Why ISPs Hope You Don't Know Why DNS Encryption Protocols Are Different

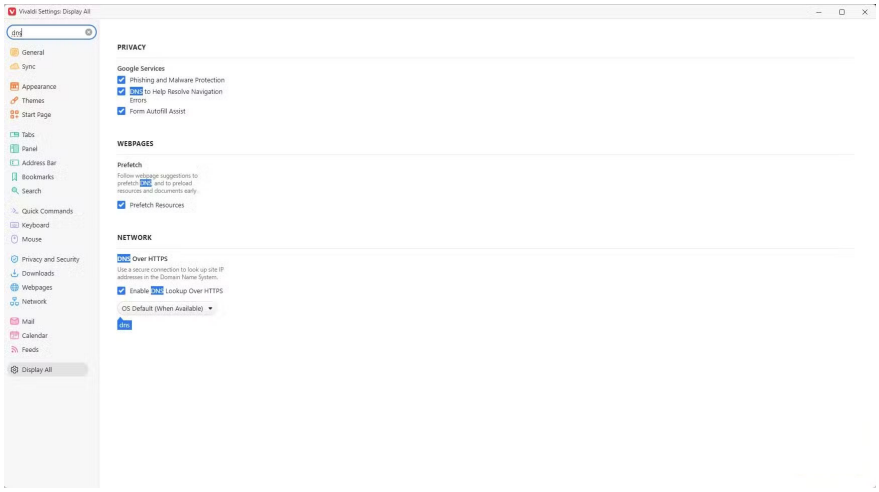
The good news is that you can encrypt those DNS requests to prevent prying eyes from seeing the websites and services you're using.

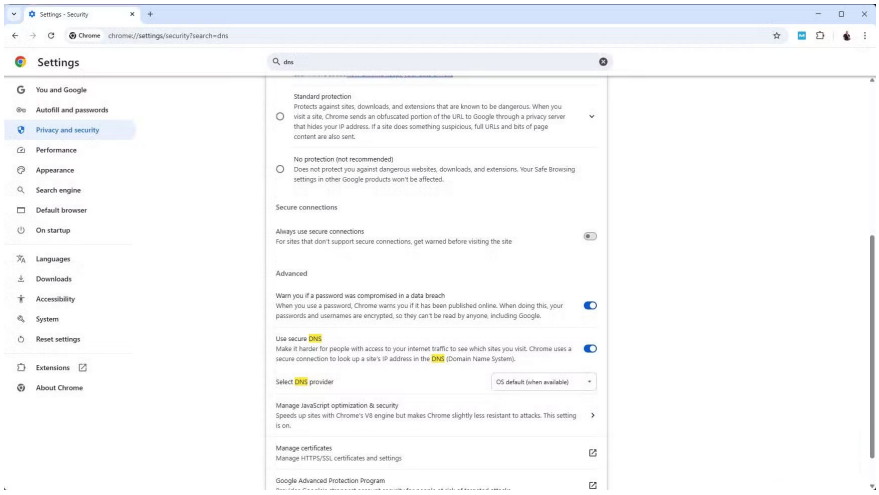
While we use easy-to-remember web addresses, the Internet actually runs on a system of IP addresses and remote servers. Behind the scenes, it relies on the Domain Name System (DNS), which translates those domain names into IP addresses—a format your device can understand.

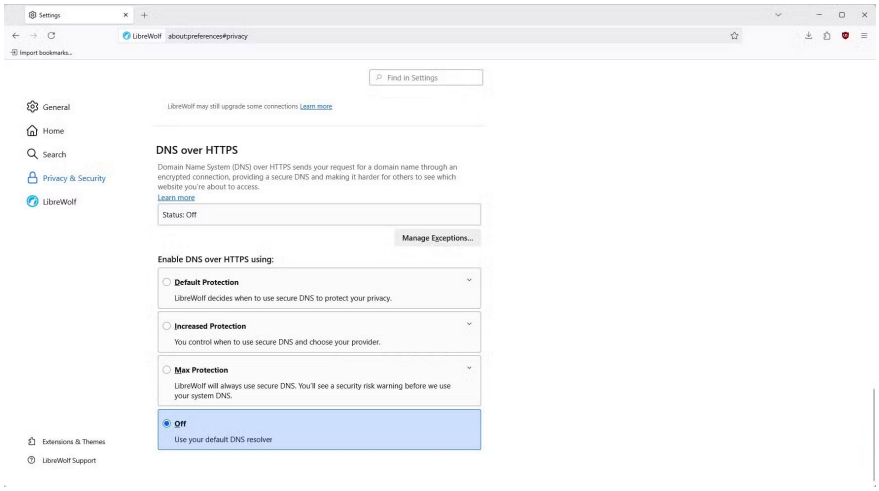
The good news is that you can encrypt those DNS requests to prevent prying eyes from seeing the sites and services you use. The bad news is that it's not as simple as flipping a switch and protecting all your DNS requests. While some methods protect you from your ISP, others still expose metadata and usage patterns that make it easy to find out who you are and where you are. This is why it's important to understand the differences between DNS encryption methods! If you think encryption equals privacy, your data will end up in the wrong hands.

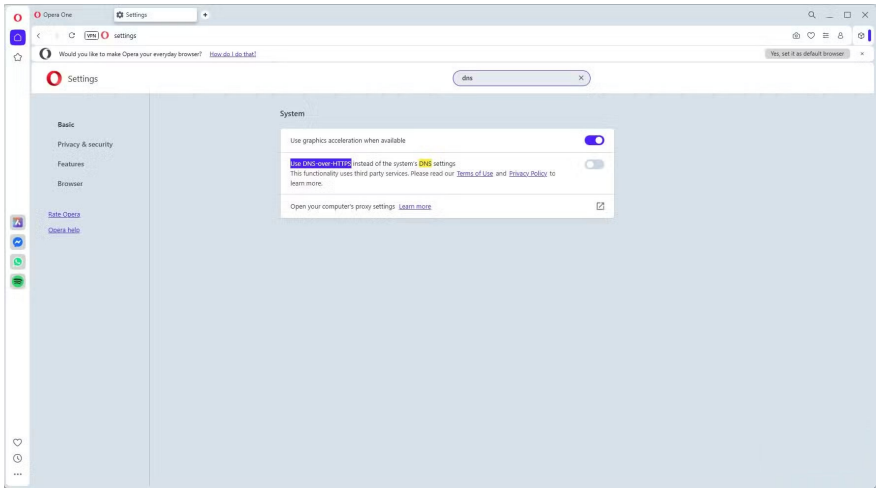
Internet Service Providers (ISPs) and the DNS Protocol

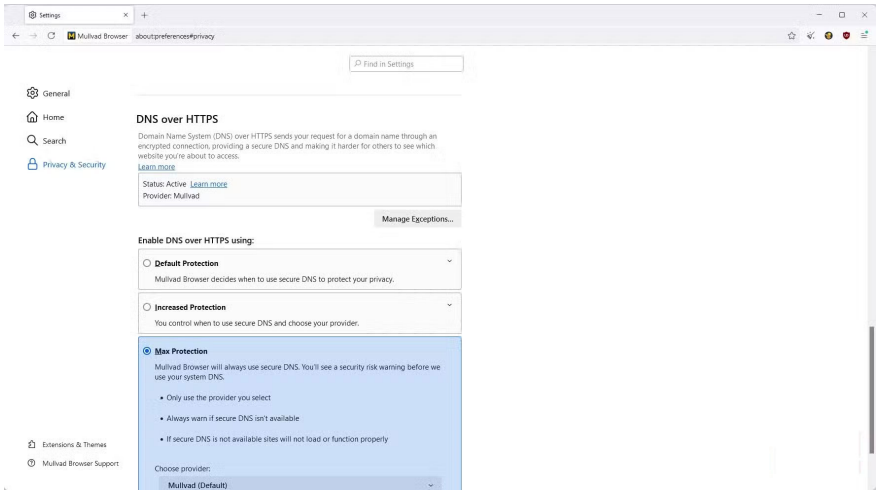
ISPs care about the DNS protocol you use




Settings - Security
Chrome
chrome://settings/security?search=dns
Settings
dns
You and Google
Autofill and passwords
Privacy and security
Performance
Appearance
Search engine
Default browser
On startup
Languages
Downloads
Accessibility
System
Reset settings
Extensions
About Chrome
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).
Select DNS provider
OS default (when available)
Manage JavaScript optimization & security
Speeds up sites with Chrome's V8 engine but makes Chrome slightly less resistant to attacks. This setting is on.
Manage certificates
Manage HTTPS/SSL certificates and settings
Google Advanced Protection Program


Settings
LibreWolf
about:preferences#privacy
Import bookmarks...
Find in Settings
General
Home
Search
Privacy & Security
LibreWolf
Extensions & Themes
LibreWolf Support
LibreWolf may still upgrade some connections Learn more
DNS over HTTPS
Domain Name System (DNS) over HTTPS sends your request for a domain name through an encrypted connection, providing a secure DNS and making it harder for others to see which website you're about to access.
Learn more
Status: Off
Manage Exceptions...
Enable DNS over HTTPS using:
Default Protection
LibreWolf 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
LibreWolf will always use secure DNS. You'll see a security risk warning before we use your system DNS.
Off
Use your default DNS resolver


Opera One
Settings
settings
Would you like to make Opera your everyday browser?
How do I do that?
Yes, set it as default browser
Settings
dns
Basic
Privacy & security
Features
Browser
Rate Opera
Opera help
System
Use graphics acceleration when available
Use DNS-over-HTTPS instead of the system's DNS settings
This functionality uses third party services. Please read our Terms of Use and Privacy Policy to learn more.
Open your computer's proxy settings
Learn more

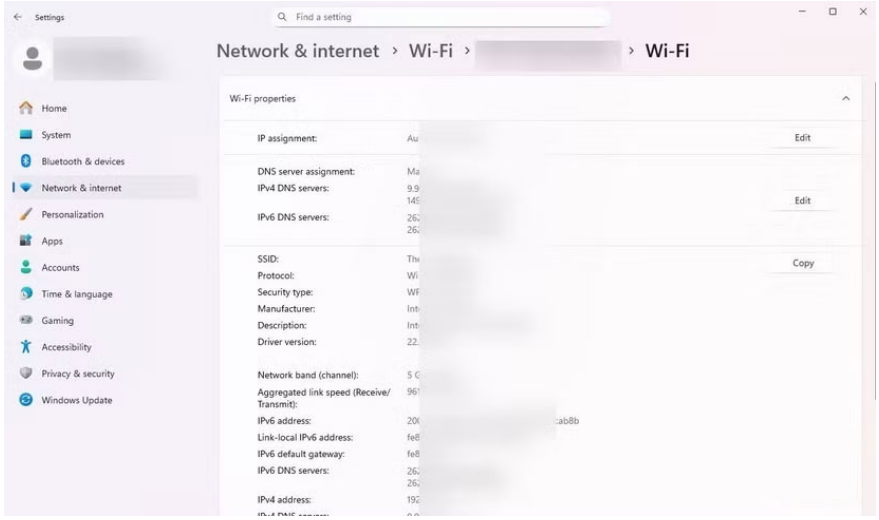


DNS traffic is the easiest way for your ISP to identify the website you visit. When you type a domain name into your browser, even if you are protected by HTTPS , the next DNS request can show you the website you are trying to access. It may not show the specific pages on the site you are visiting, but it will generally show you the domain you are visiting. ISPs can use this visibility for network management purposes. It can also be a source of revenue; the Federal Trade Commission has reported that ISPs inject ads and make money from DNS query data.

It would be harder for ISPs to continue this business model if your DNS queries were encrypted. You can use protocols like DNS over HTTPS (DoH) and DNS over TLS (DoT) to make it difficult for ISPs and anyone not on the network to see the domain names you look up. This completely eliminates the traditional revenue stream for ISPs, while also providing you with privacy benefits, although it does shift trust to a third party to resolve DoH/DoT (e.g., Cloudflare, Google).

Main protocols

DoH, DoT vs ODoH



DNS encryption isn't always a unified standard. This means that each DNS encryption protocol can take slightly different approaches to solving the problem. DNS over HTTPS (DoH) and DNS over TLS (DoT) are popular and widely deployed encryption protocols. Both protocols aim to encrypt DNS queries so that they can't be read in plain text, but their design and implementation results in each protocol providing a different user experience.

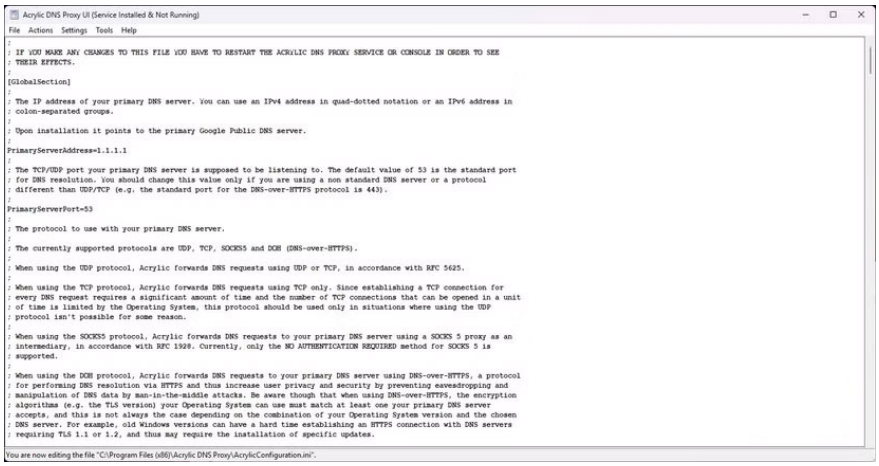
DoH blends seamlessly into all your traffic because it runs over HTTPS. Popular browsers like Google Chrome and Mozilla Firefox can easily enable it directly, and networks can't easily block this traffic without disrupting everything. DoT is quite different. It's usually implemented at the system or router level and runs on a dedicated port (853) using TCP with TLS encryption. It's more of a network-level service, but it can be more easily blocked by a firewall or ISP if needed.

Note : DNSCrypt is another lesser-known option that provides strong authentication and encryption, predating DoH and DoT. It is not standardized by the IETF but is actively maintained through proxy implementations that can support newer protocols like ODoH.

All of these protocols offer some form of protection, but choosing one or the other ultimately means choosing between ease of deployment, where you can trust, and censorship resistance.

The intermediary problem

Encryption can still expose you



Encrypted DNS doesn't make you completely invisible online. Different protocols can make it difficult for anyone outside the network to read your queries, but the resolver can still see the domain name you visited and your IP address. So you're trading off visibility from your ISP for visibility on a large public resolver.

Your traffic patterns can also leak metadata. Even if the data content is encrypted, factors like timing, frequency, and packet size can still be analyzed to infer browsing habits. In some cases, this traffic can be used to suggest domains you visit without decrypting the requests.

Additionally, the limited number of providers raises the issue of centralization, especially since the majority of encrypted DNS traffic is routed through these limited options. While these companies build strong protections, a single subpoena, data breach, or regulatory policy could expose user activity.