warmy

Email Channel. Reliable

WARMY RESEARCH INSIGHTS

2026 March



COMPREHENSIVE RESEARCH

SURBL (SPAM URI REALTIME BLOCKLIST)

Email deliverability is increasingly dictated by the integrity of the content and the reputation of the domains linked within a message.

Our research aims to provide a comprehensive analysis of the SURBL (Spam URI Realtime Blocklist) mechanism, identifying the core triggers for URI listing and establishing a proactive framework for monitoring, prevention, and remediation of link-based delivery failures.

The SURBL system is a sophisticated, real-time database that tracks the reputation of domains and URIs found within email bodies worldwide. This system serves as a critical security layer for mailbox providers, distinguishing between malicious or "cracked" websites and legitimate resources used by authentic senders

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

WARMY.IO

RESEARCH TEAM



Oleg Sherbak
Head Of Research Team



Oleksiy Lutskin
Senior Deliverability Expert



Artem Klymenko
Deliverability Expert



Warmy
Assistant

DEFINITIONS

KEYWORDS

URI
The link (URL) inside the email.
SURBL blocks links, not sender IPs.

Payload
The body (content) of your email.
This is where SURBL "hunts" for blacklisted links.

Cracked Site
A hacked legitimate website.
You can be blocked if your site was hacked without you knowing.

Spam Trap
A "decoy" email address used as a trap.
If you send a link to this address, that link is instantly blacklisted.

Redirect
Sending a user from one link to another.
Spammers use this to hide; SURBL "follows" the path to find the truth.

False Positive
A mistake by the filter.
When a "clean" link is blocked by accident (requires manual removal).

INTRODUCTION

SURBL (SPAM URI REALTIME BLOCKLIST)

Unlike traditional DNSBLs (like Barracuda or Spamhaus IP) which focus on who is sending the mail (IP reputation), SURBL focuses on what is inside the mail. It is a proactive database of URIs (Uniform Resource Identifiers) that have appeared in unsolicited messages.

In-Depth Analysis of Specialized Lists

SURBL is not a single list but a collection of specialized databases designed to categorize different types of threats:

- **PH (Phishing)**: Contains URIs used in phishing heists (identity theft, credential harvesting).
- **MW (Malware)**: Targets sites hosting spyware, viruses, or ransomware.
- **CR (Cracked Sites)**: A unique list of legitimate websites that have been compromised/hacked and are being used by spammers without the owner's knowledge.
- **AB (AbuseButler)**: General spam domains identified through massive volume and automated analysis.
- **Multi**: A combined "super-list" that allows mail servers to query all sub-lists in a single DNS lookup.

The "Deep Content" Methodology

SURBL's accuracy stems from its ability to look past the SMTP envelope and inspect the payload:

- **Redirect Deciphering**: Spammers use link shorteners (Bitly, Rebrandly) or 301/302 redirects to hide their destination. SURBL "unwraps" these layers to find the final target URI.
- **Low False-Positive Rate**: Because SURBL identifies the advertised site rather than the sending IP, it avoids "collateral damage." If a spammer uses Gmail to send links to a malicious site, SURBL blocks the link, not all of Gmail.
- **Human-Machine Hybrid**: Similar to Barracuda, SURBL uses automated "honeypots" combined with manual verification by security researchers to ensure that legitimate business domains aren't blacklisted due to anomalies.

EARLY WARNING SIGNS:

PREDICTIVE INDICATORS OF BEING LISTED

A SURBL listing often results in "silent" delivery failures or specific bounce-back codes. Look for:

- **"Message Content Rejected"** (554 Error): If your IP is clean but you get this error, it's almost always a URI block.
- **Sudden Drop in Click-Through Rates (CTR)**: Major ISPs (Gmail, Outlook) use SURBL data to disable links in the inbox, making them unclickable.
- **Redirect Depth Alerts**: Mail logs showing "Too many hops" when the recipient server attempts to scan your links.
- **Domain Reputation Volatility**: A high volume of complaints (FBL) specifically tied to the URL in your signature.

WHY IS MY DOMAIN/URI LISTED ON SURBL?

Being listed on SURBL is often more critical than an IP block because it implies your brand's assets are perceived as malicious. Common reasons include:

- **Hacked Web Infrastructure**: Your website (CMS like WordPress) has a hidden folder or redirect script installed by a bot.
- **Affiliate Marketing Contamination**: You are using "dirty" affiliate links that have been blacklisted because other marketers spammed them.
- **Snowshoe Link Tactics**: Using dozens of subdomains for the same landing page, which mimics the behavior of "snowshoe" spammers trying to spread their reputation.
- **Insecure Contact Forms**: Spammers found a "Tell-a-friend" or "Contact Us" form on your site and are using it to send their links to third parties.
- **New Domain Velocity**: Linking to a domain registered in the last 24–72 hours.

WHAT TECHNOLOGIES DOES SURBL USE?

- **Global Honeypot Network**: Millions of "spam trap" addresses that exist only to catch links being advertised in bulk.
- **URI Extraction Engine**: A sophisticated parser that strips HTML/CSS to find hidden or obfuscated links (e.g., links hidden in transparent 1x1 images).
- **Sandboxing & Scoping**: When a new URI is detected, SURBL's bots visit the site in a sandbox to check for malware signatures or phishing kits before adding it to the list.
- **Zero-Hour Detection:** Real-time updates that allow the system to block a brand-new "throwaway" domain within minutes of its first appearance in a spam trap.

PROACTIVE MONITORING & COMPLIANCE

To maintain a "Clean" URI status:

- **Link Sanitization**: Audit all links in your email templates, including social media icons and tracking pixels.
- **WAF (Web Application Firewall)**: Use services like Cloudflare or Sucuri to ensure your site isn't "cracked" and used as a redirector.
- **Subdomain Isolation**: Use a dedicated domain for outbound outreach (e.g., getcompany.com) to protect your primary corporate domain (company.com).
- **HTTPS Enforcement**: SURBL increasingly flags non-secure (HTTP) links as suspicious in marketing contexts.

EXAMPLES

HOW TO CHECK AND SUBMIT A REMOVAL REQUEST

If your emails are bouncing with a SURBL reference, follow these steps:

Step 1: Status Lookup

Go to surbl.org/lookup and enter your domain. The result will tell you which specific list (PH, MW, CR, etc.) you are on.

Step 2: Remediation (Crucial)

SURBL will not remove a domain if the underlying issue persists.

- If you are on the CR (Cracked) list, you must scan your site and remove the malicious files first.
- If you are on the AB (Abuse) list, you must stop the high-volume outreach that triggered the traps.

Step 3: Formal Request

Fill out the removal form on their site. Provide a technical explanation of what was fixed.

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



© 2026 Warmy.io