DNS Blocking: What it is, when to use it, and how to set it up safely

Gridinsoft Help Center

What it is

DNS blocking is a simple filter for where devices are allowed to go on the internet. When a user tries to visit a domain on the block list, the DNS resolver refuses or sends them nowhere - so risky or unwanted sites never load.

How it works

- Your device asks a DNS resolver for a site’s IP.

- The resolver checks policies/lists first.

- If the domain is blocked (malware, phishing, adult, gambling, etc.), the lookup is denied or redirected to a safe page.

Good uses

- Security: stop malware/phishing domains before connections happen.

- Productivity & policy: block gambling, pirated content, or shadow IT at work/school.

- Parenting: filter adult sites and risky downloads at home.

Limits & gotchas

- Not a silver bullet: won’t see encrypted IP-only traffic or block VPNs.

- Overblocking happens: legit sites can be mislabeled-allowlist when needed.

- Bypass risk: users can change DNS or use DoH/DoT unless you enforce it on the network.

Quick setup tips

- Choose a reputable DNS filter (supports categories, malware feeds, custom lists).

- Enforce at the router/firewall: force all DNS to your resolver; block outbound 53/853 to others.

- Turn on DoT/DoH to your chosen resolver to prevent tampering.

- Start in monitor mode for a week, review hits, then tighten.

- Maintain allow/deny lists and review alerts for false positives.