Tor - what it is, how it protects privacy, and smart ways to use it safely

Gridinsoft Help Center

What it is

Tor (The Onion Router) is a free tool that hides where you're coming from online. When you use Tor Browser, your traffic is bounced through several volunteer-run relays before it reaches a website. Each hop only knows the next one, so sites can't easily tie your activity to your IP or location. It's privacy tech-not a magic cloak-and it doesn't make risky downloads or bad passwords safe.

Why it matters

Tor helps keep your browsing more private on public Wi-Fi, reduces tracking, and lets people reach sites that might be blocked in their country. Journalists, researchers, and everyday users rely on it to avoid profiling and snooping.

How it works

- Layers ("onion"): your request is wrapped in layers of encryption.
- Relays: traffic passes through entry -> middle -> exit relays.
- Exit: the last relay talks to the website; your real IP stays hidden.
- Tor Browser: adds anti-tracking and fingerprinting defenses by default.

Red flags

- Logging into personal accounts (school, bank, social) can reveal who you are despite Tor.
- Sites without HTTPS let exit relays see what you send.
- "Free Tor" apps that aren't Tor Browser (malware or fake services).
- Torrents and some plugins can leak your real IP.

Do it right

- Get Tor Browser from the official site and keep it updated.
- Prefer HTTPS; don't enter private details on HTTP pages.
- Avoid logging into accounts that tie back to your real identity.
- Don't install extra browser add-ons; they can fingerprint you.
- If Tor is blocked, use bridges (built-in option) to connect.