:: Dicas

Dicas de segurança na internet

Introdução

Se você toma alguns cuidados para garantir sua proteção quando sai de casa é porque sabe do risco de assaltos e outros crimes. A internet também se mostra como um lugar perigoso e é necessário alguns cuidados para evitar golpes, roubo de arquivos e senhas, ou espionagem de suas atividades nas contas de e-mail ou até mesmo em seu PC. É para ajudá-lo a lidar com isso que o InfoWester apresenta 12 dicas para manter a segurança de seus dados na internet e em seu computador.

1 - Saia usando Logout, Sair ou equivalente

Ao acessar seu webmail, sua conta num site de comércio eletrônico, 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 porque 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. Mais orientações sobre senhas podem ser encontradas aqui (/tutsenhas.php).

3 - Use navegadores diferentes

O Windows está presente na grande maioria dos computadores e, conseqüentemente, o Internet Explorer também. O problema é que existe uma infinidade de pragas digitais (spywares, vírus, etc) que exploram falhas desse navegador. Por isso, use navegadores como o Opera (http://www.opera.com) ou o Firefox (http://www.spreadfirefox.com/?q=affiliates&id=145699&t=62), pois embora estes também possam ser explorados por pragas, isso ocorre com uma freqüência muito menor neles. Se preferir usar o Internet Explorer, use um navegador alternativo nos sites que você considerar suspeitos (sites que abrem muitas janelas, por exemplo).

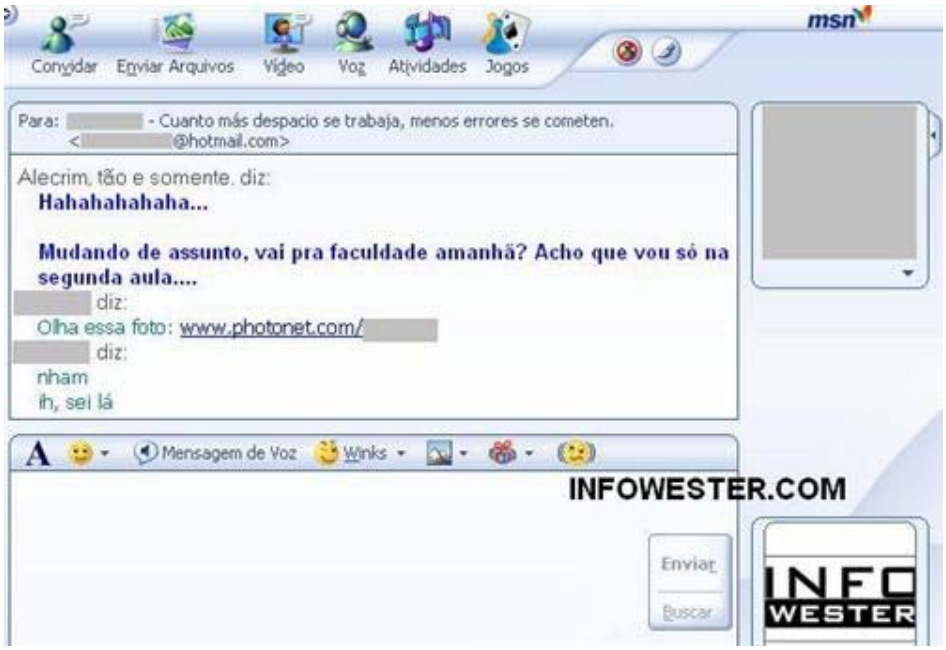
4 - Cuidado com downloads

Se você usa programas de compartilhamento de arquivos como KaZaA ou eMule, fique atento ao que baixar. Ao término do download, verifique se o arquivo não possui mais de uma extensão (por exemplo, *cazuza.mp3.exe*), se ele possui um tamanho muito pequeno ou se suas informações parecem suspeitas, pois muitos vírus 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.

5 - Atente-se ao usar MSN, Google Talk, AIM, ICQ, entre outros

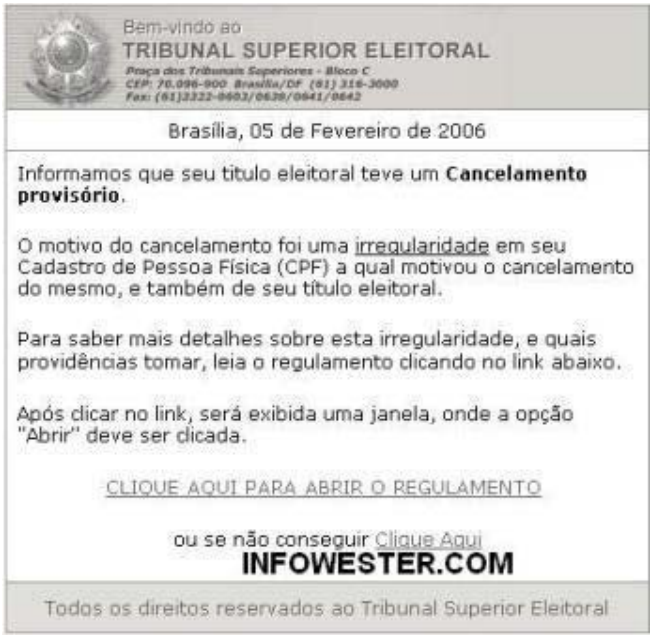
Alguns vírus já estão explorando sistemas de mensagens instantâneas, tais como MSN Messenger, AOL Instant Messenger, ICQ, Yahoo! Messenger, entre outros. Essas pragas são capazes de emitir uma mensagem que contém um link para um vírus ou para um programa-espião automaticamente numa conversa. Nessa situação, 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.

6 - 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?



Ou, ainda, a mensagem te oferece prêmios ou cartões virtuais de amor? É provável que se trata 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 (dicasmailsfalsos.php);
- Fique atento: scams usam sustos para enganar internautas (col200305.php).

7 - 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, hackers ou que tenham qualquer conteúdo duvidoso.

8 - Cuidado com anexos de e-mail

Essa é uma das instruções mais antigas, mesmo assim, e-mail é a principal forma 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.

9 - Atualize seu antivírus e seu anti-spyware

Muita gente pensa que basta instalar um antivírus e seu computador estará 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 anti-spyware com freqüência para tirar arquivos e programas maliciosos de seu computador. Uma boa opção é o Spybot (http://www.safer-networking.org/). Assim como no antivírus, o anti-spyware também deve ser atualizado para que este conheça as pragas novas.

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

10 - 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.

11 - Não revele informações importantes sobre você

Em salas de bate-papo, no Orkut (http://www.orkut.com) ou em qualquer meio em que você esteja lidando com um desconhecido: evite dar detalhes da escola ou da faculdade que você estuda, do lugar onde você trabalha e principalmente de onde você mora. Essas informações podem ser usadas para criminosos te localizarem. De igual forma, não revele seu número de telefone. Golpistas podem usá-lo para fazer ameaças ou alguém mal-intencionado pode te passar trotes.

12 - 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. **Essa dica é válida principalmente para sites que cadastram currículos.**

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 (col160106.php);

- Fique atento: scams usam sustos para enganar internautas (col200305.php);
- Ataques de engenharia social na Internet (col120904.php);
- Dicas contra spywares (/dicaspywares.php);
- Dicas contra e-mails falsos (dicasmailsfalsos.php);
- Dicas contra SPAM (/dicascontraspam.php);
- Como criar senhas seguras (/tutsenhas.php).

Escrito por Emerson Alecrim - Publicado em 06/02/2006 - Atualizado em 06/02/2006