warmy

Email Channel. Reliable

WARMY RESEARCH INSIGHTS

2026 March

MEET THE TEAM

ABOUT WARMY AND THE RESEARCH TEAM

Warmy is the leading email deliverability technology, helping businesses improve their inbox placement, sender reputation, and overall email performance. Powered by AI-driven strategies.

The Warmy Research Team is a dedicated group of email deliverability-certified experts focused on analyzing and optimizing email-sending practices.

Through continuous testing, data-driven insights, and innovative methodologies, they uncover factors that impact deliverability and translate findings into actionable improvements for Warmy's platform. Their expertise helps businesses navigate the complexities of email deliverability with confidence.

Daniel Shnaider
CEO Warmy.io & AnyBiz.io

Alexandr Panchenko
Technical Deliverability Expert

COMPREHENSIVE RESEARCH

WHAT IS THE SPAMHAUS BLACKLIST AND WHAT IT DOES TO YOUR EMAIL DELIVERABILITY?

- Spamhaus is a DNS-based Block List (DNSBL) that provides threat data to thousands of providers globally.
- A listing results in near-total cessation of email delivery to major providers. Microsoft enforces a zero-tolerance hard block; Gmail treats it as a damaging reputation signal.
- Spamhaus operates five distinct lists (SBL, XBL, PBL, DBL, and ZRD) each with a different cause, severity level, and required fix.
- This comprehensive research by Warmy covers crucial information on how Microsoft and Google respond to a Spamhaus listing and its potential implications.

WARMY.IO

RESEARCH TEAM

Oleksiy Lutskin
Senior Deliverability Expert

Artem Klymenko
Deliverability Expert

Warmy
Assistant

IN-DEPTH ANALYSIS

SPAMHAUS

Spamhaus is widely considered the most influential and severe DNS-based Block List (DNSBL) in the email industry. Unlike local filters (like Gmail's internal AI), Spamhaus provides threat data to thousands of ISPs and enterprise networks globally.

Why it is critical: *A listing on Spamhaus results in a near-total cessation of email delivery to major providers.*

Microsoft (Outlook, Hotmail, Office 365):
Microsoft relies heavily on Spamhaus (specifically the Spamhaus ZEN blocklist, which combines their IP and domain data).

- **The Hard Block**: If your sending IP or domain is listed on Spamhaus, Microsoft enforces a near-immediate, zero-tolerance block at the connection level.

- **The Bounce:** You will see immediate hard bounces, typically with error codes like 550 5.7.1 or 550 5.7.501, explicitly stating: "Service unavailable, Client host blocked using Spamhaus."

- **The Resolution:** Microsoft's own internal support and delisting portal (SNDS) will often refuse to help you or mitigate the block until you have successfully resolved the listing directly with Spamhaus. They essentially outsource a massive chunk of their frontline spam defense to Spamhaus.

IN-DEPTH ANALYSIS

SPAMHAUS

Google (Gmail & Google Workspace): Nuanced and AI-Driven
Gmail handles Spamhaus very differently than Microsoft. Gmail does not use Spamhaus for zero-tolerance, connection-level hard blocks.

- **Internal Systems First:** Google relies primarily on its own proprietary, highly sophisticated machine learning algorithms and massive internal data sets (user engagement, complaint rates, Google Postmaster Tools data).

- **Spamhaus as a "Signal," Not a "Rule":** While Google doesn't publicly disclose exactly how they weight third-party blocklists, it is widely accepted in the deliverability industry that Spamhaus is used as an input for Gmail's reputation scoring, rather than a hard rule.

- **The Impact:** If you end up on Spamhaus, Gmail is highly unlikely to give you a 550 connection-level bounce purely because of the listing. Instead, the Spamhaus listing will severely damage your domain/IP reputation score within Google's brain. This usually results in your emails being routed directly to the Spam folder or being rate-limited (temporary deferrals) rather than outright rejected at the door.

DEFINITIONS

KEYWORDS

DNSBL
A global "central database" of bad actors.
Spamhaus is the most powerful DNSBL; if you are on it, almost no one will receive your emails.

SBL / DBL
IP vs. Domain block.
SBL means your server (IP) is blocked; DBL means your website address (Domain) is "burned" and cannot be used anywhere.

UBE (Unsolicited Bulk Email)
The technical term for Spam.
This refers to sending large volumes of email to people who did not explicitly ask for it.

Data Hygiene
The process of "cleaning" your list.
Removing old, inactive, or fake email addresses to prevent hitting Spam Traps.

Zero Reputation (ZRD)
A "newborn" domain.
Domains registered in the last 24 hours have zero trust. Sending mail too early triggers an automatic block.

ANATOMY OF THE LISTS

Spamhaus is not a single list; it is a collection of datasets. The remediation strategy depends entirely on which list the client is on.

1.1. SBL (Spamhaus Block List) — The Severity Level: Critical

- **Definition**: A database of IP addresses verified to be sources of spam.
- **Trigger**: Direct evidence of "Unsolicited Bulk Email" (UBE), hitting Spam Traps (pristine or recycled honeypots), or a high volume of user complaints.
- **Implication**: The sender has bad data hygiene or is spamming cold contacts.

1.2. XBL (Exploits Block List) — The Security Breach

- **Definition**: IPs showing signs of infection (botnets, open proxies, malware).
- **Trigger**: The sender's server or computer is likely compromised by a virus sending spam in the background.
- **Action**: Do not delist until the infrastructure is scanned and patched.

1.3. PBL (Policy Block List) — The Configuration Error

- Definition: IPs that should not be sending email directly (e.g., dynamic residential IPs).
- Trigger: Sending mail directly from an ISP connection without using a proper SMTP server/relay, or missing rDNS (PTR) records.
- Action: This is technical. Configure authentication and use a proper SMTP relay.

1.4. DBL (Domain Block List) — The Toxic Asset

- Definition: A list of Domain Names (e.g., company.com), not IPs.
- Trigger: The domain (or a subdomain) has been used in spam message bodies or headers.
- Crucial Note: Changing IPs will not fix this. The domain itself is "burned."

1.5. ZRD (Zero Reputation Domain) — The Newcomer

- Definition: Domains registered within the last 24 hours.
- Trigger: Sending mail immediately after purchasing a domain.
- Action: Wait. New domains must "age" (minimum 24+ hours) before warm-up begins.

THE FIX

REMEDIATION PROTOCOL

WARNING: Spamhaus penalizes "Shoot First, Fix Later." Asking for removal without fixing the root cause will lead to an "Escalated" listing, which is much harder to remove.

Phase 1: Stop & Audit (Internal)

Kill Switch: Pause all campaigns associated with the IP/Domain.

Data Hygiene:

- Remove all unengaged contacts (did not open in 3-6 months).
- Remove "Role Accounts" (admin@, support@).
- Verify the list again to remove hard bounces.

Security Check: If XBL, scan for malware and change SMTP passwords.

Phase 2: The Removal Request (External)

Only proceed here after Phase 1 is complete.

Go to the Spamhaus removal form.

- **The Response Strategy:** Write a human response. Do not use templates.
- **Bad:** "We are not spammer, please remove."
- **Good:** "We identified the cause (a user uploaded an unverified legacy list). We stopped sending at 10:00 AM. We have deleted the list segment and implemented double opt-in for new signups. We have secured the server. We request removal."
- **Accountability:** Admitting the error works better than denial.

Phase 3: Post-Delisting Recovery

- Once removed, the reputation is fragile (reset to zero or negative).
- Do not resume full volume immediately.
- Restart Warm-up: Use a specialized warm-up tool (like Warmy) starting with very low volumes to demonstrate to Spamhaus (and Microsoft) that the traffic pattern has normalized.

PREVENTION

BEST PRACTICES

- **Avoid Spam Traps:** Traps are often old, recycled email addresses. Aggressively prune inactive subscribers to avoid hitting them.
- **Double Opt-In (DOI):** The best defense against SBL. Ensure users confirm their email before adding them to the list.
- **Separate Streams:** Do not send transactional email (password resets) and cold marketing email from the same IP. If marketing gets blocked, your core business shouldn't stop.

warmy

Email Channel. Reliable

WE DON'T SEND EMAILS
WE GET THEM SEEN

We are passionate about solving email deliverability challenges and making email a reliable channel for every business