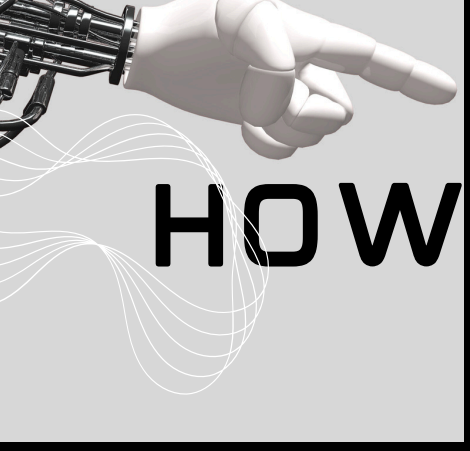


HOW TO : USE TOR

Phantom

What is Tor?

Tor is a service operated by volunteers that helps users maintain both privacy and anonymity online. It hides your identity and location, while also ensuring you stay anonymous even within the Tor network itself.

For users who occasionally need private and anonymous web access, the **Tor Browser** offers a simple and convenient way to connect to the Tor network.

Functionally, the Tor Browser resembles standard web browsers like Chrome, Firefox, or Safari. However, unlike those, it routes your internet traffic through the Tor network. This makes it much harder for anyone watching your activity to track what you're doing or trace your location.

It's important to note that **only the activities you perform inside the Tor Browser are anonymized**. Simply installing Tor Browser does not make all actions on your computer anonymous. If you use other software or browsers outside of Tor, those activities remain exposed—unless additional privacy steps are taken.

Some Tips to Keep in Mind When Using Tor :-

Tor is a powerful tool for maintaining online privacy and anonymity, but it's important to understand that perfect anonymity is rarely achievable. By recognizing Tor's limitations and following key safety practices, you can reduce risks and protect yourself more effectively:

- **Web browsing over Tor is slower**, and some websites may not load or function properly.
- **Only your activity within the Tor Browser is anonymized**. Other apps and services on your device do not use the Tor network by default.
- **Logging into accounts or entering personal details in Tor Browser** can compromise your anonymity, as the websites you interact with can identify you and detect Tor usage.
- **Tor can help bypass censorship**, but observers—such as internet service providers or governments—can still detect that you are using Tor.
- **Avoid installing browser extensions or plugins** in the Tor Browser. It's already configured with privacy protections, and extra plugins can undermine your anonymity.
- **Be cautious when opening downloaded files**, especially while Tor is active. Some documents may access external resources when opened outside of Tor, potentially exposing your real IP address.

Check the Tor Project's official resources regularly for updated advice and best practices to stay safe while using the network.

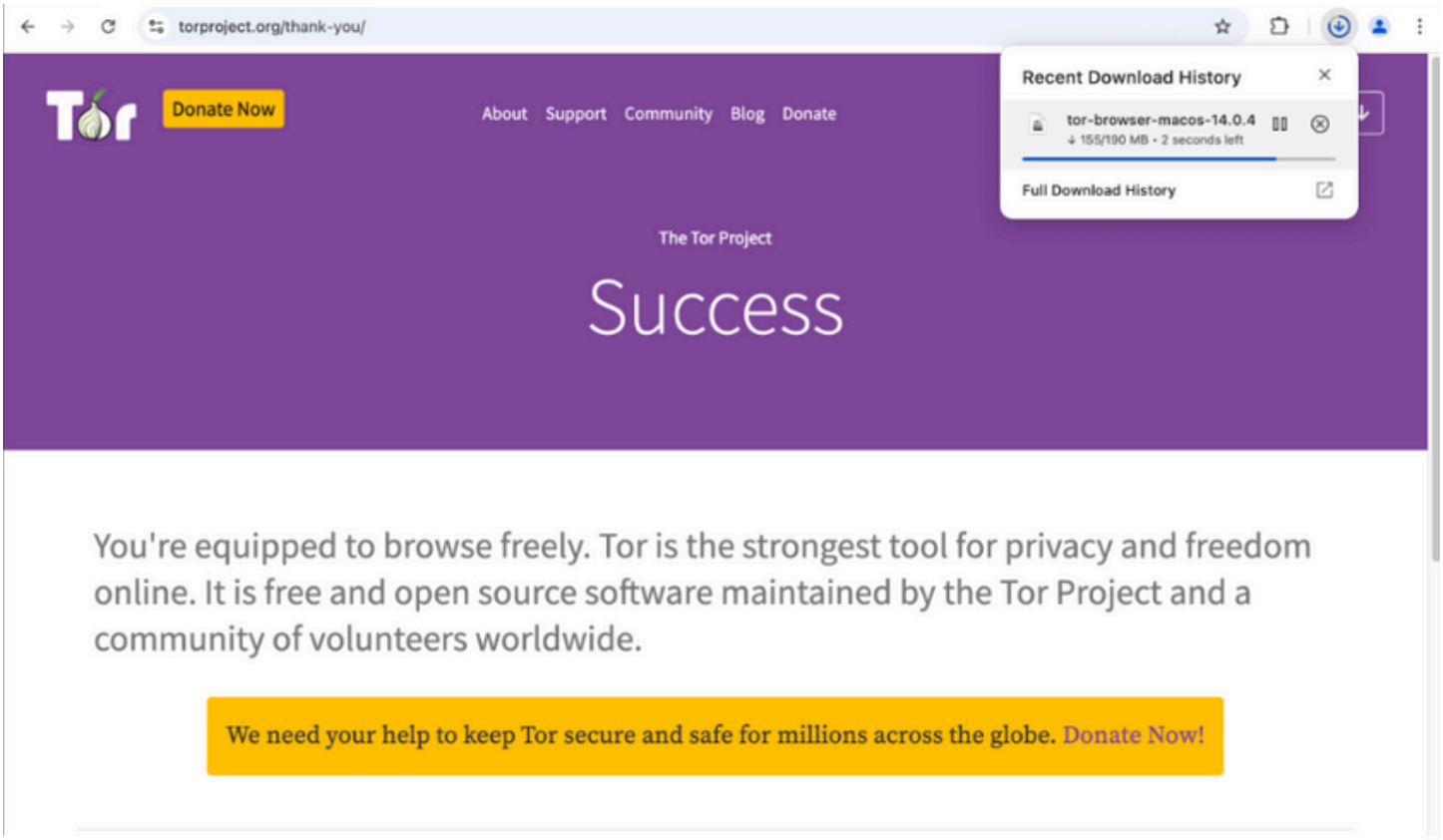
1. Tor Browser allows you to visit both the regular internet and **".onion" sites**, which exist exclusively on the Tor network. Unlike traditional websites that use public IP addresses, **.onion addresses are hidden, unique, and offer end-to-end encryption**.
2. You can explore several **EFF-hosted .onion sites**, such as **Surveillance Self-Defense**—though note that these links will only open when using the **Tor Browser**.

Getting the Tor Browser

- Open a browser like Firefox or Chrome and go to:
- https://www.torproject.org/download/
- If you are using a search engine to look for the Tor Browser, make sure that the URL is correct.
- Note - Only download Tor from the official website, and if you are prompted to accept atlernative HTTPS (SSL/TLS) security certificates, do not proceed.

Click the **“Download” icon** that matches your operating system. Depending on your browser, you may be prompted to confirm the download—otherwise, the application should begin downloading automatically.

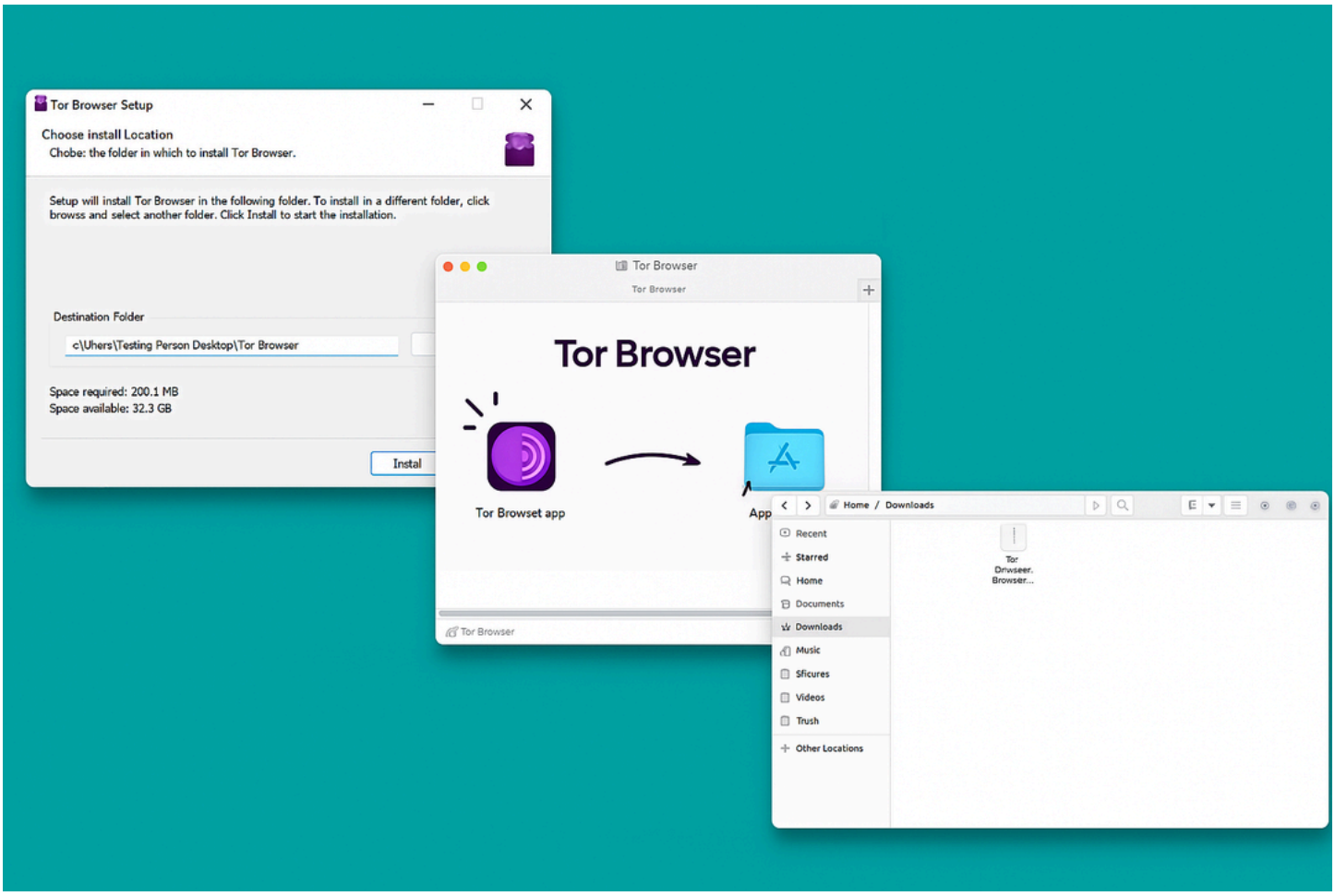
At the time this guide was written, the latest version of Tor Browser was **14.0.4**. However, newer versions may have been released since then, so be sure to download and use the **most up-to-date version** available from the **Tor Project** website.



Downloading Tor directly from its **official website** is generally safe. However, if you're ever uncertain, you can follow **Tor's verification guide** to confirm the authenticity of your download using its digital signature.

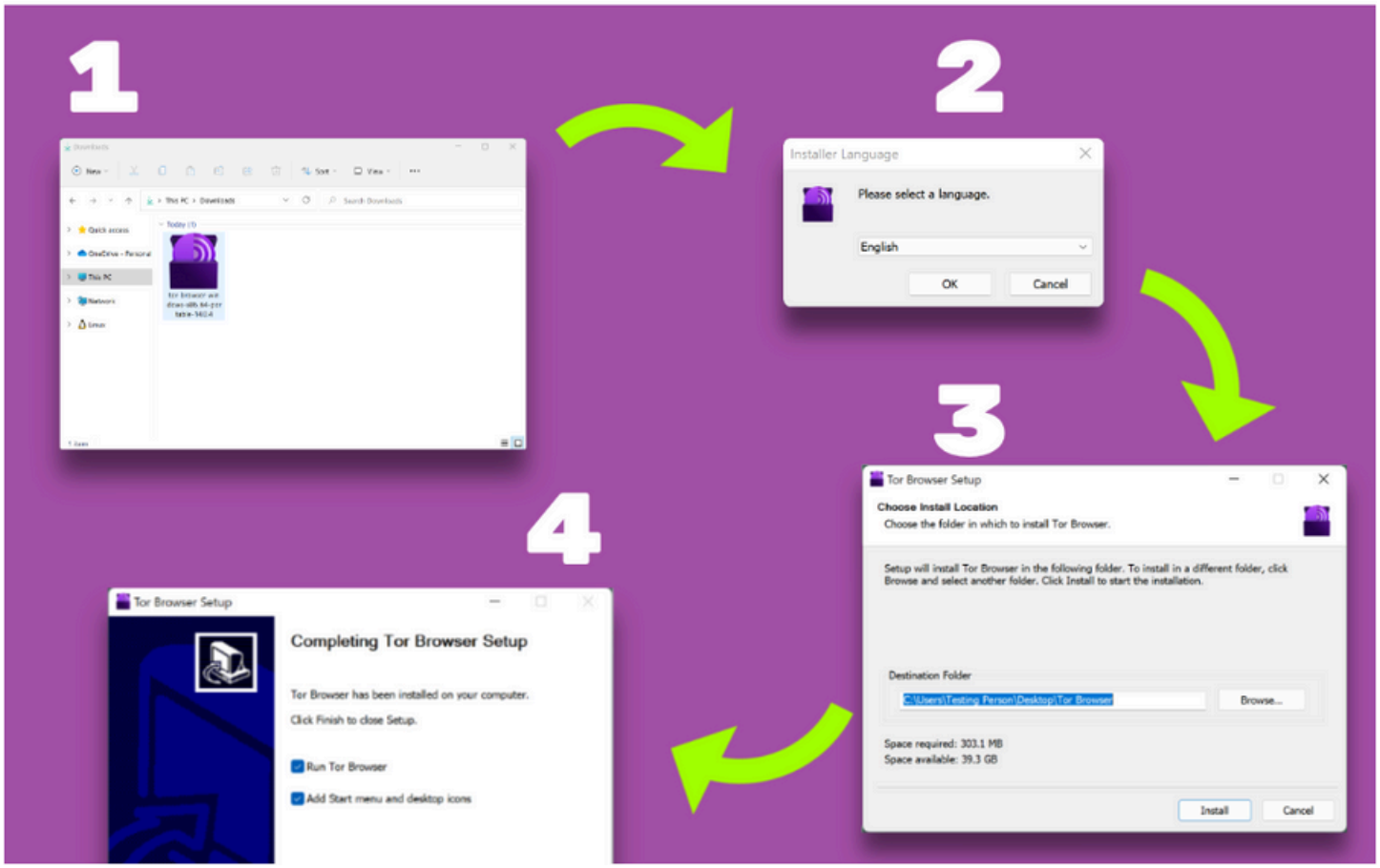
Installing the Tor Browser

Once the download finishes, navigate to your **"Downloads" folder**. Before installing any software, it's important to ensure it's trustworthy and obtained from a reliable source. In this case, since the file came from the Tor Project's official **HTTPS-secured website**, you can confidently proceed with the installation process.



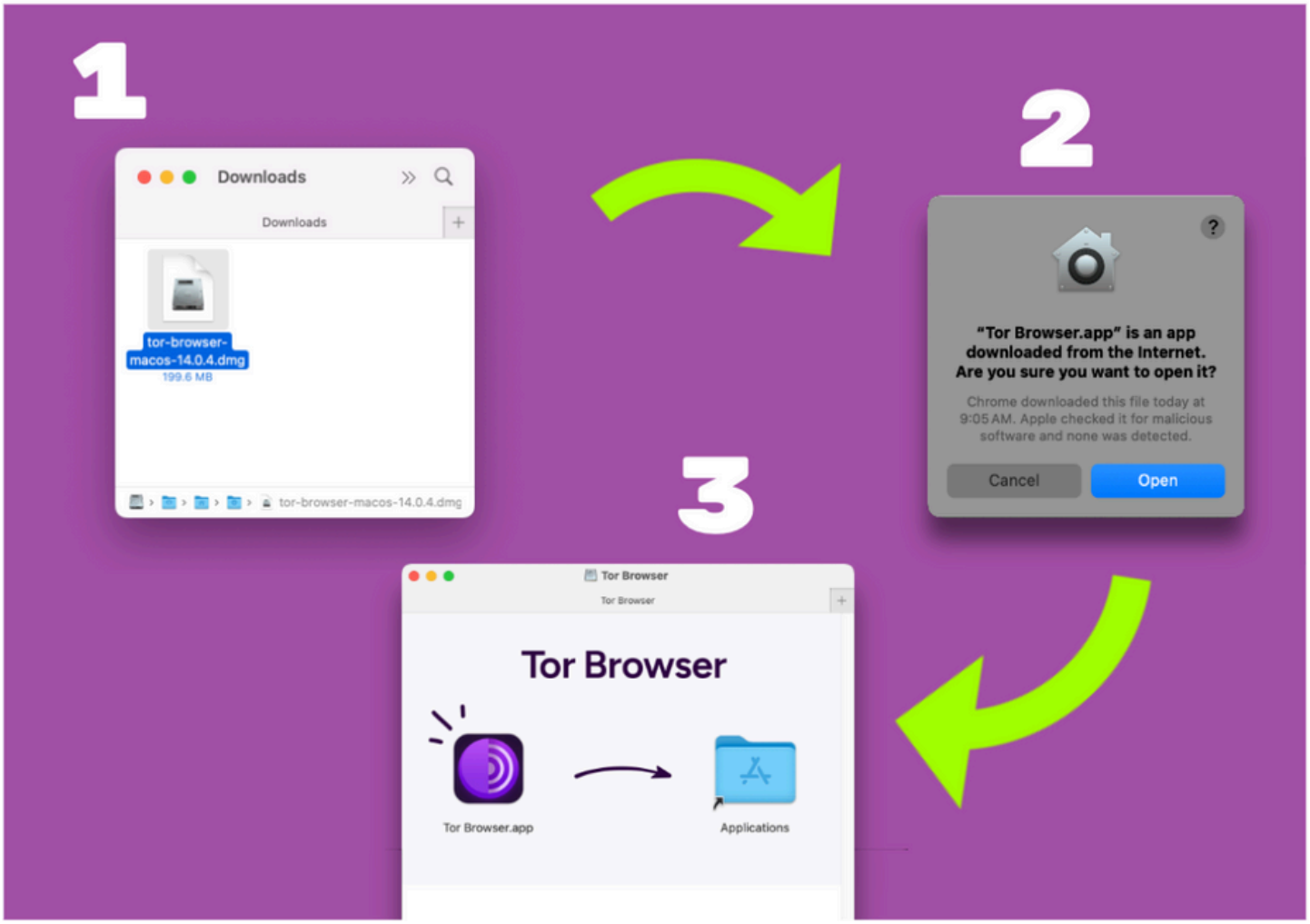
Windows

1. Double-click the downloaded file—**in this case, "torbrowser-windows-x86_64-portable-14.0.4.exe."** When you do, you may see a warning about the source of the software. Always treat such warnings seriously. Ensure the software is from a trusted source and downloaded securely from the official site. Since this copy is verified and came from the Tor Project's HTTPS-secured website, click **"Run."**
2. Next, **select your preferred language** and click **"OK."**
   You'll then be asked to choose an installation location—**the default is your Desktop**, but you can select a different folder if you prefer. When ready, click **"Install."**
3. Once installation finishes, a confirmation window will appear. Click **"Finish"** to launch Tor Browser immediately. Shortcuts labeled **"Start Tor Browser"** will also be added to your **Start Menu** and **Desktop**.



macOS

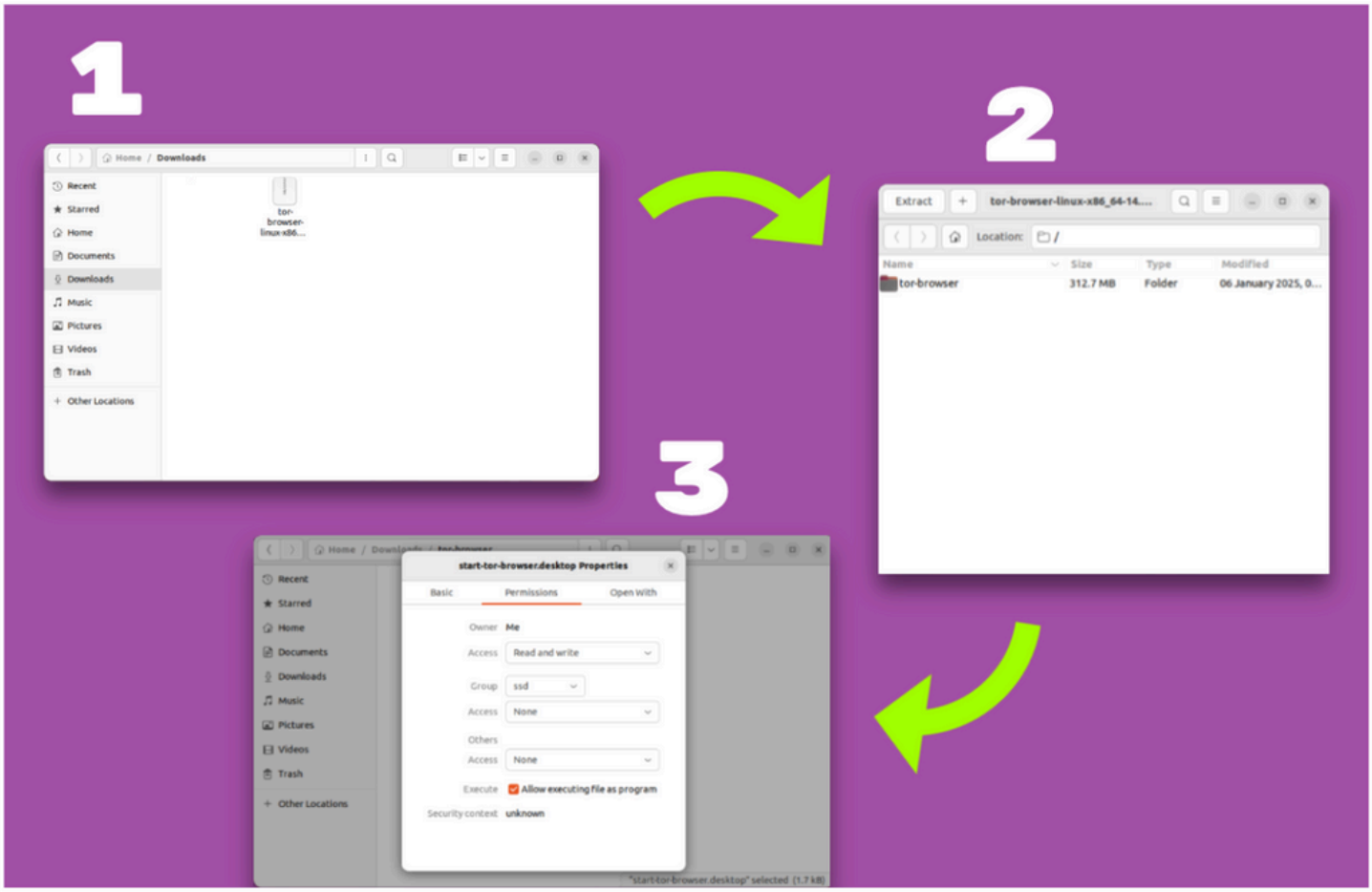
- Double-click the downloaded file—**in this case, "tor-browser-macos-14.0.4.dmg."** macOS will automatically verify the app to ensure it hasn't been modified. You may be prompted to approve the installation in **System Settings > Security & Privacy**, especially since this is a third-party app. Since the download came from the Tor Project's official, secure HTTPS site, click **"Allow."**
- A window will then appear prompting you to **drag the Tor Browser into your "Applications" folder**. Complete this step, and the Tor Browser will be successfully installed in your Applications folder.



Linux

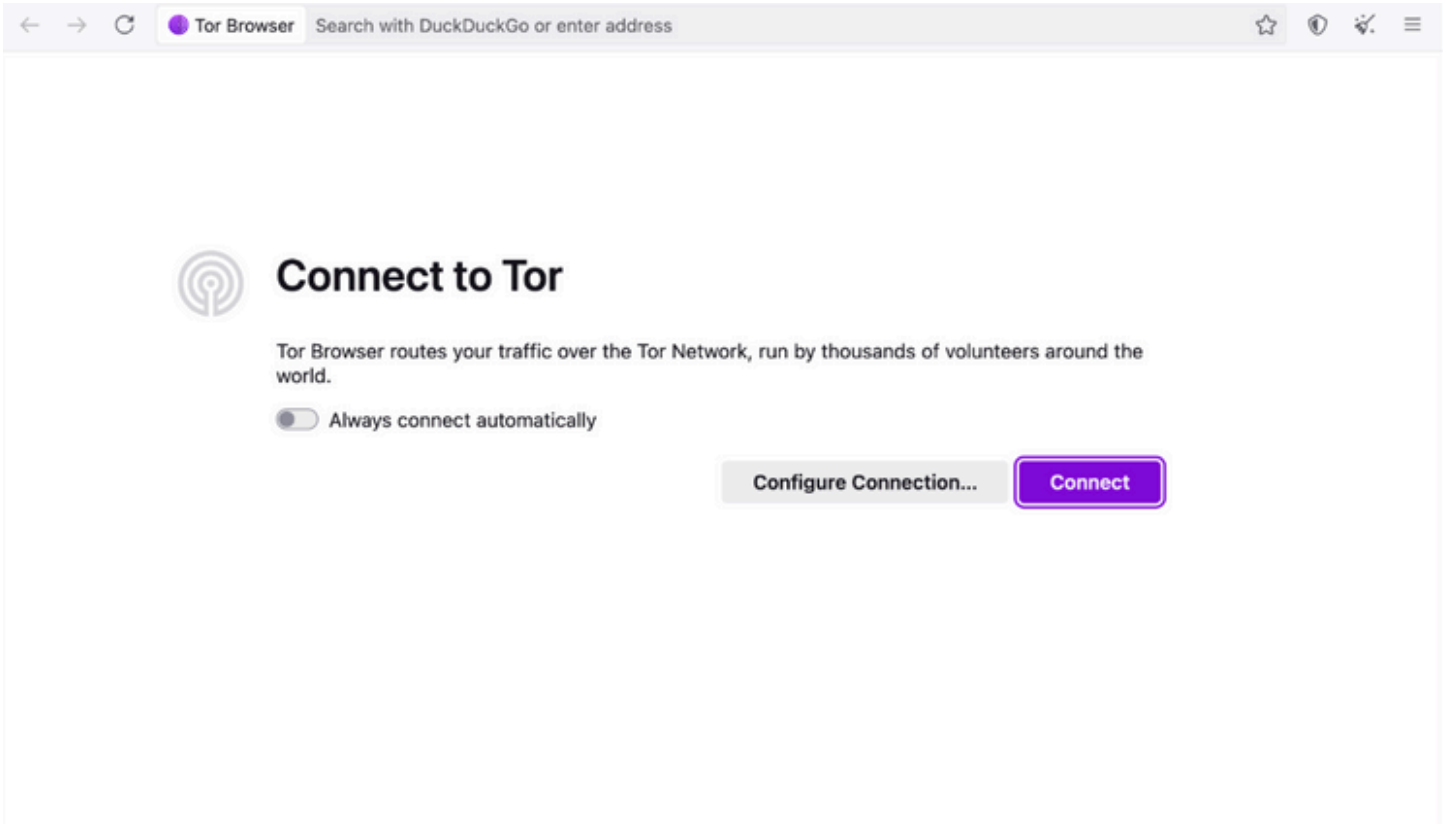
1. Double-click the downloaded file—**in our case, "tor-browser-linux-x86_64-14.0.4.tar.xz."**
   Click **"Extract"** and choose a destination folder for the extracted files.
2. Once extraction is complete, open the **"tor-browser"** directory.
   Right-click on the **"start-tor-browser.desktop"** file and select **"Properties."**
   Navigate to the **"Permissions"** tab and ensure that the **"Execute"** option is checked.
3. Finally, return to the file and double-click it. If prompted, confirm that you want to run the application.

If the file doesn't launch, you might need to perform extra setup steps—**check Tor's official installation guide** for detailed troubleshooting instructions.

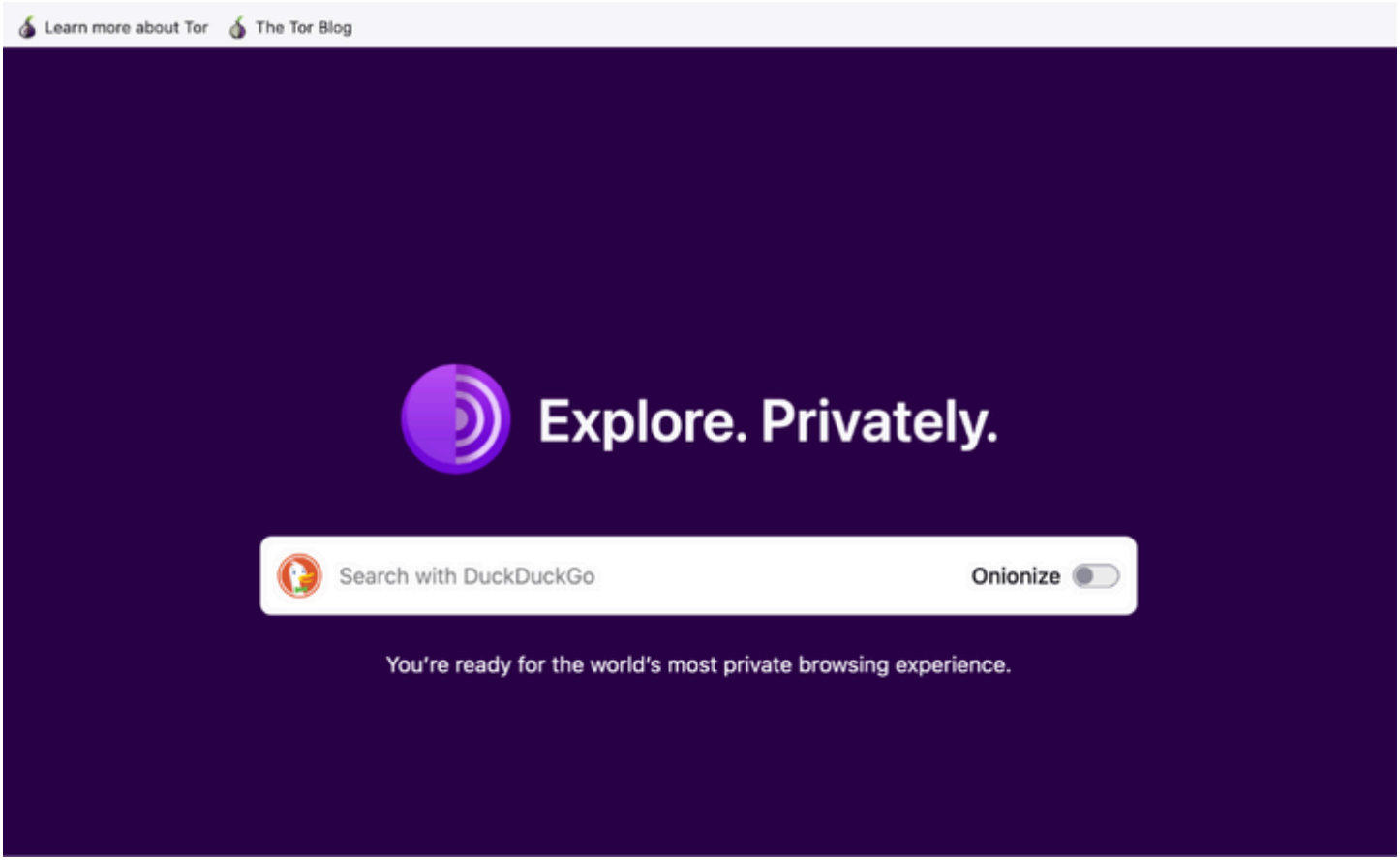


Using Tor Browser

When you launch Tor Browser for the first time, a setup window will appear allowing you to adjust certain settings. You can return to these later if needed. For now, simply click **“Connect”** to join the Tor network.

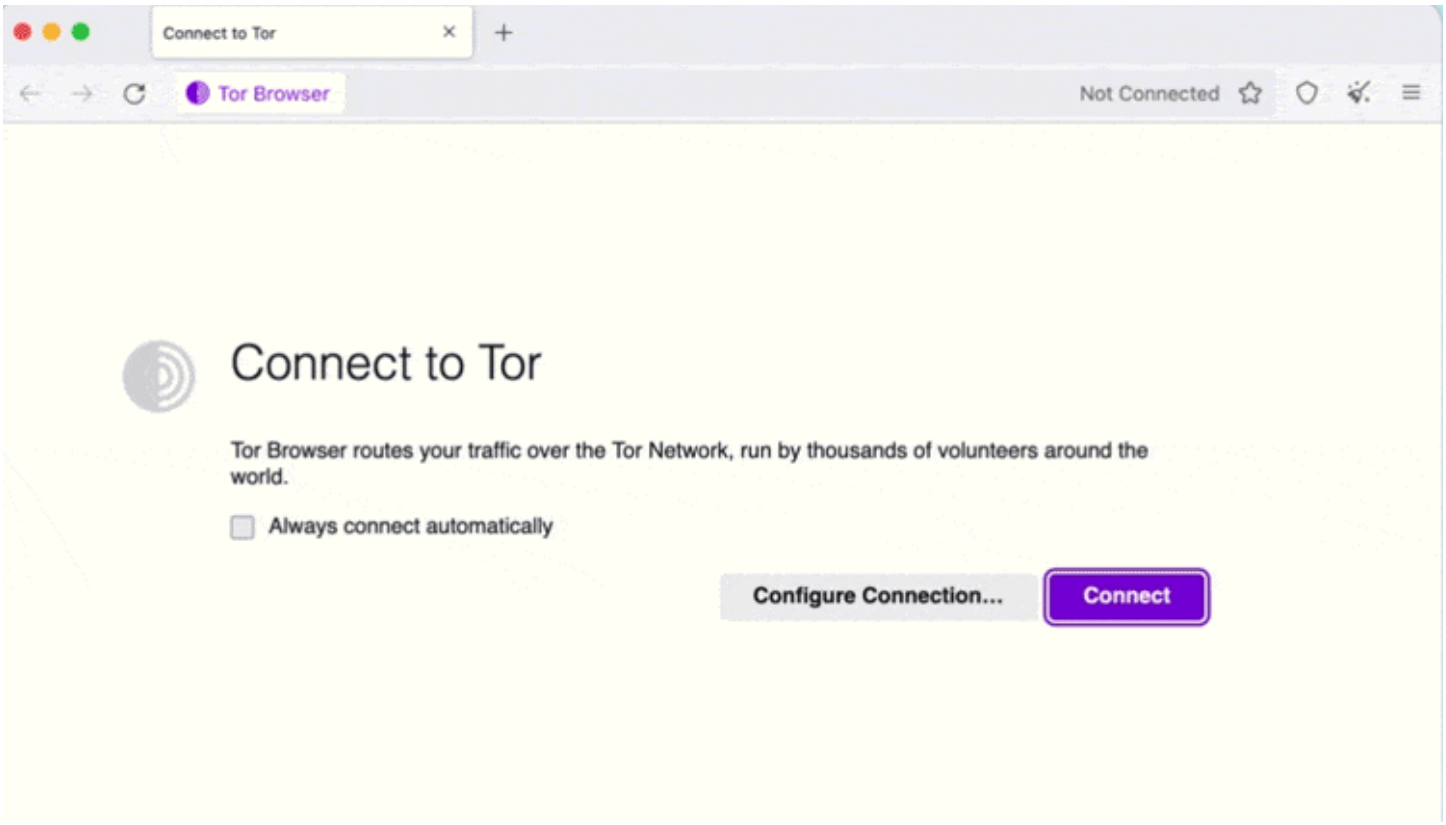


Once connected, you'll see a search bar with an option labeled **"Onionize."** Selecting this will direct your search through the **.onion version of DuckDuckGo**, offering greater privacy—though it may load more slowly than the standard version.



At this stage, you're ready to start browsing. However, if Tor is blocked in your area, the **Connection Assist** feature will automatically appear to help you select a suitable **bridge**

based on your location.



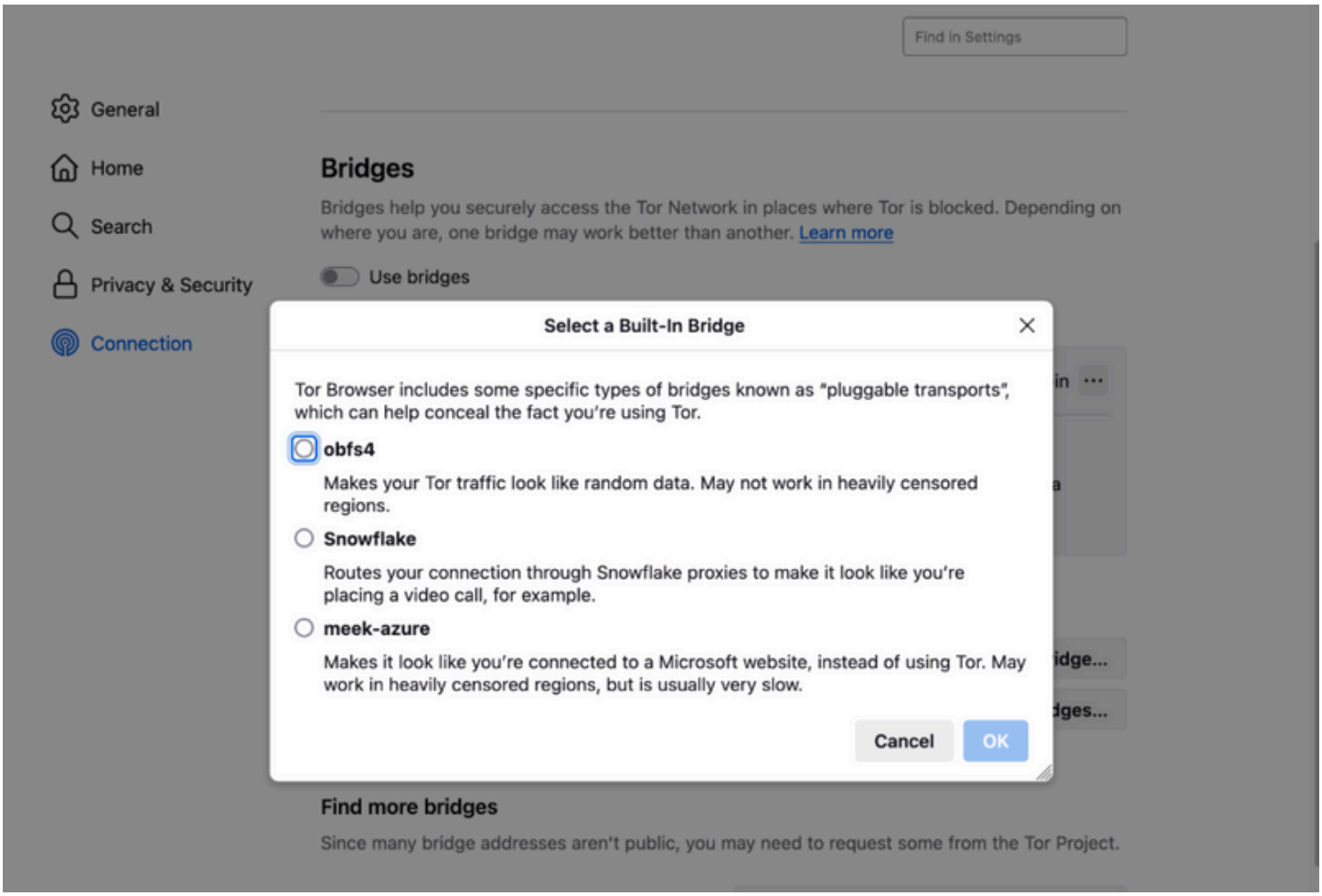
The **Connection Assistant** in Tor usually selects a compatible bridge automatically. However, if you're still unable to connect—especially in regions where Tor is blocked—you can manually set up a bridge:

1. Click the **three-line menu icon** in the top-right corner of the browser.
2. Go to **Settings** > **Connection**.
3. Scroll down to **"Select a built-in bridge..."** and click it.

You'll be presented with three bridge options:

- **Obfs4**: Obscures your traffic and can bypass some forms of censorship. Best used where Tor isn't heavily blocked.
- **Snowflake**: Disguises your traffic to resemble video or voice call data.
- **Meek-azure**: Routes your connection through Microsoft's infrastructure to make it appear like you're accessing a Microsoft site. It's very slow but may work when others fail.

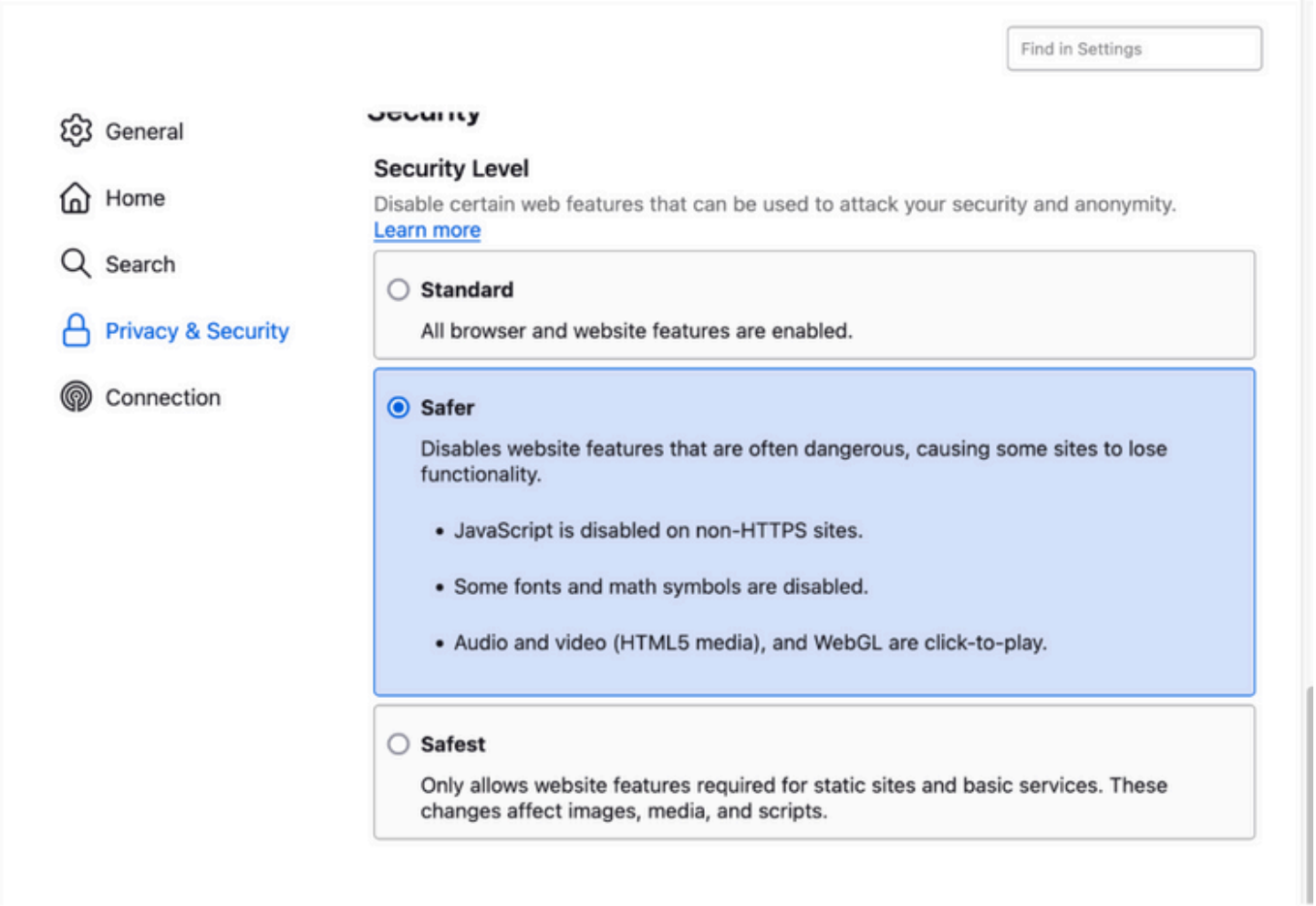
If none of the built-in bridges work, you can manually enter bridge addresses. Visit the **Tor Project's Bridges page** for instructions and up-to-date options.



Tor Browser's default **security level** helps protect against many privacy and security threats that affect typical browsers. It comes with **HTTPS-only mode** and **NoScript** enabled by default. If needed, you can further increase your protection.

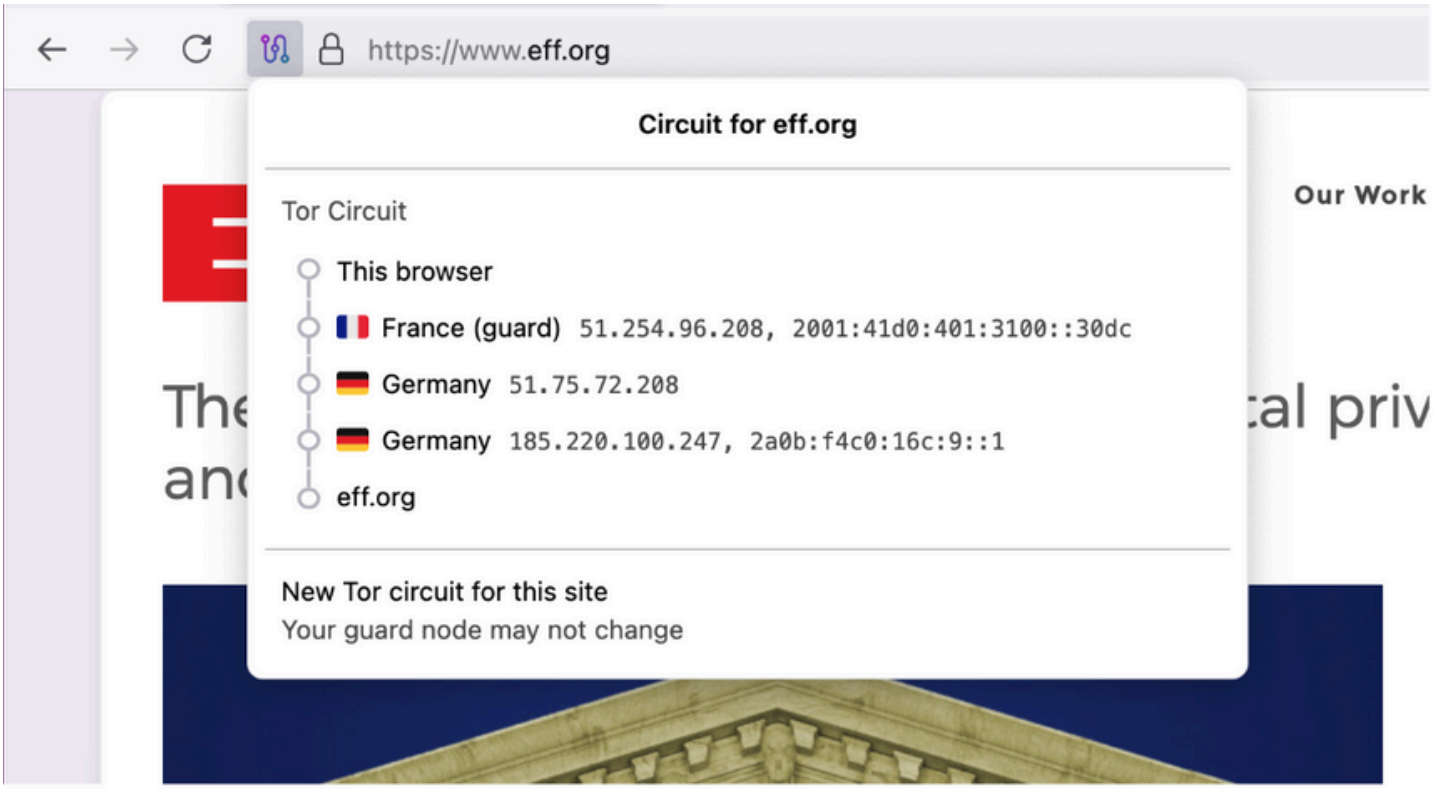
To do this, click the **shield icon** in the top-right corner, then select **"Settings"** to access the **Privacy & Security** menu. There, you can adjust the **"Security Level."** Setting it to **"Safest"** disables various web features that might be exploited by advanced attackers. While this offers stronger protection—especially against well-funded adversaries or unknown browser vulnerabilities—it may cause some websites to break or display improperly.

The default **"Standard"** level is suitable for general use, but choose **"Safest"** if you're facing higher risk or don't mind reduced website functionality.



Tor anonymizes your browsing by routing your traffic through a series of randomly selected **nodes**, creating what's known as a **circuit**. You can view the current nodes you're connected through by clicking the **"circuit" icon** located next to the lock symbol in the URL bar and even request a new circuit if needed.

While it's technically possible for **exit nodes** to be monitored, this doesn't expose your actual traffic or identity. The greater concern lies with the operators of those exit nodes, not with users.



Lastly, browsing with Tor differs in several ways from typical web browsing. To maintain your anonymity effectively, I highly recommend reviewing these **best practices for using Tor Browser**.

Published By - Deeptansh Nagar

Team : 2 - Deeptansh Nagar & Keshav GoyaL

Team 2, Week 3, How to Guide