Imprimir

As coisas mais perigosas que você pode fazer na internet

Por Renan Hamann
Fonte: www.tecmundo.com.br/7528-As-coisas-mais-perigosas-que-voce-pode-fazer-na-internet.htm

Sexta-Feira 7 de Janeiro de 2011

Confira quais são os erros mais comuns dos usuários de internet e saiba como proteger o seu computador.

A internet conecta milhões de pessoas, isso não é novidade. E desses milhões, há muitos que estão apenas procurando por computadores vulneráveis a ataques. O pior é que grande parte desses ataques não são feitos de maneira direta pelos crackers, mas são realizados porque usuários acessam links maliciosos e abrem as portas para invasões.

Não apenas isso, também há diversos outros hábitos, muito comuns, que fazem com que os computadores fiquem abertos a ataques. Confira alguns dos erros mais frequentes que a maioria dos usuários cometem e também saiba como evitar os riscos que atrapalhem a sua estadia na internet.

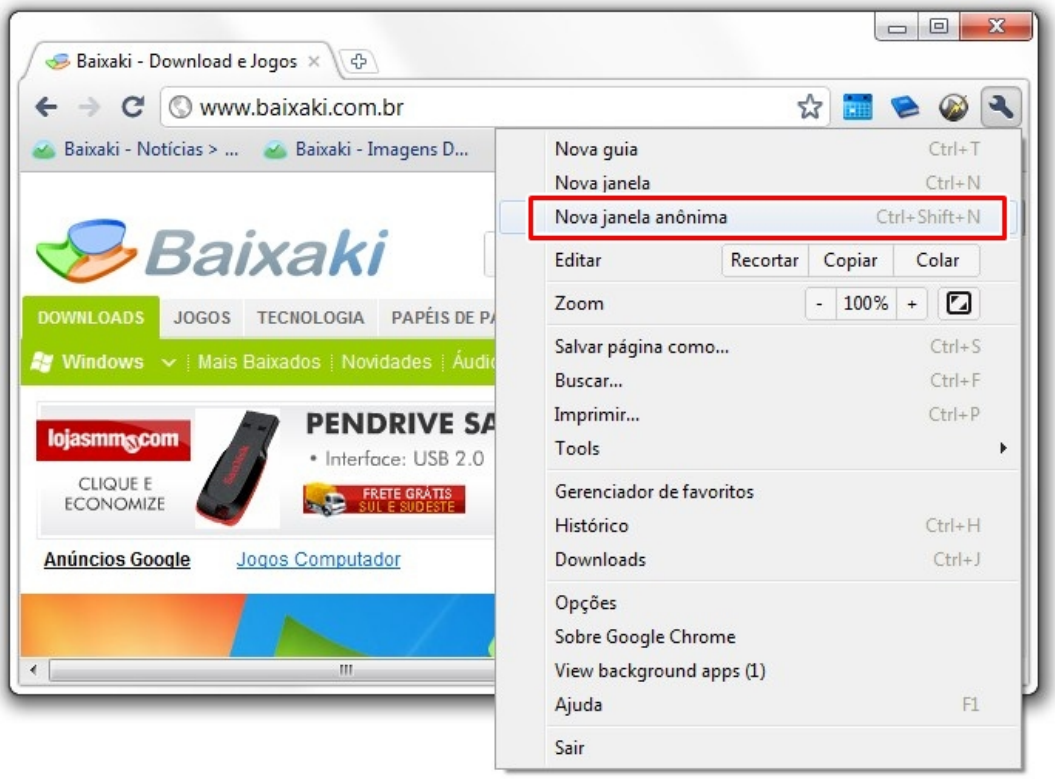
"Manter-me conectado"

Serviços de email e redes sociais possuem a opção "Manter-me conectado" para que os usuários não precisem digitar seus logins e senhas a cada vez que desejarem acessar suas contas. Isso pode ser muito útil para qualquer pessoa que não divida o computador, mas quando isso é feito em computadores públicos, o perigo é grande.

Computadores de lan houses e universidades são utilizados por muitas pessoas em períodos curtos. A qualquer momento pode surgir um usuário que, ao perceber que algum serviço já está logado, altera dados e insere informações caluniosas sobre a vítima, que só vai perceber os danos muito mais tarde.

Métodos de proteção

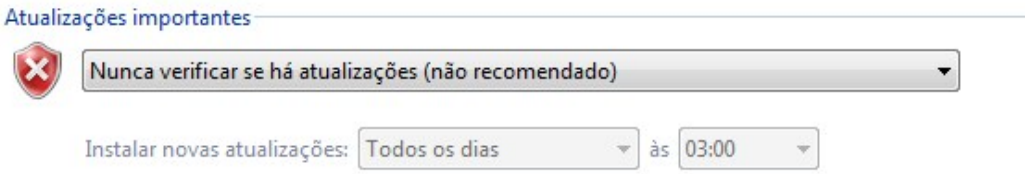
O modo mais básico para se proteger deste tipo de invasores é evitando marcar as caixas de seleção com dizeres similares a "Manter-me conectado" ou "Keep me loged in" (para sites em inglês). Mas também é importante que, ao final das sessões de utilização, cada usuário clique sobre os botões de saída do sistema.



Outra opção bastante recomendada é apagar o histórico e os cookies do navegador. Para isso, confira neste artigo as dicas que o Baixaki preparou. Por fim, ainda há a possibilidade de utilizar as janelas privadas dos navegadores. Dessa maneira, não são salvos endereços, cookies, histórico ou sessões iniciadas por qualquer usuário. Também é de suma importância que, em hipótese alguma, as senhas digitadas no computador sejam salvas.

Não atualizar aplicativos

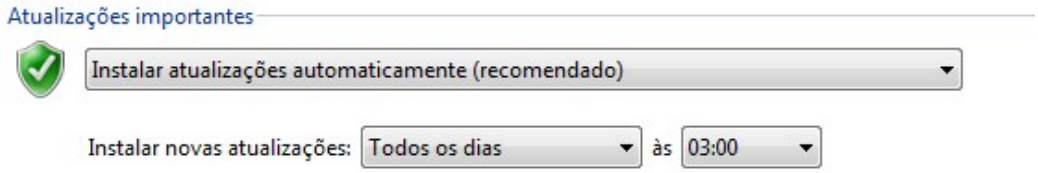
Programas vitais para o funcionamento do computador não podem ser deixados de lado na hora de realizar as atualizações. Sistema operacional e aplicativos com comunicação a servidores online (Adobe Flash, Adobe Reader e Java, por exemplo) podem ser verdadeiras portas de entrada para pragas virtuais.



Atualizações, por menores que sejam, são muito importantes para corrigir possíveis falhas estruturais que deixam os aplicativos vulneráveis e não efetuá-las, consequentemente, pode prejudicar os computadores.

Métodos de proteção

É muito simples livrar-se deste tipo de ameaça: permitindo que os programas sejam atualizados sempre que surgirem pacotes de correções. Desse modo, dificilmente alguma brecha será aberta para que usuários mal-intencionados roubem suas informações ou danifiquem o seu sistema operacional.



Interessante também configurar todos os programas para que as atualizações sejam buscadas automaticamente. Assim não há riscos de os usuários se esquecerem de buscar por atualizações, mantendo sempre o sistema com o máximo de segurança possível.

Procurar “escapulidas” de famosos

É difícil encontrar um usuário que nunca tenha se deparado com informações sobre traições de seus artistas favoritos, ou supostas gravações de vídeos adultos que fizeram com seus namorados, que prometeram “nunca mostrar para ninguém” e assim por diante. Muitos usuários mal-intencionados se aproveitam dessa curiosidade para espalhar vírus e outras pragas para o mundo.

Infectando uma enorme quantidade de computadores, é muito provável que senhas de cartões de crédito, listas de emails e outros dados que podem ser utilizados para causar danos sejam roubados.

Métodos de proteção

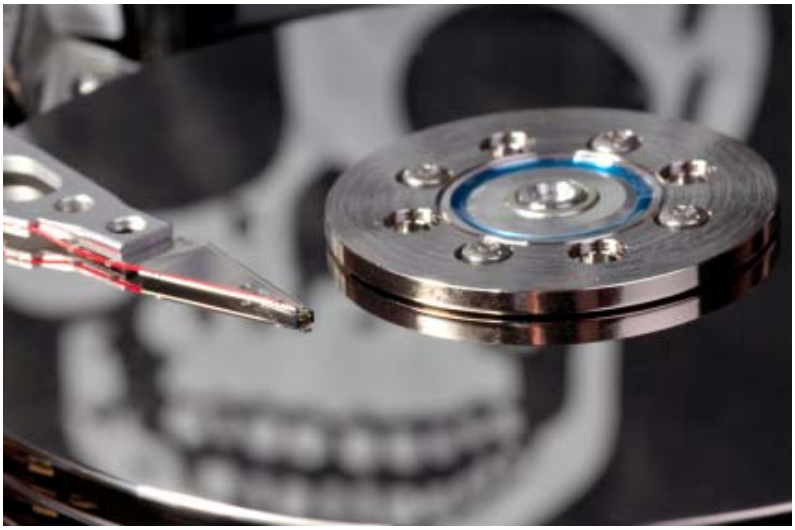
Não há uma dica mais certa do que: “Tome cuidado!”. 99% dos links que prometem vídeos comprometedores de artistas são apenas iscas para infectar computadores de usuários desavisados. Não clique nos links que mandam por email, muito menos em resultados de sites desconhecidos que são mostrados no Google.

Se sua curiosidade for maior que a necessidade de manter o computador livre de problemas, a possibilidade mais indicada (e ainda assim, pouco recomendada) é a utilização de agregadores confiáveis para buscar os conteúdos.

Baixar filmes e softwares ilegais

Muitos veem na pirataria, uma saída para gastos com programas de computador, jogos e filmes. O problema é que (além de desrespeitar as leis de direitos autorais) muitas destas fontes oferecem os mesmos riscos que o caso anterior.

Sites maliciosos são criados para atrair usuários em busca de licenças e softwares piratas e “fazem a festa” com as portas que são abertas. Ao “clicar para baixar”, os usuários também estão “clicando para infectar”, “clicando para permitir o acesso de crackers”, ou seja, deixando o computador vulnerável.



Métodos de proteção

Não baixe pirataria, essa é a grande dica para qualquer usuário. Além de correr muitos riscos de infecção no seu computador, ao baixar e instalar programas ilegais, você também estará deixando de incentivar a criação de novos softwares e infringindo leis de direitos autorais.

Procura por conteúdo adulto

Desde que a internet chegou aos computadores pessoais, sites de conteúdo adulto começaram a surgir e a se multiplicar de maneira exponencial. Logo chegaram os crackers e se aproveitaram desta enorme demanda por conteúdo adulto para criarem o império dos links maliciosos e das propagandas ilegais.

Não são raros os popups com técnicas e produtos para melhorar o desempenho sexual, propostas para cadastros em redes sociais apenas para maiores de idade e muitas outras opções que completam uma enorme gama de possibilidades.

Isso acontece porque esta busca é inerente ao ser humano. Desde que há (e enquanto houver) internet, vai existir procura por materiais do gênero. Um prato cheio para desenvolvedores maliciosos, que conseguem infectar um número enorme de computadores em pouquíssimo tempo.

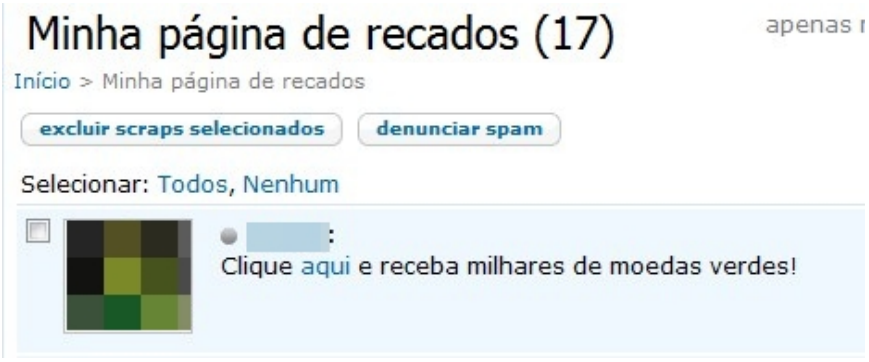
Métodos de proteção

Muitos antivírus possuem sistemas de proteção ativa, realizando varreduras em links antes de os usuários acessá-los. Utilizando este tipo de recurso, é possível saber se as páginas oferecem riscos ou se são confiáveis, mas este não é o único modo de se proteger.

Outro conselho que podemos dar é: “Sempre desconfie de conteúdo adulto gratuito na internet”. Caso queira muito acessar fotos e vídeos do gênero, converse com seus amigos para que lhe indiquem algum endereço confiável, sempre buscando por links que ofereçam o menor risco possível.

Jogos online e armadilhas escondidas

Além dos riscos oferecidos pelos jogos piratas disponibilizados na internet, baixar jogos gratuitos também pode ser um problema. Isso porque alguns não são realmente gratuitos, mas são anunciados como tal para atrair usuários, sem falar que alguns instaladores podem conter vírus e outros arquivos parecidos.



Jogos de redes sociais (como o Facebook e Orkut) oferecem perigos diferentes. Permitindo que recursos extras sejam adquiridos por meio de compras com dinheiro real, muitos deixam brechas para que crackers criem anúncios falsos com promessas de produtos grátis em links maliciosos.

Casos não faltam. Há algum tempo foram criados vários links maliciosos com a promessa de moedas verdes gratuitas para os jogadores do Colheita Feliz. Enviados por emails, o vírus comportava-se de maneira similar a outros também do Orkut (como os clássicos “Veja as fotos da festa, ficaram ótimas” e “Não acredito que ela fez isso. Kkkkk”) para se espalhar.

Métodos de proteção

Assim como a grande maioria das dicas dadas neste artigo, para evitar as contaminações neste tipo de caso é necessário não clicar sobre os links disponíveis nos websites. Dificilmente as empresas que desenvolvem jogos para redes sociais disponibilizam recursos gratuitos para seus usuários.

Em casos raros em que isso acontece, são emitidos avisos diretamente na interface do jogo, nunca são enviados emails ou recados para as páginas dos jogadores.

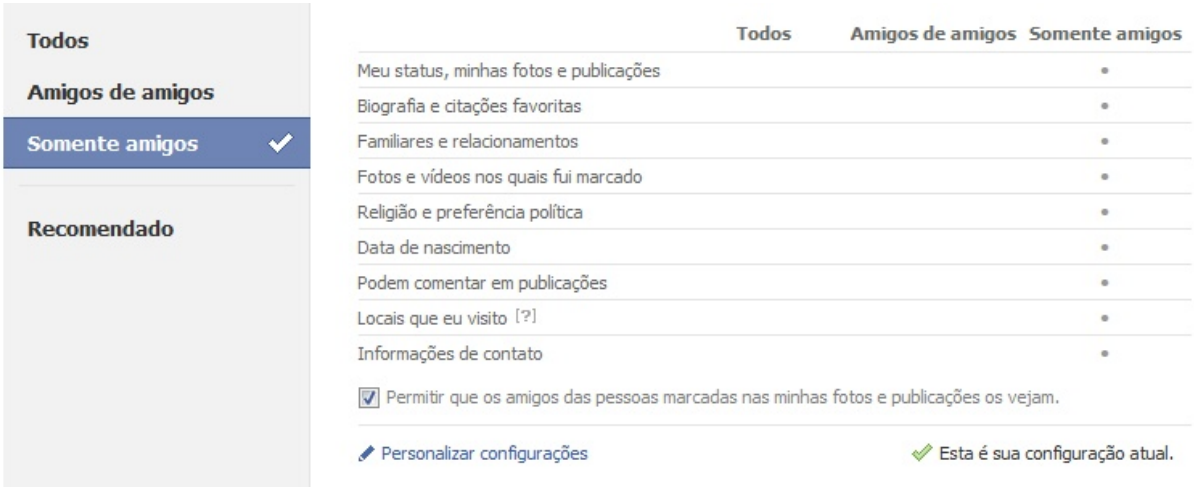
Não cuidar da privacidade em redes sociais

Facebook e Orkut permitem que seus usuários enviem uma grande quantidade de fotos para os servidores, garantindo que possam ser mostradas suas viagens, festas e tantas outras ocasiões. Quem sabe se prevenir, altera as configurações para permitir que apenas amigos próximos possam ter acesso a estas imagens.

O problema é que grande parte dos usuários não sabe realizar este tipo de modificação e acaba deixando tudo à mostra para qualquer um. Isso facilita que outras pessoas roubem suas fotos e informações, criando perfis falsos e realizando montagens maldosas com as imagens obtidas, causando danos morais muito sérios às vítimas.

Métodos de proteção

Há várias formas de proteger sua privacidade nas redes sociais, impedindo que usuários desconhecidos possam visualizar suas fotos e obter informações sobre seus interesses. Para o Orkut, basta acessar o menu de configurações e marcar todas as opções possíveis em “Apenas meus amigos”. Já no Facebook, o processo é um pouco mais complexo (clique aqui para acessar as dicas do Baixaki).



Acessar redes Wi-Fi desconhecidas

Precisando acessar seu email e seu modem 3G resolveu dar problemas? Verificou a lista de redes Wi-Fi disponíveis e encontrou várias sem proteção? Então tome muito cuidado, pois nem todas as redes ficam liberadas porque os administradores são “bonzinhos”. Não é raro encontrar redes sem proteção criadas por quem quer apenas roubar dados.

Como tudo o que você digita passa pelo modem não é difícil fazer com que seus movimentos sejam registrados em um log de utilização. Nisso podem ser capturados endereços de email, senhas, códigos de acesso a serviços diversos e números do cartão de crédito, por exemplo.

Métodos de proteção

Sempre que estiver em um local que disponibilize o acesso a redes sem fio, certifique-se de que a que você acessar é a oficial do estabelecimento. Shoppings e hotéis podem estar no raio de alcance de redes particulares com nomes modificados para enganar os usuários e roubar informações.

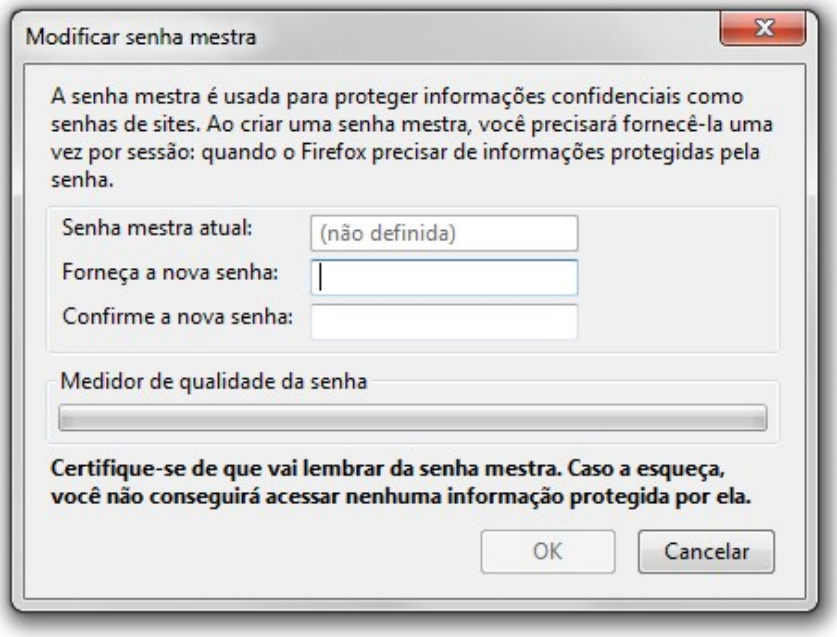
Pergunte aos administradores do local qual a rede certa para acessar. Outra dica é evitar ao máximo qualquer rede particular que esteja sem proteção. Desse modo, muitos transtornos podem ser evitados. Lembre-se de não permitir o compartilhamento de arquivos quando estiver em redes públicas.

Mesma senha para tudo

MSN, Orkut, email, Facebook e conta no Baixaki. Todos os seus perfis possuem a mesma senha de acesso? Se sim, você está correndo um grande risco. Caso você tenha uma senha roubada, o ladrão poderá acessar todas as suas informações de uma só vez, conseguindo invadir suas contas em qualquer local que você esteja cadastrado.

Métodos de proteção

Um bom modo de se proteger é criando uma senha para cada serviço acessado, ou então uma para cada tipo de serviço. Redes sociais ganham um código, contas de email ganham outro e cadastros em jogos online, por exemplo, utilizam uma terceira senha. Outra forma é criando uma senha mestra em seu navegador.



Clique para ganhar um iPad

Parece brincadeira, mas ainda existem muitos banners falsos na internet. “Você é nosso visitante 1.000.000.000! Clique aqui e ganhe um iPad, um Playstation 3 e um Boeing. Infelizmente não é tão fácil assim ganhar um prêmio, por isso, tome muito cuidado com os links, muitos deles são apenas atalhos para sites maliciosos.

Métodos de proteção

Sabe aquela expressão: “Isso é bom demais para ser verdade!”? Bem, geralmente é mesmo. Por isso não clique em nada que prometa algo muito bom para qualquer pessoa. Essa é a única forma de livrar-se das pragas que podem tentar invadir seu computador em sites diversos ao redor do mundo virtual.

.....

Estes são os principais erros que grande parte dos usuários cometem quando estão na internet. Sabemos que você já cometeu e, acredite, até mesmo a equipe do Baixaki já cometeu alguns deles. Você conhece mais algum erro frequente que os internautas cometem? Deixe um comentário para nos contar!

Imprimir