AvoidingFpsForSenders

Some Tips for Legitimate Senders to Avoid False Positives

Sections found below:

- General Guidelines – These guidelines can be useful if you haven't yet sent out your email(s), and want to keep the scores low (or negative) to avoid false-positive problems.
- Fixing FPs – Your email was flagged as a spam – how to avoid this next time
- Newsletter Aids – Your newsletter is confirmed opt-in / double opt-in, never spams, and you want to gain some negative (i.e. NOT spam) scoring traits.
- Other Resources – Where else can you look for guidance?

General Guidelines

These guidelines can be useful if you haven't yet sent out your email(s), and want to keep the scores low (or negative) to avoid false-positive problems.

Tip: Don't worry too much about specific rules within SpamAssassin. The rules catch spam. If your email isn't spam, you shouldn't be matching the rules. Even if you do hit an occasional rule, unless your email actually is spam, it shouldn't score high enough to be a problem.

Tip: Be honest in your headers. Be accurate in who you are (From), and which systems the email goes through, preferably from your own servers, using your own domain name. Make sure the the To header indicates the recipient. If the recipient is a list or a class of people, state so. Don't insert strange Received headers, or any other unwarranted header.

Spammers need to try to fake out filters by hiding their source and destination; if you try to hide your source and destination you'll look like spam too. Likewise, spammers often try to track their spam and guage its effectiveness through tracking headers they add to emails. If you add unnecessary headers to your emails, this can make them look like spam.

Tip: Use a domain name which is identified by a verifiable IP address. Make sure that if someone checks on the domain of your From address and Reply-To address that these addresses are valid, and the machine that would receive any Reply email can be identified.

Tip: Using SPF identification for your domain helps. It won't flag you as a good guy directly, but it will prevent bad guys from successfully masquerading as you.

Tip: Use an intelligent message id which ties correctly to your system. Use an intelligent mailing agent, one which identifies itself in the headers and which isn't heavily used by spammers. Make sure your date header is correctly formatted and in the correct time zone.

Tip: Use email composition and mailing tools that work correctly. Well constructed emails (technically correct) can be readily identified as not-spam. Emails with missing mime sections, invalid or missing message-ids, invalid or missing date headers, subject or other headers with unescaped unicode, etc., are frequently signs of spam.

Tip: Avoid useless or needless encodings. Don't use base-64 encoded text unless you need to.

Tip: Don't include a disclaimer that your email isn't spam. Don't claim compliance with some legal criteria, especially one which is not actually law in your country. Only spam needs to *claim* compliance – non-spam is supposed to already be in compliance.

If your email is covered by anti-spam laws, do make sure you are in actual compliance. Skirting the edge of compliance is a frequent spam trick, and is accordingly flagged by SpamAssassin.

Tip: Use normal conversational language, be sure not to use excessive spacing and or capitalization on your subject.

Tip: Be open and honest and plain in your emails. If you try to hide things, or try to use tricks to bypass spam filters, you'll look like a spammer and you'll be treated like a spammer. The statistics for use of these various techniques show that it occurs far more frequently in spam mail than non-spam, and the rules reflect that.

Do not use "cute" spellings, Don't S.P.A.C.E out your words, don't put str@nge |etters 0r characters into your emails.

Tip: If you're using HTML emails, use high quality HTML emails. Don't use tools which generate horrendous HTML (example: MS Word). They often leave signs behind (like empty tags, eg: <B></B>) which are generally found in spam. Make sure your HTML is valid (run it through a decent validator). Unbalanced tags and invalid tags will also flag an email as spam. If you use a title, make sure the title is meaningful – the default titles generated by HTML tools are often used as spamsign.

Tip: If you're using HTML emails, do not use invisible text within those emails. Make sure your text colors and sizes are distinct enough and large enough to read. Invisible text is often identified as a sign of spam.

Tip: If you're using HTML emails, do not use invisible web-bugs to track your emails. If you must track your emails and whether they're read, use visible graphics as part of your email, not invisible graphics.

Tip: If you're using HTML emails, include a text part in the email as well, for recipients (and anti-spam checkers), and keep that text as close to the HTML copy as possible. The closer they're related, the less likely your email will be seen as spam.

Very important: Don't insult your recipients by telling them to get a different email client so they can view your email. People use the email client they want, and if they're not using Outlook Express or some other basic, dumb, free, and automatically installed client, chances are they're doing so *intentionally*. If you want them to view your HTML, give them a web link they can follow in their web browser. (Give them this *in addition* to the non-HTML text.)

Tip: OK – one suggestion which actually does relate to SpamAssassin rules; don't include gratuitous references to spam subjects. Don't talk about rolex watches, sexually oriented activities or drugs, or debt treatment, unless those topics directly relate to your email. And if they do, limit your email to one topic at a time. An email which mentions rolex watches, Viagra, porn, and debt all in one email will very possibly hit several rules that flag it as spam, even if everything else is clear.

Tip: Don't use 'bulk-mailing' tools used by spammers (i.e., advertised in spam). These are overwhelmingly used to send spam, so SpamAssassin blocks mail sent by those tools as soon as possible. In particular, if the product's feature list includes 'stealth sending' or similar, that's a danger sign.

Tip: Be careful where you advertise, and be careful which advertisements you carry. If you advertise with companies that send out spam, your domains will be flagged as being related to spam. If you carry advertisements for those who spam, your domains will be flagged as being related to spam.

Tip: Be careful which domains/companies you allow to advertise in your emails (if any). Allowing spammers to advertise will get your emails flagged by the URI blacklists. On the other hand, don't advertise your domains with spammers – having your domain name listed in their spams can also get you flagged by some URI blacklists.

Tip: Be visible and public in your domain and hosting registrations. If people who check for you to see whether you might be a spammer, or to complain /ask about your emails, finds bogus entries in your registrations, or "private" or "hidden" annotations, that strongly suggests you are a spammer, hiding from an outraged public. If you are open about who you are in your registration emails, you'll get some complains and some queries. Answer those honestly and fully, and you should stay out of blacklists.

Make sure you have active and monitored abuse <at> and postmaster <at>
addresses. Register them with abuse.net.

Tip: Make sure your privacy policy, including enforcement, and including query contact information, is easily found and clearly stated on your web site. It's good to include this information (where to find this policy, contact information), in your emails. Again, people who need to find out whether you're spammer will often look for that information.

Tip: Test your email with SpamAssassin. Send your draft to/through a system with SpamAssassin running, and see how it scores. If your email hits a number of high-scoring SA rules, then you can determine why and reduce your email's score.

Fixing False Positives

Your email was flagged as a spam. These tips may help you figure out how to avoid this next time.

Tip: examine exactly which rules were triggered if a message was marked as spam or nearly marked as spam. Take careful note of the *points* listed beside each rule name – low-scoring rules do not make much of a difference, it's the ones with high scores that need to be avoided.

Tip: if there are hits in the body of your mail-out, try rephrasing those sentences. We find that spam often uses *exactly* the same phrases, over and over again, so we detect specific lines of text, and in most cases, synonyms are ignored.

Tip: if a subscriber reports that SpamAssassin is blocking mails they want, and they did not ask their ISP to set it up – get them to ask the ISP to take them off the filtering list! (Spam filters should not be installed on an account unless the person *wants* it there, in our opinion, since even nowadays some people don't get as much spam as others. As a result, we ask ISPs to let the users enable or disable the filter.)

Newsletter Aids

Your newsletter is confirmed opt-in / double opt-in, never spams, and you want to gain some negative scoring traits.

Tip: there are several whitelisting services which lower scores for sites using SpamAssassin network tests:

- Return Path (http://www.returnpath.net/)
  Return Path's Sender Score Certified is an email accreditation program (or "whitelist") with strict standards for both infrastructure and practices.
  Return Path also operates the Sender Score Safelist, with somewhat different criteria.
  Given that, as a result, we can count on mails from these programs being non-spam, we're happy to give it "bonus points" and allow it through filters.
- dnswl.org
  DNSWL.org provides a Whitelist of known legitimate email servers to reduce the chances of false positives while spam filtering.

Please report any spam that is given bonus points for either of these services to the respective service.

Other methods for receiving "bonus points":

- HashCash (http://hashcash.org/)
  See http://hashcash.org/faq and http://hashcash.org/draft-hashcash.txt.
  This is a technological solution, while Bonded Sender is an economic solution and Habeas is a legal solution. Hashcash may not be appropriate for large mailing lists, as it requires substantial computational power to send each email.

Other Resources

Where else can you look for guidance?

Some useful links:

- Frugal Marketing: That's not Spam, That's My Newsletter! http://www.frugalmarketing.com/dtb/notspamnews.shtml
- SpamCon Foundation: Best practices for marketers: http://www.spamcon.org/directories/best-practices.shtml

- Bulk e-mail HOWTO: http://spam.abuse.net/marketerhelp/bulk-howto.shtml