Amazon Simple Email Service
Email Sending Best Practices

July 2012

(This paper isn't maintained. Please see
http://docs.aws.amazon.com/ses/latest/DeveloperGuide/best-practices.html
for the latest information.)

Contents

Abstract

Getting your email into your targets' inboxes can sometimes seem challenging. A number of different factors, including your content, your list quality, and the infrastructure between you, the sender, and your target recipient, can influence email delivery. This paper discusses these factors and provides many best practices and recommendations that will enhance the probability of your email reaching its target.

Introduction

You might send email for a variety of reasons, including enhancing an existing relationship with a customer, marketing new products and offers, educating a group of people sharing a common interest, or notifying customers of an event. Some examples include:

- Newsletters (e.g., recipe of the month club digests)
- Receipts (e.g., purchase confirmations)
- Travel itineraries (e.g., airline tickets)
- Account notifications (e.g., password resets)
- Legal notices (e.g., changes in privacy policy)

How you manage the electronic communication with your recipients through email can be called your *email program*.

To run a successful email program, you must be aware of a few topics that can affect your delivery and ultimately your impact on email recipients. We'll start by discussing the value attributed to your email by your recipients and the Internet Service Providers (ISPs) responsible for protecting their inboxes. Then we'll explain what the emailing process looks like, who's involved, and what their roles are. Finally, you'll learn how to optimize value and drive it up based on some best practices we've compiled.

By the time you finish reading this, you should have many of the tools you need to make your email program a success!

How Email Gets Delivered

Have you ever thought about how and why email gets delivered? *Deliverability* refers to the likelihood that an email message you send will actually arrive at its intended destination. Emails don't always make it to the intended recipient's inbox. They can be delivered to the *junk folder* (sometimes referred to as the *spam folder*), rejected by the receiver's email infrastructure (usually in the form of a *bounce*), or disappear altogether (for example, when the receiving system drops the message without informing the sender or recipient). Some ISPs have even created default folders based on user engagement to help recipients better organize their messages, and email will be delivered to these folders, rather than the inbox itself.

As an email sender, you want as many messages as possible to be delivered to your recipients' inboxes. The best way to improve delivery is to send high-quality email; that is, email that recipients find valuable. Email recipients only want your email if they can extract value from the message. That value can come in many forms, such as offers, order

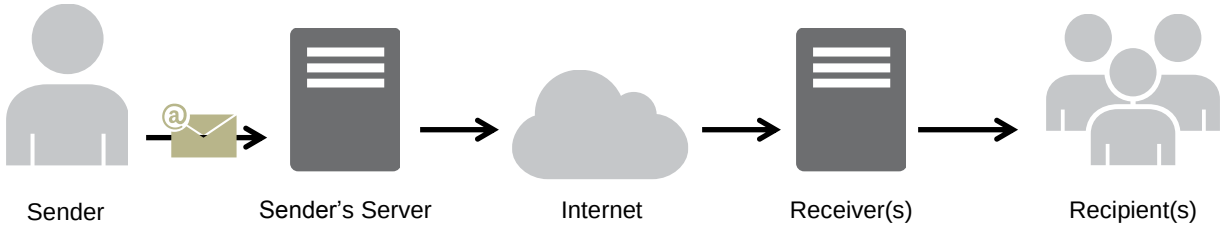
confirmations, sweepstakes notifications, or even social network communications. Value, of course, is a loaded word, since different things make email messages valuable to different people.

Email quality equals value to the email recipient. Despite its subjectivity, ISPs try to predict email quality as accurately as possible using a variety of metrics to gauge whether a message is wanted (and thus valuable) or is not wanted (and thus considered spam). These metrics include various internal computations based on anti-spam technology and recipient inputs that ISPs attempt to quantify.

You, as the sender, build trust with a *receiver* (whomever or whatever is behind the address you're sending to) by sending high quality email over time. This trust is referred to in the industry as *reputation.* Receivers use metrics to assess the value of a sender's email. These metrics are often combined into scores, and are typically referred to as a sender's reputation.

Email Flow

The diagram below depicts the entities involved in sending and receiving email.



Email Receivers and Email Delivery

Email receivers decide whether your email gets delivered. They comprise the entire federation of network systems, software, and policies that manage email delivery. There are several different classes of email receivers, and you must know the class of receiver you're sending to in order to ensure that you're optimizing your email program for deliverability.

Internet Service Providers

An ISP (Internet Service Provider) usually hosts email services for subscribers. Typically, B2C (business to consumer) emails are sent to addresses hosted at ISPs. Sites like Yahoo!, Gmail, and Comcast fall under this category. These large providers make decisions across millions of mailboxes about whether your email is spam, and they base these decisions on many recipients' feedback.

Most often, this feedback comes in the form of a complaint – when a recipient marks a message as spam in their email client – but it can also include whether recipients are opening or clicking on your email. The amount of recipient feedback at an ISP's disposal for reputation calculations is usually vast, but ISPs tend to implement a "one size fits all" reputation system that they can easily roll out across all mailboxes.

Corporate Systems

A corporate system usually refers to the independently-hosted email system used by employees, students, governmental agencies, or certain paid or non-profit associations. This system is commonly referred to as a B2B (business to business) system. A corporate system also can include the hosted email services that ISPs offer to run inbound email systems. Often the rules for spam prevention are set by the in-house Information Technology (IT)

department, or the rules are defaults provided by the email-receiving Mail Transfer Agent (MTA) solution, like Microsoft Exchange.

Homegrown Systems

If a mailbox isn't managed by an ISP or an IT department, chances are it is run in the cloud or on a personal server (e.g., sitting in someone's garage). Dealing with a homegrown system involves dealing with a nonstandard set of rules that can be set up *ad hoc* by the server's owner. If you want your email to reach someone sitting behind their personal email server, you must comply with their specific definition of high quality email.

All of the above classes of receivers employ several means of defense against unwanted email. Amazon Simple Email Service (Amazon SES) handles most of these defenses for senders at the infrastructure layer (e.g., email DNS setup, send rate, throttling, automatic retries, etc.). However, you still need to know which class of receiver you're sending to in order to best adhere to their email rules and get your messages into your recipients' inboxes.

The bottom line is that **recipients rule!** Anyone can send email, but email delivery into an inbox is a privilege reserved for those senders who know how to respect the recipient.

Metrics That Define Your Success

The following list of metrics is not meant to be exhaustive. It simply indicates areas where there could be problems with your email program. Don't be fooled into thinking that if you just manage the metrics in these problem areas that your delivery is guaranteed. Remember, you know your customers best.

Bounce Rate

A bounce indicates the failed status of the attempted delivery, which is a useful piece of information that a receiver reports back to you.

Receivers generate both hard bounces and soft bounces. *Hard bounces* are persistent delivery failures such as "mailbox does not exist," whereas *soft bounces* are temporary sending failures such as "mailbox full." Bounces can be either synchronous or asynchronous. If the bounces are *synchronous*, they are communicated while the email servers are talking to each other. Bounces are *asynchronous* if they are sent after the message is initially successfully accepted for delivery by the receiver. In Amazon SES, you won't see returned success responses (i.e., "250 OK"). Amazon SES handles soft bounces automatically by retrying with optimal settings for the domain you're sending to. Hard bounces that are generated either synchronously or asynchronously are passed back to you automatically. For more information, see Bounce and Complaint Notifications in *the Amazon Simple Email Service Developer Guide*.

A high rate of hard bounces strongly indicates to email receivers that you don't know your recipients very well. Therefore, high hard-bounce rates can have a negative impact on your deliverability. You can find some suggestions about how to reduce hard bounces, below.

Complaint Rate

When an email recipient marks a message as spam by clicking the "mark as spam" button in the web email client, the ISP records the event as a complaint. If there are too many of these complaint events, the ISP will probably decide that you're sending spam. Some ISPs allow senders to have more transparency into what their recipients are doing by providing *feedback loops*, in which the ISP tells the sender that a recipient has complained about a message. Amazon SES

automatically forwards complaints from ISPs that offer feedback loops to you. For more information, see How Amazon SES Handles Email in *the Amazon Simple Email Service Developer Guide*.

As you can imagine, too many complaints can result in poor deliverability. **A high complaint rate strongly indicates to email receivers that you're sending email that recipients don't want.** You can find some suggestions about how to reduce complaints, below.

Content Issues

The content of the email provides the communication or message. Email receivers have cracked down on malicious communication from spammers, such as phishing, malware and virus distribution, or scams, by implementing robust *content filters.* These content filters perform automated reviews of email content to look for unwanted email. Technically savvy users rely on open source content filters like the Apache Spam Assassin. Enterprises are more likely to rely on content filters like Google's Postini or Symantec's BrightMail. Amazon SES uses content filtering technologies to help detect and block messages containing viruses or malware before they can be sent**.**

If the receiver's content filter has determined that your content has spam-like characteristics, your content will likely get flagged and diverted from a recipient's inbox. You can find some suggestions about how to avoid having your email content caught in filters, below.

Recommended Best Practices

Even when you have your recipients' best interests in mind, it can be tricky to fine-tune your program for optimal impact. We've put together some pointers for you, so you can more easily do the right thing by your recipients and thus the ISPs.

General Recommendations

- Put yourself in the recipient's shoes. Ask yourself, "Is this something that I would want in *my* inbox?" If you find yourself answering anything but a resounding "yes!" then you probably shouldn't send it.
- Be forewarned. It's unfortunate for the good guys, but some industries have a reputation for poor quality email practices. It's as simple as that. If you're in any of the following industries, you should watch your reputation metrics closely to immediately rectify any problems.
    - Home mortgage
    - Credit
    - Pharmaceuticals
    - Tobacco
    - Alcohol
    - Adult entertainment
    - Gambling
    - Work-from-home programs

Domain and "From" Address Considerations

- Think carefully about the addresses you send your email from. The "From" address will not only be visible to recipients in their email client (including in the preview pane), but will also collect reputation at some ISPs. This, along with the Subject line, will create the first impression a recipient will have of your email.
- Think carefully about the domain of the address(es) from which you send your email. There are two reasons for this:
    - ISPs garner reputation across all email sent from a domain, regardless of how you've split up your mailings.
    - Recipients need to be able to recognize your domain. Don't collect an email address from a web form hosted at *www.example-foo.com* and then send an email from *sender@example-bar.com*. You will lose recognition and drive recipients to the spam button this way.
- If you're sending significant volumes of email, don't send email *from* an ISP-based email address such as *sender@hotmail.com*. For example, if Yahoo! notices a significant volume of inbound messages coming from *sender@hotmail.com*, that email will be treated differently than if it were coming from a proper outbound email-sending domain (i.e., a domain that you own).
- Include correct WHOIS information for your domain so that receivers can look up details about who owns your sending domain. Your domain registrar will provide instructions about how to set up your WHOIS record. Receivers trust more established and transparent domains that are fully listed with the Internet registry over domains that are not.

Authentication

- Make sure that your domain is authenticated with **Sender Policy Framework (SPF)** and **SenderID.** These authentication methods lend credibility to your sending domain by confirming to email recipients that an email is actually from the domain it claims to be from. For more information, see Authenticating Your Email Address in the *Amazon Simple Email Service Developer Guide*. Test your authentication settings by sending email to an ISP inbox that you own (e.g., a Gmail account), and viewing the headers in the source of the message. The headers will tell you whether your authentication attempts have succeeded.
- You should also use **DomainKeys** or **DomainKeys Identified Mail (DKIM)** to sign your outbound email. This authentication step will lend credibility to your email by confirming to recipients that the content has not been changed in transit from sender to receiver. For a brief explanation of the difference between SPF and DKIM, go to the Wikipedia article, Email authentication. Test your authentication settings by sending email to an ISP inbox that you own (e.g., a Gmail account), and viewing the headers in the source of the message. The headers will tell you whether your authentication attempt succeeded.

SPF AND SENDERID IN AMAZON SES

Amazon SES comes ready for use with preconfigured DNS records. Additionally, Amazon SES has SPF set up – all IPs sending from amazonses.com are authenticated via SPF. However, we recommend that you also authenticate with SenderID by adding a pointer to our domain in your TXT record

Building and Maintaining Your List

- Be careful how you collect email addresses. Many times in online forms or other sign-ups, people will provide bogus email addresses that, when you send email to them, will generate hard bounces and appear to the ISP as irresponsible sending.

- If your form continues to collect addresses that are hard bouncing on their first email attempt, ensure that the recipient confirms the address they're entering. Present the address for confirmation, require duplicate fields for email address to ensure entries match, and disable client-side auto-fill if possible.
- You can utilize *double opt-in* (only sending email to an address whose owner has clicked on a verification link) to ensure that you don't repeatedly send email to a bad address.
- You can use third-party vendors to check the viability of an email address before you send to it.
- You can also check the syntax of an email address to ensure that the address is at least reasonably correct (e.g., is the address composed correctly with a local part and @ symbol? Does the address resolve to a domain with an MX record?).
- You should be careful about allowing any user-defined input to be passed along to Amazon SES and the ISPs unchecked. Forums and form submissions can be especially tricky since the content can be completely user-generated (and spammers can fill out forms with their content), but email receivers don't care – it's your responsibility to ensure that you're only sending email with high-quality content.
- It is highly unlikely you'll ever have a standard alias (such as postmaster@, abuse@, or noc@) sign up for your email intentionally. You should have control over how you acquire email addresses, and only send email to addresses that belong to a real person who wants your email. This applies especially with role accounts, which are usually reserved for email watchdogs. Role accounts can be maliciously added to your list as a form of Internet sabotage to get you blocked. Ensure that your list does not include any role account aliases. For a complete list of role accounts you should watch out for, see Mailbox Names for Common Services, Roles and Functions.
- Don't send email to third-party lists (purchased, rented, or otherwise collected outside of your purview). When you send email to a third-party list, you're taking the risk of emailing addresses of an unknown origin. This could invite enforcement from ISPs if it turns out that the list contains *spamtraps* (special addresses set up by ISPs to monitor unsolicited email), bouncing addresses, or recipients who complain. Even if the email addresses on the third-party list are valid, you still don't know whether the recipients will actually want your email and thus whether they will consider it spam. You should collect the email addresses yourself, directly from recipients.

Compliance

- Whether you're sending email to recipients in the United States or to recipients in other countries, you are responsible for following the laws and regulations applicable to your email practices. This guide does not address those compliance issues, so be sure to learn and follow applicable laws.

Avoiding Bounces

- Generally, you should keep your bounce rate below five percent. This is one way to prove to ISPs that you have a clean list (i.e., you know the state of your recipient addresses). This percentage can change with industry trends and is not universal across all ISPs, but it is a reasonable rule of thumb.
- If you have an old list that you haven't emailed to in a while, don't email to that list through any provider that limits your bounce rates (which includes Amazon SES), unless you've verified the state of the addresses (e.g., by checking login activity on your site, purchase history, etc.). Otherwise, you may incur a lot of bounces from old unused email addresses while you try to clean your list, and you risk being blocked by both ISPs and Amazon SES.

- If you're providing critical information to your customer, such as a password reset, provide an alternative form of communication in addition to email, in case the email addresses bounce. Alternatives might include in-browser secret questions, postal mail, or SMS. You should also display the address to which you will be sending and allow the recipients to choose a different workflow, such as SMS, if the email address is in fact incorrect.

Handling Bounces

- Do not send to an email address that has hard bounced due to a permanent delivery failure. If it's a true permanent delivery error, repeated attempts will not deliver the message, but the bounces will stack up, damaging your reputation with ISPs.
- Do not point your bounce submission address to a mailbox that is itself bouncing; make sure it can receive email. Additionally, if you outsource your inbound email system to an ISP, as opposed to receiving email through your own internal servers, be aware that an influx of bounces can land in your spam folder or be dropped completely. Ideally, you should not use a hosted email address to receive bounces. If you must, however, then check the spam folder often, and don't mark the bounce messages as spam. In Amazon SES, you can specify the address to which bounces are sent. For more information, see Bounce and Complaint Notifications in *the Amazon Simple Email Service Developer Guide*.
- Usually, a bounce will provide the address of the mailbox refusing delivery. However, if you need more granular data in order to map a recipient address to a particular email campaign, include an X-header with a value you can trace back to your internal tracking system. For more information, see the Header Fields Appendix in *the Amazon Simple Email Service Developer Guide*.

Avoiding Complaints

- Generally, you should keep your complaint rate below 0.1 percent. This is one way to prove to ISPs that you are sending valued email. This rate can change with industry trends and is not universal across all ISPs, but it is a reasonable rule of thumb.
- Don't continue to send a recipient the same type of email that generated a complaint. For example, you shouldn't send more marketing email to someone who complained about a marketing email, but you could still send transactional email to this address if the recipient makes a purchase from your site. Resending the same type of email will only generate more complaints, which will pile up over time and amplify your complaint rate. Simply remove the addresses from the appropriate lists.
- As with bounces, if you have a list that you haven't sent email to in a while (for example, if you're a new Amazon SES customer), ensure that your recipients know why they're getting an email. We strongly recommend that you send a welcome message, or in some other way remind the recipients who you are to avoid running into complaint issues with both ISPs and Amazon SES.

Handling Complaints

- As with bounces, do not point your complaint submission address to a mailbox that is bouncing; make sure it can receive email. Additionally, if you outsource your inbound email system to an ISP as opposed to receiving email through your own internal servers, be aware that an influx of bounces can land in the spam folder or be dropped completely. We recommend that you do not use a hosted email address to receive complaints. If you must, however, then check the spam folder often and don't mark the complaint messages as spam. When you use Amazon SES, you specify the address to which complaints are sent. For more information, see Bounce and Complaint Notifications in *the Amazon Simple Email Service Developer Guide*.

- A complaint message will usually contain the email content (as opposed to a bounce message, which will usually only have the headers). However, complaints will often have the original complaining address redacted due to ISP privacy concerns. It's up to you to ensure, through the use of a custom X-header or a value embedded in the content, that you know how to map the complaint to the complaining email address.

Creating Quality Content

- Most content filters today are comprehensive; they look at content fingerprints as opposed to following hard and fast rules. A few years ago, having punctuation or all capital letters in a subject line meant that your email was likely to be sent straight to the spam folder. Now, it's more about the combination of different content characteristics, and whether that combination has been commonly seen in spam. You can use Spam Assassin or a third-party reputation service such as Return Path to help identify content issues.
- Checking the URLs that you use in your emails against blacklists can provide very useful information, because some ISPs will block email with blacklisted links. URIBL.com and SURBL.org are two very useful sites that you can use to determine whether your links are listed. Remember to check any links provided to you by a third party or any link shorteners, which have become increasingly dangerous because they obfuscate the final domain.
- Avoid broken links in your emails; make sure that you actually have pages behind your links. If you have an unsubscribe link, make sure that it works. It's easy to forget to test every single link when you're building out new email programs or changing existing email templates.
- Make sure that the Privacy and Terms pages work on your site. Recipients may not trust your email if they can't find the standard fine print on your site, which will diminish your email's value and deliverability potential.
- If you're sending high frequency content (e.g., daily deals), ensure that the content is actually different each day. With higher cadence comes greater responsibility to ensure that the content is timely and relevant.

Closing Thoughts

Despite the challenges of navigating the various systems between you and your target recipients, email can be an incredibly effective communication mechanism if you use it correctly. We hope that you now have a better grasp of what factors influence whether your email reaches your target inboxes, and that you also have a list of things you can do to make your email program better.

While the list above is by no means a comprehensive list of absolutely everything you can do to help your email quality (and therefore its deliverability), we hope that you find it a good place to start. As you build out your email program, you need to remember two vital things:

1. Provide value.
2. Send only to people who want your email.

If you take care of these two things by following these tips, your email program will be well on its way to success!

Glossary

- **Asynchronous bounce –** A bounce that is sent after the message is initially successfully accepted for delivery by the receiver.
- **Bounce –** A message that indicates the failed status of the attempted delivery.
- **Complaint –** A message that is generated when a recipients mark a message as spam by clicking the "mark as spam" button in their email client.
- **Content filters –** Automated reviews of email content to look for unwanted email.
- **Deliverability –** The likelihood that an email message you send will actually arrive at its intended destination (usually the recipient's inbox).
- **Double opt-in –** A system that requires a subscriber to both request to be subscribed and click a verification link that is subsequently sent to them.
- **Email program –** How you manage the electronic communication with your recipients through email.
- Email quality – Email that is deemed to be of value to the email recipient.
- **Feedback loop –** The system by which an ISP tells the sender that a recipient has complained about a message.
- **Hard bounce** – A message indicating a persistent delivery failure such as “mailbox does not exist.”
- **Internet Service Providers (ISPs) –** Organizations that provide access to the Internet.
- **Junk folder –** Also called a spam or bulk folder, where email messages that various filters determine to be of lesser value are collected so that they do not arrive at the inbox but are still accessible to the recipient.
- **Receiver –** The system(s) supporting the recipient's email infrastructure – whomever or whatever is behind the email address you're sending to.
- **Recipient –** The person or entity receiving an email message; the recipient is named in the To, Cc, or Bcc field of the message.
- **Reputation –** The trust built up by email senders by sending high quality email over time, usually influenced by a combination of factors.
- **Sender –** The person or entity sending an email message.
- **Soft bounce** – A message indicating a temporary sending failure such as “mailbox full.”
- **Spamtraps –** Special addresses set up by ISPs to monitor unsolicited email.
- **Synchronous bounce –** A bounce communicated while the sender's and the receiver's email servers are actively transmitting and receiving the email message.

Additional Resources

More information about some of the recommendations in this whitepaper

- To find out more about email regulation in the United States, visit the FTC's site – http://business.ftc.gov/documents/bus61-can-spam-act-compliance-guide-business
- To find out more about Amazon SES solution providers, visit the Amazon SES resources page – http://aws.amazon.com/ses/resources/
- To find out how to test your email authentication settings, visit the ESPC site – http://www.espcoalition.org/senderid/

More information about Amazon SES

- Overview – http://aws.amazon.com/ses/
- Developer Documentation – http://aws.amazon.com/documentation/ses/
- Community Forum – https://forums.aws.amazon.com/forum.jspa?forumID=90
- AWS Support – https://aws.amazon.com/support

Amazon SES Solution Providers

- Deliverability: Return Path – http://aws.amazon.com/solution-providers/si/return-path
- Preview rendering and analytics: Litmus – http://aws.amazon.com/solution-providers/si/litmus/
- Full service and strategy: Zeta Interactive – http://aws.amazon.com/solution-providers/si/zeta-interactive-1320423244
- Strategy: Synchronicity Marketing – http://aws.amazon.com/solution-providers/si/synchronicity-marketing
- Technology integration: Cambridge Technology Enterprises – http://aws.amazon.com/solution-providers/si/cambridge-technology-enterprises

ISP postmaster pages

- AOL – http://postmaster.info.aol.com/
- ATT – http://www.att.com/esupport/postmaster/
- BellSouth – http://www.att.com/esupport/postmaster/
- Charter – http://www.charter.com/customers/support.aspx?supportarticleid=1953
- Comcast – http://postmaster.comcast.net/
- Cox – http://postmaster.cox.net/confluence/display/postmaster/Postmaster+Home
- Facebook – http://postmaster.facebook.com/
- Frontier – http://postmaster.frontier.net/
- Gmail – https://mail.google.com/support/bin/answer.py?answer=81126&topic=12838
- Hotmail – http://postmaster.msn.com/

- RoadRunner – http://postmaster.rr.com/
- United Online – http://unitedonline.net/postmaster/
- USA.NET – http://postmaster.usa.net/
- Yahoo! – http://postmaster.yahoo.com/