GRIDINSOFT
HELP CENTER

OFFICIAL SUPPORT GUIDE

T

Tor and Tor Browser: How They Work, Limits, and Safe Use

Tor separates the source of a connection from its destination. Tor Browser adds privacy defenses, but it does not make accounts, downloads, or HTTP safe.

PUBLISHER	UPDATED	READ TIME
Gridinsoft Support	Oct 8, 2026	3 min

Tor is an anonymity network that routes traffic through a distributed set of volunteer-operated relays. **Tor Browser** is the hardened browser most people use to send web traffic through that network. The Tor Project explains that websites see a connection from Tor rather than the user's real IP address, while a local network observer cannot directly see which websites are visited.

Tor is a privacy tool, not a guarantee of invisibility or device security. Its protection depends on using the correct software and understanding which traffic and identifying actions remain outside its scope.

How a Tor circuit works

1. **Entry or guard relay:** sees the user's IP address but not the final destination.

2. **Middle relay:** passes encrypted Tor traffic without knowing both ends.
3. **Exit relay:** connects to an ordinary internet service. It sees the destination but not the original IP.

Encryption is layered so each relay learns only what it needs for its hop. Onion services use a different design in which both parties connect through Tor without an ordinary exit relay.

What Tor Browser helps protect

- it hides the source IP from destination websites;
- it reduces local observation of browsing destinations;
- it isolates site data and reduces common tracking and fingerprinting differences;
- it supports bridges and pluggable transports where direct Tor access is blocked.

Use the official Tor Browser documentation and download links. A third-party browser claiming to include Tor may not provide Tor Browser's privacy protections.

What Tor does not protect

- **Identity you disclose:** logging into a personal account, entering a phone number, or reusing a distinctive username can identify you.
- **Non-Tor applications:** Tor Browser does not automatically route another browser, torrent client, updater, or messaging app through Tor.
- **Unencrypted application data:** ordinary HTTP remains plaintext between the exit and destination. Prefer HTTPS.
- **Malware or hostile files:** Tor does not make downloads trustworthy. A document opened in another application may make direct network connections.
- **Powerful traffic correlation:** an observer able to monitor both ends for long enough may correlate timing and volume.

Safer Tor Browser practices

- keep Tor Browser and the operating system updated;
- do not install extra extensions or change privacy-related defaults casually;
- use HTTPS and verify onion addresses through a trusted source;
- do not use BitTorrent through Tor;
- avoid opening downloaded documents while online when anonymity matters;
- separate anonymous activity from accounts and details tied to your identity.

Tor vs. a VPN

A VPN sends traffic to one provider that can know the subscriber and destination. Tor distributes trust across a circuit and normally requires no account. A VPN may cover more applications, while Tor Browser provides browser-specific anti-fingerprinting measures. Combining them changes who can observe the connection but does not automatically make the setup safer; high-risk users should follow a threat model rather than generic “Tor plus VPN” advice.

Tor FAQ

Is Tor illegal?

Tor is general-purpose privacy technology. Laws and network policies differ by location, so users must follow applicable rules.

Is every onion site dangerous?

No. Onion services are a technical feature. Their content should be judged just as cautiously as content elsewhere.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com