D

DNSBL and RBL: How Email Blocklists Work and How to Get Delisted

A DNSBL publishes reputation data through DNS, commonly for mail-sending IP addresses. A listing is one signal governed by that list’s policy, not universal proof of spam.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

A **Domain Name System blocklist (DNSBL)** publishes reputation or policy data through DNS. Mail systems commonly query a sender's IP address during delivery and use the answer to reject, defer, quarantine, tag, or score the message. **RBL**, real-time blackhole list, is a widely used related term.

A listing is not a global ban and does not automatically mean an organization intentionally sent spam. Each list has its own scope, evidence, response codes, expiration, and removal policy. Receiving systems decide whether and how to use it.

How a DNSBL query works

1. The receiving server obtains the connecting mail server's IP address.

2. For an IPv4 DNSBL, it reverses the octets and appends the provider's query zone. For documentation address `192.0.2.25`, the form would begin `25.2.0.192`.
3. DNS returns no listing or a provider-defined answer, often in `127.0.0.0/8`.
4. The mail filter interprets that exact result according to the list's documentation and local policy.

Do not assume every return code means the same thing. It may identify spam, compromised hosts, open relays, dynamic ranges, policy listings, or a query error. RFC 5782 documents terminology and operational considerations for DNS blocklists and allowlists.

IP, domain, and URL lists are different

- **IP DNSBL:** evaluates the connecting or sending IP address.
- **Domain blocklist:** evaluates a domain found in mail, DNS, or another transaction.
- **URI/URL list:** focuses on domains or hosts appearing in message links and content.
- **Internal reputation list:** belongs to one receiver and may not offer a public lookup.

Check the rejected object before requesting removal. Delisting a website domain will not fix a sending-IP listing, and changing the visible From address does not change the connecting IP.

Safe use for receiving mail

- choose lists whose scope, data sources, error handling, and delisting policy match your environment;
- test in score or tag mode and measure false positives before rejecting mail;
- combine reputation with SPF, DKIM, DMARC, content, URL, rate, and behavioral signals;
- cache within published DNS time-to-live values and handle lookup failure safely;
- log the list, return code, timestamp, connecting IP, and policy decision;
- provide a useful SMTP rejection that lets a legitimate sender identify the issue.

A large number of lists is not automatically more accurate. Correlated or low-quality sources can repeat the same error and add latency.

How senders should investigate a listing

1. Read the full bounce message and identify the rejecting receiver, exact IP or domain, named list, SMTP code, and time.
2. Confirm the listing directly through the list operator's documented lookup. Third-party aggregate checkers may be stale or include lists the receiver never uses.
3. Determine whether mail actually left through that IP and whether delivery failures affect meaningful recipients.
4. Read the listing category and evidence before changing DNS or requesting removal.

Fix the cause before delisting

Investigate compromised accounts and hosts, exposed relays, stolen API keys, unexpected senders, forwarding abuse, list acquisition, bounce handling, complaint rates, and sudden volume. Stop unauthorized mail, rotate affected credentials, patch systems, tighten relay and account controls, and clean recipient data.

Then verify the sending identity: stable hostname, correct HELO/EHLO, matching forward and reverse DNS where required, SPF, DKIM, and DMARC alignment. Follow only the list operator's removal process. Some entries expire after the cause stops; others require evidence or an IP-owner request. Do not pay an unrelated service promising guaranteed removal.

Amazon SES also notes in its DNSBL FAQ that a bounce without the characteristic blocklist information may have another cause.

DNSBL FAQ

Does one listing mean all email will fail?

No. Impact depends on which receivers use that list and how they score its result.

Should a sender change IP addresses?

Not to evade reputation. Moving without fixing the cause often repeats the listing and can damage another address range.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com