Tor Browser 4.0.1

Now Theresa May can't discover **Ben Everard**'s rampant online cat-video viewing habits. Your move, GCHQ.

DATA

Web
www.torproject.org
Developer
The Tor Project
Price
Free under various free software licences

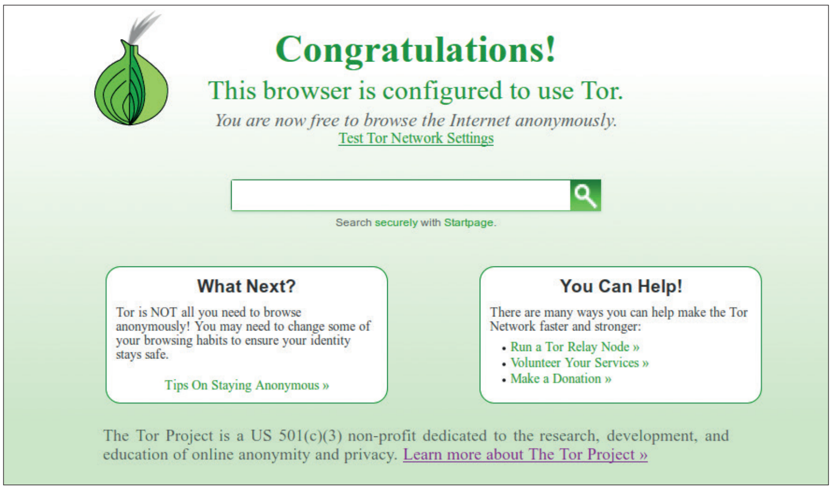
The *Tor Browser* was originally funded by the US State Department as a way for non-technical people living in countries with few internet freedoms to access their online material, such as the Voice of America news site. The goal was simple: take the best censorship-resisting online anonymity software and democratise it so that it becomes accessible to everyone, not just geeks. That was nine years and four version numbers ago. Few people at the time realised just how popular it would become.

The *Tor Browser* comes as a Zip file that contains the executable. You just extract it and run. It will automatically connect to the *Tor* network, and start *Firefox* (now version 31 ESR). *Firefox* is customised to improve security. It defaults to the StartPage privacy-protecting search engine, and includes the NoScript addon. By default, the NoScript settings are quite lax, so you may want to investigate these if you're worried about attacks on your anonymity.

In future versions, *Tor Browser* will have a security slider that will enable you to easily change the security vs convenience settings (such as NoScript). There's a beta version of *Tor Browser 4.5* available now that includes this, but it's not yet considered stable.

Problems change

The Free Software Foundation's HTTPS Everywhere addon is also installed. This forces the browser to use HTTPS whenever it's available even when following links that point to the non-SSL version of the page. So, for example, if you enter **www.wikipedia.org** into a normal version of Firefox, you'll go to the non-secure site, whereas if you enter it in the *Tor Browser*, you'll go to the SSL-secured version of the site. This is important because even through the *Tor Browser* stops people being able to link who you are to what you're browsing, unless you use SSL, it's still possible to see what data is being sent (which could well be used to identify who's sending it).



Congratulations!

This browser is configured to use Tor.

You are now free to browse the Internet anonymously.

Test Tor Network Settings

Search securely with Startpage.

What Next?

Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.

Tips On Staying Anonymous »

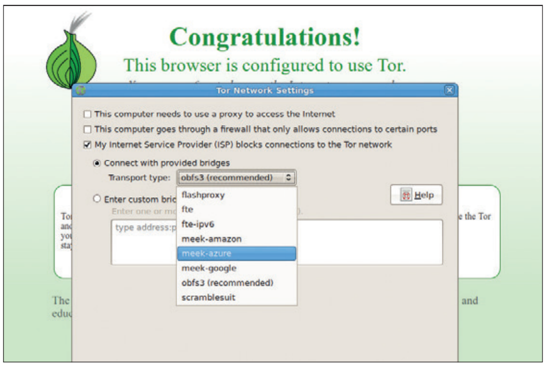
You Can Help!

There are many ways you can help make the Tor Network faster and stronger:

- Run a Tor Relay Node »
- Volunteer Your Services »
- Make a Donation »

The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn more about The Tor Project »

When the *Tor Browser* starts, it will verify that *Tor* is working properly. If you don't see this page, then there's a problem



Congratulations!

This browser is configured to use Tor.

Tor Network Settings

☐ This computer needs to use a proxy to access the Internet
☐ This computer goes through a firewall that only allows connections to certain ports
☑ My Internet Service Provider (ISP) blocks connections to the Tor network
● Connect with provided bridges
Transport type: obfs3 (recommended)
○ Enter custom bric

The new transports dramatically increase the difficulty for anyone trying to stopping people accessing *Tor*.

The challenges faced by the *Tor Browser* today are very different from when it launched. Originally, it was a way to access content that was blocked; now the actual *Tor* network itself is blocked in some countries. This has meant that the *Tor* developers have had to find ways to access the network even when all the IP addresses of computers on the network are blocked.

Rather than try to come up with a single solution to this, *Tor* uses plugable transport modules. These are methods of obfuscating the Tor communication so it's harder to block. The more pluggable transports there are, the more challenges for anyone trying to prevent people connecting to the network. These transports have been around for a while, but *Tor Browser 4* both makes them easier to use, and introduces some powerful options. The Meek pluggable transport (new in the *Tor Browser 4*) is believed to work out-of-the box in China, one of the countries that has had most success in blocking access to *Tor*. This transport diverts traffic through popular content delivery networks (CDNs) which means that if a government wants to block Meek, they have to block every site that uses these CDNs, and that includes a large proportion of the web. The idea is to make the level of collateral damage of blocking *Tor* too high for it to be feasible.

Regardless of whether you're trying to bypass censorship, or keep your private internet communication private, the *Tor Browser Bundle* should find a place in your network toolkit.

LINUX VOICE VERDICT

Preventing snooping and bypassing censorship has never been easier.
★★★★★