IDG NOW! tecnologia em primeiro lugar http://www.idgnow.com.br

SEGURANÇA > PRIVACIDADE

10 dicas para navegar com segurança

(http://idgnow.uol.com.br/seguranca/2010/05/25/10-dicas-para-navegar-com-seguranca)

Por CIO.com/EUA

Publicada em 25 de maio de 2010 às 07h00
Atualizada em 25 de maio de 2010 às 07h25

Ajustes e plugins para o browser ajudam a esconder seus passos dos bisbilhoteiros da internet.

Quem teria pensado que uma copiadora digital não era segura? E você sabia que as novas tecnologias tornam mais fácil do que nunca seguir seu rastro online? Manter seguro online costumavam ser simples: use um software antivírus. Não mais. Há toda uma nova geração de ameaças à sua segurança e privacidade online. Vamos ver alguns dos mais recentes truques que os cibercriminosos desenvolveram, e 10 dicas para te ajudar a escapar dessas armadilhas.

Você não vai (ou pelo menos espero que não) atirar seus extratos bancários na lixeira sem rasgá-los. Mas se você jogar fora multifuncionais top de linha, sem retirar o disco rígido, está pedindo para ter problemas, diz Kevin Brown, gerente de testes no ICSA Labs, que testa produtos de segurança. Isso porque algumas copiadoras digitais e impressoras mantêm cópias de tudo o que produzimos em um disco rígido ou um módulo de memória flash. Se alguém encontrar esse dispositivo, não é difícil os ler.

Sim, isso soa muito forçado. Mas a Comissão Federal de Comunicações está preocupada o suficiente para investigar este problema, e alguns fabricantes de copiadoras estão dando um software que irá ajudá-lo a limpar um drive. E lembre-se, simplesmente apagar arquivos não faz desaparecer as informações. Ele apenas as torna mais difícil de encontrar.

Há outra ameaça relacionada às copiadoras também. Se você copiar coisas pessoais no trabalho (e quem já não fez isso) é simples para um administrador ver o que você xerocou, se a máquina está em rede. Além do mais, as senhas padrão para copiadoras em rede podem ser encontrada na internet, diz Brown.

Dica 1: Certifique-se de remover e limpar os HDs da impressora/copiadora antes de livrar-se delas.

Dica 2: Não copie nada pessoal em uma copiadora em rede de seu escritório que você não queira que o patrão veja.

Derrote os cookies Flash e os "supercookies"

Vários navegadores lhe dão a opção de selecionar uma opção de privacidade que supostamente permite navegar na Web sem deixar impressões digitais. Não acredite nisso.

Essa opção geralmente faz com que o navegador pare de armazenar as URLs das páginas que você visitou. Mas ele não faz nada para esconder as páginas e imagens que você viu de anunciantes que desejam veicular anúncios sob medida para você, ou pior ainda, de bisbilhoteiros como detetives privados e agentes da lei.

A solução antiga, apagar os cookies ou clicar em uma configuração que impede seu navegador de aceitá-los, é muito menos eficaz do que costumava ser. Isso porque muitos sites estão usando agora uma coisa chamada "Flash cookie", que é mantido pelo plugin Adobe Flash por causa dos aplicativos Flash embutidos em páginas da Web, diz Peter Eckersley, pesquisador da Electronic Frontier Foundation.

Ao contrário dos cookies normais, os Flash cookies e uma variação conhecida como supercookie são armazenados fora do controle do navegador e os usuários não podem vê-los ou excluí-los diretamente, e eles nunca expiram. Eles podem rastrear os usuários de todas as formas que os cookies HTTP tradicionalmente fazem, e podem ser armazenados ou recuperados quando um usuário acessa uma página que contém um aplicativo Flash, diz Eckersley.

Há não muito tempo, o pior que podia acontecer é que você fosse rastreado e visse anúncios veiculados com base em seus hábitos de navegação, ou talvez tivesse o azar de alguém abrir seu navegador quando você estava longe do computador e visse um anúncio mostrando o que você estava fazendo online.

Agora, porém, parece que as informações que usuários dão voluntariamente para as redes sociais, além dos dados recolhidos pela nova geração de cookies, podem ser colocados juntos para realmente identificar um indivíduo. "Sites de redes sociais como Facebook, LinkedIn e MySpace estão dando à nuvem de empresas com fome de monitoramento uma maneira fácil de adicionar o seu nome, listas de amigos, e outras informações aos registros que já mantêm de você", diz Eckersley.

Dica 3: Se você usa o Firefox, um add-on chamado BetterPrivacy acaba com os Flash cookies. É gratuito e você pode encontrá-lo **aqui**.

Dica 4: Escolha uma boa política de cookies para seu navegador, como "mantenha os cookies apenas até eu fechar meu browser", ou os aprove manualmente.

Dica 5: Use as extensões para Firefox **RequestPolicy** e **NoScript** para controlar quando sites de terceiros podem incluir conteúdo em suas páginas ou executar código no seu navegador, respectivamente. Estas ferramentas são muito eficazes, mas esteja ciente, diz Eckersley, que são difíceis de usar: muitos sites que dependem de JavaScript terão de ser colocados como exceção antes que funcionem corretamente.

Dica 6: Use o plugin **Targeted Advertising Cookie Opt-Out**. Ele automaticamente excluirá você de rastreadores que peçam para aceitar um cookie. Esteja ciente de que nem todos irão oferecer a opção de exclusão (opt out), ou que alguns podem interpretar isso como "não me mostre anúncios segmentados", em vez de "não espione meu comportamento online".

Armadilhas de privacidade no Facebook

Um inteligente, e muito paciente repórter do New York Times recentemente descobriu que o Facebook tem mais de 50 botões de privacidade, levando a mais de 170 escolhas. Não posso guiá-lo através desse labirinto, mas há uma série de medidas de senso comum que você pode tomar para minimizar os danos se você não apertar o botão certo.

Dica 7: Nunca aceite um convite de app de alguém que você não conhece. E se o software parecer suspeito, verifique-o usando a busca do Facebook.

Dica 8: Não se esqueça de que, quando alguém tem a sua data de nascimento completa (dia, mês, ano), estás a apenas algumas etapas de ter informação suficiente para fazer alguns danos sérios, tais como hackear sua conta bancária. Então, seja inteligente. Não incluia esses dados em seu perfil.

Dica 9: Pela mesma razão, remova seu endereço de casa e número de telefone do seu perfil.

Dica 10: Pode parecer mau, mas classifique as pessoas de acordo com o quão bem você as conhece e confia. Coloque-as em grupos. As que melhor você conhece, mais podem ter acesso aos dados de sua página.

Bill Snyder