Computer und Internet

TOR - BROWSER

Jeder sollte den Tor Browser haben, denn kein anderer schützt Ihre Privatsphäre so gut und als Nebeneffekt öffnet sich damit auch die Tür zum Darknet. Der Tor Browser lässt sich auch auf dem Handy installieren.

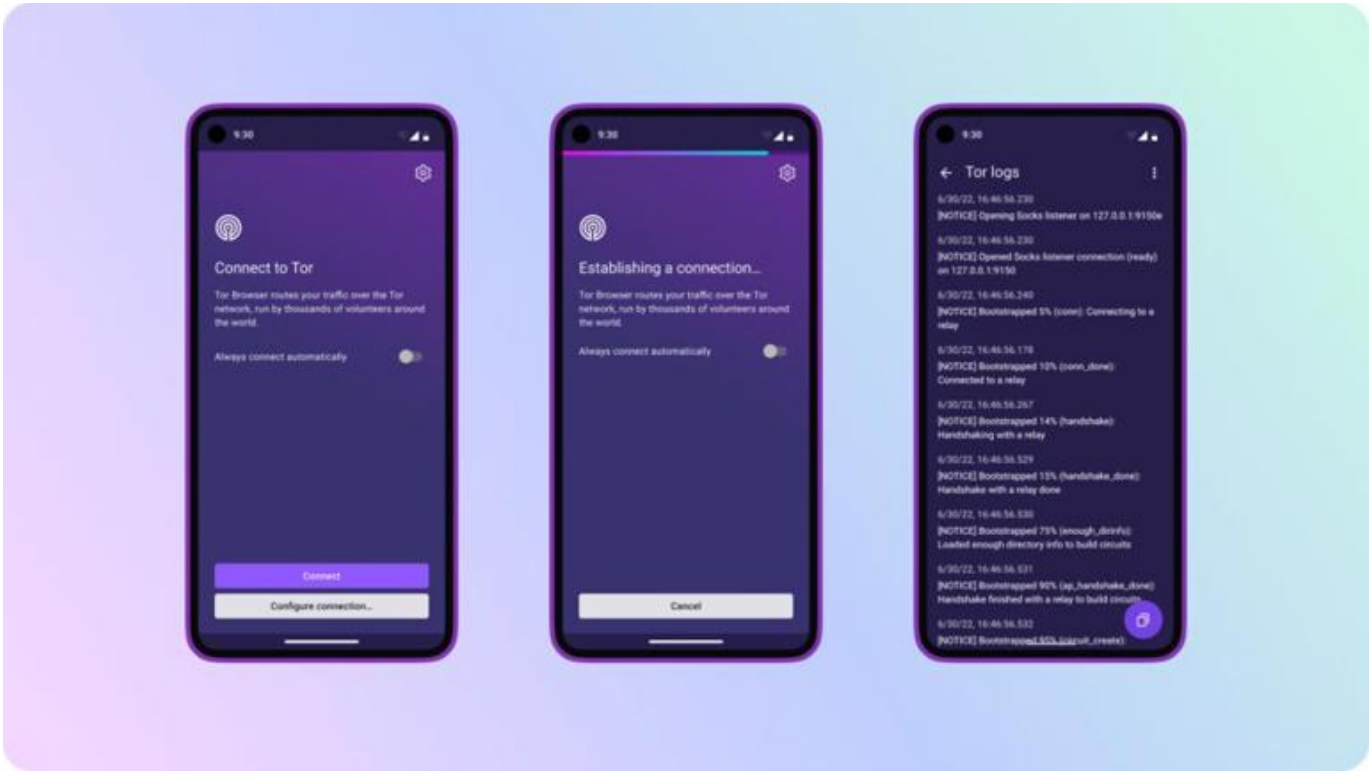
Der Tor Browser gilt als Darknet-Browser, denn ohne ihn lässt sich der "verborgene Teil" des Internets nicht erkunden. Aber man muss mit dem Tor Browser nicht zwingend ins Darknet.

Tor Browser funktioniert auch im sichtbaren Web und bringt dabei einen großen Vorteil mit: den Schutz Ihrer Privatsphäre, denn sämtliche Anfragen werden durch das Tor-Netzwerk geschleust. Da der Tor Browser auf Firefox ESR setzt, müssen Sie sich auch bei der Bedienung nicht umgewöhnen.

Die Entwickler sind auch immer fleißig mit neuen Funktionen.

Der Tor Browser ermöglicht anonymeres Surfen im Internet mit dem Open-Source-Browser Firefox.

Das ist neu im aktuellen Tor Browser 13.5



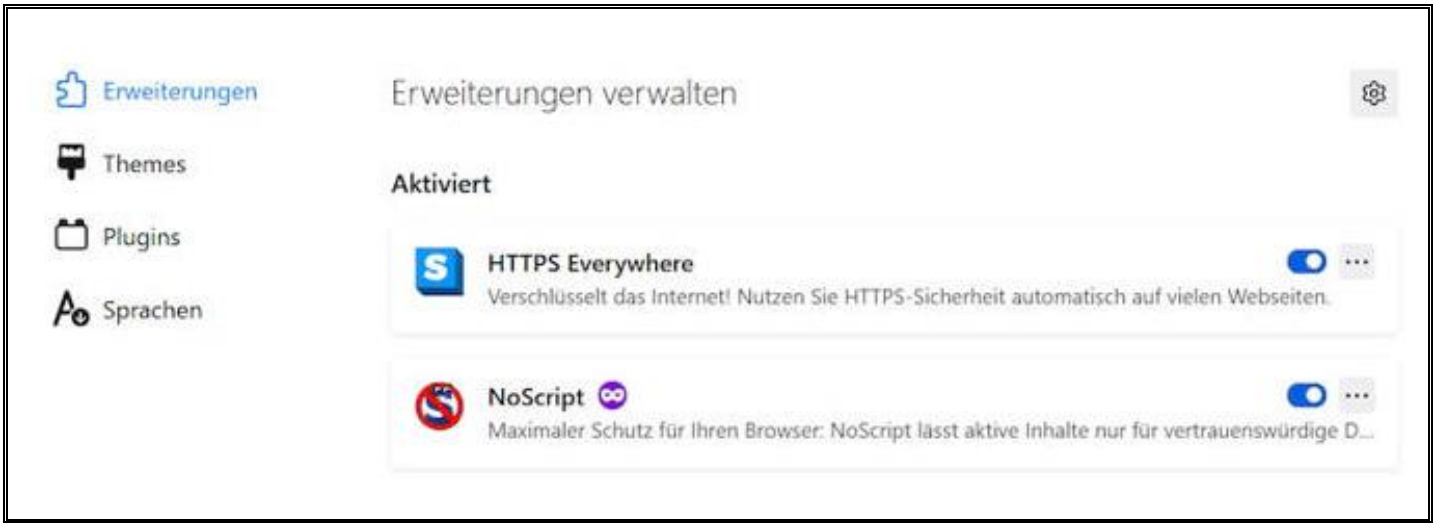
Wer den Hintergrund nicht kennt, vermutet hinter der Darstellung oft einen Fehler. Jetzt gibt es Einstellungen, wie Tor Browser die Darstellung beim Verändern der Fenstergröße anpassen soll. Per Doppelklick auf den grauen Rand lässt sich die Darstellung der Inhalte jetzt leicht auf die nächste vordefinierte Fenstergröße anpassen.

Wer Brücken nutzt, kriegt mit dem Update eine einfachere Verwaltung spendiert. Außerdem lassen sich die "Bridges" aus neuen Quellen hinzufügen, zum Beispiel über Telegram-Kanäle.

Die Android-Version hat zur Verbindung ins Tor-Netzwerk ebenfalls eine neue Optik erhalten. Die soll ein erster Schritt hin zur Integration der Funktion Connection Assist sein, die es bereits in der Desktop-Version gibt. Mit ihr soll sich die Zensur des Tor-Netzwerks automatisch durch Bridge-Konfigurationen umgehen lassen. Die Android-Version orientiert sich dabei auch optisch am Desktop-Browser und kann auf Wunsch die Verbindung ins Tor-Netzwerk automatisch herstellen.

Die kostenlose Android-App des Tor Browsers ermöglicht Ihnen sicheres und anonymes Surfen im Internet auf mobilen Plattformen.

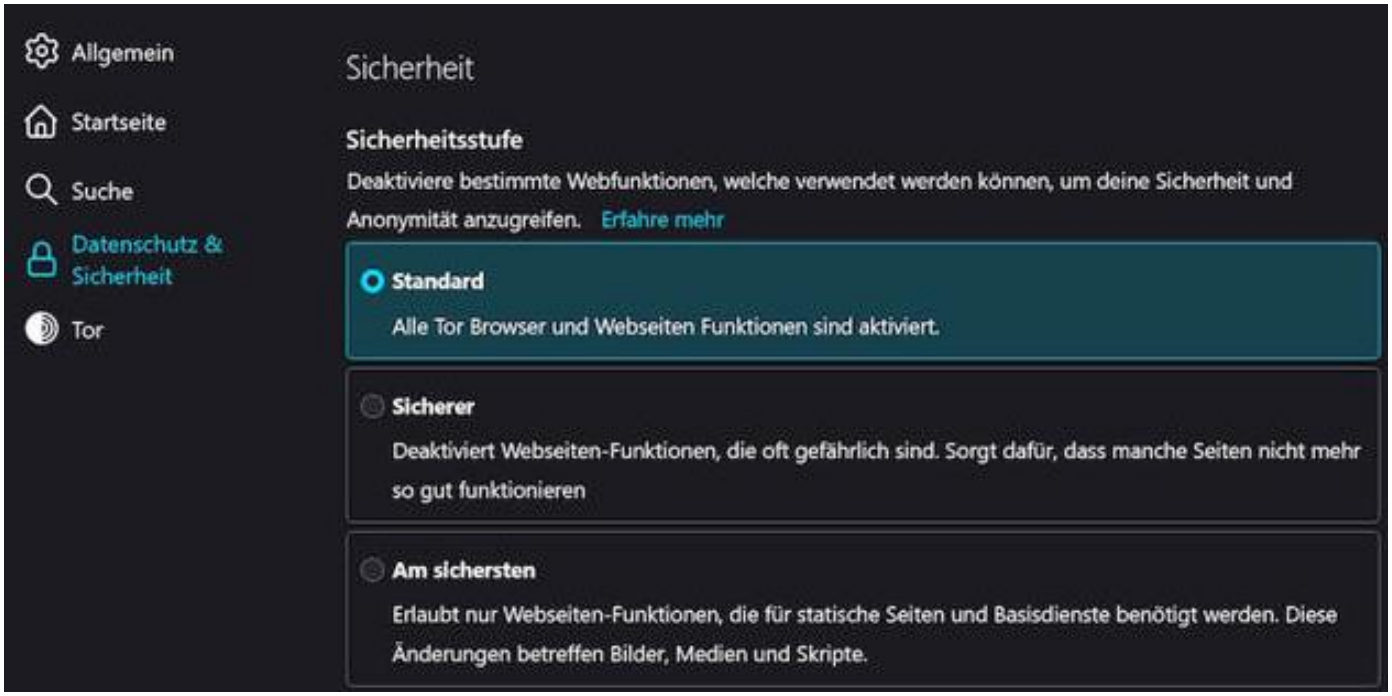
Tor-Browser: Firefox ESR plus 2 Erweiterungen



Der Tor-Browser baut auf Firefox ESR auf und packt zwei Erweiterungen obendrauf. HTTPS Everywhere und NoScript dürften vielen Nutzern ein Begriff sein. Die eine Erweiterung sorgt dafür, dass man, wenn möglich, auf verschlüsselten Seiten landet und die andere blockiert JavaScript von nicht vertrauenswürdigen Seiten.

Auf zusätzliche Erweiterungen sollten Sie verzichten, weil diese die Anonymität unterwandern könnten. Noch sicherer sind Sie jedoch unterwegs, wenn Sie JavaScript generell deaktivieren. Navigieren Sie dazu in die Einstellungen unter "about:config" und setzen "javascript.enabled" auf "false".

Sicherheitsstufen zur Auswahl



Die Macher des Tor-Browsers sind erfahren und wissen genau, dass ein zu stark abgesperrter Browser in der Praxis zu Problemen führen kann. Deshalb sind die gewählten Einstellungen nicht an jeder Stelle so sicher wie möglich. Das lässt sich aber leicht ändern. Klicken Sie dazu „auf das Schutzschild“ neben der URL-Leiste und danach auf "Change".

Die Sicherheitsstufe steht voreingestellt auf "Standard", weil das die wenigsten Schwierigkeiten verursacht. Wählen Sie besser "Am sichersten" und bestätigen Sie mit "Ok". Sollte eine Webseite mit diesen restriktiven Einstellungen kollidieren, können Sie eine Stufe zurück auf "Sicherer" schalten.

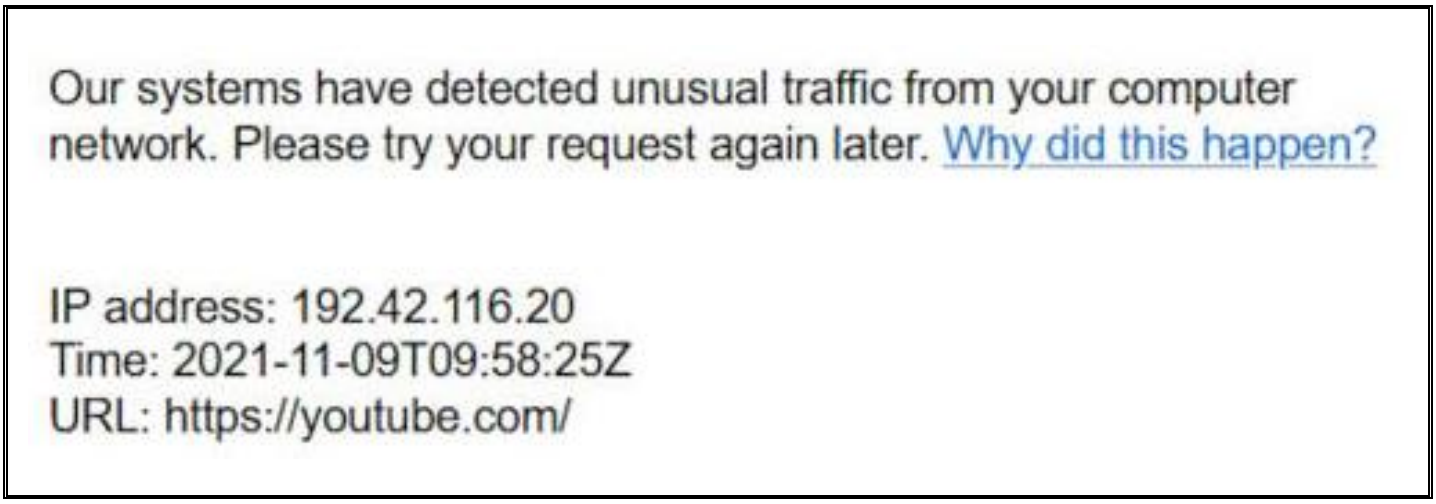
Surf-Probleme lösen

Im Prinzip sollten Sie nicht mehr am Tor Browser verändern, weder Fenstergröße noch sonst irgendwelche Einstellungen. Der Grund: Wer vom Standard abweicht, ist für Tracking anfällig. Die erhöhten Sicherheitseinstellungen sind eine Ausnahme dieser Regel, weil sie JavaScript deaktivieren und für Videos und Musik auf Click-to-Play setzen.

Sie müssen jetzt selbst ins kalte Wasser springen und Tor Browser einfach mal nutzen. Dabei können Probleme auftreten, etwa werden Dienste wie Google-Suche in fremden Sprachen erscheinen. Das hängt damit zusammen, dass die Geolokalisierung nicht funktioniert, Ihre IP-Adresse verrät nicht mehr, dass Sie in Deutschland sitzen.

Dann einfach ein Bookmark für „google.de“ anlegen. Google fordert oft auch dazu auf, ein „Captcha“ abzutippen, wenn zu viele Anfragen von einer IP-Adresse kommen. Das muss man hinnehmen, oder man klickt auf den Tor Button und holt sich eine "Neue Identität".

Probleme beim Einloggen



Probleme treten oft auch auf, wenn man sich auf Webseiten einloggen will, etwa bei „Gmail“ oder „Facebook“. Google verschickt dann zum Beispiel gerne Mails mit dem Hinweis, dass möglicherweise das Mail-Konto geknackt wurde. Das liegt daran, weil Google aus Sicherheitsgründen ein Auge darauf hat, von wo aus die Zugriffe erfolgen.

Kommt der erste Zugriff aus Polen, zwei Stunden später aus Südafrika und eine halbe Stunde später aus den USA, dann nimmt Google an, dass das Konto gehackt wurde. Sie können diese Hinweise ignorieren. Besonders sicherheitsbewusste Nutzer loggen sich mit Tor Browser überhaupt nirgends ein, weil sie sich kein Tracking ins Haus holen wollen. Für Facebook, Gmail & Co. kommt dann ein anderer Browser zum Einsatz.

Neue Identität und Updates holen

Im Tor-Netzwerk ist man einer von vielen Nutzern und taucht in der Masse unter. Trotzdem ist es eine gute Idee, den Schutzmantel ab und zu zu wechseln. Klicken Sie dazu einfach auf das Besen-Icon rechts neben der URL-Leiste.

Bestehende Installationen werden derzeit noch nicht automatisch auf Tor Browser 12 aktualisiert. Um den Browser selbst zu aktualisieren, klicken Sie wie in Firefox in die Einstellungen | Hilfe | Über Tor Browser.

Über das Tor-Netzwerk und den zugehörigen Tor Browser wird viel gestritten. Meist geht es darum, wie gut sich damit die Privatsphäre wirklich noch schützen lässt. Meine Meinung: Es ist nicht perfekt, aber es gibt keine bessere Alternative. Zumindest als Zweit-Browser neben Firefox oder Chrome macht er eine gute Figur.