“Confiança não se compra, se conquista” Parte 2

10 de outubro de 201513 de outubro de 2015 / Methz

Dando continuação à Parte 1 do artigo “Confiança não se compra, se conquista”, veremos Proteção Antirrastreamento (diferente do *Não Me Rastreie*), como criar Senha Mestra e entender um pouco sobre Conexões Seguras. Recomendamos que você leia o primeiro artigo para entender alguns conceitos importantes e outras funcionalidades já demonstradas.

Proteção Antirrastreamento

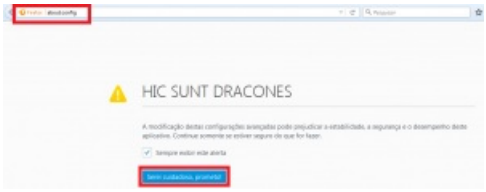
No primeiro artigo mostramos como o *Não Me Rastreie* funciona, percebemos que seu funcionamento depende diretamente do site visitado, e não podemos depender do bom senso das pessoas né!? A **Proteção Antirrastreamento** bloqueia sites previamente listados que são conhecidos por rastrear usuários.

Como Usar

Digite o seguinte endereço na *barra de endereços:*

about:config

OBS: Se aparecer o aviso ***“HIC SUNT DRACONES”,*** clique em “Serei cuidadoso, prometo!”.

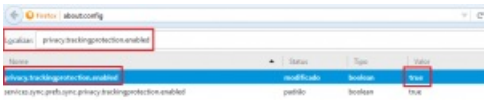


Acervo pessoal

Na barra *Localizar*, pesquise por:

privacy.trackingprotection.enabled

Dê 2 cliques rapidamente na linha em destaque até o campo ***Valor*** alterar para ***true.***



Acervo pessoal

Pronto! Tudo certo, caso queira desativar futuramente, apenas siga os mesmos passo até que o valor mude para *false*. Para mais informações, clique aqui.

Senha Mestra

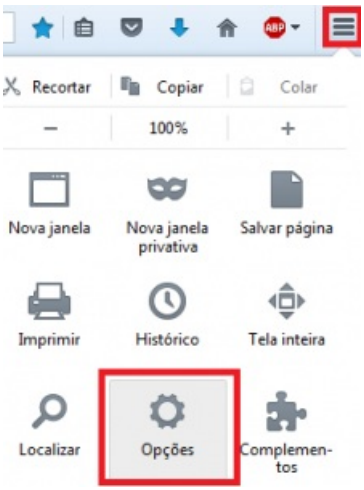
Hoje em dia a maioria dos sites exigem ***login*** e ***senha*** para desfrutar de alguma funcionalidade específica. Visando agilidade, muitas vezes optamos pela opção do **Firefox** *“Memorizar senha”* para sempre nos conectarmos diretamente sem a necessidade de digitar a senha novamente. Mas o problema, é que essas senhas ficam salvas no computador e qualquer um com acesso e conhecimento pode visualiza-las.

Com a **Senha Mestra** ativada, não teremos mais problemas com isso, pois a cada vez que o Firefox iniciar, irá solicitar a **Senha Mestra** que não está salva em seu computador, evitando quebra de identidade.

OBS: A **Senha Mestra** só se aplica as senhas salvas pelo **Firefox** e não pela opção do site. Por exemplo, o Facebook oferece a opção *“Mantenha-me conectado”*, isso é uma funcionalidade do site que trabalha de forma totalmente independente das configurações do **Firefox.** Mas as vezes pode requisitar também.

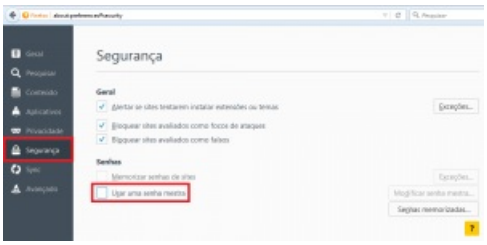
Como Usar

Primeiramente você deve acessar seu Menu>Opções:



Acervo pessoal

Agora selecione a aba Segurança e selecione a caixa ***"Usar uma senha mestra"*** como na imagem a seguir:

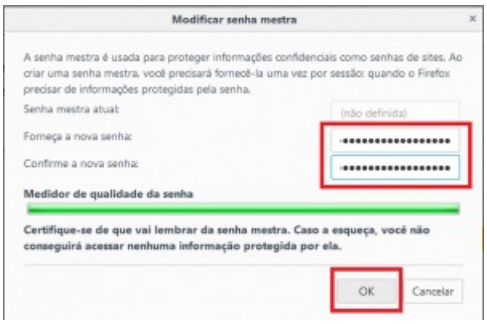


Acervo pessoal

OBS: Você também pode acessar essa opção digitando no seu navegador o endereço abaixo.

about:preferences#security

A janela *"Modificar senha mestra"* aparecerá, você deve escolher uma senha, preencher os 2 campos em brancos e ir acompanhando o medidor de qualidade de senha, lembrem-se de escolherem uma senha com caracteres alfanuméricos, símbolos, números e letras maiúsculas.

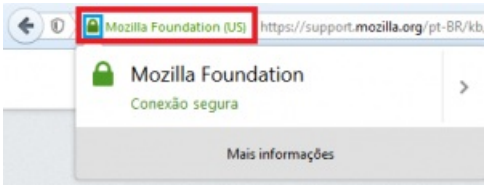


Acervo pessoal

Para mais informações acesse o artigo oficial. Para aprender gerenciar suas senhas de forma mais abrangente, acesse aqui. O Firefox também mostra de forma muito criativa e intuitiva de como criar senhas seguras.

Conexões Seguras

Essa parte do artigo não é um tutorial, iremos esclarecer de forma simples como funciona e os tipos de Conexões Seguras. O Firefox tem o botão de identidade, um recurso de segurança que contém informações importantes do site visitado, como criptografia usada, se foi verificado, quem é o proprietário do site e quem fez a verificação. Esse botão:



Acervo pessoal

O ícone do cadeado verde destacado, indica qual a Conexão identificada no site. São 5 Conexões possíveis: um globo cinza, um triângulo cinza, um triângulo laranja, um cadeado cinza ou um cadeado verde.

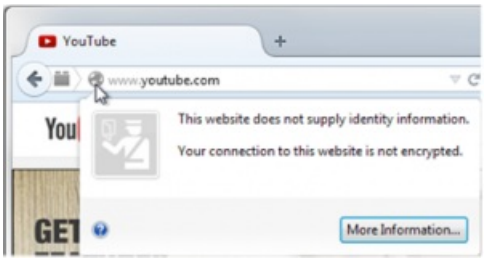
Mozilla

Globo cinza

“Um globo cinza indica que:

- O site não fornece informações de identidade.
- A conexão entre o Firefox e o site não é criptografada ou apenas parcialmente criptografada e não deve ser considerada segura contra espionagem.

A maioria dos sites terão o globo cinza, porque não envolvem passar informações sensíveis e por isso não precisam ter identidades verificadas ou conexões criptografadas. Ela se aplica a sites servidos sobre HTTP (não criptografado) ou HTTPS (parcialmente criptografado).“



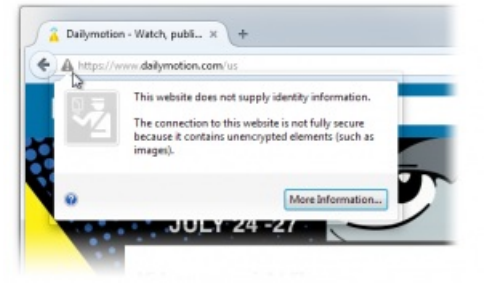
Mozilla

Triângulo Cinza

“Um triângulo cinza indica que:

- O site não fornece informações de identidade.
- A conexão com esse site não é totalmente segura, pois contém elementos não criptografados (como imagens).”

Isso significa que os dados transmitidos podem ser vistos em sua forma original por alguém que estiver espionando. Pode ser mensagens de texto, áudios e até arquivos de *backup.*



Mozilla

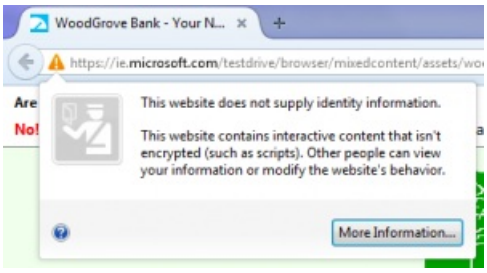
Triângulo Laranja

“Um triângulo laranja indica que:

- O site não fornece informações de identidade.
- A conexão entre o Firefox e o site é apenas parcialmente criptografada e não evita a espionagem.

Isso implica que você já permitiu o conteúdo misto servido por HTTPS a ser exibido no site, apesar dos riscos.

Recarregar o site irá bloquear novamente certas solicitações HTTP para reduzir as ameaças, alterar o ícone ao seu estado anterior (globo cinza para conteúdo misto e cadeado cinza de outra forma) e mostrar o escudo de conteúdo misto. Para obter informações sobre o bloco de conteúdo misto, consulte Como o conteúdo que não é seguro afeta a minha segurança?."



Mozilla

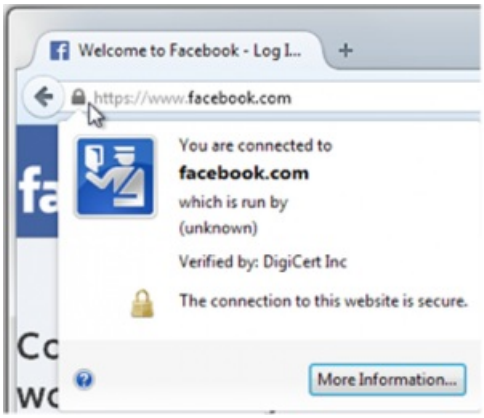
Cadeado Cinza

"Um cadeado cinza indica que:

- O endereço do site foi verificado.
- A conexão entre o Firefox e o site está criptografada para evitar espionagem.

Quando um domínio é verificado, significa que as pessoas donas do site, compraram um certificado provando que o domínio é delas e ele não é falso. Por exemplo, o Facebook tem esse tipo de certificado e uma conexão criptografada, de modo que o botão de identidade do site mostra um cadeado cinza. Quando você clica sobre o cadeado, diz-lhe que você está realmente conectado ao *facebook.com* certificado pela DigiCert Inc. Também garante que a conexão é criptografada, de modo que ninguém pode espionar a conexão e roubar suas informações de login do Facebook.

No entanto, isso não verifica na verdade quem possui o domínio em questão. Não há garantia de que o facebook.com é realmente de propriedade do Facebook. As únicas coisas garantidas são que o domínio é válido e que a conexão está criptografada."



Mozilla

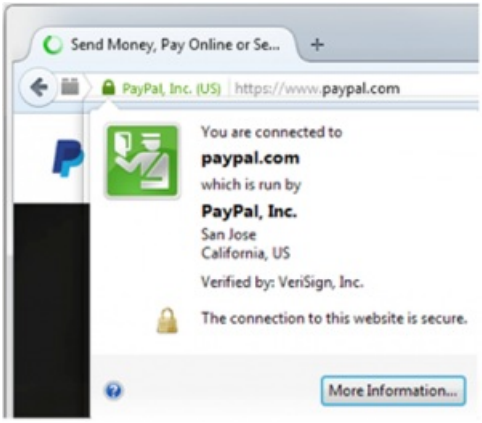
Cadeado Verde

"Um cadeado verde indica que:

- O endereço do site foi verificado através de um Certificado de Validação Avançada.
- A conexão entre o Firefox e o site é criptografada para evitar espionagem.

Um cadeado verde mais o nome da empresa ou organização em verde significa que o site está usando um Certificado de Validação Avançada. Um certificado de Validação Avançada é um tipo especial de certificado do site que requer um processo de verificação de identidade significativamente mais rigoroso do que outros tipos de certificados. Enquanto o cadeado cinza indica que o site usa uma conexão segura, o cadeado verde indica que a conexão é segura *e* que os proprietários do domínio são quem você espera que sejam.

Com o certificado de Validação Avançada, o Botão de Identificação do Site garante que paypal.com é de propriedade da Paypal Inc., por exemplo. Não só o cadeado torna-se verde no site Paypal, mas também se expande e exibe o nome do proprietário no próprio botão. O diálogo de Identificação do Site contém mais informações.”



Mozilla

Conclusão

Recomendo a leitura de TODOS os links com os artigos originais da Mozilla, principalmente o Antirrastreamento, que exige um grau de conhecimento maior. Eu pessoalmente não achei necessário mudar as explicações de cada tipo de Conexão, por isso estão todas entre aspas, foram retiradas do artigo oficial da Mozilla com algumas alterações e adições. Espero que tenham gostado, pois terá a **Parte 3**.