

“Am I A Spammer?”

You’re likely to be blacklisted as a spammer if you act like a spammer. In fact you may be a spammer, without meaning to be, or maybe you’re in denial.

You are a spammer if:

- ▶ **You make enough people complain. All it takes is:**
 - 1-2% recipients of your mailings complain to their ISP directly.
 - 1-2% of your recipients use a manual spam filter in their mail client to mark your messages as spam. (This is communicated to their ISP and/or a third-party blacklisting service.)

- ▶ **Your insecure machines become “owned” by spammers:**
 - If a machine on your network is infected and has become [an evil zombie member of a botnet](#), it will be sending out thousands of spam messages a minute, or doing other evil things.
 - If there is an insecure mail form on your website and a spammer is using it to send out spam, that’s on you too.

- ▶ **You cross the line between direct mail and spam:**
 - Using disreputable third party bulk mailing services means they’ll be doing a lot of things listed in this document on your behalf.
 - Sending your own bulk mail without clear control of your recipient lists—addresses that are valid and connected to a record of the owner opting into your list—means you will make a lot of people complain. You may end up sending mail to a spam trap address, and that will get you blacklisted.

Things that make people complain:

- ▶ Sending mail to people who did not subscribe directly to your list.
- ▶ “Repurposing” emails. Someone who makes a “technical contact” through a form on your site *did not ask* to be on your mailing list.
- ▶ Ignoring unsubscribe requests.
- ▶ Not being clear about privacy/disclosure, or not following your policy.
- ▶ Anything you do that is irritating. If you wouldn’t like it done to you...

Mail server misconfiguration can make you look like a spammer and may get your filtered. To avoid this:

- ▶ Make sure that your mail server not only has an entry mapping its domain name to its IP address, but also one that maps its IP address back to its domain name (a *PTR record*). If your mail server sends mail on behalf of more than one domain, make sure you have a reverse-mapping entry for each domain. Where possible, do the same with the sending client, if it submits mail via SMTP.

- ▶ Ensure that your sending IP address not only has a valid PTR record, but that PTR exactly matches the name given in the HELO command, which identifies the sending host to the receiving host. The recommended identification is the sender's FQDN (the Fully Qualified Domain Name, e.g. mail.example.com).

Everyone with a mailing list should:

- ▶ Remember this is a process, not an event.
- ▶ Only send mail to people who have asked for it and keep a record of their consent.
- ▶ Use a double opt-in subscription system.
- ▶ Only send mail that recipients will likely find relevant, and make it clear what they should/should not expect (volume, subject, etc.) when they sign up.
- ▶ Monitor and update your contact lists.
- ▶ Configure your outgoing mail properly so it doesn't look suspicious.
- ▶ Explicitly remind subscribers why they are receiving mail from you at the top of each mailing.
- ▶ Always include unsubscribe instructions.

Proactive steps for high volume mailers:

- ▶ Get on an automated feedback loop with major ISPs so they tell you when people complain about you.
- ▶ Remind subscribers why they are getting your mailings. A small text to that effect can go in every mailing.

Further Reading:

- ▶ [When They Say You Are a Spammer](#) (New York Times, Small Business Section, 2007)
- ▶ [How Not to Be Seen as a Spammer](#) (Ferris Research)
- ▶ [Seven Ways to Be Mistaken for a Spammer](#)