Marketing Tips & Techniques

How to Improve Email Delivery

Honeywell Partner Concierge
www.PartnerConcierge.com
Honeywell@PartnerConcierge.com
480.704.4775

Email Delivery Tips & Techniques

All customers have a lifecycle with your company or brand. They become a customer when they make a certain number of purchases or engage with your sales team. When the purchases or engagements decline, they eventually exit your brand. Believe it or not, email is still a very reliable, robust and cost effective way to both acquire new customers and turn your existing customers into loyal, repeat customers.

Over the past few years, many sales and marketing professionals are questioning the effectiveness of email marketing for two specific reasons:

1. Most emails are caught by junk mail and spam filters
2. Email open and click-through rates have been dropping significantly

Although not the primary reason, there is a direct correlation between delivery and email open or click-through rates. How can you cut through the spam and junk mail filters, get to your customers and prospects inbox and grab their attention in less than 3 seconds?

In this two part series we are going to give you the best practices for:

1. Email delivery tips & techniques – how to improve email delivery
2. Email design tips & techniques – how to get your message across

First, we will start with Email Delivery Tips & Techniques to help you navigate around the spam filters and reach more contacts in your database.

How to Improve email delivery

Following tips and techniques are provided as recommendations to help you improve your marketing efforts.

1. Comply with National SPAM Laws and Regulations

If you are executing (or planning) email-marketing campaigns, compliancy is not an option!
In the United States, the CAN-SPAM Act* covers all commercial messages, which are defined as: "...any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service".
Do everything you can to comply with these 7 main requirements:

a. Don't use false or misleading header information
b. Don't use deceptive subject lines
c. Identify the message as an ad
d. Tell recipients where you're located
e. Tell recipients how to opt out of receiving future email from you
f. Honor opt-out requests promptly
g. Monitor what others are doing on your behalf

2. Do not use Attachments or Executable files

In general, .jpg, .gif, .png and .pdf attachments are safe to send provided you include some content in the email along with them. However, executable attachments such as .exe, .zip, .swf, etc. should be avoided at all costs. In general, only send executable files to those who are expecting them.

If you need to email a large attachment or a type of attachment that can easily be flagged as spam or trigger virus scanners, we recommend using a free service such as DropBox.com or other file sharing services. If the attachment contains sensitive data, you should consider using your company's secure FTP server.

3. Avoid Spam Trigger Words

Any email containing a spam trigger word is more likely to end up in a spam folder. Unfortunately, there is no definitive list of trigger words to avoid. Use common sense and don't use words that you would find suspect (free, great deal, offer, etc.) when receiving an email from someone unfamiliar.

You will have a better chance of staying out of the spam box by avoiding grammatical and misspelling errors and finally, never ask for personal information.

4. Get off All Blacklists

A blacklist is a list of addresses and domains that have been identified as spammers and are blocked from sending to mail providers. If your email server ends up on one of these lists, it becomes extremely difficult to reliably deliver email, especially to new people on your list. To check if your email server is on a blacklist, use a free service such as blacklistmonitoring.com, blacklistmaster.com, or paid services such as constantcontact.com.

If you find that you have been added to a blacklist, contact the site that has you listed and discuss prompt removal of your domain. It can be a tedious and time-consuming process but getting your domain removed is crucial to ensuring your emails are delivered correctly.

5. Use Spam Checkers before Sending Your Emails

Before sending emails out to your entire list, it's worth the time to utilize a spam checking service. Following sites and many others offer free spam checking services to verify your email is free of any spam emailspamtest.com, spamcheckservice.com, MailingCheck.com

If you don't have the time or resources to use these services, send your email to www.IsNotSpam.com. In addition to checking for spam triggers, this service will check for other items that could hinder your email deliverability.

6. Avoid Spam Traps

Spam Traps are email addresses that are flagged by ISPs as being no longer used by individuals (e.g. admin@, support@, etc.). Since these are general email addresses, the ISPs know there was no opt-in selection process to receive the emails. Most often, ISP removes not only the suspect email, but also all emails in the domain.

7. Make sure your DKIM, SPF, Sender-ID and Domain Keys are setup properly

Make sure your email server supports these protocols and that they are properly implemented: DKIM, SPF, Sender-ID and Domain Keys. These codes help ISPs determine the authenticity of your email from a technical perspective. You can contact your technical support team or ISP for more information.

8. Use Permission Marketing Techniques

Permission marketing is defined as, privilege to deliver anticipated, personal, and relevant messages to people who actually want to get them. Permission marketing maintains that treating people with respect is the best way to earn their trust and attention.

It is important to tell people what they can expect from your emails and how often to expect them. Once they opt-in, don't change the rules. Permission marketing requires patience and humility, but it will pay off in the long run.

9. Use multiple IPs

Each IP has its own sender reputation, which is what ISPs use to make filtering decisions. In order to truly optimize your email program, isolate your transactional email streams to one or more IPs. This way you can better monitor and diagnose potential delivery failures by email type. If your "monthly newsletter" email messages are being junked, then it's easier to take action and solve your problem quickly.

10. Use secure email servers

Make sure you don't have an open relay or open proxy. Follow industry standard best practices for network and server security. All the best mailing practices don't matter if you don't have control of your environment. This is not an issue if you are using a third party tool or have a fully hosted server with a reputable ISP.

*http://www.business.ftc.gov/documents/bus61-can-spam-act-compliance-guide-business
We do not endorse or guarantee the accuracy, relevance, pricing or timeliness of the organizations listed in this document.