PRIVACY GUIDE

Tor

The principles, in plain language

What it is, how it hides who you are online and how far it goes.

01

What Tor is

Tor is a network that lets you use the internet without websites knowing who you are, and without anyone watching your connection knowing what you visit. It runs on thousands of computers donated by volunteers around the world, and it is free to use through a browser called Tor Browser.

NO COMPANY IN THE MIDDLE

There is no single intermediary that knows everything: the work is split across several.

RUN BY VOLUNTEERS

Anyone can contribute a computer so the network grows and becomes harder to block.

OPEN SOURCE

Anyone can read how it works, review it and propose improvements.

02

Five ideas first

If you already know how browsing the internet works, jump straight to section 4.

1. **The IP address.** It is like your postal address on the internet. Websites see it when you visit, and it usually reveals your city and your provider.
2. **Metadata.** This is the data about your activity: who you connect to and when. Even when the content is encrypted, metadata says a lot about you.
3. **The intermediary.** Whoever acts as a bridge between you and a website. If there is only one, it has to know everything about you.
4. **Encryption.** It turns a message into something unreadable for anyone without the key.
5. **Layers.** Encrypting several times in a row, like wrapping a gift in three sheets of paper. Each person removes one, and only one.

03

The problem: your address follows you everywhere

Every time you visit a website, that website receives your IP address. Your internet provider also sees which servers you connect to. With HTTPS encryption the content of what you do is protected, but not who you talk to. And advertising companies can link all your visits to build a profile of you.

> **One intermediary is not enough.** A VPN or a proxy hides your address from the website, but its owner does know it, and also knows what you visit. You have only changed whom you trust. Tor spreads that trust across several parties.

04

The three privacy principles

Tor protects your anonymity with three ideas that work at the same time.

THREE RELAYS

Three hops

A path through three different computers.

THREE WRAPPINGS

Layers of encryption

Each computer removes only its own layer.

NOBODY KNOWS EVERYTHING

Separate roles

Whoever sees your IP does not see your destination.

Three hops

Instead of going straight to the website, your traffic passes through three volunteer computers called relays: an entry relay, a middle relay and an exit relay. Each one only knows the one before and the one after. It is like a message handed through three couriers who have never met.

Layers of encryption

Before leaving your computer, the message is wrapped in three layers of encryption, one for each relay. The first removes its layer and passes the result to the second, which removes its own, and so on until the third. That is why it is called onion routing: the information sits inside several layers that are peeled off one by one.

Nobody knows everything

The entry relay sees your address but does not know which website you visit. The exit relay sees the website but does not know who you are. The middle relay knows neither. To find out who visits what, someone would have to control both the entry and the exit of the path at the same time.

> The three mechanisms work together: the path splits the knowledge, the layers prevent anyone from reading what passes through, and the separate roles stop anyone from putting it all together.

05

One visit, step by step

1. Your browser downloads a public, signed list of the available relays.
2. It picks three: an entry relay, a middle relay and an exit relay.
3. It agrees a secret key with each one, without anyone else being able to discover it.
4. It wraps your request in three layers of encryption, one per relay.
5. Each relay removes its layer and forwards the result. The exit relay delivers the request to the website.
6. The reply comes back along the same path, and each relay adds its layer. Your browser removes them all.

06

What keeps the network secure

A DIRECTORY BY CONSENSUS

A group of independent servers in different countries publishes the list of relays every hour. A majority has to agree.

BRIDGES FOR PEOPLE WHO ARE BLOCKED

These are relays that are not on the public list and that disguise themselves as normal traffic, so a censor cannot block them all.

Tor also lets you create sites and services whose location is hidden, with addresses ending in .onion. The visitor does not know where the server is, and the server does not know who visits it. Tor Browser also makes all its users look the same.

REFERENCE

Quick glossary

TERM	IN ONE SENTENCE
Relay	A volunteer computer that forwards traffic through the network
Guard	The entry relay, which sees your address and stays fixed for weeks
Exit relay	The last one, which sees the destination website
Circuit	The path of three relays your traffic follows
Onion service	A site with a hidden location, whose address ends in .onion
Bridge	A relay not listed publicly, for people who have Tor blocked

> **Next step.** The complete guide, "Tor in depth", explains each of these pieces in more detail, with their ciphers and formulas, chapter by chapter.

Sources: The Tor Project, Help Net Security and CyberInsider.