Tor Browser: Você NÃO está seguro

Geralmente, quem utiliza o Tor Browser tem uma leve noção de que é vigiado quando está usando a internet comum. E isso é a mais pura verdade. Com isso, quando queremos ter algum nível de liberdade, buscamos o serviço desse navegador para se tornarem 'anônimos' e usufruir dos benefícios do anonimato.

Realmente, o Tor Browser é um ótimo navegador quando se trata de mascarar o seu IP para administradores de sites, e ocultar do seu provedor de internet o conteúdo que você acessa (mas o provedor ainda podem ver que você está conectado ao Tor).

Apesar disso, você ainda **não** está seguro. O Tor Browser mais parece caminhar para o lado de um imenso *honeypot* do que para um serviço que realmente se esforce para garantir o máximo de privacidade e anonimato possível para seus usuários.

Sabe aquele escudo no lado superior direito que você configura o seu nível de privacidade com o JavaScript? Ele não funciona de verdade.

Desde a versão 10.0 do Tor Browser, quando você escolhe a opção '*segurança máxima',* O JavaScript não é mais desativado do browser como era feito automaticamente com essa configuração, o que abre uma brecha para a identificação do usuário.

Além disso, coisas importantes que poderiam levar a identificação como impressões digitais (o WebGL por exemplo) estão nativamente ativos no navegador, coisa que não faz sentido nenhum já que o foco seria proteger a identidade do usuário.

Visto isso, escrevi esse tópico para trazer configurações que devem ser feitas manualmente nas configurações avançadas do Tor Browser (e outras nas configurações comuns) caso desejem aumentar ainda mais a sua privacidade e anonimato.

Para começar, digite ***about:config*** na barra de endereços do seu Tor Browser e clique em 'aceito o risco e continuar'.

- Os nomes de preferência em **PRETO** já estão configurados por padrão, mas é sempre bom verificar
- Os nomes de preferência em **VERMELHO** precisam ser configurados manualmente.

// Todas essas configurações também se aplicam ao mozilla firefox comum caso tenha interesse.

Nome de preferência	Valor	Ação
app.normandy.enabled	False	Duplo clique para alternar
extensions.pocket.enabled	False	Nenhum, é falso se o nível de segurança for mais seguro
Javascript.enabled	False	Nenhum, é falso se o nível de segurança for mais seguro
Network.prefetch-next	False	Nenhum, é falso se o nível de segurança for mais seguro
Browser.cache.disk.enable	False	Nenhum, deve ser o padrão
Browser.send_pings	False	Nenhum, deve ser o padrão
Geo.enabled	False	Nenhum, deve ser o padrão

Media.peerconnection.enabled	False	Nenhum, deve ser o padrão
Browser.safebrowsing.downloads.remote.enable	False	Nenhum, deve ser o padrão
Browser.cache.memory.enable	False	Duplo clique para alternar
Browser.chrome.site_icons	False	Duplo clique para alternar
browser.shell.shortcutFavicons	False	Duplo clique para alternar
Dom.storage.enabled	False	Duplo clique para alternar
Media.autoplay.enabled	False	Nenhum, deve ser o padrão
Media.autoplay.allow-muted	False	Nenhum, deve ser o padrão
Media.webm.enabled	False	Duplo clique para alternar
Network.websocket.delay-failed-reconnects	False	Duplo clique para alternar
services.sync.prefs.sync.network.cookie.lifetimePolicy	False	Duplo clique para alternar
Services.sync.prefs.sync.network.cookie.cookieBehavior	False	Duplo clique para alternar
media.play-stand-alone	False	Duplo clique para alternar
Network.cookie.cookieBehavior	1	Nenhum, deve ser o padrão
media.autoplay.default	1	Duplo clique e modifique
Network.http.sendRefererHeader	0	Duplo clique e modifique
Browser.display.use_document_fonts	0	Duplo clique e modifique
Network.IDN_show_punycode	True	Duplo clique para alternar
Pdfjs.disabled	True	Duplo clique para alternar
media.autoplay.enabled.user-gestures-needed	True	Nenhum, deve ser o padrão
Webgl.disabled	True	Duplo clique para alternar

// Os nomes de preferência relacionados a reprodução automática foram movidos das configurações avançadas para a sessão de privacidade nas configurações comuns. Vou mostrar como desabilitar a seguir.

Além configurações acima, você deve também bloquear as solicitações dos recursos de acessibilidade do navegador, que também são brechas abertas para sua identificação. Acesse as configurações do seu Tor Browser e acesse a sessão de privacidade e segurança, e altere as seguintes permissões:

Opção de acessibilidade	Ação
Localização	Bloquear novas solicitações de permissão para acessar sua localização
Câmera	Bloquear novas solicitações de permissão para acessar sua câmera
Microfone	Bloquear novas solicitações de permissão para acessar seu microfone
Notificações	Bloquear novas solicitações de permissão para exibir notificações
Reprodução automática	Na parte superior esquerda clique em Bloquear áudio e vídeo
Realidade virtual	Bloquear novas solicitações de permissão para acessar seus dispositivos de realidade virtual

// Os usuários de Tails terão que refazer todas essas configurações sempre que reiniciarem o sistema. É recomendável que essas configurações sejam feitas antes do navegador de fato se conecte ao Tor. Uma dica é que anotem essas configurações em um papel, ou imprimam este manual. Ou, se você utiliza o modo persistente, salve o arquivo ***pref.js*** já configurado, e apenas substitua o *pref.js* não configurado do Tor.

Com essas configurações, você já triplicou a privacidade e anonimato do seu Tor Browser. Mas nada disso adianta se você não tiver cuidado com suas ações, sempre vai existir uma brecha desconhecida. Por isso você deve ter cuidado com plug-ins/extensões.

Plug-ins/extensões além dos que já vem por padrão no Tor Browser não devem ser instalados. Plug-ins que não são padrões podem **contornar a rede Tor** e obter acesso direto a sua rede, **revelando a sua identidade real**.

É recomendado também sempre fazer a limpeza do computador antes e após o uso do Tor. Para isso utilize o **Ccleaner** com as seguintes configurações:

> Opções > Definições > Eliminação segura: Eliminação segura de ficheiros (mais lenta): Substituição muito complexa (35 passagens);
Marque as caixas ‘Limpar fluxo de dados alternativos’ e ‘Limpar pontas de clusters’;
Se você tiver mais de um disco, selecione todos eles na caixas abaixo;
Marque também a caixa ‘Limpar o espaço livre MFT’.

Lembrando que para quem utiliza SSD, não existe maneira 100% confiável de limpar seus rastros, por mais que você confie no programa utilizado. Por isso, é preferível que você utilize um disco rígido, que é bem mais confiável.

A limpeza de espaço livre é muito demorada, ainda mais se seu HD/SSD for muito grande em armazenamento. Eu recomendo fazer essa limpeza uma vez por semana, ou duas se você apagar muitos arquivos com frequência.

Você pode evitar todo esse trabalho de limpeza se utilizar o **Tails**. Com um pendrive de 8GB você roda o sistema direto do pendrive, utilizando apenas a memória RAM do seu computador, que é muito mais fácil de limpar.

Desconectando seu computador ou notebook de qualquer fonte de energia (isso inclui a bateria) e apertando o botão power por mais ou menos 15 segundos, você elimina toda a energia que estava contida na placa. Com isso, os dados que ficam salvos na memória RAM serão perdidos, dificultando em graus altíssimos a recuperação forense.