DNS Filtering: What it is, why it helps, and how to set it up safely

Gridinsoft Help Center

Why it matters

Most threats start with a click. Stopping connections at the DNS layer cuts off malware downloads, command-and-control beacons, and fake login pages -without slowing users or breaking trusted sites.

How it works

- Your device asks DNS for a site’s address.
- The resolver compares the domain to threat feeds and your rules.
- Allowed domains resolve normally; blocked domains return nothing or a safe page.
- Categories (malware, phishing, adult, piracy, crypto-mining) make policy easy.

Good uses

- Security: block malware/phishing and C2 call-outs by default.
- Compliance & productivity: restrict categories at work/school.
- Home safety: filter adult content and scam sites across all devices.

Limits to know

- Doesn’t see IP-only traffic or traffic sent through some VPNs.
- Users can try alternate DNS unless you enforce it on the network.
- False positives happen-keep an allowlist and review logs.

Quick setup

- Pick a reputable DNS filtering service with categories and custom lists.
- Force all DNS to your resolver at the router/firewall; block outbound 53/853 to others.
- Enable DoH/DoT to your chosen resolver to prevent tampering.
- Start in monitor mode for a week, review hits, then enforce.
- Maintain allow/deny lists; alert on malware/phishing blocks.