DNS-based Blackhole List (DNSBL/RBL): What it is, how it helps, and how to use it safely

Gridinsoft Help Center

What it is

A DNS-based Blackhole List is a reputation list you can query via DNS to spot known bad senders - IP addresses or domains tied to spam, malware, or abuse. Mail and security gateways check these lists in real time to block or flag risky traffic before it lands.

How it works

- Your server receives a connection or message.
- It queries one or more DNSBLs with the sender’s IP/domain.
- If there’s a match, the server can reject, quarantine, or tag the message as spam.
- Multiple lists (spam sources, open relays, botnets, phishing domains) improve accuracy.

Good uses

- Email defense: cut spam volume and malware payloads at the edge.
- Abuse control: throttle or block connections from botnet or VPN/proxy ranges as policy allows.
- Triage: add "listed on X" headers so downstream filters score messages correctly.

Limits to know

- False positives happen: dynamic IPs or shared hosts can get listed. Maintain an allowlist for trusted senders.
- Coverage varies: no single list sees everything - use a combination.
- Aging/appeals: listings may lag behind reality; senders need a clear delisting path.

Safe setup

- Use reputable, maintained DNSBLs; read their policies and SLAs.
- Score results (don’t auto-block) while you tune; then enforce with confidence.
- Combine DNSBL checks with DKIM/DMARC/SPF, content scanning, and URL filtering.
- Log decisions and monitor hit rates; adjust allow/deny rules as sender behavior changes.
- For outbound mail, watch your own IP/domain reputation to avoid self-listing.