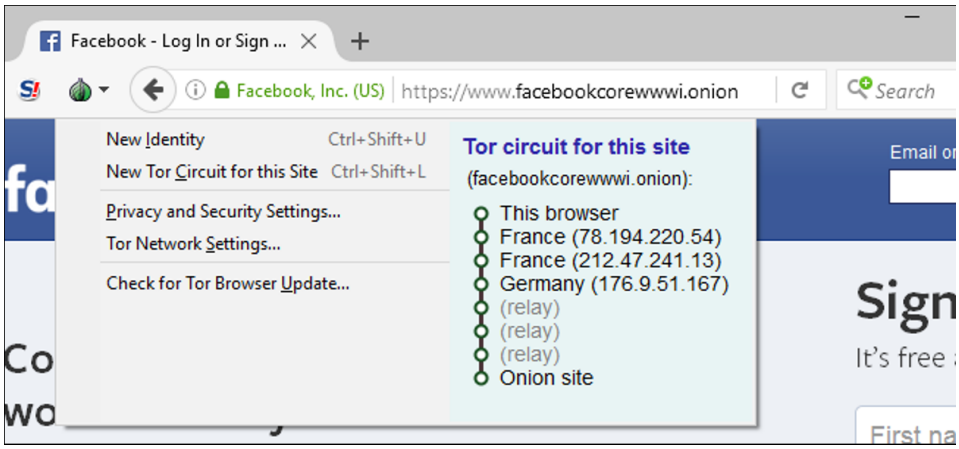
How-To Geek

How to Access .onion Sites (Also Known as Tor Hidden Services)

CHRIS HOFFMAN @chrisbhoffman
UPDATED JAN 4, 2021, 12:40 PM EST | 3 MIN READ



Website addresses that end in ".onion" aren't like normal domain names, and you can't access them with a normal web browser. Addresses that end with ".onion" point to Tor hidden services on the "deep web".

Warning: Lots of .onion sites contain very nasty things, and many of them are likely scams. We recommend staying away from "browsing" .onion sites–instead, use this only if you have a specific site you want to access for a good reason.

What Is a .onion Site?

RELATED: ***How to Browse Anonymously With Tor***

Tor–short for "the onion router"–is an anonymizing computer network. It's partially funded by the US government, and is

designed to help people in countries where Internet access may be censored or monitored. When you connect to Tor, your internet activity is sent through the Tor network, anonymizing your Internet activity so it can't be snooped on, and so that you can access websites that may be blocked in your country.

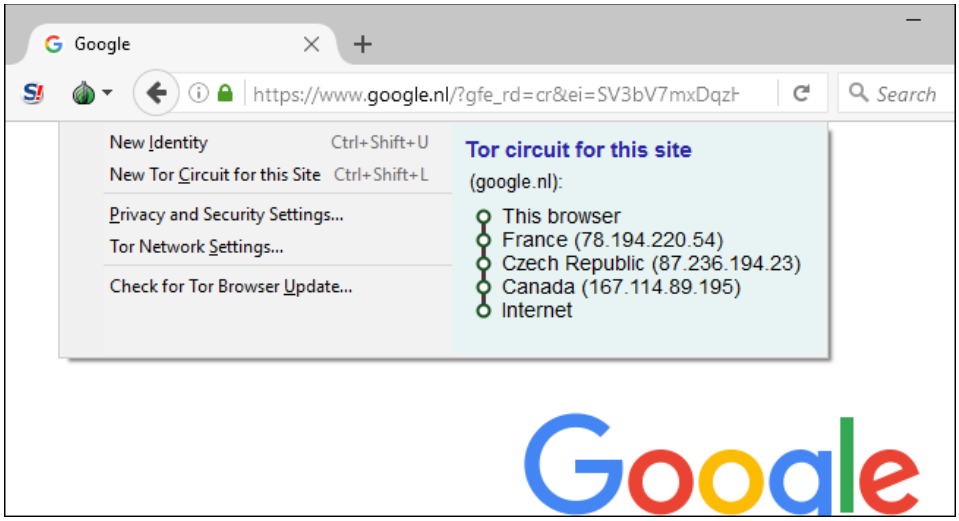
So, when you access google.com through Tor, your request bounces from Tor relay to Tor relay before it reaches an "exit node". That exit node then contacts Google.com for you, and it sends you back the data Google responded with. Google sees this as the exit node's IP address contacting it instead of your IP address.

RELATED: ***Is Tor Really Anonymous and Secure?***

But that means that "last mile" of traffic can be snooped on by an organization monitoring or even running the exit nodes–especially if your traffic is unencrypted. A ".onion" address points to a Tor hidden service, which is a server you can only access through Tor. This means that your browsing activity can't be snooped on by someone watching the Tor exit nodes. It also means that someone hosting a website can hide that server using the Tor network, so no one can find it–in theory.

For example, Facebook maintains an official Tor hidden services address at "https://facebookcorewwwi.onion/". This allows you to access Facebook through Tor, and your connection doesn't ever leave Tor where it can be snooped on. This may be useful in countries that block Facebook, for example.

You don't necessarily want to use Tor all the time, as it's slower than just browsing normally. But it's a useful tool for anonymizing your Internet activity and bypassing censorship.

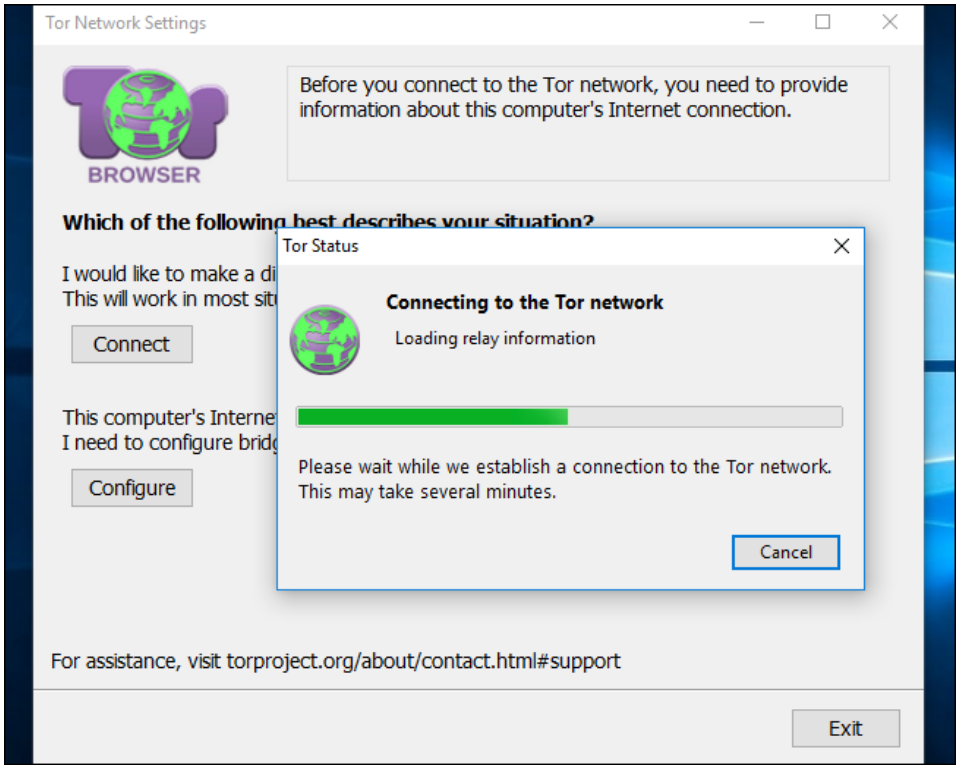


How to Access .onion Sites with the Tor Browser

To access a .onion address, you'll need to access it through the Tor Browser. It's a modified version of Firefox that's configured to connect to sites through the Tor network.

Download the Tor Browser from the Tor project's website to continue. It's available for Windows, Mac, Linux, and Android.

On Android phones and tablets, we previously recommended the Orbot proxy app or Orfox browser from Google Play. The Tor project still offers no official Tor apps for iPhone or iPad, but some third-party apps are available in Apple's App Store.



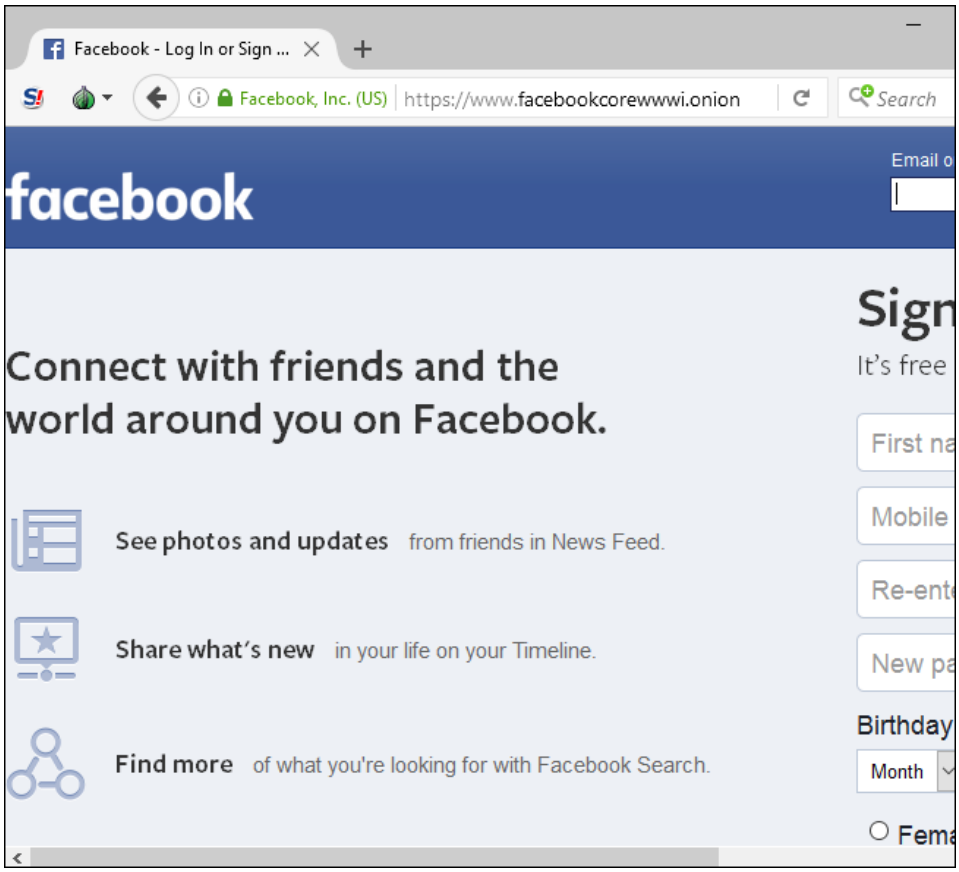
After launching the Tor browser, type the .onion address into its address bar. For example, to access Facebook's hidden service, you'd enter the following address:

```
https://facebookcorewwwi.onion/
```

Or, to access the DuckDuckGo search engine's hidden service, you'd enter:

```
http://3g2upl4pq6kufc4m.onion/
```

While using the Tor browser, you can click links to .onion addresses and they'll load normally. But they'll only work in the Tor browser, while connected to Tor.



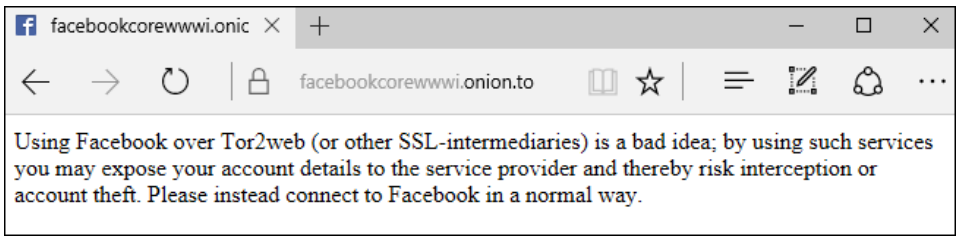
Don't Access .onion Sites Through Proxies Like Tor2Web

You can also access .onion sites without running Tor through proxies that connect to Tor for you. The proxy connects to Tor for you and then forwards you the traffic over the regular Internet.

This, however, is a very bad idea! You're losing the anonymity you normally have when you connect to a .onion site through the Tor browser. That's the whole point of a .onion address, after all. The website you access maintains its anonymity, but someone monitoring your connection can see which website you're connecting to. The service provider can also see what you're connecting to and snoop on any passwords and other private information you provide over the connection.

Tor2web functions in this way, but you shouldn't use it. For example, if you attempt to connect to Facebook's hidden service using Tor2web, Facebook blocks the connection and tells you it's a

bad idea.



Looking for lists of .onion sites? Search the web for lists of .onion sites and you'll find some places to start. Many of the directories of .onion sites are themselves stored on .onion sites, though, which you can only access through Tor.

Again, beware: Lots of .onion sites contain very nasty things, and many of them are likely scams. We recommend staying away from them, if possible. This trick is best used when you want to browse to a specific .onion site.

CHRIS HOFFMAN

Chris Hoffman is Editor-in-Chief of How-To Geek. He's written about technology for over a decade and was a PCWorld columnist for two years. Chris has written for The New York Times, been interviewed as a technology expert on TV stations like Miami's NBC 6, and had his work covered by news outlets like the BBC. Since 2011, Chris has written over 2,000 articles that have been read nearly one billion times---and that's just here at How-To Geek.

READ FULL BIO »

The above article may contain affiliate links, which help support How-To Geek.