



Smart E-Marketer's Guide

30 insider tips to maximise your
email deliverability rate



30 insider tips

Step 1.

Ensure the domain you use for sending emails is configured to enable authentication (SPF / Sender ID/ DomainKeys).

Step 2.

Sending your emails at a steady rate, from a dedicated and consistent IP address will help to build your reputation with the ISP's.

So use a dedicated domain name and IP address for your regular marketing email sends. Some email service providers, including dotMailer.co.uk, will provide a ready configured domain - set up for authentication. This will also ensure you avoid the threat of an ISP blacklist impacting your day to day emails sent from your business domain.

Step 3.

Ensure your messages are sent from a meaningful 'friendly' from address in the message header - NOT from a string of numbers

Step 4.

Display a privacy policy opt-in statement, and declare your identity and how you intend to use an email address at the time of collecting it.

Step 5.

Do not email to contacts who have not given you prior permission to email them your marketing messages. (There are legitimate exclusions to this rule. Please refer to the DMA Direct Marketing Code of Practice for further information).

Step 6.

Gain permission to email contacts, by providing a positive 'Opt-in' box for them to check.

Step 7.

Confirm email address validity and your permission to email, by sending a 'non-commercial welcome email' to all new contacts.

Step 8.

Use the welcome email to invite new contacts to add you to their 'Safe/Trusted Senders' list within their inbox or to add you to their address book.



Step 9.

Consider using a 'double opt-in' for new contacts. Here, your welcome email will require the contact to click through and confirm their details and consent. Double opt-in has pros and cons. It may build you a database of highly engaged and responsive contacts. But it may also increase the chance of drop-out and limit the size of your database.

Step 10.

Ensure opt-ins are collected offline (i.e. via call centre, customer care, sales team, registration cards) for new contacts captured via these channels.

Step 11.

Ensure email addresses collected offline are emailed and validated (i.e. not hard-bounced back) before they are added to your main contact database.

Step 12.

Always provide a highly visible unsubscribe link in all your email messages

Step 13.

Ensure your unsubscribe link requires no more than 2 clicks on the part of the unsubcriber.

Step 14.

Ensure your unsubscribe page is branded with your company name, logo etc, to instill trust in unsusubscribers and encourage them to use this channel for unsubscribing, rather than clicking the 'Junk' button in their inbox.

Step 15.

Ensure your Unsubscribe Link processes unsubscribe requests in real-time.

Step 16.

Ensure offline points of contact are available for unsubscribers (e.g. a phone number and postal address) and that these requests are processed in a reasonable time frame.

Step 17.

Make sure you keep your lists clean by deleting all hard bounces (hard bounces are undeliverable emails due to a permanent error)

Step 18.

Handle soft bounces (these are undeliverable emails due to a temporary error such as a full inbox or an Out of Office reply). Depending on your frequency of send, 3 consecutive soft bounces could be enough to classify a contact as a hard bounce.

Step 19.

Treat your email database like you would treat your mailing database - keep it clean, up-to-date, deduped, and free of gone-aways. Flag 'dead' contacts and long-term inactive recipients who never respond, test email them to see if they can be reactivated, and if not then stop emailing them.

Step 20.

Identify from your email database who the key ISPs for your campaigns are, and establish a relationship with them. Contact them to introduce yourself, explain your opt-in policy and ask for advice on how to avoid their blacklist.

Step 21.

If you receive a bounce back with a black list message, always contact the ISP and get a named contact to speak to about the black listing. Have a copy of the bounced message to send them and be ready to explain your privacy and opt-in policies and to ask for advice on how to avoid their black list.

Step 22.

Consider subscribing to a Delivery Monitoring Solution that will provide continuous monitoring of your reputation and black list status and provide snapshots of your authentication levels. Email Service Providers (ESPs) provide this service by default.

Step 23.

Consider using an Email Service Provider (ESP). Sending your emails via an ESP such as dotmailer.co.uk means you can benefit from their acquired reputation, white listings, accreditation and IPS relationships, built up over many years and over large volumes of legitimate email marketing. This level of reputation is priceless.

Step 24.

Choose an ESP that is signed up to 'Feedback Loops' on the major ISPs such as Hotmail, AOL and Yahoo. A 'Feedback Loop' allows the ISP to send an unsubscribe mail to your database when a recipient of your email hits the 'Report Spam' button. This enables you to unsubscribe/suppress the complaining recipient from future sends, avoiding repeat complaints and protecting your reputation.

Step 25.

Double check that your email content isn't being caught by spam content filters at the last hurdle, by using a spam checker to analyse and score your templates.

Step 26.

Use an 'Inbox Preview' or 'Email Proofing' tool to check how your email templates render in different ISP inboxes - particularly when images are turned off. Spam checking and email proofing tools are offered by email marketing provider dotmailer.co.uk

Step 27.

Avoid large graphics, or a high proportion of graphics to plain English text, that can be scanned by a spam content filter.

Step 28.

Don't use lots of different colours for text and links.

Step 29.

Don't include an excessive number of links relative to the number of words in your email.

Step 30.

Avoid suspicious subject lines . Aside from the obvious, web text words such as 'free', 'special offer', etc should be avoided as much as possible, as should words in full caps and lots of exclamation marks - they're beloved of spammers. Consider using graphics to display words like 'FREE' if necessary.

For more guidance and advice, contact dotMailer's email marketing consultants:

Tel: 0845 337 9193

email: contactus@dotmailer.co.uk

www.dotmailer.co.uk

This document is copyright of Ellipsis Media Ltd. 2008.

