7 Dicas para Segurança e Navegação na Internet

Spam, *phishing*, vírus, etc, são ameaças constantes à sua segurança enquanto navega na Internet. Para melhorar a segurança da sua navegação, indicamos alguns dos cuidados básicos a seguir:

1– Atenção às *Passwords*

São muitos os serviços da Internet em que é necessário definir uma *password* de acesso: *email*, banco *online*, "sites" de compras, etc. Desta forma, tenha em consideração as seguintes regras ao definir / utilizar uma *password*:

- Nunca faculte a sua *password* a terceiros nem a escreva em papéis, em ficheiros no computador ou no meio de contactos de telemóvel. Em caso de perda ou roubo, a "password" ficará acessível.

- Altere a *password* com frequência (recomendamos de 2 em 2 meses). Além disso, não deixe que as páginas de Internet a memorizem. Pode até poupar tempo nos *logins*, mas qualquer pessoa com acesso ao computador ficará também com acesso à *password* e consequentemente à informação a que esta dá acesso.

- Ao definir / alterar a *password*, tenha o cuidado de não utilizar sequências simples ou óbvias (ex.: aaaaa ou 123456). Evite também definir uma *password* semelhante ao próprio *username*/endereço, ou igual ao seu nome, data de nascimento, clube ou cor preferida.

- Para aumentar o grau de segurança da sua *password* opte não só por aumentar o número de caracteres (8 caracteres é razoável), mas também por utilizar em simultâneo caracteres minúsculos (abcd…), caracteres maiúsculos (ABCD…), números (12345…) e caracteres especiais (!”#$%...). Por exemplo: Taurus=2.

- Uma ideia simples para criar uma *password* muito segura e simples de memorizar: pense numa frase que tenha significado para si. Vamos utilizar como exemplo a frase “Ser ou não ser, eis a questão.”. Escolha apenas as iniciais de cada palavra e fica com “Sons,eaq”. Substitua uma das letras por um algarismo que seja semelhante (o S é semelhante ao 5), e aí tem a *password* final: “5on5,eaq”.

2 – *Logout* obrigatório

Sempre que pretenda sair do seu *email* (webmail), banco *online* ou qualquer outra página de Internet, em que previamente tenha introduzido um *username* e *password* para aceder, clique no botão / *link* de *Logout*, *Logoff*, Sair, Desconectar ou equivalente. É arriscado não o fazer, pois assim a página de Internet pode não receber a instrução de encerrar o acesso naquele momento. Entretanto, alguém mal-intencionado pode abrir a página e ter acesso à sua informação.

3 – Antivírus sempre actualizado

É frequente pensar-se que basta instalar um antivírus no seu computador para este estar protegido, mas não é bem assim. É necessário actualizá-lo regularmente, caso contrário, o antivírus não saberá da existência de vírus novos. Actualmente, quase todos os antivírus disponíveis permitem configurar uma actualização automática. Além disso, utilize também um *anti-spyware* (disponível na Internet) com frequência para tirar arquivos e programas maliciosos do seu PC. É também importante manter o sistema operativo actualizado, bem como os programas (especialmente os que acedem à Internet como *browsers* / navegadores de Internet). As novas versões muitas vezes vêm corrigir falhas de segurança das versões anteriores.

4 – *Downloads* sempre vigiados

Antes de abrir um ficheiro que descarregou para o seu PC, faça *scan* do mesmo com o seu antivírus.

5 – Evite *links* e sites de conteúdos duvidosos

É comum encontrar vírus que exploram os serviços de mensagens instantâneas, tais como o SAPO Messenger ou o MSN. Esses vírus são capazes de, durante uma conversa com um contacto, emitir mensagens automáticas que contêm *links* para vírus ou outros programas maliciosos. Mesmo durante uma conversa, se receber um *link* que não estava à espera, pergunte ao contacto se de facto ele o enviou. Se ele negar, não clique no *link* e avise-o de que o seu computador pode estar com um vírus.

Da mesma forma, desconfie de *emails* ou páginas de Internet com ofertas de programas milagrosos capazes de:

Aumentar a velocidade de seu computador ou da Internet;

Melhorar a performance do seu PC, ou que detectou vírus e promete resolver se instalar um executável (ficheiro com terminação .exe). Não instale esses programas / ficheiros no seu computador, pois ao fazê-lo poderá estar a instalar um vírus.

6 – Compras na Internet ou usar *sites* de bancos

Fazer compras pela Internet é uma grande comodidade, mas só o faça em páginas de venda reconhecidas. Caso esteja interessado num produto vendido num *site* desconhecido, faça uma pesquisa na Internet para descobrir se existem reclamações contra esse *site*.
Evite aceder à sua conta bancária através da Internet em computadores públicos. Verifique sempre se o endereço do *link* é mesmo o serviço e siga todas as normas de segurança recomendadas pelo banco.

7 – Guarde para si as suas informações pessoais

Muitos *sites* exigem o preenchimento de dados para usufruir dos seus serviços. Faça previamente uma pesquisa na Internet para verificar se aquele endereço tem registo de alguma actividade ilegal.

Além disso, tenha muita atenção com *emails* ou páginas de Internet que lhe peçam dados ou refiram acessos e *passwords* expirados. Muito provavelmente esses *emails* são falsos e pretendem roubar-lhe as informações de acesso aos respectivos serviços (por exemplo, *emails* que pedem para actualizar os seus dados de acesso ao seu banco *online*). Neste caso, valide com a empresa se realmente solicitaram essa informação. Por fim, nunca carregue em *links* enviados por *email* de páginas de Internet que conhece / utiliza. Ao clicar, poderá estar a entrar numa página muito parecida, mas que na realidade é falsa, e ao fornecer os dados de acesso, estará a enviá-los para quem criou essa página falsa. Este fenómeno chama-se *phishing* e infelizmente, tem-se tornado comum.

Fonte: Sapo Tek - Dezembro 2009