Atualize seu sistema operacional**

O Windows é o sistema operacional mais usado no mundo e quando uma falha de segurança é descoberta nele, uma série de pragas digitais são desenvolvidas para explorá-la. Por isso, vá em Iniciar / Windows Update e siga as orientações no site que abrir para atualizar seu sistema operacional. Fazer isso uma vez ao mês é suficiente para manter seu sistema operacional atualizado.

Se for usuário de outro sistema operacional, como o Mac OS ou alguma distribuição Linux, saiba que essa dica também é válida. Falhas de segurança existem em qualquer sistema operacional, por isso, é importante aplicar as atualizações disponibilizadas pelo desenvolvedor.

**13 - Atualize também os seus programas**

Também é importante manter seus programas atualizados. Muita gente pensa que as versões novas apenas adicionam recursos, mas a verdade é que elas contam também com correções para falhas de segurança. Por isso, sempre utilize a última versão dos seus programas, especialmente os que acessam a internet (navegadores de internet, clientes de e-mail, etc). Muitos aplicativos contam com uma funcionalidade que atualiza o programa automaticamente ou avisa do lançamento de novas versões. É um bom hábito deixar esse recurso ativado.


**14 - Não revele informações importantes sobre você**

Em serviços de bate-papo (chat), no Orkut, em fotologs ou em qualquer serviço onde um desconhecido pode acessar suas informações, evite dar detalhes da escola ou da faculdade que você estuda, do lugar onde você trabalha e principalmente de onde você mora. Evite também disponibilizar dados ou fotos que forneçam qualquer detalhe relevante sobre você, por exemplo, fotos em que aparecem a fachada da sua casa

ou a placa do seu carro. Nunca divulgue seu número de telefone por esses meios, tampouco informe o local em que você estará nas próximas horas ou um lugar que você freqüenta regularmente. Caso esses dados sejam direcionados aos seus amigos, avise-os de maneira particular, pois toda e qualquer informação relevante sobre você pode ser usada indevidamente por pessoas má-intencionadas, inclusive para te localizarem.

**15 - Cuidado ao fazer cadastros**

Muitos sites exigem que você faça cadastro para usufruir de seus serviços, mas isso pode ser uma cilada. Por exemplo, se um site pede o número do seu cartão de crédito sem ao menos ser uma página de vendas, as chances de ser um golpe são grandes. Além disso, suas informações podem ser entregues a empresas que vendem assinaturas de revistas ou produtos por telefone. Ainda, seu e-mail pode ser inserido em listas de SPAMs.

Por isso, antes de se cadastrar em sites, faça uma pesquisa na internet para verificar se aquele endereço tem registro de alguma atividade ilegal. Avalie também se você tem mesmo necessidade de usar os serviços oferecidos pelo site.

## Finalizando

Se proteger no "mundo virtual" pode ser um pouco trabalhoso, mas é importante para evitar transtornos maiores. A maioria dos golpes e das "ciladas" pode ser evitada se o usuário estiver atento, por isso é recomendável praticar as dicas mencionadas nesta página. Se quiser ir mais a fundo, o InfoWester possui outras matérias que lidam com segurança:

- Hoax: a corrente dos boatos, das lendas e dos golpes;
- Fique atento: scams usam sustos para enganar internautas;
- Ataques de engenharia social na internet;
- Dicas contra spywares;
- Dicas contra e-mails falsos;
- Dicas contra SPAM;
- Como criar senhas seguras.

*Escrito por Emerson Alecrim - Publicado em 06/02/2006 - Atualizado em 27/03/2008*