Guia rápido de segurança na WEB

Para entender melhor como você pode aproveitar com segurança tudo que a internet tem a oferecer, preparamos um guia rápido, com seis passos, que você pode consultar sempre que quiser.

1 - Verifique a segurança do site

Toda vez que navegamos em sites ou blogs estamos sujeitos a problemas, isso acontece porque esses sites solicitam suas informações pessoais para conectar-se à sua conta ou para concluir uma transação. Crackers, ladrões e programadores de spyware sabem disso, e muitas vezes tentam interceptar suas informações durante essas transações.

- **Sempre use sites e empresas seguros.**
- **Forneça suas informações somente para empresas respeitadas, conhecidas pela idoneidade.**
- **Verifique se o site da empresa usa um endereço da Web que começa com "https" e se possui um símbolo de cadeado na barra de endereço ou na parte inferior do navegador**. Isso significa que o site criptografa suas informações, praticamente inutilizando os dados para qualquer ladrão ou hacker que possa interceptar a transmissão.

2 - Escolha senhas fortes e variadas

Muitas pessoas acreditam que a senha por si só já é suficiente para garantir a segurança. Não é bem assim. Quando criar uma senha procure usar uma combinação de letras e números e inclua sempre que possível, um símbolo. Isso reforça sua senha e dificulta que alguém maliciosos a obtenha.

- Não use a mesma senha para tudo: os crackers escolhem sites com pouca segurança para acessar dados dos usuários e senhas correspondentes. Já pensou se você usa o mesmo login e senha para acessar sua conta no banco, por exemplo?
- Procure usar as autenticações oferecidas pelos sites – como quando vamos fazer o login e para validar a informação temos que usar um código que é enviado para um dispositivo selecionado ou para u smartphone. Isso dificulta muito a invasão de um terceiro à sua conta.
- Dê preferência ao uso de teclados virtuais, quando disponíveis.

3 - Não abra links em e-mails e mensagens sem prestar atenção antes

Se você não sabe quem foi que enviou a mensagem, evitar clicar em qualquer link, caso tenha algum. Isso serve tanto para mensagens instantâneas (Google Talk, Facebook, MSN, Skype, etc) quanto e-mails.
Os serviços atualmente contam com ótimos filtros de spam, mas alguma coisa pode passar.

- Desconfie de mensagens enviadas por remetentes desconhecidos. Nunca clique em nada nesses e-mails – um único clique basta para comprometer o seu computador.
- Cuidado com mensagens enviadas com supostos vídeos relacionados a grandes acontecimentos ou tragédias. Esses e-mails são feitos para que as pessoas, curiosas, abram a mensagem e anexos e é nesse momento que crackersroubam senhas e informações bancárias do usuário.
- Verifique se o site é realmente idôneo, passando o mouse por alguma imagem ou o logo/marca da empresa ou algum link disponibilizado na mensagem. Observe no canto inferior esquerdo, na sua tela, se o endereço que aparece é o mesmo do site que você está acessando. Se não for, farol vermelho: interrompa o acesso.

4 - Muito cuidado nas redes sociais

Acessadas por bilhões de pessoas – um prato cheio para os mal intencionados.

- Cuidado com aplicativos que são oferecidos! Nunca autorize aplicativos que não conhece a procedência ou que você não tenha 100% de confiança. A probabilidade de ser um golpe é grande e de se alastrar rapidamente também, prejudicando as pessoas de sua rede de contatos.
- Privacidade: Dividir nossas fotos e momentos é maravilhoso mas para evitar qualquer constrangimento, configure com atenção suas permissões e questões de privacidade; assim você compartilha apenas o que você quiser, com quem você escolher.

5 - Cuidado com *downloads*

Se você tem o costume de baixar *torrents*, já sabe que há risco dos arquivos estarem infectados com *malwares*. Se você baixa de sites na internet, também corre o risco de ser infectado.

- Alguns sites disfarçam um link maldoso com letras garrafais para chamar a atenção, enquanto o link real para o arquivo está escondido em letras menores.
- Desconfie se for informado para você instalar um software para gerenciar o download: é cilada.
- Evite instalar barra de ferramentas. Elas têm pouco a adicionar à sua navegação e costumam vir cheias de *malwares* ou apenas mudar as configurações do seu navegador.
- Cuidado com arquivos com as extensões exe. e dll. Certifique-se da origem antes de baixar ou instalar algo.

6 - Mantenha *softwares* (e apps) sempre atualizados

Isso não serve apenas para o antivírus. É fundamental que tudo esteja atualizado. Deixar seu navegador na versão mais recente vai diminuir os riscos de se navegar na web, afinal, as atualizações normalmente corrigem falhas de versões anteriores que podem ser exploradas por alguém mal intencionado.