Learn

The ABCs of ISPs

SendGrid

Email deliverability is critical to the success of any email program.

One of the best ways to ensure your email gets delivered is by complying with guidelines set by Internet service providers (ISPs—also called mailbox providers) like Gmail, Yahoo!, and Outlook.

Learn

What's Inside

As email continues to evolve, it's important to follow the best practices that will help your email reach the inbox. At SendGrid, we communicate with ISPs to help us stay on top of issues that affect our clients' deliverability. In this guide, you'll learn how to get delivered at the major Internet service providers.

01

Overview

The Email Delivery Landscape is Ever Changing

As the email industry has grown more sophisticated, it's become congested by legitimate mailers who use email to communicate with their customers, but also by spammers who continue to invent ways to thwart mailbox providers.

According to *Mashable*, in 2012, over 144 billion emails were sent worldwide every day and 65% of those were spam **(figure 1)**.[1] Mailbox providers are doing an amazing job at keeping spam out, but with a problem this big, many times legitimate messages fail to get through. This is why it's important to understand the factors that affect delivery, and implement the best practices that can help mailbox providers identify good mail and keep out the bad. The ISPs' goal is to protect consumer inboxes from malicious email, not to stop your email from getting through.

As an aside...

Mailbox providers include ISPs and spam filtering solutions. We will use these terms interchangeably within this guide to include the entire group.

FIGURE 1 *Email statistics from Mashable*

01

The True Meaning of Undelivered Email Today

22% of commercial email never makes it to the inbox.[2] **Transactional email** is especially vulnerable—the 2012 Websense Threat Report revealed that 92% of spam contains a web link.[3] Transactional email tends to achieve higher deliverability, because it's more desired by customers. Unfortunately, it still falls victim to the same email traps and filters as commercial email, and the effect can be detrimental to any brand.

If email drives any of your revenue, you can quantify the impact of email not reaching the inbox. Even with softer goals like new user acquisition or engagement, you're missing out on a huge segment of potential users and customers.

According to our survey:

- **80.5%** rely on email for signups and subscriptions
- **76.5%** for password recovery and account changes
- **49.8%** for order and shipping confirmations
- **28%** use for friend/follower requests and confirmations

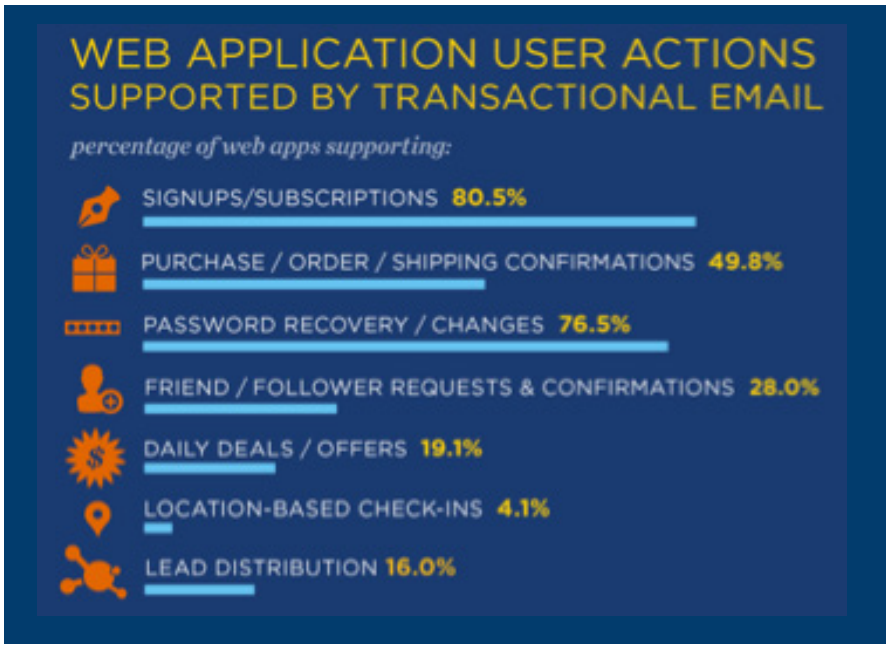


FIGURE 2

SendGrid: The Evolution of Transactional Email

For many companies, especially web apps, growing your user base is imperative for driving business and attracting more investors. Paying close attention and understanding how mailbox providers view your email is essential for the success of your email program.

02

Email Deliverability Strategies

Getting Delivered Starts with Your Reputation

Email deliverability is the total number of emails successfully delivered to the ISPs divided by the total number of emails sent. The higher your deliverability rate, the more emails make it to the inbox.

Email deliverability is influenced by a lot of factors, including signing your mail, keeping clean lists, sending wanted content, having a good sending reputation, and much more. Your sending reputation is how ISPs identify you as a legitimate sender. Every time you deploy an email campaign, you are providing them with valuable data that says whether or not you follow proper sending practices. There are two types of reputation—IP Reputation and Domain Reputation.

IP Reputation

Email is sent from IP addresses, which serve as unique identifiers of email streams. Some companies send from a shared IP, which means multiple companies use the same IP address to deploy their email. Senders with more volume usually opt to send from a dedicated IP address that belongs only to their organization. By using a dedicated IP, you can better control your IP reputation because you're not impacted by other senders' bad practices. At SendGrid, a dedicated IP address is offered with **all packages Silver and higher**.

Domain Reputation

Your domain reputation is based on your sending *domain* instead of your IP address. This means that your *brand* takes precedence when it comes to ISP filtering decisions.

There has been a sharp move towards domain reputation predicated by the move from IPV4 networks to IPV6 networks. While it's not yet common practice to use domain reputation, required under IPV6 (though Gmail is already the strongest proponent), the ISPs are starting to use the combination of IP and domain reputation until IPV6 is fully adopted.

(Continued on next page)

02

The idea of “portable reputation” is very appealing to senders who want the flexibility to add new IPs, move IPs, or change email service providers (ESPs) without losing the good reputation they’ve already built from their sending activity. Domain reputation also eliminates the need to warm up new IPs since ISPs use the reputation of the entire domain as their filtering metric. (With IP reputation, you lose all reputation history and data when you change IPs or ESPs.) As a result, new protocols have been developed to help facilitate domain reputation as the next frontier for filtering.

Most importantly, with domain reputation, you can’t change an IP address to fix reputation problems. Email sending mistakes can now affect your domain reputation and your brand in a bigger way than it ever has before. This is why it’s so important to have good sending practices.

Authentication

To help safeguard your reputation, senders should start with email authentication. Authentication helps ISPs identify which IPs and domains rightfully belong to you. Here’s how it works **(figure 3).**

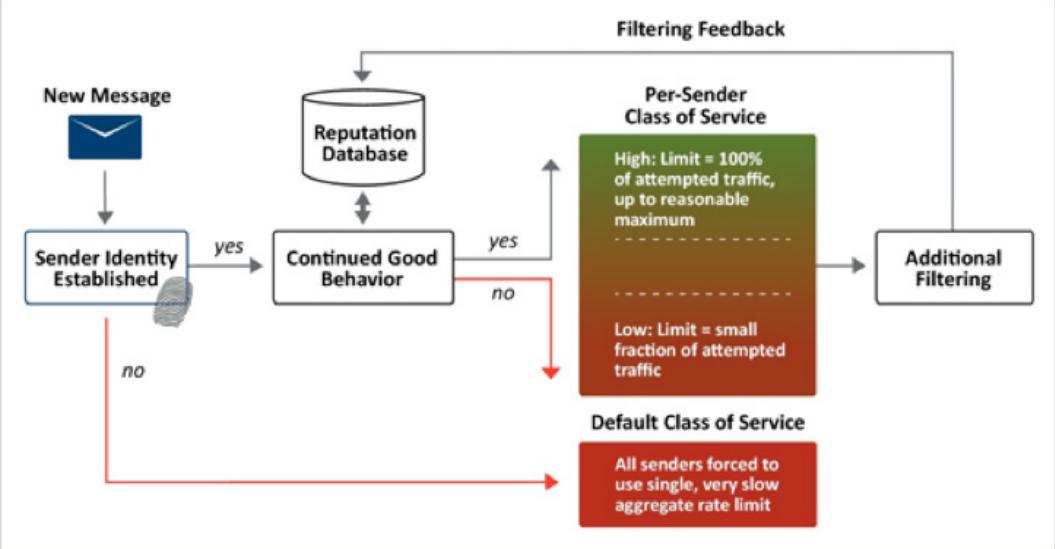


FIGURE 3 *How email authentication works courtesy of Cloudmark, a provider of tools and services that protect against messaging abuse.*[4]

02

There are several authentication methodologies the **Messaging Anti-Abuse Working Group** suggests you implement:

> *Senders should incorporate as many authentication standards and technologies as their systems can support for each of their messaging streams: Transactional, Marketing, and Corporate. These standards can range from mechanisms that help identify mailers by linking IPs to domains (Sender Policy Framework, known as SPF, and Sender ID) to more complicated cryptographic technologies like Domain Keys Identified Mail (DKIM).*[5]

DKIM and SPF are imperative in tracking reputation, but **Domain-Based Message Authentication, Reporting, & Conformance** (DMARC) is the next evolution of email authentication. DMARC allows email senders to specify how ISPs should treat emails that have not been authenticated using SPF or DKIM. Senders can opt to send those emails to the junk folder or block them all together. ISPs can then better identify spammers and prevent malicious email from invading consumer inboxes, while minimizing false positives and providing better authentication reporting for greater transparency in the marketplace. To learn more about DMARC compliance, **read our blog post on the topic here**.

Recommended Reading

Learn more about how to authenticate your email and the different authentication methods by **downloading the SendGrid Email Infrastructure Guide**.

02

Consistent Delivery = Sending + Engagement

Mailbox providers use a series of reputation and engagement metrics to determine email deliverability. By understanding all of these factors, you can better influence the outcome of your email program.

Reputation Metrics

Each ISP makes filtering decisions based on a series of reputation metrics. While thresholds vary by ISP, it's important to know that each time you deploy messages to your email list, your reputation is impacted. Three key factors that will affect your reputation include:

Spam Complaint Rate

This is the percentage of subscribers who have reported your email as spam. A high complaint rate is the number one factor used by ISPs to determine whether or not to deliver your email messages. If too many people are flagging your mail as spam, ISPs will take action to block your messages.

Unknown Users

This is the number of emails on your list that are non-existent email addresses, which bounce back messages. Common reasons for this include misspelled emails and full inboxes. If an email address has bounced more than once, you should remove the address from your list.

Spam Traps

This is the number of messages sent to email addresses set up specifically to catch spammers. Spam traps (or "honey pots") often appear if you have poor email acquisition practices or if your email list is too old. ISPs set up specific accounts or often reclaim accounts with no activity and monitor the messages that are sent to those inboxes. Since these addresses will never open or click on your messages, it's important to practice good list hygiene and proactively remove non-engaging addresses.

02

Engagement Metrics

ISPs consistently enhance filtering algorithms by adding metrics to identify legitimate email. There is a new focus on email engagement that evaluates whether your users are actually interacting with your messages.

Many ISPs now look at customer activity to determine whether or not to deliver email. ISPs often use custom algorithms to measure engagement, but common metrics may include the following:

Open Rate

This measures how many subscribers "looked at" your email. However, the only way this metric is counted is if the images included in the message are downloaded. However, many subscribers have images automatically turned off, so despite viewing your message, they will not be counted in the open rate.

Clicks

This is the number of subscribers who clicked on one or more links in your email message.

TiNs Data

This is collected when users actively click a button that says "This is Not Spam." It shows that users want your email and will help improve your reputation **(figure 4)**.

FIGURE 4 *Courtesy of www.webdevelopersnotes.com*

02

Saving to Folders

Retaining email by moving it from the inbox to another primary folder is a sign of engagement. Negative engagement would be mass deleting or a user taking no action.

Panel Data

A panel of users who determine whether email messages have been correctly marked as spam based on criteria specified by the email providers.

Trusted Reporter Data

Compiled accounts that have proven to be real users who demonstrate normal behavior when interacting with their email messages.

Inactive Accounts

Mailboxes that do not have regular activity.

Recent Interaction

The number of users who have interacted within a specific period of time demonstrates the value of your offer.[6]

Engagement Tip: Get Rid of the "No Reply."

Let customers reply directly to your email. Your goal is to stimulate a two-way conversation with your user. Using "no reply" in your from address can elicit a negative response from your customer. So, send your emails from an email address that can be regularly monitored for responses.

To do that, use the **SendGrid Parse Webhook** to extract data from your emails and send responsive emails to your customers. For example, offer your users a 15% discount if they reply to your email. When they respond, an automatic message can be sent with a discount code.

03

Email Deliverability Tools

Your Reputation Is Always In Your Control

The anti-abuse community is fairly small, and they communicate regularly. So, word will get around very quickly if you make an effort to do the right thing. On the flip side, bad deeds will not go unpunished. Your reputation is always in your control, but you first have to understand where you stand. Here are several resources for checking your sending reputation:

SenderScore.org

Like a credit score, a Sender Score is a measure of your reputation. Scores are calculated from 0 to 100. The higher your score, the better your reputation and the higher your email deliverability rate. Numbers are calculated on a rolling 30-day average and illustrate where your IP address ranks against other IP addresses. This service is provided by Return Path.

Senderbase.org

Senderbase is a product of Cisco and provides you with the tools to check your reputation by ranking you as Good, Neutral, or Poor. Good means there is little or no threat activity. Neutral means your IP address or domain is within acceptable parameters, but may still be filtered or blocked. Poor means there is a problematic level of threat activity and you are likely to be filtered or blocked.

BarracudaCentral

Barracuda Networks provides both an IP and domain reputation lookup via their Barracuda Reputation System; a real-time database of IP addresses with “poor” or “good” reputations.

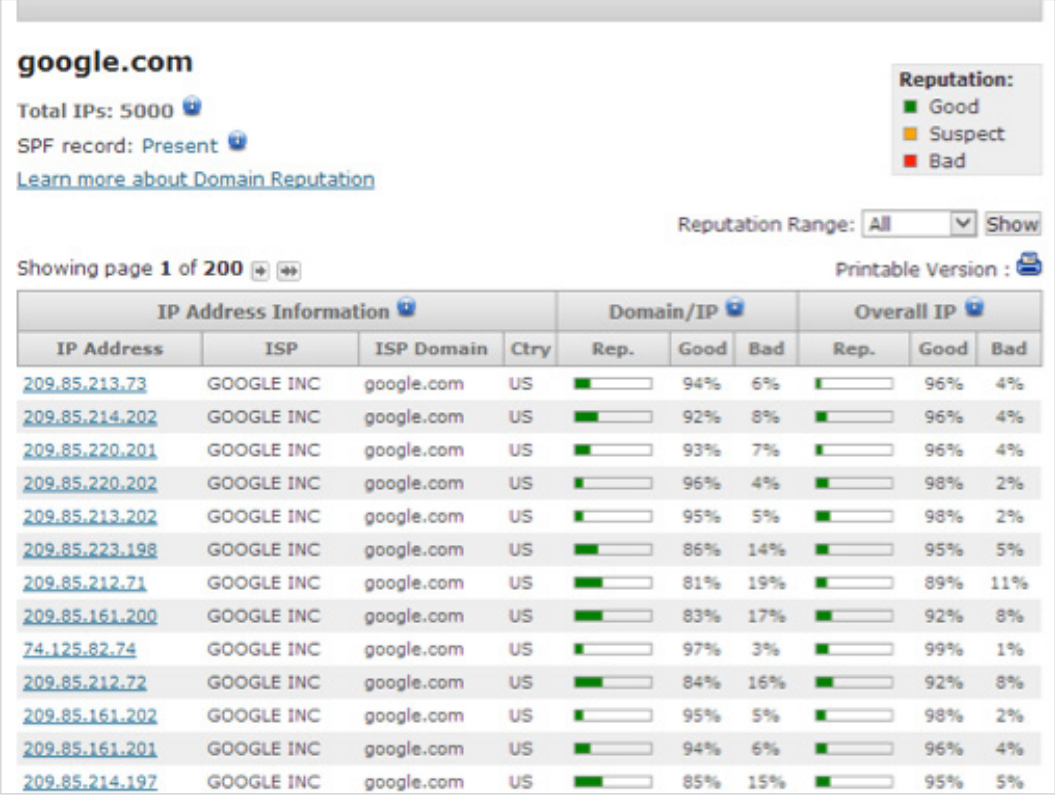
TrustedSource

TrustedSource is a site very similar to **senderbase.org**, but run by McAfee. It provides information on both your domain’s email and web reputations as well as affiliations, domain name system (DNS), and mail server information. It also provides details on the history, activation, and associations of your domain.

03

ReputationAuthority

WatchGuard's ReputationAuthority helps protect business and government organizations from unwanted email and web traffic that contain spam, malware, spyware, malicious code, and phishing attacks. You can look up your IP address or domain, receive a reputation score from 0-100, and get the percentage of emails that were good versus bad **(figure 5)**.



google.com

Total IPs: 5000

SPF record: Present

Learn more about Domain Reputation

Reputation:
- Good
- Suspect
- Bad

Reputation Range: All Show

Showing page **1** of **200**

Printable Version :

IP Address Information				Domain/IP			Overall IP		
IP Address	ISP	ISP Domain	Ctry	Rep.	Good	Bad	Rep.	Good	Bad
209.85.213.73	GOOGLE INC	google.com	US		94%	6%		96%	4%
209.85.214.202	GOOGLE INC	google.com	US		92%	8%		96%	4%
209.85.220.201	GOOGLE INC	google.com	US		93%	7%		96%	4%
209.85.220.202	GOOGLE INC	google.com	US		96%	4%		98%	2%
209.85.213.202	GOOGLE INC	google.com	US		95%	5%		98%	2%
209.85.223.198	GOOGLE INC	google.com	US		86%	14%		95%	5%
209.85.212.71	GOOGLE INC	google.com	US		81%	19%		89%	11%
209.85.161.200	GOOGLE INC	google.com	US		83%	17%		92%	8%
74.125.82.74	GOOGLE INC	google.com	US		97%	3%		99%	1%
209.85.212.72	GOOGLE INC	google.com	US		84%	16%		92%	8%
209.85.161.202	GOOGLE INC	google.com	US		95%	5%		98%	2%
209.85.161.201	GOOGLE INC	google.com	US		94%	6%		96%	4%
209.85.214.197	GOOGLE INC	google.com	US		85%	15%		95%	5%

FIGURE 5 *IP lookup for ReputationAuthority*

03

You Can Always Fix Your Reputation

Another way to check your reputation is to find out if you are on any blacklists (a.k.a. blocklist). Blacklists contain lists of IPs or domains that pose a threat to consumer inboxes. Your email service provider may automatically alert you if you're added to one, but it's good to check for yourself. If you are on a blacklist, act quickly. Just a few spam complaints can add a legitimate sender to a blacklist.

There are many blacklists, but you should check to see if your IPs or domains are on any of these popular lists:

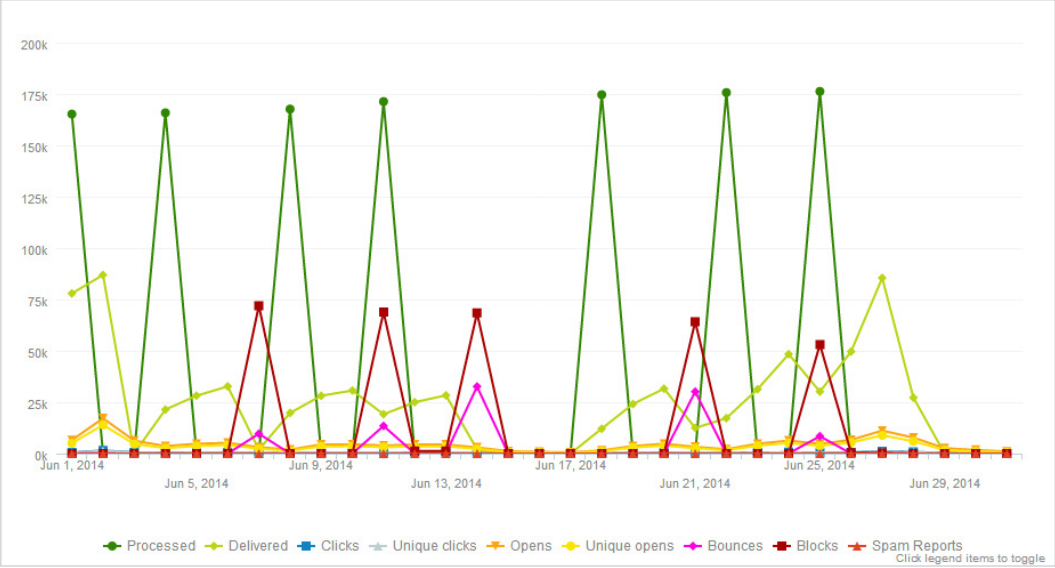


FIGURE 6 *Image of SendGrid user who was blocked*

Barracuda Reputation Block List

BRBL is a free DNS blacklist (DNSBL) of IP addresses known to send spam.

Invaluement

The Invaluement anti-spam DNSBL blocks elusive types of spam where the sender is sending unsolicited bulk email and escaping traditional detection methods.

03

MXToolBox

MXToolbox shows you whether or not your domain or IP address is blacklisted and can perform checks on your DNS to see how it is configured.

MultiRBL

This free multiple DNS Blacklist service cross-references other blacklists by IPV4, IPV6, or domain.

SpamCop

The SpamCop Blocking List (SCBL) lists IP addresses that had mail reported as spam by SpamCop users.

Spamhaus

The Spamhaus Project maintains a number of DNSBLs as part of their effort to identify and track spam sources, and provide anti-spam protection. To be removed from this list, visit their **blacklist removal center**.

SURBL

Unlike most lists, SURBLs are not lists of message senders. SURBLs are lists of websites that have appeared in unsolicited messages.

Tools to help you earn the reputation you deserve.

It can be time consuming to stay on top of your reputation and monitor your presence on blacklists, which is why it can be good to find a tool that offers blacklist alerts and gives you insight into delivery failures so you can resolve issues. SendGrid has plans that include a dedicated technical account manager who monitors blacklists on behalf of our customers. To learn more about them, **visit our Pricing Page**.

03

ISP Tools to Help Manage Deliverability

Feedback loops are provided by mailbox providers and ISPs to alert senders if messages are reported as spam. Below is a list of ISP postmaster pages and feedback loops, with links to each (where applicable), to help you register your IP or domain.

Postmaster	Feedback Loop
AOL	
AT&T	
BlueTie/Excite	
Comcast	
Cox	
Earthlink	
Fastmail	
Gmail*	
OpenSRS (Tucows)	
Outlook (Hotmail)	
Rackspace	
RoadRunner (TWC)	
Synacor	
USA.net	
United Online/Juno/Netzero	
Verizon.net	
Yahoo!	
Zoho.com	

Note: SendGrid automatically registers its customers for all ISPs that offer feedback loops.

*Gmail has a feedback loop that is only available for ESPs who are MAAWG members and are approved by Google as good senders.

04

Email Deliverability Tactics

Email Delivery Differentiators by ISP

Worldwide, the number of mailboxes is predicted to reach 4.1 billion by the end of 2015.[7] Yahoo!, Outlook (formerly Hotmail), and Gmail make up the top three ISPs and are likely your primary concern, but other ISPs are also important.

While the makeup of your email list will determine where you focus your efforts, following best practices will get you delivered at practically any ISP. Weighting of delivery criteria varies, filtering algorithms change often, and specific thresholds for each ISP are not publicly available. But remember, best practices are universal. To give you a head start, here are a few tactics from some of the most popular ISPs to help you achieve optimum email deliverability at their mailboxes.

Caution! This doesn't mean that you can forgo one best practice over another. It simply means that one ISP might put greater emphasis on certain practices when delivering mail than another. Following all best practices available to you is the best way to make it to the inbox at any ISP.

AOL

- Sign up for the AOL Feedback Loop.
- Authenticate your email with DKIM.
- Apply for the AOL whitelist.
- Monitor your IP status **http://postmaster.aol.com/Reputation.php**

AT&T

- Separate large quantities of email into sections and deliver at periodic intervals.
- Don't send email from an IP address where the sender's identity changes often.
- Include proper header information on all email messages.

Comcast

- Sign up for Comcast Feedback Loop.
- Stay off of blacklists, monitor abuse accounts, and treat attacks seriously.
- Avoid dynamic IPs.
- Review error messages sent by Comcast.
- Watch your sending limits which are determined by SenderScore.

04

Gmail

» Get added to user contact lists.
» Authenticate your mail with DKIM. Gmail is the biggest proponent of domain reputation.
» Include a “List-Unsubscribe” header.
» Watch your engagement levels.
» Spam communication: Gmail provides a message about why your email was filed as spam.

Outlook.com (Hotmail)

» Join the Junk Email Reporting Program.
» Access the Smart Network Data Services program.
» Watch your engagement levels.
» Apply for Yahoo’s Bulk Sender Program.

Time Warner Cable (Road Runner)

» Avoid dynamic IPs. Dynamic IP addresses change from time to time making it difficult for you to maintain your IP reputation and for ISPs to know who you are.
» Handle your bounces, especially ones that tell you that the address does not exist.
» Separate your marketing and transactional email streams.
» Maintain a consistent identity when sending by using the same email address and domain.

Yahoo!

» Sign up for Yahoo! Mail Feedback Loops.
» Authenticate your mail with DKIM.
» Include a “List-Unsubscribe” header.
» Watch your engagement levels.
» Send from the same email address.

04

Email Deliverability Results

Getting In Means Staying Out

There are many things you can control when it comes to your email reputation. Paying attention to the signs and maintaining list integrity will go a long way in keeping you out of the spam folder and earning you the results you want.

Pay Attention to the Signs

Focus on negative engagement

Concentrate on building an active audience by monitoring your response rates. If your response rates are good one month, then suddenly drop, analyze the problem and make adjustments. Mailbox providers are looking at engagement data to determine deliverability.

View your statistics by ISP

In addition to segmenting your list by demographics, purchasing behavior, or other criteria, try viewing your statistics by ISP to identify specific problems. For instance, if your Yahoo! open rates drop significantly, determine whether you are bulking, or if your subscribers have lost interest. If Gmail is performing better than Yahoo!, identify the differences and adjust accordingly.

Watch out for email fatigue

Sending too much email to your users can drive high unsubscribe and/or complaint rates. Offer a **preference center** so that users can control the flow of their email. Consider your email cadence and focus on relevancy.

Monitor abuse@ emails

Users may be informing you of spam or phished mail coming from your domain so monitor your abuse@ emails diligently. Alternatively, users may reply to your email with complaints or unsubscribe requests providing a first clue that an email campaign is not being well received.

05

Maintain High List Integrity

Remove role account emails

Remove info@ or admin@ emails from your email file. These role accounts are usually not individual users, so they should not be mailed to. If you can, automatically exclude them from your list, or ask users to provide a personal or business email address. (SendGrid can provide a list of common role accounts. There are about 30 common accounts.)

Create a sunset policy

Proactively eliminate users who have not logged into their account or clicked on an email in the last three months. Unused or dormant addresses may be spam traps that can hurt your reputation, so it's best to remove non-responders frequently. Alternatively, send out a reconfirmation or win-back email campaign to see if they want to remain on your list.

FIGURE 7 *Reconfirmation email from Lands' End requesting that the user confirm their email preferences.*

05

Stop buying lists

Buying emails from third-party email lists (even Jigsaw) often have bad email addresses and yield high complaint rates. We know that marketers have to grow their email lists and often purchase email addresses, however, we strongly discourage this practice and recommend a more targeted approach. Just one spam trap mistake can impact your domain reputation.

Don't share your lists

Sharing email addresses with other parties reduces trust with your company. Even if you disclose sharing in your privacy policy, recipients don't always expect this email, and will mark it as spam.

Don't hide the "unsubscribe"

Make it easy for recipients to remove themselves from your list. It's always better for subscribers to opt-out than reporting your email as spam.

The Inbox is Your Ultimate Reward

Here are the five strategic takeaways that should guide your email strategy to make sure you get to the inbox every time:

- Send the right email at the right time to the right person at the right frequency.
- Focus on quality over quantity.
- Send relevant content and monitor your email deliverability.
- If there is a problem, or you make a mistake, fix it fast.
- Listen to customers by monitoring engagement.

Get to Know SendGrid

SendGrid helps you focus on your business without the cost and complexity of owning and maintaining an email infrastructure. We manage all the technical details, from scaling the infrastructure, to ISP outreach and reputation monitoring, to whitelist services and real-time analytics. We offer world-class deliverability expertise to make sure your emails get delivered, and handle ISP monitoring, DKIM, domain keys, SPF, feedback loops, whitelabeling, link customization, and more. To learn more, visit **www.sendgrid.com**.

Learn More

Read Our Customer Success Stories

Sign Up

Sources

1. "Did You Know 144.8 Billion Emails Are Sent Every Day." *Mashable.* BrandSpeak. 27 Nov. 2012. http://mashable.com/2012/11/27/email-stats-infographic/

2. "Email Intelligence Report: Placement Benchmarks 2013." *Return Path.* 29 Jan. 2013. http://landing.returnpath.com/placement-benchmarks-2013

3. "2012 Websense Threat Report." *Websense.* 2012. http://www.websense.com/content/websense-2012-threat-report-download.aspx

4. Bujack, Michal. "SMTP Abuse Prevention in IPv6 Networks Positive Reputation Class of Service Method." *Cloudmark.* June 2012. http://www.cloudmark.com/en/whitepapers/smtp-abuse-prevention-in-ipv6-networks http://www.cloudmark.com/releases/docs/whitepapers/SMTP_Abuse_Prevention_in_IPv6_Networks_v01.pdf

5. "MAAWG Sender Best Communications Practices Executive Summary and MAAWG Sender Best Communications Practices." *Version 2. Messaging Anti-Abuse Working Group.* Sept.2011. http://www.maawg.org/sites/maawg/files/news/MAAWG_Senders_BCP_Ver2a-updated.pdf

6. "Email Engagement: Often Talked About, Never Defined." *DMA Email Marketing Council.* February 2013. http://dmaemailblog.com/wp-content/uploads/2013/02/EngagementDiscussionPaper.pdf

7. Radacati, Sara and Hoang, Quoc. "Email Statistics Report, 2011-2015." *The Radicati Group, Inc.* May 2011. http://www.radicati.com/wp/wp-content/uploads/2011/05/Email-Statistics-Report-2011-2015-Executive-Summary.pdf