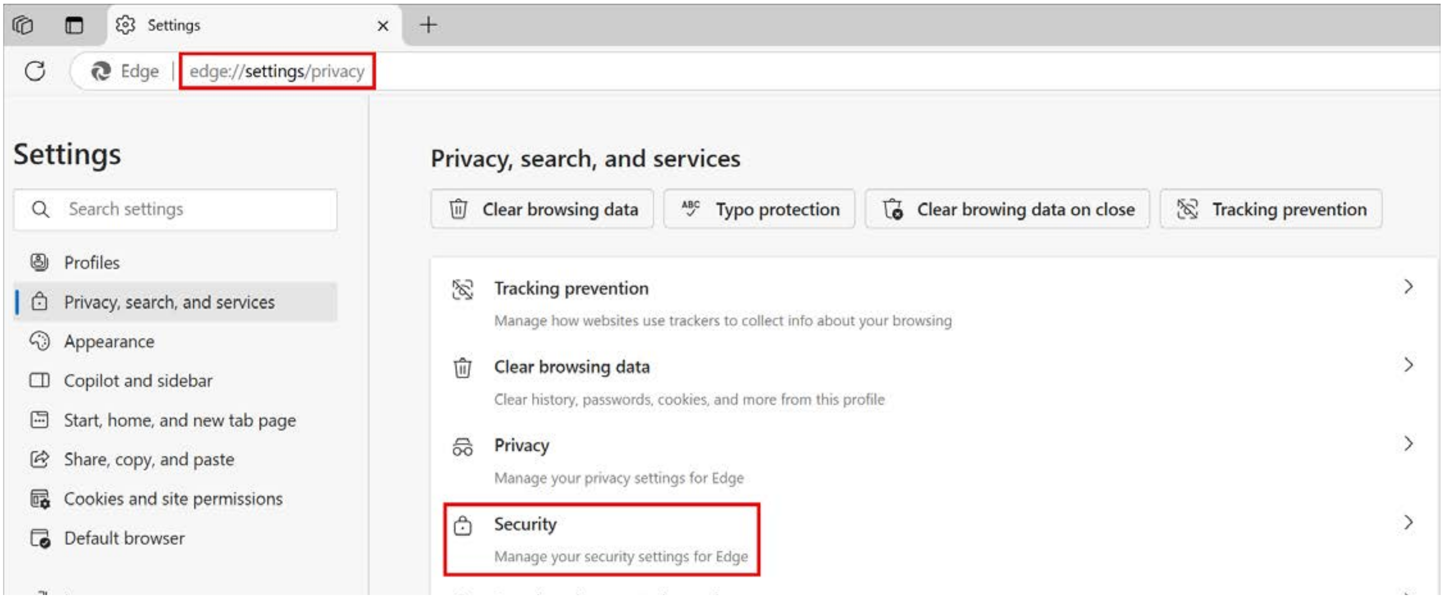
How To Disable DNS-over-HTTPS (DoH) in Major Browsers

This guide explains how to disable DNS-over-HTTPS (DoH) in Microsoft Edge, Safari, Firefox, and Chrome. Disabling DoH ensures your computer uses your network's default DNS servers, which may be necessary for local filtering or troubleshooting.

Microsoft Edge

1. Open Microsoft Edge.

2. In the address bar, type: edge://settings/privacy



Privacy, search, and services

Tracking prevention
Manage how websites use trackers to collect info about your browsing

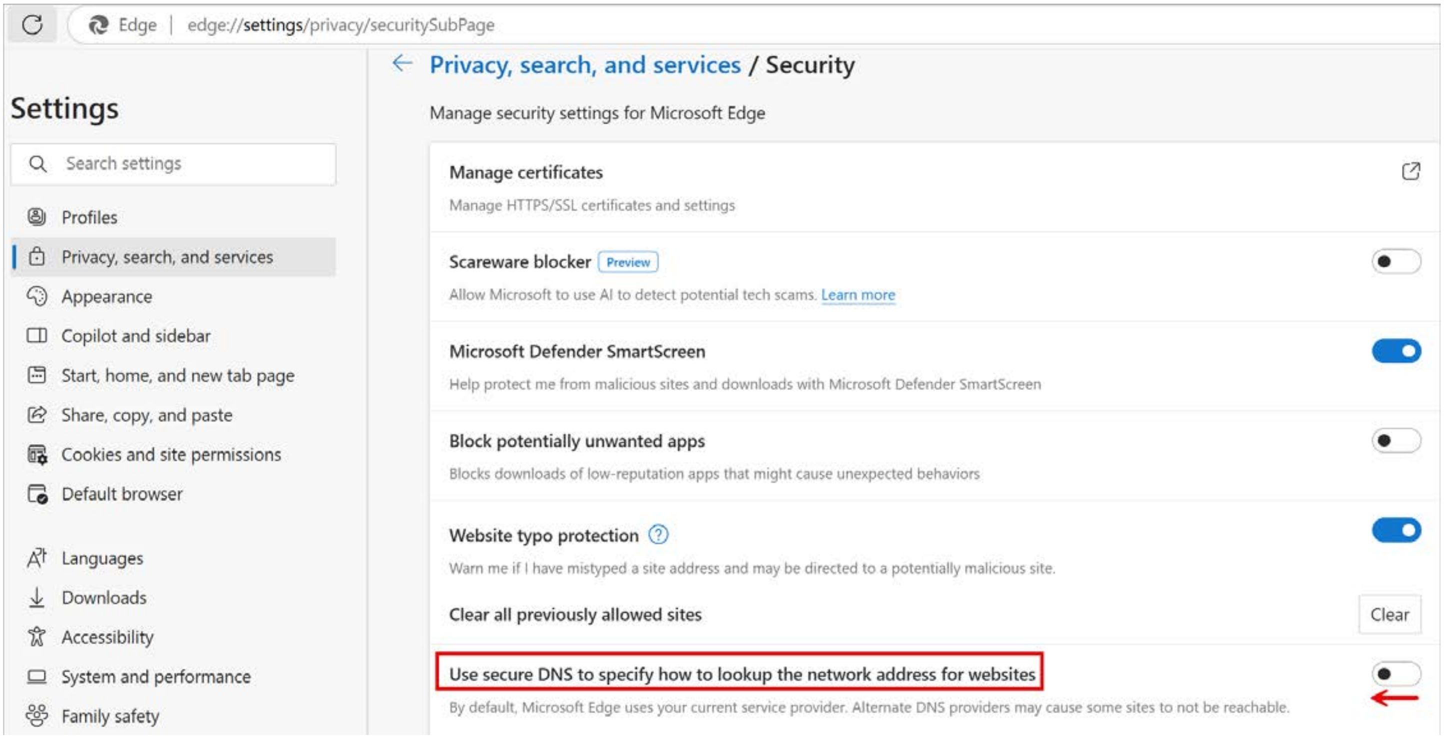
Clear browsing data
Clear history, passwords, cookies, and more from this profile

Privacy
Manage your privacy settings for Edge

Security
Manage your security settings for Edge

3. Scroll to the Security section.

4. Find 'Use secure DNS to specify how to lookup the network address for websites'.



Privacy, search, and services / Security

Manage security settings for Microsoft Edge

Manage certificates
Manage HTTPS/SSL certificates and settings

Scareware blocker ○
Allow Microsoft to use AI to detect potential tech scams.

Microsoft Defender SmartScreen ●
Help protect me from malicious sites and downloads with Microsoft Defender SmartScreen

Block potentially unwanted apps ○
Blocks downloads of low-reputation apps that might cause unexpected behaviors

Website typo protection ●
Warn me if I have mistyped a site address and may be directed to a potentially malicious site.

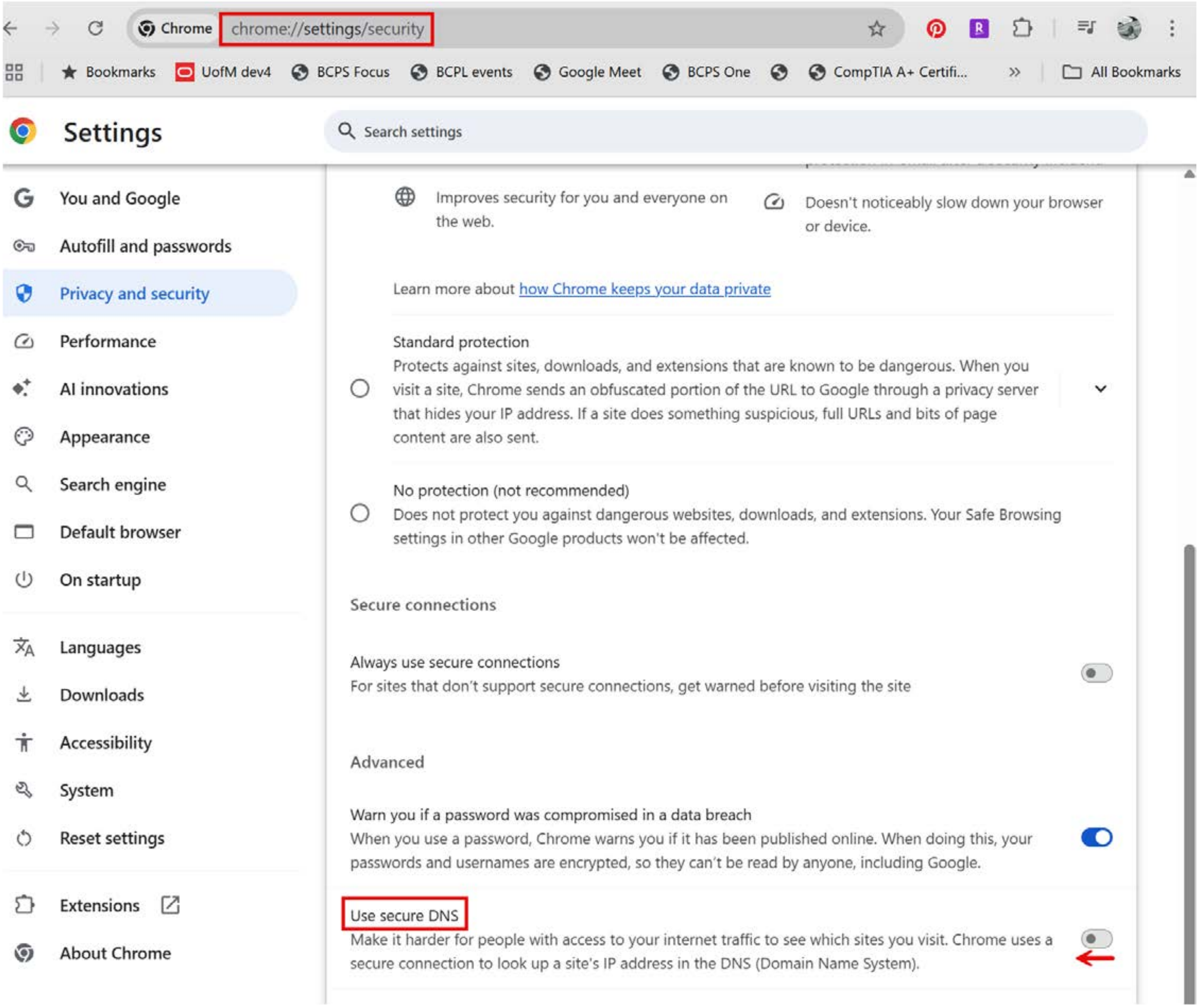
Clear all previously allowed sites

Use secure DNS to specify how to lookup the network address for websites ○
By default, Microsoft Edge uses your current service provider. Alternate DNS providers may cause some sites to not be reachable.

5. Turn the switch Off.

Google Chrome

1. **Open Chrome.**
2. **In the address bar, type: chrome://settings/security**



Improves security for you and everyone on the web.

Doesn't noticeably slow down your browser or device.

Learn more about how Chrome keeps your data private

○ Standard protection
Protects against sites, downloads, and extensions that are known to be dangerous. When you visit a site, Chrome sends an obfuscated portion of the URL to Google through a privacy server that hides your IP address. If a site does something suspicious, full URLs and bits of page content are also sent.

○ No protection (not recommended)
Does not protect you against dangerous websites, downloads, and extensions. Your Safe Browsing settings in other Google products won't be affected.

Secure connections

Always use secure connections
For sites that don't support secure connections, get warned before visiting the site

Advanced

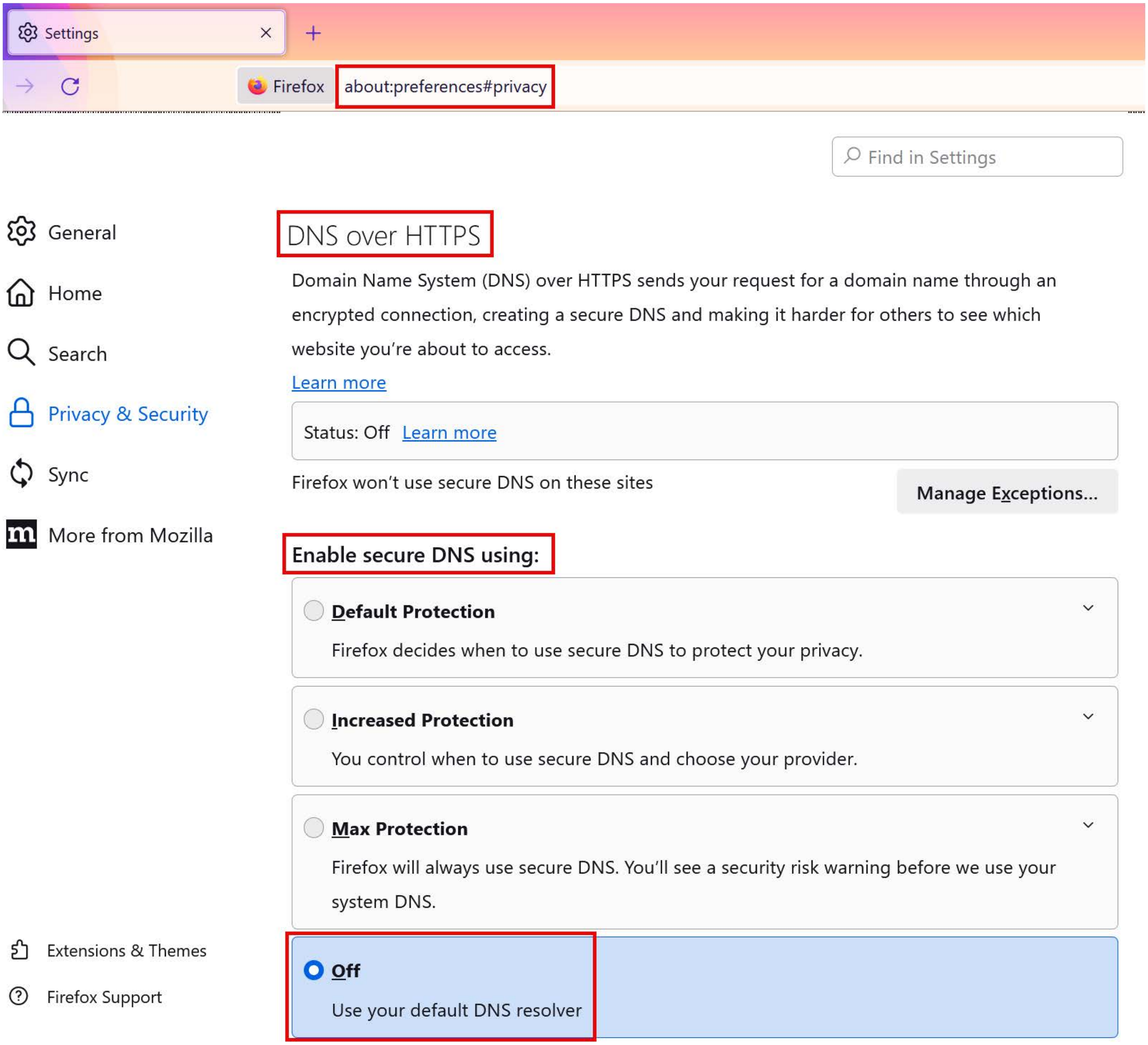
Warn you if a password was compromised in a data breach
When you use a password, Chrome warns you if it has been published online. When doing this, your passwords and usernames are encrypted, so they can't be read by anyone, including Google.

Use secure DNS
Make it harder for people with access to your internet traffic to see which sites you visit. Chrome uses a secure connection to look up a site's IP address in the DNS (Domain Name System).

3. **Scroll to the section labeled 'Use secure DNS'.**
4. **Turn the switch/select Off.**

Mozilla Firefox

1. Open Firefox.
2. In the address bar, type: about:preferences#privacy



Settings

Firefox about:preferences#privacy

Find in Settings

- General
- Home
- Search
- Privacy & Security
- Sync
- More from Mozilla
- Extensions & Themes
- Firefox Support

DNS over HTTPS

Domain Name System (DNS) over HTTPS sends your request for a domain name through an encrypted connection, creating a secure DNS and making it harder for others to see which website you're about to access.

Learn more

Status: Off Learn more

Firefox won't use secure DNS on these sites — Manage Exceptions...

Enable secure DNS using:

○ **Default Protection**
Firefox decides when to use secure DNS to protect your privacy.

○ **Increased Protection**
You control when to use secure DNS and choose your provider.

○ **Max Protection**
Firefox will always use secure DNS. You'll see a security risk warning before we use your system DNS.

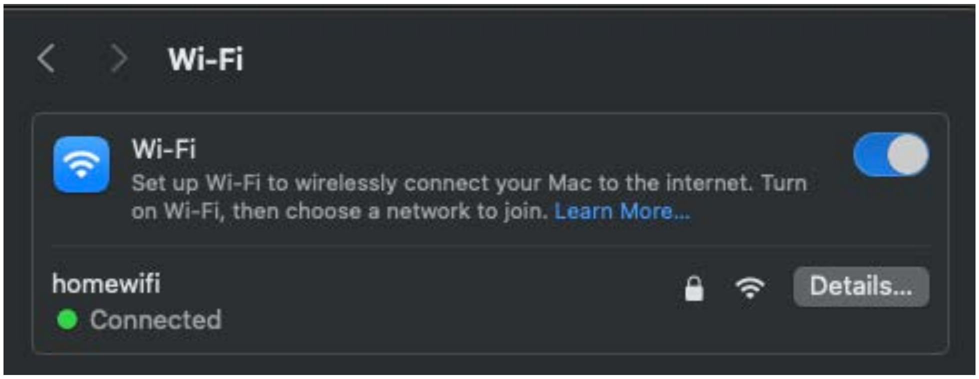
● **Off**
Use your default DNS resolver

3. Scroll down to the 'DNS over HTTPS' section.
4. Under 'Enable secure DNS using:', select 'Off'.

Safari (on macOS)

Safari uses your Mac’s system DNS settings.

1. Click the Apple menu -> System Settings.
2. Go to Network and choose your connection (e.g., Wi-Fi).

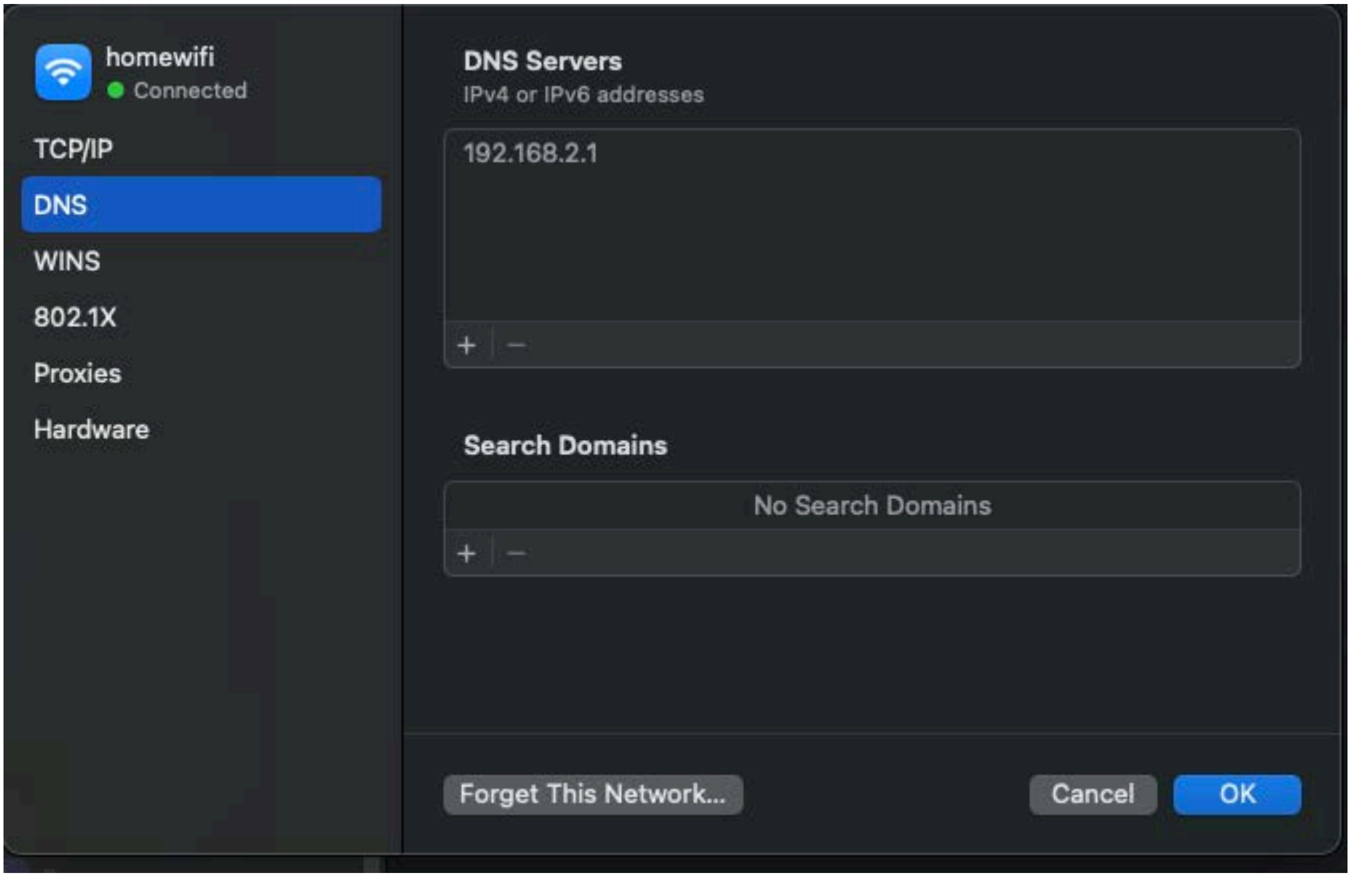


Wi-Fi

Wi-Fi
Set up Wi-Fi to wirelessly connect your Mac to the internet. Turn on Wi-Fi, then choose a network to join. Learn More...

homewifi
Connected

3. Click Details -> go to the DNS section.



homewifi
Connected

DNS Servers
IPv4 or IPv6 addresses

192.168.2.1

Search Domains

No Search Domains

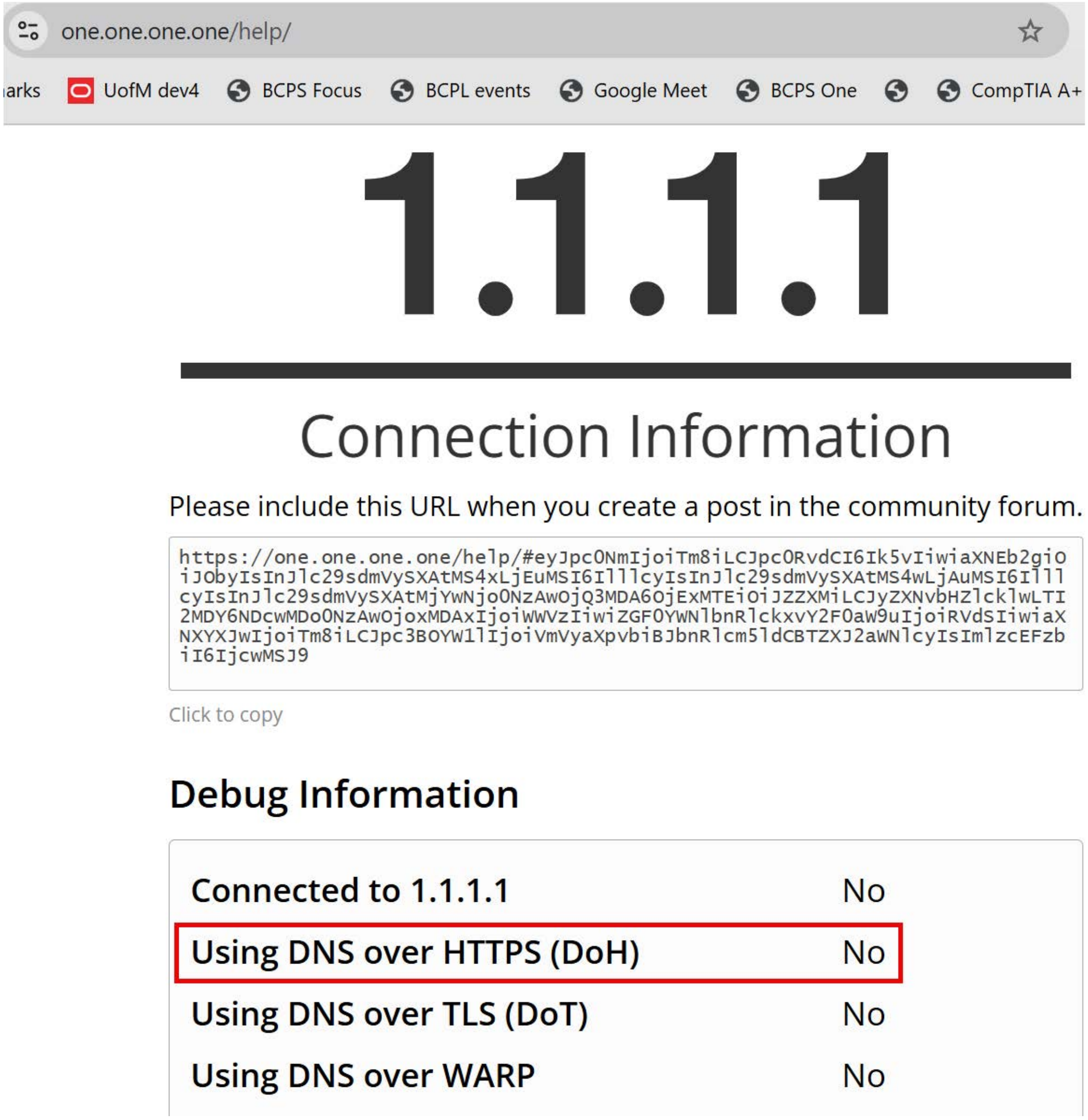
4. If you see DNS servers like 'dns.google' or 'cloudflare-dns.com', remove them.

How to Check if It Worked

1. Open your browser.

2. Visit: https://1.1.1.1/help

3. Look for the line: 'Using DNS over HTTPS (DoH): No' - If it says No, you're all set!



Connection Information

Please include this URL when you create a post in the community forum.

```
https://one.one.one.one/help/#eyJpc0NmIjoiTm8iLCJpc0RvdCI6Ik5vIiwiaXNEb2giO
iJObyIsInJlc29sdmVySXAtMS4xLjEuMSI6Ill1cyIsInJlc29sdmVySXAtMS4wLjAuMSI6Ill1
cyIsInJlc29sdmVySXAtMjYwNjo0NzAwOjQ3MDA6OjExMTEiOiJZZXMiLCJyZXNvbHZlcklwLTI
2MDY6NDcwMDo0NzAwOjoxMDAxIjoiWWVzIiwiZGF0YWNlbnRlckxvY2F0aW9uIjoiRVdSIiwiaX
NXYXJwIjoiTm8iLCJpc3BOYW1lIjoiVmVyaXpvbiBJbnRlcm5ldCBTZXJ2aWNlcyIsImlzcEFzb
iI6IjcwMSJ9
```

Click to copy

Debug Information

Connected to 1.1.1.1	No
Using DNS over HTTPS (DoH)	No
Using DNS over TLS (DoT)	No
Using DNS over WARP	No