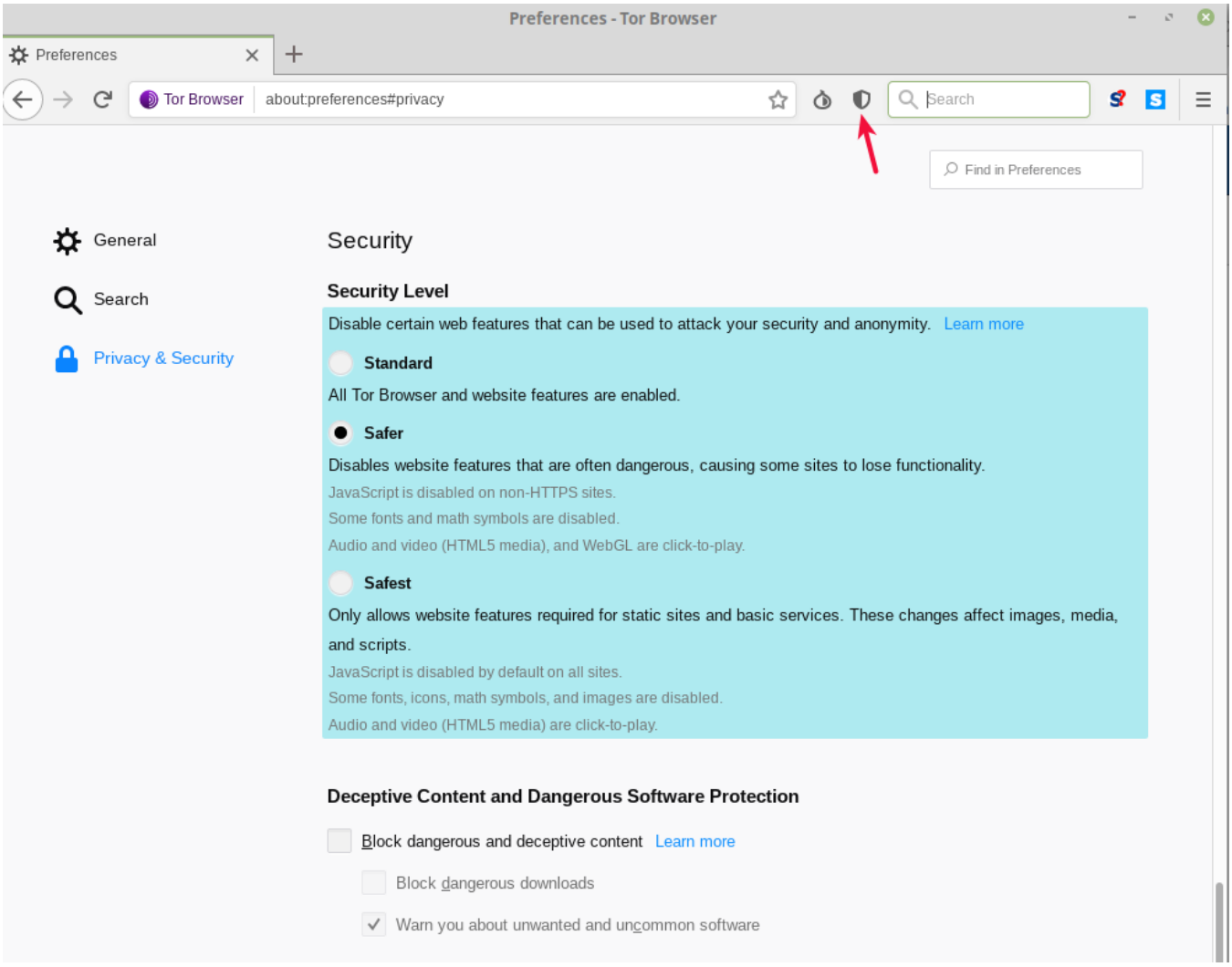
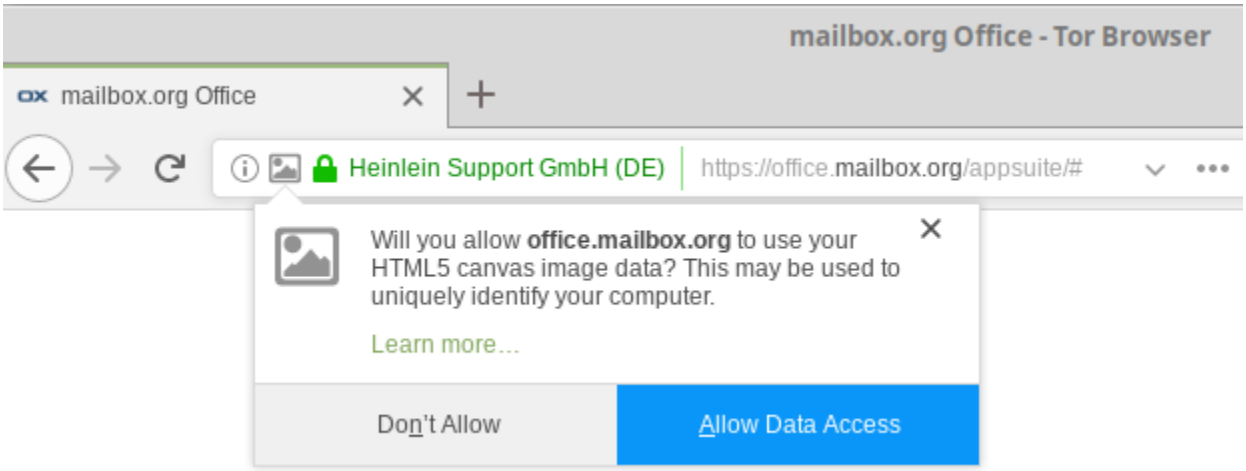
How to configure the Tor Browser

Users can access the mailbox.org Office web interface via the Tor Browser. For this, we recommend setting the security level to ***Medium-High*** as shown in the screen shot below.



Open-Xchange uses canvas for wordprocessing and spreadsheet. During login the canvas function is tested and you will see the following message. You have to allow the extraction of canvas image data for the domain office.mailbox.org. Otherwise it isn't possible to login to the mailbox.org office.



Use the Tor exit node in our data center to access our services

Further, users should make sure to route all data traffic between their client and mailbox.org through our ***dedicated Tor exit node***. Why? In previous years, there has been evidence of attempted attacks on Tor-secured communications via malicious network exit nodes. These nodes were set up to employ false SSL-certificates to perform man-in-the-middle attacks on encrypted connections (e.g., in 2013: Connections to Wikipedia or E-mail via IMAPS).

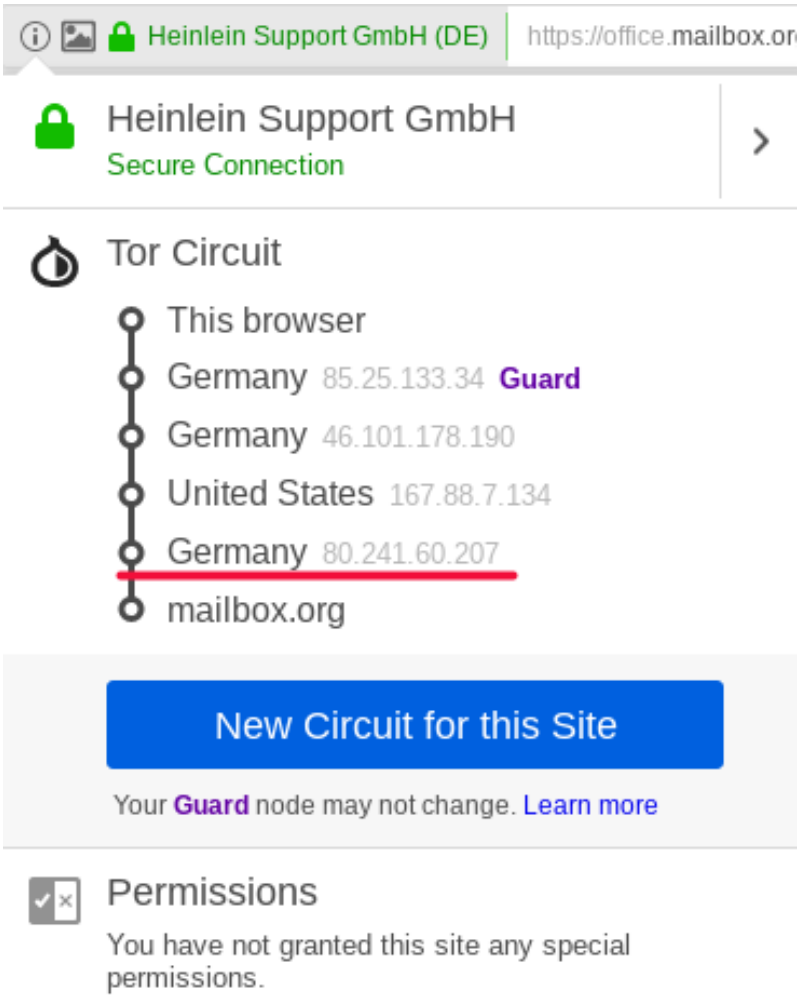
In order to protect our customers who use Tor against such attacks, we operate a dedicated Tor node (nickname: mailboxorg) within our data centre. It just takes a simple configuration step to use this node as an exit node for Tor. Doing so will secure any access to our web pages and mail servers and eliminate the dangers posed by malicious Tor exit nodes in other networks.

Open the file **Browser/TorBrowser/data/Tor/torrc** in a text editor and add the following lines at the end of the file:

```
MapAddress mailbox.org mailbox.org.85D4088148B1A6954C9BFFFCA010E85E0AA88FF0.exit MapAddress *.mailbox.org *.
mailbox.org.85D4088148B1A6954C9BFFFCA010E85E0AA88FF0.exit
```

These settings will make sure that any data traffic to mailbox.org will be channelled through the Tor network to the servers located in our data centre. In essence, this setup resembles something quite similar to a VPN connection.

After you have made the changes above, save and close the file, then restart the Browser and open the web page “mailbox.org”. Now open the Tor Button menu and confirm the new Tor network route is as follows:



The route through the Tor network should comprise **four nodes** (instead of the usual three), and the **last Tor node** must have the **IP address 80.241.60.207**. This is the IP of our exit node.

This connection offers the same level of security than that to a Tor Hidden Service (Tor Onion Site). However, there is a distinct advantage: Because any references to proper domain names are preserved, this method can validate the relevant SSL-certificates without running into those problems that can occur with a hidden service.

After everything has been set up as described, you can now use the mailbox.org Office in your browser as usual. For e-mail connections, please consider the separate Guide to using Mozilla Thunderbird with Tor.

Related Articles

- Browser add-ons settings
- Compatible web browsers

- The Tor exit node of mailbox.org
- How to configure Tor Messenger
- How to use Thunderbird with Tor Onion Router