Quase 40 milhões ficarão sem segurança na internet em 1º de janeiro

Diversos países emergentes ao redor do mundo, assim como alguns cidadãos brasileiros, ficarão parcialmente desprotegidos ao navegar na internet já nas primeiras horas do dia 1 de janeiro de 2016. Ao todo, serão quase 40 milhões de usuários deixados para trás com a atualização dos protocolos de segurança da web.

Hoje, ao usar o Google Chrome, Mozilla Firefox ou Microsoft Edge, um ícone de um cadeado e a sigla HTTPS surgem no início da maioria dos endereços eletrônicos disponíveis na web. Isso indica que a página que você está tentando acessar é devidamente criptografada e segura - como o Facebook e o Gmail.

O certificado que garante a um site sua segurança é conhecido atualmente como SHA-1. Contudo, o CA/Browser - grupo que determina quais páginas ganham essa certificação - decidiu que o SHA-1 não é mais tão seguro, e, a partir de 1 de janeiro de 2016, só emitirá certificados no padrão SHA-2.

É aqui que entra o problema. Navegadores ou sistemas operacionais mais antigos não possuem suporte para o novo padrão, e, por isso, não serão capazes de validar a autenticidade de páginas como a do Facebook e outras áreas criptografadas da internet. Na prática, celulares lançados há mais de 5 anos, por exemplo, não terão mais a mesma segurança para navegar na web.

Dependendo da plataforma e do navegador usado, é possível que esses sites sequer sejam liberados para o usuário que não tiver suporte ao SHA-2. Na China, por exemplo, cerca de 6% dos internautas serão afetados pela mudança, que atinge principalmente mercados emergentes.

Organizações como a CloudFlare e o próprio Facebook já se mobilizam para evitar que 40 milhões de pessoas sejam prejudicadas na virada do ano. A rede social já até apresentou sua alternativa: construir um mecanismo de código aberto que permita aos desenvolvedores habilitarem versões mais antigas de seus browsers ao SHA-2.

Se você usa uma versão do Google Chrome superior à 39; Mozilla Firefox 37 ou mais novo; ou Microsoft Edge, navegador padrão do Windows 10; não há com o que se preocupar. Esses browsers já possuem suporte ao padrão SHA-2. Mas se estiver em um Android 2.2, ou mesmo no Windows XP, seus dias de segurança na web estão contados. Pelo menos enquanto uma solução definitiva não for encontrada.

Fonte: http://olhardigital.uol.com.br/noticia/quase-40-milhoes-ficarao-sem-seguranca-na-internet-em-1-de-janeiro/53727