Email Deliverability

Do's, Don'ts and How To Reach The Inbox

Hi, and thanks for downloading Email Deliverability: Do's, Don'ts and How to Reach the Inbox!

That you've taken the time to download and read this guidebook shows that you're aware that there's a difference between **sending** an email, and **delivering** an email. You want to make sure your email marketing campaigns actually get to your subscribers.

Like any topic with such a technical-sounding name, email deliverability probably **seems at times like a bunch of mumbo-jumbo**. Terms like "hard bounces," "soft bounces," "spamtraps" and acronyms like SPF and DKIM come up often. And that's not even looking at the numerous bounce codes that ISPs may send back when they reject a message.

The truth is, email deliverability, for the most part, isn't rocket science. Are there some technical things that you should entrust to someone who specializes in getting email delivered? Sure. But **you control many of the factors that determine your email deliverability**, too.

How – or whether – you exercise that control goes a long way toward determining whether your email gets to the inbox, falls in the junk folder, or goes missing entirely. We wrote this guidebook to show you the things you can do to help your email get delivered – and the things you can do to inadvertently ruin your email deliverability.

Let's get right to it...

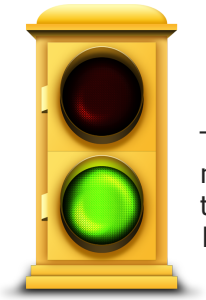
DO Monitor Blocklists.

While major ISPs such as AOL and Yahoo maintain their own internal blocklists, there are also many publicly available lists that are used by regional ISPs and corporate domains. These lists are used to identify IP addresses that are believed to be sending spam, as well as URLs that appear in spam messages.

Monitor these lists to make sure that neither your IP addresses and website URL/s are not listed. If you find that they are, get in touch with the administrator of the list to find out what caused you to be listed and how you can get de-listed.

Deliverability services that can monitor blocklists for you include:

Delivery Monitor - **http://www.DeliveryMonitor.com**
Sender Score - **http://www.SenderScore.com**



DO Authenticate Your Email.

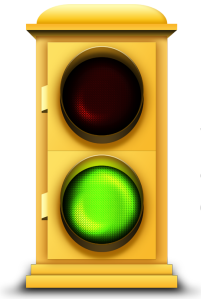
This is the latest weapon in the long-running battle between ISPs and spammers. You can now provide ISPs with a list of mail sources that are "legitimate" for you – sources that you take responsibility for. The idea is, if an ISP gets a message that looks like it's from you, but it's not actually from one of the sources you are responsible for, the ISP refuses the message.

There are three major authentication standards:

- **SPF**
- **Sender ID**
- **DomainKeys**

For best results, authenticate your email according to all three. If you're working with an email marketing service, they may authenticate your email campaigns for you (make sure they do!).

Learn More About Authentication.



DO Communicate With ISPs

We've come a long way from the days when email deliverability was a battle between ISPs and anyone sending a lot of email to them. Now, ISPs and ethical email marketers collaborative to separate spam from legitimate marketing email.

Many ISPs offer feedback loops, where you can be notified automatically whenever one of their users marks one of your messages as spam. This helps you to:

- Automatically Unsubscribe People Who No Longer Want Email
- Monitor Your Complaint Rate (if it gets too high, the ISP may stop delivering your mail)
- Learn What Campaigns Cause More Complaints

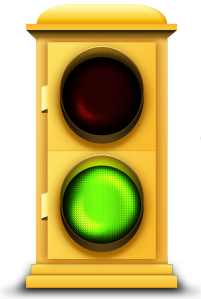
Many ISPs also offer whitelisting. While it doesn't guarantee that your messages will get preferential treatment, much like authentication it demonstrates to an ISP that you recognize the importance of taking responsibility for your email marketing. As ISPs shift their focus from content to reputation when determining what is and isn't spam, proactive steps like getting whitelisted and authenticating your email make their job easier... and your deliverability better.

If you're using an email marketing service, they should already have set up whitelisting and feedback loops (if they don't, ask them to!). They can then pass spam complaints along to you.

Do Get Subscribers to Whitelist You

Client-side whitelisting (where subscribers add your address to their Address Book or "Safe Senders" list) helps ensure that after your messages get through the gauntlet of ISP filters, they don't end up just getting dropped into the "Spam" folder by recipients' email programs.

Additionally, even if your message makes it to the inbox, if a subscriber's email program doesn't recognize you as an allowed sender, certain content in your messages (including links) may be disabled by default.



DO Check Your Content For Filtering

Content isn't as big a factor as it used to be – reputation matters more (see above).

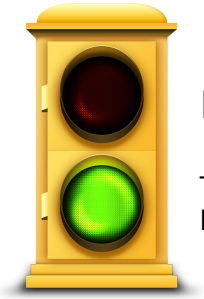
However, content filters can still affect your email deliverability.

While major ISPs keep their content filters a secret for obvious reasons, you can check your content prior to sending using publicly available filtering programs such as SpamAssassin. Ask your email marketing service about automatically checking your content against such filters prior to the message being sent.

DO Track Your Inbox Deliverability

Just like you, your subscribers have a "spam" folder. And just like you, they probably don't do much more than skim it now and then before deleting everything in there. You don't want your message to be skimmed and deleted... you want it to be opened, read and acted on!

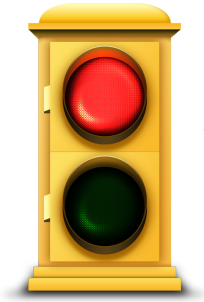
Keep tabs on how effectively your emails are reaching the inbox using a deliverability service. You'll find that certain messages reach the inbox better than others, and then you can apply the lessons you learn to make future messages more deliverable.



DO Provide Relevant, Valuable, Permission-Based Email Messages

The most deliverable email marketing campaigns don't just reach the inbox the first time, but continue to do so over time.

Long-run deliverability derives largely from reputation, and your reputation comes from your subscribers. Get their explicit permission before emailing, and provide them valuable, relevant content, and you'll be much more likely to keep getting your messages to them.



Don't Ignore Plain Text

You've put together a great-looking HTML message. It's jam-packed with two columns of great content, attention-grabbing imagery, and the design matches the feel of your website perfectly.

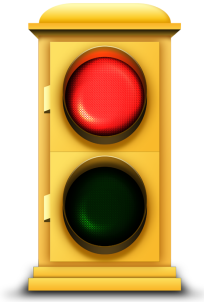
After all, HTML just looks and works better than plain text, right?

It can... if the message is delivered. But sending an HTML-only message without an accompanying plain text version is something spammers do... and you don't want to give an ISP any reason to draw parallels between you and spammers.

Plus, as great as your HTML message is, some of your readers may prefer or need plain text:

- They May Prefer to Read HTML
- They May Read Email on a Mobile Device that Doesn't Support HTML

If you're not meeting the needs of that segment of your readers, they may be unwilling – or unable – to read your message. This can lead to an increase in spam complaints, which can negatively affect your deliverability.



Don't Buy Email Lists

If people haven't given you explicit permission to email them... don't email them.

It might seem at first glance like a good way to "blast your message out" to a bunch of people in a hurry, but besides being a short-term approach to a long-term challenge, this tactic can have a serious negative impact on your deliverability even after you abandon it.

Email deliverability starts with permission, and no matter what sort of "assurances" you may get from someone offering to sell you an email list, you don't have the permission of someone on a purchased list to email them... many such lists are made up of addresses harvested online, including spamtraps, and even if the addresses are real and represent people who requested ***something***, that's a far cry from them knowing you and requesting information from you. You simply can't be relevant enough in those circumstances.

Spend your marketing dollars on something that will produce results, not on buying email lists.

Don't Keep Subscribers Guessing

Want an easy way to get a bunch of spam complaints and unsubscribes? Send emails that don't contain the type of content your subscribers expect to receive from you, in the format they expect, on the timeline they expect.

From the point that subscribers opt in to your email list, let them know:

- How often they can expect to hear from you
- What kind of content they can expect to receive
- What your message looks like

Reinforce those expectations with your welcome message.

By clearly setting and then meeting expectations, you drive your subscribers to not only trust you as a reliable business partner, but also to anticipate your messages and to do what they can (adding you to their address book, contacting you if they miss a message) to make sure your emails reach their inboxes.

Don't Assume That Your Subscribers See What You See

You pour time, money and heart into building your brand and image. A poorly-rendered email message can wreck that image as fast as you can say "what do you mean you can't read it?"

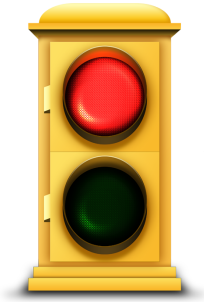
Your subscribers don't all use Outlook (even if they do, they don't all use the same version of it). There are dozens of different software-based and web-based email clients, and each one displays your message differently.

Test your message content in a variety of environments to ensure that it renders the way you want it to. Test traditional "work" email clients:

- Outlook
- Lotus Notes
- Thunderbird

But don't overlook major web-based clients. These programs can manage business email addresses with the convenience of being accessible anywhere. You need to test them, too:

- Yahoo
- Gmail
- Hotmail
- AOL



Don't Go Phishing – Or Make Someone Think You Are

Marketing without tracking... isn't marketing at all. You already know this. That's why you track clickthroughs in your email messages.

But do it the wrong way, and ISPs may think you're trying to rip off their users.

Phishing refers to trying to trick someone into giving you sensitive information such as bank account numbers or logins and passwords to various websites.

Briefly, the way it works is the spammer sends a link that purports to go to one website (whose address is displayed to the reader), but behind-the-scenes the link actually goes to the spammer's website, which is designed to look like the legitimate site, fooling the reader into providing the desired information.

Here's how this applies to you: most clickthrough tracking works by sending the reader to a tracking URL, which records the click and immediately redirects the reatder to your page.

If in the design of your message you type out the full URL and track clickthroughs on it, it looks to an ISP like you're tricking readers - telling them you're sending them to your page, but instead sending them through the tracking page.

If you're sending HTML messages, do not type out the full URL in your message design. Instead, link appropriate phrases or images to your pages. Besides improving your deliverability, this just reads more smoothly and provides a better user experience.

GOOD

See how we can increase your ROI.

BAD

See how we can increase your ROI.

http://www.example.com

Where Do I Go From Here?

If you got your hands on this guidebook by dropping your email address into our download form, you'll be getting supplemental advice sent to you (actually, you should already have a first message in your inbox!). You'll get more detail about these Do's and Don'ts, how they affect your deliverability and what you can do to get your email to the inbox.

(If you were forwarded this from someone else, and want to get a copy of those supplemental tips, just go to the download form and plug in your email address!)

We talked about a few deliverability keys that a third-party email marketing service is best-suited to manage for you. Email deliverability is one of the top reasons that thousands of businesses use AWeber every day to manage their opt-in subscribers and send out their email campaigns.

We invite you to try us out risk-free – if you decide we're not for you, that's fine, just let us know, we'll refund you and we can go our separate ways. (But we think you'll like our service!)

Have a few questions first? Get in touch with our expert, US-based Support Team – they'll be happy to take care of you!

If you're not in the market for an email service right now, but still want to learn more about email marketing and deliverability, check out our blog – thousands of loyal readers stop by for the articles and commentary published there a few times per week. Many of them even sign up for free email updates.

Thanks again for downloading this email deliverability guidebook!

-The Whole Team at AWeber Communications