

Onion routing, **step by step**

1 Pick three relays
Your Tor software chooses an entry, a middle and an exit relay run by volunteers.

2 Wrap in three layers
Your request is encrypted once for each relay, like the layers of an onion.

3 Each relay peels one layer
It learns only the relay before it and the relay after it.

4 The exit reaches the site
The reply returns the same way. HTTPS keeps the exit from reading it.

ONION SERVICES

The site hides too.

- Addresses end in .onion
- You and the service meet at a rendezvous relay
- Six relays in all, and no exit relay
- Traffic is encrypted end to end
- Neither side learns the other's address

Tor, I2P and VPNs

	VPN	TOR	I2P
How it works	One company relays your traffic	Three volunteer relays, three layers	Every user's router relays; one-way tunnels
Who you trust	The VPN company, completely	No single relay sees both ends	No central directory; tunnels are one-way
Good for	Public Wi-Fi and hiding sites from your network	Anonymous browsing and onion services	Services inside I2P, called eepsites, and peer-to-peer apps
Watch out	Pay for one you researched. Free ones must earn money somehow	Slower. Use HTTPS. Do not log in as yourself	More setup, and mostly an inside network

No tool makes you anonymous by itself. We do not recommend any VPN provider. Learn how to judge one.

Why it matters, and where to look

Private by right

Freedom of opinion and expression includes the freedom to seek and share information. Anonymity and encryption help people exercise it: reporters, sources, activists, researchers, survivors and anyone under surveillance.

Real-world onion sites

Mainstream sites that also offer onion services, such as:

- BBC News
- Deutsche Welle
- ProPublica
- The Guardian
- DuckDuckGo
- Proton Mail
- Debian
- SecureDrop tip lines

Find current addresses in the real-world-onion-sites list on GitHub. Check them against each site's own page.

PrivacySafe

- PrivacySafe Search, privacysafe.is, has a .onion address
- PrivacySafe Bot, privacysafe.bot, has a .onion address
- PrivacySafe.app Chat, Inbox, Storage and Contacts are end-to-end encrypted, and work over Tor and I2P

Search and Bot are run by the Foundation.

Your safe-browsing plan

- ☐ Get Tor Browser from the official Tor Project site
- ☐ Keep it updated, and leave its settings alone
- ☐ Prefer HTTPS and onion addresses from a site's own page
- ☐ Do not log in as yourself if you need to stay anonymous
- ☐ If you use a VPN, pay for one you have researched
- ☐ Never download or share material that may not be legal. Leave and report it
- ☐ Know the laws and rules where you live and work
- ☐ Use end-to-end encrypted apps for what must stay private

DISCUSSION

Who needs anonymity most, and what would they lose without it?

How should a society handle the harms that private networks can also enable?