EMAIL DELIVERABILITY

Marketo®

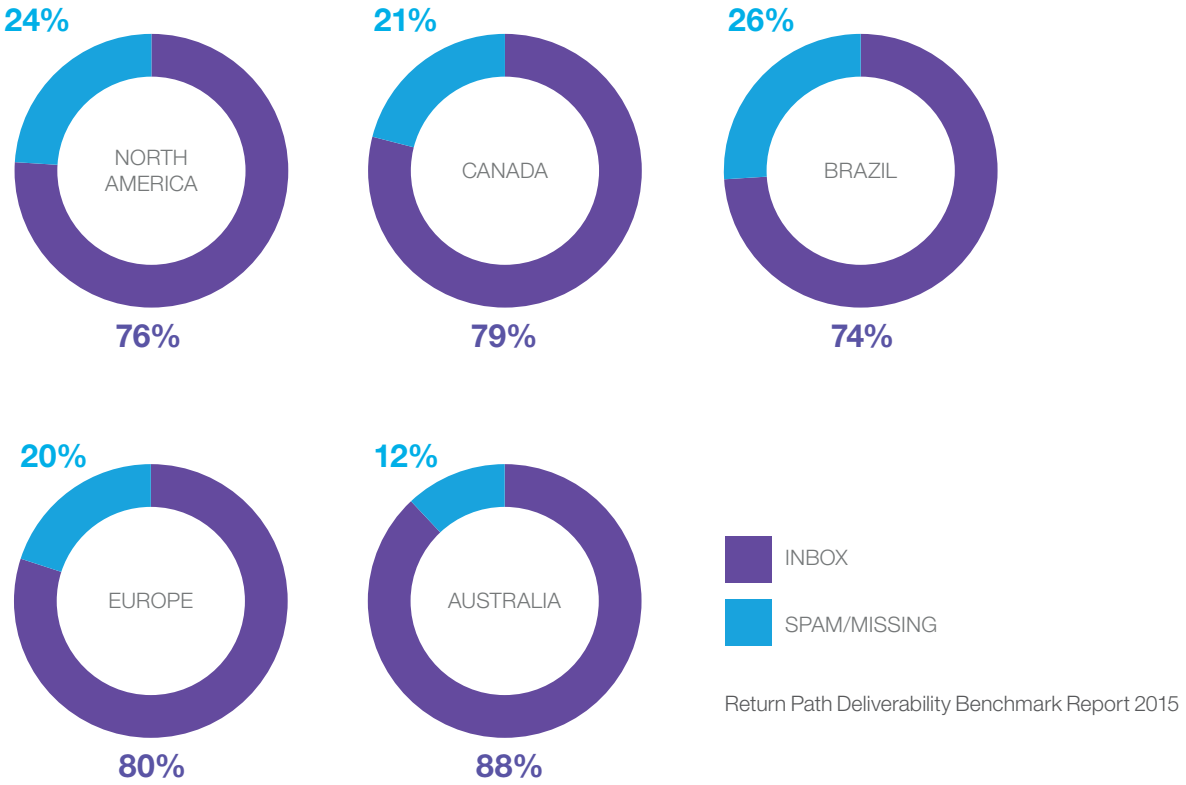
EMAIL DELIVERABILITY

There's no question that email software and the people who use it are getting better at filtering out spam. This is good since it makes it easier for engaging emails to get through — but without a strong focus on deliverability, sometimes even quality, permission-based emails can get filtered out of your subscriber's inboxes.

According to **Return Path's Deliverability Benchmark Report 2015**, worldwide, 21% of permission-based emails get sent to a spam folder or go missing. This means that for every five emails you send, one of them never reaches your subscriber.

Spam filtering and subscriber engagement are critical factors in the decline in inbox placement rates, which decreased by 4% since 2014, with significant declines for US and Canadian businesses.

In this section, we review what drives modern email deliverability and show how the best practices of engaging email can improve your deliverability.



Return Path Deliverability Benchmark Report 2015

EMAIL DELIVERABILITY

Your Reputation as a Sender Is Crucial

Email deliverability is more and more about your reputation as a sender and less about the actual content of your emails. This does not mean that content is not important, but it does mean that marketers need to give plenty of attention to how their emails are being delivered.

When it comes to modern email delivery, it's good to know the fundamentals.

Algorithmic Filters

Most email applications use algorithms to compare all incoming emails to those marked as junk. Any email with a similar sender, links, or content is more likely to be considered spam. But the analyzing doesn't stop there: The subscriber's internet service provider (ISP) remembers the URLs and domains in the spam. If those URLs and domains are reported, then any other email containing them has a harder time getting through to the recipient — even if it's from a completely different sender.

Spam Traps

A spam trap is an inactive, deliverable email address owned by an ISP to catch spammy senders. So, you want to be scrupulous about your email list building and email sends or you could severely hurt your deliverability and sender reputation. Worse, your IP address could be put on a blacklist, an online database of spammy senders. And once your IP address is on a blacklist, it'll be even more difficult to get your emails delivered.

If you're not a spammer, you're probably thinking that you don't have to worry about spam traps. But it can be all too easy to end up with spam trap email addresses on your contact lists if you're not using secure opt-in techniques, or if you're buying or borrowing email lists from unsavory sources.

> "More than 80% of all delivery issues arise because of a problem with your sending reputation."
>
> **– George Bilbrey,**
> **President of Return Path**

EMAIL DELIVERABILITY

Blacklists

Blacklisting is a process of actively monitoring the Internet for reports of senders sending unsolicited commercial email, and then publicly listing that information on Internet sites for others to reference as a measure to fight spam. Many ISPs and independent organizations use these blacklists as a reference filter applied to their inbound mail servers to aid in preventing spam, and to encourage internet security.

Bounce Handling

ISP and email receiving systems are moving away from standard email address validation more and more by using their own custom bounce codes. Modern email marketing service providers need to know what all the different new bounce codes mean so they can properly process soft and hard bounces while giving senders the visibility they need to manage their email campaigns.

Shared or Dedicated IP

If you are a low-volume sender, a shared IP address might suffice, but if you are a high volume sender, a dedicated IP is usually best (assuming you are a “good” sender).

Authentication Protocols

Use protocols to help email receivers separate legitimate messages from spam and malware, so less false-positive filtering occurs. The most common email authentication protocols are DKIM (DomainKeys Identified Mail), SPF (Sender Protection Framework), and SenderID.

Receiver and ISP Relations

Your email provider should be able to handle relationships with ISPs and receivers, especially if your legitimate emails are getting marked as false-positive spam.

Marketo®

EMAIL DELIVERABILITY

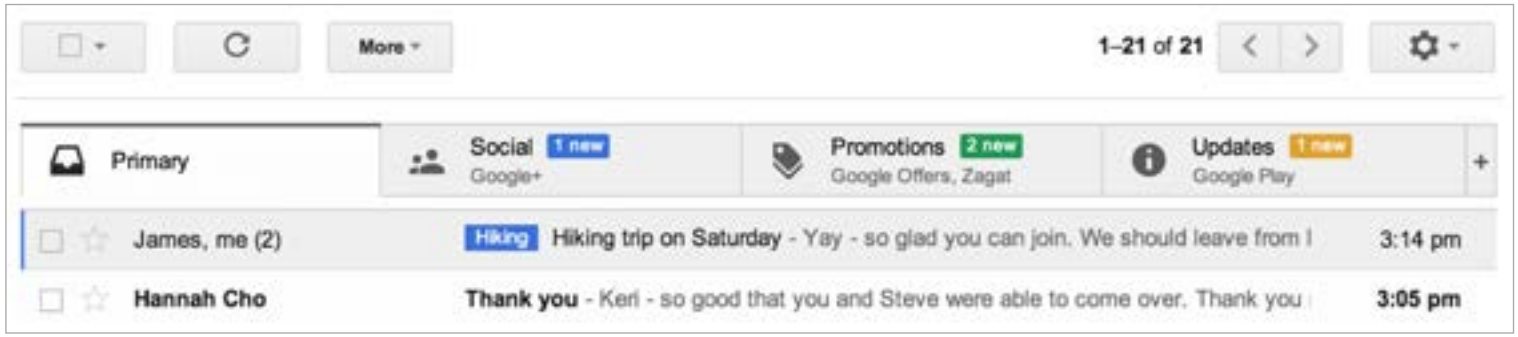
Gmail's Tabbed Inbox?

Gmail's new tabbed inbox automatically filters incoming email into one of several "buckets" (tabs) – primary, social, promotions, updates, and forums:

1. **Primary** – Email from your family and friends, as well as other messages not classified as bulk (one to many). Also, any message that does not fit nicely into the other tabs will fall here.
2. **Social** – Email from social media networks such as Facebook, LinkedIn, Twitter, Google+, and so on.
3. **Promotions** – Email marketing messages from companies, brands, and individuals – any messages that are sent from an email service provider and/or marketing automation company as well as any "mass" (bulk) mailings will probably land in this tab.
4. **Updates** – Email from blog commenting services, confirmation/transactional emails, Google calendar reminders, and other "updates." Note: Sometimes "promotional" emails will end up here as well.
5. **Forums** – Email from any listservs or other "groups" (forums) you are part of.

There's been lots of discussion about what this means for email marketers ("does the new Promotions tab kill email marketing?"). We think not. But it means that the themes of the guide become more important than ever. If you send timely, relevant, engaging, valuable, human emails to people who want them, the Gmail changes will have little impact.

This is because if someone wants your email, they'll find it. And if they know your emails are consistently valuable and/or enjoyable, they'll open them – even if they're sitting next to a bunch of other, less engaging emails.



EMAIL DELIVERABILITY

Engagement Matters to Deliverability

How your recipients engage with your emails is a major factor in future deliverability. Engagement data is a prominent measure of deliverability at some of the major ISPs. Big league email providers, such as Yahoo!, Gmail, Hotmail, and Outlook, have made it clear that they analyze which emails their users open and click through to gauge whether emails from a particular sender are spam. If users are not opening and clicking certain emails, to the spam folder they eventually go.

Yahoo! has acknowledged that as it more precisely analyzes user behavior to weed out spam, some genuine senders might find themselves facing deliverability challenges. And due to smarter spam filtering algorithms and features like Gmail's category tabs, your emails may not even make it to your recipient's primary inbox if they are not engaging them.

This is why engagement matters even for deliverability.

Consumers use the spam button to tattletale on companies that send unwanted emails, even if they initially opted in to receive them. If recipients don't want or expect your emails, they are more likely to mark them as spam. Disturbingly, Return Path reports that recipients are more likely to tag your email as spam than to simply unsubscribe, even if your "unsubscribe" link is conspicuous.

EMAIL DELIVERABILITY

Content still matters

We haven't yet talked much about the actual content of your emails. This is not because content is meaningless; it's just that reputation and engagement matter more. However, if you find that your emails are landing in junk boxes, despite your adherence to all the deliverability best practices we've mentioned, then it's probably time to review your content.

Trigger Words

The rules of content are ever-changing. It used to be that if your emails included certain "trigger" words, such as "free," there was a pretty good chance they would never reach the inbox. Today, however, those once-forbidden words no longer cause email marketing messages to get blocked.

Here's the best advice we can give you for determining what not to do with content: **Look at the emails in your own spam folder, and don't do what those guys are doing!**

Check Your Content

You can use a spam content check tool, such as Marketo's Email Deliverability Power Pack solution, to get a sense of whether or not your email content is "spammy" and make sure your content isn't inadvertently raising red flags with ISPs or email clients.

Screenshot: Marketo Email Deliverability Power Pack

EMAIL DELIVERABILITY

Deliverability: a Partnership between Email Provider and Sender

With all the issues surrounding deliverability of your marketing emails, you can see how important it is for a sender (that's you) to work closely with a provider (your email marketing service) to make sure sent emails are getting through to recipients. Deliverability is a shared responsibility. Here's how it breaks down:

The Provider's Responsibility

1. Your provider is responsible for making sure its email technology is up-to-date and compliant with today's legal requirements. This means it must optimize the back-end of its delivery platform for reduced friction with corporate filtering systems. A good provider must also cultivate good relationships with receivers by applying proactive issue resolutions, feedback loops, and whitelisting practices.
2. A modern email marketing service provider will allow you to segment your contact lists into sub-lists so that you can target specific customers with specific messages. This is essential to keeping your audience engaged with relevant content and making sure the right person gets the right message at the right time.

The Sender's Responsibility

1. As a sender, you must keep your lists clean, take the time to understand your audience, and craft carefully-targeted messages that are relevant to specific subscriber sub-lists.
2. You are ultimately responsible for what you send and to whom it's sent. Corporate email systems keep a close eye on how the subscribers under their watch are interacting with your emails. They score you based on your engagement levels, so you want your subscribers to open, click, forward, save, and print on a steady basis. If your subscribers are ignoring you, you are in danger of being blacklisted.
3. If you send relevant messages to a willing opt-in list, you'll build a good deliverability reputation; if you don't, your reputation will suffer.

EMAIL DELIVERABILITY

Seven Best Practices for Deliverability

Take the following proactive steps to give your emails the best chance of hitting the inbox:

1. **Follow the trust and engagement mantra.**
   Give your subscribers a good reason to opt in and set clear expectations about what's to come. Then, follow through on your promises with timely, targeted, valuable emails.

2. **Use responsible methods to build your lists.**
   Verify all new email addresses before sending your messages, and regularly scrub your contact lists to remove inactive addresses.

3. **Choose a solid email marketing service provider.**
   Make sure the vendor you choose is sophisticated enough to handle bounce codes, feedback loops, and connection optimization.

4. **Create engaging content.**
   On its own, bad content won't prevent your emails from being delivered, but if your content is boring or irrelevant, people won't engage with it or, worse, will mark your emails as spam.

5. **Manage your complaint rate.**
   If your email marketing service warns you that complaints made against you are high, take the warning seriously. Set up an email address — abuse@your-domain.com — that a representative of your email marketing service or an anti-spam organization can use to contact you with any complaints. Register that email address with www.abuse.net, an anti-spam advocacy group and resource center, to show anti-spam organizations that you are responsible and that you've given thought to the email abuse issue.

6. **Be proactive about closely monitoring your reputation metrics.**
   Get your email reputation score to learn what you need to change about your program in order to improve your reputation and your inbox placement rates. Return Path, a leader in email intelligence, offers a product called Sender Score, which, in addition to providing you with your reputation score, shows you how your email marketing program stacks up against your competitors'. Sender Score's proprietary algorithm ranks a sending IP address on scale of 0 to 100, where 0 is the worst score and 100 is the best. Ranking is based on factors such as complaints against you, volume of your emails, your external reputation, number of unknown users, and amount of rejected emails. Another reputation monitoring option is SenderBase. Part of the Cisco IronPort SenderBase Security Network, SenderBase rates your IP as good (little-to-no threat activity), neutral (within acceptable parameters), or poor (showing a problematic level of threat activity).

7. **Be transparent.**
   Let your subscribers and potential subscribers know how you're doing when it comes to complaint rates, bounces rates, and your Sender Score rank. Here's how Marketo presents this data to give our clients confidence that their emails are getting delivered. For more on this, see Marketo's Trust page. (marketo.com/trust)

	Trusted IPs		All IPs	
Month	**Cisco SenderBase** Good/Neutral/ Poor	**Return Path Sender Score** 0 to 100	**Cisco SenderBase** Good/Neutral/ Poor	**Return Path Sender Score** 0 to 100
June 2013	Good	99	Good	97
May 2013	Good	99	Good	96
April 2013	Good	99	Good	96
March 2013	Good	99	Good	98
February 2013	Good	99	Good	95
January 2013	Good	99	Good	95
December 2012	Good	98	Good	95

LEGAL ISSUES

Being a law-abiding email marketer is a big part of establishing trust, not just with your audience but also with ISPs and other companies.

With email marketing, the "country of reception" principle usually applies. This means the law of the country of the recipient of an email applies, even if you (the sender) are situated abroad. This makes it important to understand the nuances of each country you market in. Wikipedia has a big list of Email Spam Legislation by Country.

This guide is not meant to be a legal document, and we're not lawyers, so we can only give you an overview of legal compliance. Play it safe – be sure to consult with legal counsel or a member of your company's compliance team for specifics of the laws in your region.

United States

When it comes to the legalities of email marketing in the U.S., the Controlling the Assault of Non-solicited Pornography and Marketing Act of 2003 — also known as the CAN-SPAM Act — is the governing law. The CAN-SPAM Act, updated in 2008, makes it possible for spammers to be fined $11,000 per violation. Yes, that's right —$11K for sending one inappropriate email! Authentic marketers must stay on their toes to avoid using deceptive language in their email headers, subject lines, and from and reply-to addresses.

The following brief from the Bureau of Consumer Protection Business Center breaks down the law into seven main requirements for email marketers:

1. Don't use false or misleading header information.
2. Don't use deceptive subject lines.
3. Identify your messages as ads.
4. Tell recipients where you're located.
5. Tell recipients how to opt out of receiving future emails.
6. Honor opt-out requests promptly (within 10 days).
7. Monitor what others are doing on your behalf.

For more information, read the Bureau of Consumer Protection Business Center's full Compliance Guide, and the updates to the CAN-SPAM Act.

Australia

Here are the key requirements of the Spam Act of 2003:

- Consent - make sure you have consent to contact the recipient and can prove you have obtained it.
- Identify - include accurate information to identify yourself or your organisation as the authorised sender of the message.
- Unsubscribe - make sure your messages have a functional unsubscribe facility, so that recipients can unsubscribe at any time.

LEGAL ISSUES

Canada

Canada's anti-spam law, otherwise known as CASL, addresses a wide range of issues stemming from electronic communications to content and spyware. It is enforced by three different federal agencies: Canadian Radio-Television and Telecommunications Commission (CRTC), Competition Bureau, and Office of the Privacy Commissioner of Canada. And starting July 2017, individuals and organizations affected by a violation will be able to bring a private right of action in court against them.

CASL prohibits the following:

- Sending commercial electronic messages without the recipient's consent (permission). This includes sending messages to emails, on social media, and even by text.
- Altering transmission data in an electronic message that causes the message to be delivered to a different destination without express consent.
- Installing computer programs without the express consent of the owner of the computer system or its agent, such as an authorized employee.
- Using false or misleading representations online in the promotion of products or services.
- Collecting personal information by accessing a computer system in violation of federal law.
- Collecting electronic addresses using computer programs or using the addresses without permission (via address harvesting).

info@marketo.com
www.marketo.com

Contact Marketo:
+1.877.260.6586
sales@marketo.com