How Can I Prevent List Bombing?

Introduction

List bombing is an often underestimated threat to email marketers on systeme.io. Bots exploit **unprotected subscription forms**, flooding your CRM with fake or non-consenting addresses. Help article **3990** describes the attack and the **two procedures** you must implement: **reCAPTCHA** and **double opt-in**.

Prevention is cheaper than recovering from a spike in **bounces**, **spam complaints**, and a drop into **high-risk sender pools**.

What Is List Bombing? (3990)

List bombing is a **malicious attack** where automated bots target vulnerable opt-in forms and submit **thousands of fake sign-ups** in a short time. Your contact list fills with:

- Email addresses that **never consented** to your marketing.
- **Invalid or random** addresses that bounce when you email them.
- Sometimes **real people's emails** signed up without their knowledge (harassment / "subscription bombing").

Targets include funnel opt-in pages, blog forms, checkout flows, and any public form without bot protection.

Why It Matters on systeme.io

- **Bounce rate** rises → worse **sender pool** placement (pool metrics).
- **Spam complaints** from victims who receive your confirmation or campaigns.
- **Sending pauses** or reviews after suspicious list growth (import/list quality checks).
- **Distorted analytics**—fake contacts never open mail, dragging down engagement.

systeme.io groups senders by **open rate**, **spam rate**, and **bounce rate** to protect the shared IP network—your list hygiene affects everyone, including your own inbox placement.

Prevention: Two Required Procedures (3990)

To prevent list bombing from bot attacks, article **3990** requires implementing **both** measures below—not just one.

1. reCAPTCHA

Enabling reCAPTCHA blocks most bots from completing your forms.

1. Generate **Site key** and **Secret key** in Google reCAPTCHA.
2. In systeme.io, go to **Settings** → **Custom domains** → domain **Settings** → paste keys in **reCAPTCHA Settings** (add CAPTCHA to Contact us page, 1673).
3. Add the **CAPTCHA element** on protected pages (especially Contact us and forms on your verified domain).

Tip: Use CAPTCHA on any high-traffic public form. Community guidance often notes reCAPTCHA is most documented for **Contact us** flows—still configure keys at the domain level and protect every exposed endpoint you control.

2. Double opt-in

Double opt-in requires subscribers to **click a confirmation link** before they are fully active. Bots typically cannot complete this step.

1. Open your funnel **opt-in page** in the editor.
2. Click the **gear icon** on your submit button.
3. Check **Do you want to enable double opt-in on this form?**

4. **Save** the page.

Full walkthrough: How to Set Up Double Opt-In (271).

Important rules (271):

- Configured **per form**, not globally.
- Unconfirmed contacts are **deleted after 24 hours**.
- **Emails and automations are paused** until confirmation.
- Highly recommended on **blog forms** to keep bots off your list.

If You Were Already List Bombed

Article **3990** recommends this recovery checklist:

1. **Identify** which opt-in form was targeted and the **timeframe** of the attack.
2. **Implement** reCAPTCHA and double opt-in immediately on that form (and similar forms).
3. **Remove bot contacts:** filter contacts added during the attack—bot entries often have **gibberish first and last names**.
4. **Delete** those contacts and ensure they are **excluded from future emails** for deliverability recovery.
5. Follow manual list cleaning (139) and remove bounced contacts.
6. Enable automatic list cleaning for ongoing hygiene.

Do not send a full-list broadcast until bad addresses are purged—you would amplify bounces and complaints.

Additional Good Habits

- **Authenticate your domain** (SPF/DKIM/DMARC)—does not stop bombing but stabilizes legitimate mail.
- **Never use single opt-in** on anonymous high-traffic pages if you can avoid it.
- **Monitor CRM growth**—sudden spikes without ad spend are a red flag.
- **Only opt-in consent**—never import scraped lists (deliverability rules).
- Review **email statistics** (open, spam, bounce) weekly.

Troubleshooting

Issue	Fix
Bots still getting through	Enable double opt-in + reCAPTCHA; check keys on correct custom domain.

Double opt-in not sending	Customize confirmation email in mailing settings; verify sender domain.
Real leads drop after DOI	Normal trade-off—better inbox placement; optimize confirmation email.
CAPTCHA not visible	Domain verified; keys saved under Custom domains → Settings.
Metrics still red after cleanup	Wait for pool reassignment (14+ days); keep sending only to engaged segments.

Frequently Asked Questions

What is list bombing?

Bot-driven mass fake opt-ins on your forms (3990).

Two main fixes?

reCAPTCHA + **double opt-in**.

Spot bots?

Attack window + **gibberish names** → delete.

24-hour rule?

No confirm click → contact removed (271).

Deliverability impact?

Higher bounces/spam → worse **pools**.

Related Resources

- How to Set Up Double Opt-In
- How to Add a CAPTCHA to a Contact Us Page
- How to Manually Clean Your Email List
- How to Improve Your Email Deliverability

On systeme.io, treat **list bombing** as a security issue: **reCAPTCHA**, **double opt-in on every opt-in form**, and fast **cleanup** if bots slip through.

Last updated: July 3, 2026