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

SEGURANÇA > PRIVACIDADE

O guia paranoico de privacidade para os serviços da Google

(http://idgnow.uol.com.br/seguranca/2010/05/26/o-guia-do-paranoico-para-os-servicos-google)

Por Computerworld/EUA

Publicada em 26 de maio de 2010 às 07h00
Atualizada em 26 de maio de 2010 às 11h09

Há quem confie na Google como se fosse a própria mãe. Mas você já percebeu o quanto a empresa sabe ou pode descobrir sobre você?

O Google é praticamente o melhor amigo de cada um. Mas você já percebeu o quanto o Google sabe sobre você?

Você sabia que a Google pode ter gravado e armazenado cada termo de busca digitado em sua caixa de pesquisa? Pode ser que algumas dessas buscas sejam sérias ameaças à sua reputação. E que dizer do Gmail? Já enviou algum e-mail sigiloso? Quantas informações empresariais estão armazenadas no Google Docs?

A menos que tenha passado a última década totalmente offline, você deve ter construído um belo perfil de si mesmo nos servidores da Google. Dependendo de quais das dúzias de serviços da Google você usa, dados sobre seus hábitos, interesses, atividades, agendas, objetivos profissionais, portfólio de ações e registros médicos podem estar descansando em algum lugar desses servidores – junto com registros das rotas de viagem que você mapeou, os sites que visitou e muito mais.

O lado bom é que a Google torna anônimos os registros de seus servidores. Depois de nove meses, ela arranca os últimos três dígitos dos endereços de IP associados com suas buscas. Depois de 18 meses, os cookies associados também são apagados, o que torna muito difícil ligá-lo às buscas feitas há mais de um ano e meio.

Mesmo assim, há uma grande e bela janela de tempo que escancara sua vida para curiosos. E se algum ou todos os dados se tornarem públicos? Um cibercriminoso poderia, em teoria, ter acesso a sua informação na Google ao invadir diretamente os servidores, ou mesmo sua conta individual.

Quantidade enorme

“Há uma enorme quantidade de dados na Google”, diz o vice-presidente de pesquisas da Gartner, Jay Heiser, “e seria tolice ignorar que toda essa informação seria de enorme interesse para uma ampla variedade de pessoas”.

E tem mais. O grande número de serviços que a Google oferece significa que há muitas formas de acessar esses dados. “Cada serviço traz seus próprios riscos”, diz Heiser. “Há potencial para que uma vulnerabilidade menor de um deles possa se tornar uma vulnerabilidade mais significativa quando combinada com outro.”

E os criminosos não são os únicos que poderiam potencialmente acessar seus registros na Google. Basta uma ligação do governo (ou de advogados de algum processo legal no qual esteja envolvido) e, com uma simples intimação, a Google será forçada a entregar sua informação, como prevê a política de privacidade da empresa.

Conclusão: o Big Brother sabe muito mais sobre você do que se pode imaginar. Mas não é preciso evitar a Google para manter-se razoavelmente a salvo. Em primeiro lugar, basta seguir alguns passos para prevenir que informação potencialmente perigosa seja armazenada nos servidores da Google, e proteger a integridade da sua conta.

Ao tomar algumas precauções básicas – e outras não tão básicas -, você pode minimizar sua exposição aos caras maus.

Para cada precaução, há dois níveis de conselhos sobre como se proteger a si mesmo.

Defcon 2 (boa segurança) identifica as dicas sobre o que você pode fazer com as ferramentas que já estão à disposição, para minimizar os riscos de segurança envolvidos no uso dos diversos serviços da Google.

Defcon 1 (segurança avançada) – também conhecido como “a solução das celebridades” (passos para tomar se você tem, ou pretende ter, um perfil público altamente visível) – identifica as dicas que oferecem muito mais segurança, mas são menos práticas e frequentemente exigem o uso de ferramentas de terceiros.

No fim das contas, só você pode determinar qual é o melhor equilíbrio entre segurança e conveniência.

Risco 1: busca de dados e metadados
Se você visitar a página de histórico da web da Google, verá todas as buscas que já fez na Google, enquanto estava logado em sua conta, por anos. E não está limitado a buscas de textos: o histórico inclui buscas de imagem, de vídeo, de mapas, e por aí vai. Este dado é armazenado por padrão; usuários devem ativar o Histórico da Web para acessá-lo.

A Google usa essa informação para diversos propósitos benignos, como a sintonia fina de seus algoritmos de busca e a determinação de padrões mais amplos em buscas na web para a página Google Trends. Mas embora seja útil para a empresa, é quase certo que você não vai querer que alguém veja todas as buscas que você fez.

Defcon 2:
A coisa mais simples que você pode fazer para prevenir o acúmulo de dados de busca é certificar-se de que você saiu de sua conta antes de efetuar pesquisas. Se você estiver logado, seu endereço de e-mail será mostrado no canto superior direito da página inicial da Google, das páginas de resultado ou de qualquer página da Google em que você estiver.

Também, desligue o Histórico da Web da Google. Do canto superior direito da página da Google, escolha Configurações -> Configurações da Conta, clique em Editar (à frente de Meus Produtos) no lado esquerdo da página, e clique "Remover histórico da web permanentemente". (Se você não vê essa opção, significa que nunca ativou o Histórico da Web).

Isso fará com que o serviço Histórico da Web seja desligado e apagará todos os dados específicos ligados à sua conta nos servidores da Google. A empresa manterá os dados de busca associados ao seu IP por nove meses e outras informações não pessoais por 18 meses, mas estes dados não estão especificamente ligados à sua identidade.

Contudo, o serviço de Histórico da Web pode ser de valor para usuários individuais, não apenas para a Google. Um histórico das buscas web já feitas pode ser útil para seu próprio uso. Se quiser manter o serviço e simplesmente apagar apenas buscas que poderiam "incriminá-lo", escolha Histórico da Web em Meus Produtos de sua página de Contas e clique em Remover Itens no menu esquerdo. Isso colocará uma caixa de escolha para cada pesquisa em seu histórico; selecione aquelas que você quer apagar e clique em Remover.

Você também pode clicar em "Limpar o Histórico da Web inteiro" no pé da página, para apagar todas suas buscas de uma vez, ou "pausar" o Histórico da Web por algum tempo. Para colocar o Histórico da Web no gancho, clique em Pausar no menu esquerdo, depois clique em Resume para que o ele grave suas buscas novamente.

Defcon 1:
Sair da Google evita a associação direta entre você e suas buscas, mas não a associação entre seu endereço de IP e outras informações. Para prevenir isso, torne sua navegação web anônima usando ferramentas como Tor, Anonymizer ou a extensão PhZilla para Firefox.

Risco 2: Rastreando cookies
O Google usa cookies para armazenar seus status de login para vários serviços. Assim, por exemplo, você não tem que se identificar no Google Agenda se já estiver usando o Gmail. Mas isso significa que você está deixando um rastro de logins que pode ser acessado tanto pelos servidores da Google como em seu disco rígido.

Além disso, o serviço de anúncios Doubleclick, da Google, usa cookies para rastrear a navegação pelos sites. E esta informação, combinada com o login, pode identificar exatamente que sites você visitou.

Defcon 2:
Use as configurações de segurança de seu navegador para rejeitar cookies de terceiros – isto é, cookies de outros sites além do que você está visitando.

O bloqueio de todos os cookies pode ser um problema se você quiser que sites específicos lembrem suas preferências ou informações de login. Mas bloquear apenas cookies de terceiros, por outro lado, não lhe trará aborrecimento na maioria dos sites e elevará seu nível de privacidade.

O bloqueio de cookies de terceiros não fará sumir os que já estão instalados. Você pode usar as configurações de segurança do browser para apagar todos os cookies, ou pesquisar um a um para escolher os que merecem ser apagados.

Uma opção é usar o recurso de 'navegação privada', presente em muitos navegadores. As versões mais recentes de Firefox, Safari, IE, Opera e Chrome oferecem sessões de navegação privativa, que apagam cookies e senhas quando você fecha o navegador, e também apagam seu histórico e cache.

Defcon 1:
Bloqueie scripts e anúncios completamente. Use um bloqueador como o AdSweep para Firefox, Opera e Chrome, ou o AdblockIE para o IE8 para impedir sites de oferecer anúncios. Ou usar a extensão NoScript, se usa o Firefox.

Muitos anúncios usam JavaScript para carregar. O bloqueio de scripts impedirá a carga de anúncios e de cookies de terceiros, mas também fará com que muitos sites sejam impossíveis de visitar. Você poderá criar exceções usando a lista “Sites confiáveis” do IE8, ou clicando o ícone do NoScript e selecionando Permitir para sites que você deseja receber scripts.

Risco 3: Hackers atacam a Google
Mesmo se você confia na Google como se fosse sua mãe, a quantidade de dados que a empresa guarda sobre você é de assustar – ainda mais se considerarmos o que aconteceria se alguém de fora tivesse acesso aos servidores.

Defcon 2:
Use o senso comum. “Caso se trate de propriedade intelectual absolutamente crítica, não use serviços online”, diz Mark Kadrich, CEO da The Security Consortium, uma empresa de pesquisas e serviços de segurança.

O mesmo vale para informação pessoal. Nenhum sistema é 100% perfeito. Se você não puder recuperar nenhum pedaço de informação, nenhum sistema será seguro o bastante.

Os mecanismos da Google são fortes o bastante para proteger contra as ameaças mais comuns, mas um invasor determinado que tiver acesso à sua conta poderá acessar tudo que você confiou à empresa.

É você quem deve separar a informação que pode ser confiada à Google da que não pode.

Defcon 1:
Encripte seu e-mail. Se você usa um programa de e-mail como Outlook ou Thunderbird para acessar sua conta Gmail, pode usar um produto como o PGP Desktop Home ou seu primo de código aberto GnuPG para encriptar todos os e-mails enviados. Ou usar a extensão FireGPG para encriptar a interface web do Gmail.

Empresas podem usar ferramentas como a PGP Desktop Corporate no desktop ou um dos produtos para servidor da PGP para encriptar todas as mensagens de e-mail em nível de rede.

Você terá que pedir que outros enviem a você apenas e-mail encriptado ou todos seus e-mails ainda serão em texto puro. Infelizmente não há ferramentas de encriptação para outros serviços da Google.

Risco 4: Hackers adivinham seu login
Hackear o Google pode ser difícil, mas invadir sua conta particular provavelmente não é. Muitas pessoas usam senhas simples e fáceis de lembrar. Um hacker com alguma informação básica sobre você poderia facilmente invadir sua conta.

Se você usa uma palavra existente como senha, um hacker que saiba apenas seu endereço de e-mail poderia quebrar sua conta em segundos, usando ferramentas que tentam cada palavra do dicionário.

Defcon 2:
Use um programa de gerenciamento de senha, como o KeePass ou RoboForm, para gerar e lembrar password fortes, que são impossíveis de adivinhar. E mude sua senha regularmente – uma vez ou mais por mês.

Defcon 1:
Use autenticação multifator. Usando apenas uma senha para entrar em um serviço lhe dá um ponto de falha: se alguém descobre sua senha, você está vulnerável. A autenticação multifator exige a verificação de identidade em dois ou mais meios.

“A autenticação multifator baseia-se em pelo menos duas de três coisas: algo que você sabe, algo que você tem e algo que você é”, diz Vatsal Sonecha, vice-presidente de desenvolvimento de negócios da empresa de segurança TriCipher. Serviços como o MyOneLogin da TriCipher controlam o acesso exigindo verificações adicionais, como um token de segurança ou um arquivo em seu computador ou uma impressão digital.

O MyOneLogin oferece um serviço de autorização segura grátis para usuários do Google Apps. Por 3 dólares mensais, você pode contratar um serviço que cobre toda sua atividade online.

Risco 5: Hackers quebram seu login
Mesmo que você tenha uma senha difícil de adivinhar, um hacker ainda poderia acessar sua conta na Google fazendo-o visitar um link fraudulento, ou pela instalação de malwares que roubam senhas. Se seu computador estiver comprometido, você poderá pensar que está entrando no Google mas, na verdade, está dando sua informação para um hacker.

Dica: sempre preste atenção à URL em seu navegador antes de digitar informação sigilosa, caso tenha chegado ao site por meio de um clique em link que chegou por e-mail ou em uma página de terceiros. Se o nome de domínio é estranho ou não casa com o que deveria ser, é indicador de que alguém está tentando lhe enganar.

Defcon 2:
Se você ainda está usando o Internet Explorer 6, atualize-o imediatamente. De acordo com a empresa de segurança Secunia, o IE6 tem 24 vulnerabilidades sem solução, muito mais que qualquer outro navegador em uso atualmente. Foi uma falha no IE6 que permitiu a brecha na rede da Google em dezembro de 2009.

Além disso, pratique o bom comportamento em segurança na internet: rode software antimalware em seu sistema (sim, mesmo em Macs); não clique em links de e-mails, mesmo de pessoas que você confia (ou se fizer, preste atenção à URL); não abra anexos que você não está esperando; fique longe de sites web suspeitos (pornô, transferências ilegais de dinheiro ou de warez); e nunca clique em pop-ups, nem mesmo para fechá-los (em vez disso, use os comandos Alt-F4 no Windows ou Command-W nos Macs).

Defcon 1:
Mantenha seu navegador numa "caixa de areia". Use software de virtualização como VMware Player ou Parallels Desktop para criar um sistema operacional autocontido para que vírus e malware não possam acessar seu disco rígido diretamente – e quando você estiver terminado, mate a sessão e comece outra a partir do disco de imagem original. Um browser isolado em caixa de areia, como o Sandboxie, também oferece alguma proteção ao isolar seu navegador do resto do sistema.

Nem máquinas virtuais, nem caixas de areia fornecem uma proteção completa de keyloggers e outros malwares. Mas usados apropriadamente, com outras aplicações padrão de segurança, eles podem ajudar a prevenir malware de instalar qualquer coisa no sistema.

Conselho final
Finalmente, dê uma boa olhada no que você está fornecendo à Google e o que você espera obter em retorno. "Você não pode mais ser passivo na proteção de seus rastros digitais", explica Bill Morrow, CEO da CSIdentity, provedora de serviços e soluções contra roubos de identidade. "Você tem de pensar como se seu inimigo estivesse no seu quarto, vendo tudo que você faz. Este tipo de filtragem irá reduzir não apenas onde você vai mas que informação você quer deixar para trás."

A Google pode não ser seu inimigo – agora. Mas uma mudança no gerenciamento na empresa ou sua aquisição por outra companhia (ei, isso pode acontecer) poderia mudar tudo. Mesmo um processo legal poderia dar problemas se a Google recebesse uma intimação. E as pessoas dentro das defesas da Google – um empregado descontente, alguém com uma vingança pessoal, ou um hacker – pode realmente ser seu inimigo. E naturalmente, quanto maior seu perfil público, mais você se torna alvo.

Amiga ou não, a Google terá sua informação em seus servidores por bastante tempo. Um pouco de paranóia não matará ninguém, e poderá até salvá-lo caso a empresa passe a negar seu famoso mantra "Não seja mau".

(Logan Kugler)