Enterprise Email Marketing: The 8 Essential Success Factors

How to Create High-Impact Email Marketing Campaigns When Managing Over 1 Million Sends per Month

By John H. Sellers
Certified Email Marketing Professional
Manager of iContact's Enterprise Account Management Team

Summary:

This report provides key guidelines for successfully managing large volume email campaigns. It covers "major" drivers in obtaining such success, addressing the complexities of SPAM, email-recipient considerations, and strategic testing.

Specific topics include:

1. Defining Modern Day SPAM
2. Types of SPAM Complaints
3. Minimizing and Monitoring SPAM Complaints
4. Improving Inbox Delivery
5. Understanding Email Acquisition as a Trust Relationship
6. Meeting Email Recipient Expectations
7. Lowering Email Recipient Anxiety
8. Random Sample List Testing

1. Defining Modern Day SPAM:

The definition of SPAM has changed in recent years. The general definition of SPAM is unsolicited email, UCE (Unsolicited Commercial Email), or UBE (Unsolicited Bulk Email).

“Unsolicited” is interpreted differently depending on whether you are the email sender, email recipient, or ISP Internet Service Provider that manages the recipient’s junk email.

It is thus important to clarify the definition of SPAM so that it is clear to both the sender and the recipient. SPAM is unrecognized, unexpected, or unwanted email. The most important factor in determining spam is most often the decision maker (the person who is empowered to label a message as SPAM). The email recipient is the decision maker in power. Despite the fact that your message is a targeted permission based email, if a recipient thinks it is SPAM, then it will be reported as SPAM, which impacts your sender reputation and deliverability.

Key Points:

1. SPAM reporting is controlled 100% by your email recipients and their ISP/ESP, as well as abuse networks.
2. Modern-day SPAM includes any unrecognized, unexpected, or unwanted email even if the recipient has provided explicit permission to receive the email.

2. Types of SPAM Complaints:

Marked or flagged by the recipient as SPAM or junk

Unfortunately, most recipients don't realize the impact on your sender reputation when they click the SPAM or junk buttons. These actions do impact deliverability and reputation because ISPs such as AOL, Microsoft, and Yahoo count the number of complaints received by your email recipients.

Certain ISPs have established complaint-rate thresholds (# of complaints per # of recipients). These thresholds change often and are not published by ISPs.

A good rule of thumb is to keep the complaint ratio below 5 in 1000. If you receive more than a .5% complaint rate from an ISP, you may be restricted by the ISP, or you may be required to re-confirm those addresses (send them an invitation to confirm their subscription to your email list).

Manual complaints emailed directly from recipients to ISP (Internet Service Provider) or ESP (Email Service Provider) abuse departments.

These manual complaints are looked at as serious and major complaints by both ISPs and ESPs. This is related to the fact that it takes significant effort for a recipient to file a manual complaint. The recipient must take the time to find the abuse address, and then write the email, which in most cases involves a required detailed description of why the message has been classified as SPAM. If the recipient can prove he or she did not give the sender permission to send the message, then an abuse@ email complaint (received by an ISP) may result in a blacklist of your sending domain and ip addresses. This type of complaint can also result in account disablement or possibly, termination by your ESP if the recipient's email can prove violation of set anti-SPAM policies (a quality ESP will have a strict policy).

Filed through a third-party abuse processing service such as SpamCop

Anti-Abuse networks like MAAWG, SpamCop, Spamhaus, the ESPC and others have been created in the last decade to help email recipients, ISPs, and law abiding email marketers combat SPAM. These networks aim to track known spammer gangs, hold senders of unsolicited bulk email accountable, and continue to build and improve anti-SPAM legislation. SpamCop, for example, allows any registered email recipient to post a SPAM complaint through the Spam Cop website. They empower a user who receives spoofed/unsolicited email scams and SPAM to take action. Through SpamCop, users can report any email they perceive as unsolicited by following this link: http://www.spamcop.net/anonsignup.shtml. When your ESP or ISP receives a recipient complaint from SpamCop, your ESP or ISP will certainly disable or sometimes terminate your account.

Therefore, it is a good idea to use confirmed opt-in for all subscriptions in order to verify that the recipients are the legitimate owners of their email addresses and that they wish to receive your message.

Hitting Spamtraps and Honey Pots

Some anti-abuse networks post secret email addresses on websites in the attempt to catch known spammers.

Email harvesting is a common practice used by Spammers who program computer-automated bots to scan and collect email addresses across the internet. The spammers add any collected "harvested" addresses to their email lists.

When Spammers collect email addresses from planted spam traps and honey pots, they later send unsolicited messages to those addresses without permission.

When the owner of the SPAM trap or honey pot (a member of the anti-abuse network) receives the unsolicited message, they catch the spammer in the act of harvesting.

The owner can then process the message and determine the source of the email, and take appropriate action by informing the ESP or ISP.

When SPAM trap complaints are received by an ISP or ESP, the spammer's sending privileges are usually terminated.

There are few instances where hitting SPAM traps can be legitimately excused. It is important to capture ip address, date, and time of opt-ins. This allows you to verify how you collect your email addresses and avoid a false SPAM label. In rare cases, competitors, disgruntled customers or employees can submit known SPAM traps into your opt-in signup form. If confirmation messages are not used to verify the email recipient's desire to join your list, then anti-abuse networks are forced to report the hit.

Key Points:

1. All SPAM complaints can negatively impact the sender's reputation.
2. Manual SPAM complaints have a more immediate negative impact on your sending reputation, but if you follow a strict anti-SPAM policy http://www.icontact.com/terms/antispam/ you can avoid them.
3. Hitting Spamtraps and Honey Pots has the most severe impact on your sending reputation. An isolated hit can cause you to lose your ability to send to ISPs and ESPs, and your ESP may be forced to disable or close your account.

3. Minimizing and Monitoring SPAM Complaints:

If a user signs up to receive your email on your website, or on a paper form, the user will soon have the ability to report your message as SPAM. It is thus important to analyze your content from the recipient's perspective. Unfortunately, very few of your email recipients understand the impact that pressing the SPAM and JUNK button can have on your reputation.

It is also important to consider how an ISP will view your message. If an ISP sees 2000 of your messages in its servers, it will evaluate your message and potentially label it as SPAM. ISPs can block your ability to send to their domains and servers if they are bombarded with messages without an easy to find unsubscribe option or a clearly defined value for the recipient.

Lastly, the anti-abuse network must also be considered. If an anti-abuse network such as SpamCop (http://www.spamcop.net/) receives a manual complaint from a recipient claiming to have never signed up for your message list, you could be blacklisted or blocked. Overall, it is critical to think like the decision makers who are the recipients, ISPs, the anti-abuse networks you'll encounter.

Steps to minimize complaints:

- Make your permission statement clear (with nature and frequency stated on your email capture form).
- Remind your recipients of the nature and frequency of your message upon sign up and then in every marketing message you send.
- Provide an easy to find unsubscribe link in all/most email communications.
- Send subscribers who use ISPs like AOL.com and Hotmail.com a confirmation request message. AOL and Hotmail often receive more SPAM complaints due to the ease of clicking SPAM or JUNK in both ISPs. It is often easier and quicker for an AOL or Hotmail user to report your message as SPAM (versus deleting or unsubscribing).
- Make certain your complaints are monitored:
    - Use an ESP who monitors and enforces a strict anti-SPAM policy.
    - Test your Envelope fields and Message Body with multiple tools (iContact's SPAM check button) as certain SPAM words can change daily.

Key Points:

1. Monitoring SPAM complaints requires feedback loops, which can take years to establish and maintain, most large senders require an ESP for their large volume campaigns because of this.
2. There are immediate steps you can take to minimize your SPAM complaints.
3. To successfully minimize and monitor ongoing complaints, it is sometimes necessary to seek professional assistance.

4. Improving Inbox Delivery:

The source of your email needs to have a strong reputation or it most likely won't reach the inbox. Establishing a feedback loop with ISPs is integral in improving inbox delivery.

The second step is integrating your sending application with the feedback loop's reports, so that you know, in real-time, when you receive complaints.

A white list can be a temporary solution if you don't have a feedback loop. You must continually monitor your complaints if you are to maintain your white list status.

Maintaining these relationships is a full time job, and most in-house systems do not have the required feedback loops to monitor SPAM complaints at today's required level. This is why using an ESP (Email Service Provider) for permission based email marketing has become an industry best-practice for large senders concerned about maintaining a strong-email reputation.

Steps for improving:

- Find an ESP who enforces a strict anti-SPAM policy, and who will inform you (with real-time reporting) about the number of complaints you are receiving. You need this feedback in order to continually lower your complaint number and/or maintain the current complaint levels.
- Use email authentications such as SPF or Sender ID to bypass junk filters and use verification tools to prevent spoofing and spamming by a majority of ISPs and spam filters. Top-tier email-service providers will gladly share their SPF records with you so that you can add them to your DNS settings.
- Be certain to create both a "txt" DNS record and an "spf" DNS record (BIND releases from 9.4.0 support the SPF RR type - see also RFC 4408) for you SPF record: Visit http://www.openspf.org for more details on SPF.
- Verify that your content looks "non-spammy" and that it avoids terminology or design that triggers SPAM labeling and filtering.
- SPAM words change daily, and a non-SPAM word that is fine one day could trigger junk filters the next day.
- Test your deliverability with seed addresses from the Major ISPs. If it reaches the inboxes of most of the major ISPs, then your content has passed the test.
- Re-confirm subscribers who have not opened your email in 3 months or more using a solid offer that clearly states your email's value proposition.
- If you need advanced testing use a qualified deliverability tester such as Pivotal Veracity to monitor your deliverability (http://www.pivotalveracity.com/).

Key Points:

1. Low SPAM complaints equals high inbox delivery.
2. A list of engaged subscribers will outperform a high quantity list of unengaged subscribers. For example: 400k subscribers with a 5% open rate yields 20k opens and 2k clicks (assumes 10% click-to-open ratio). 200k subscribers with a 15% open rate yields 30k opens and 3k clicks (assumes 10% click-to-open ratio).
3. Continued testing and monitoring is a must for ongoing deliverability. Never stop testing messages or monitoring recipient complaints in order to keep SPAM related issues under control.

5. Understanding Email Acquisition as a Trust Relationship:

Due to privacy trust issues and the increased volume of SPAM delivered to inboxes, recipients must trust your organization before they will share their email address with you.

Your email capture or opt-in page requires that you answer the following subscriber questions:

- What will I receive from this organization in exchange for my email address?
- What expectations should I have in terms of this organization abiding by the statements made on their email capture/opt-in page?
- How does the organization ensure that my email address will be kept private?
- Beyond the incentive offered, what value will I receive that instantly validates my decision to entrust this organization with my email address?

To overcome this lack of trust, it is important to clearly state the nature of your emails, how frequently you will send them, and what value your emails provide. Living up to the promises made on your email capture/opt-in page can build loyal client/customer relationships and help create engaged readers. This empowers your email marketing to directly impact ROI.

A final important statement on the trust relationship topic: "A bird in the hand is worth two in the bush." With that said, treat your existing customers as you would all potential email marketing opt-ins. New customers or potential customers should require direct opt-in before receiving your marketing emails. Provide an unchecked opt-in box during your online checkout process with a succinct permission statement. Send a confirmation request message to existing customers who have not yet opted-in for your marketing emails, as they must actively consent to receiving marketing emails. Not doing so will lead to a high complaint rate, which could harm your relationships with ISPs and ESPs, in addition to the customer relationships.

Key Points:

1. A trust relationship between your organization and your current and future recipients is critical to permission based email marketing. Recipients must trust you before they will give you access to their email address.
2. Your existing customers must directly opt-in before you send them marketing-natured emails.

6. Meeting email recipient expectations:

Much like the trust relationship, meeting expectations requires in-depth understanding of the customer perspective. Before creating permission statements for your opt-in email-captures page, is critical to have a strategic plan for your email-content. The content must live up to the value proposition proposed on your capture page, as it is imperative that you meet your email subscribers' expectations. To do so, you can create a succinct value proposition statement for your email campaign, and ensure that all of your content is in-line with that value proposition. Then, restate the value proposition in all of your messages, and provide a call to action for the recipient that helps them realize your proposed value. Overall, if you state that you will send emails of a certain nature and frequency, be absolutely certain to deliver on those promises.

Key Point:

1. Define and set email marketing expectations and then live up to the value proposition.

7. Lowering Recipient Anxiety:

Think about what you feel and experience when you receive a marketing email from a person or company. What is your initial reaction to this email? Do you remember giving this company permission to receive this email? Do you glance at the from-name, from-email address or subject line (also known as the envelope fields)? Do you feel a sense of hesitation before you decide to open the email? Do you analyze the email before making a final decision on your action to delete, report as SPAM, or open? Can you identify who sent the email by reading the envelope fields of the message? What motivates you to open certain emails? Why do you open some, but delete others, unsubscribe, or report as SPAM? How many email addresses do you have? Do you classify your different email addresses in terms of their use and priority?

Today, most people possess multiple email addresses. They often have one they use to register for special offers that they don't quite trust, and another--more valuable--address they only share with close friends and family. Still, people sometimes use their personal/valued email address to subscribe to trusted marketing materials.

You want to be this type of trusted message. But how do you accomplish this? Abide by the guidelines outlined in the other sections and always remember the following:

- Be prepared for your readers to forget that they signed up for your email
- Always restate your email's value proposition.
- Consistently identify your brand
- Make sure that the name of your company or of someone well known from your company is included in the envelope fields.
- Envelope fields should include the from-name, from-email address, subject lines, and the preview pane (the top 250-400 pixels of your message).
- Make sure your recipients understand why they are receiving your message.
- Restate the nature of your message (in small print at the top of your message)
- Instantly verify who you are, why you are sending a specific message, and how the recipient can easily unsubscribe from your email campaign.

Key Points:

1. Make certain that all of your messages address the email recipients' fear of SPAM.
2. Remind your subscribers:
    - why they should continue to trust you
    - how often you will send to them
    - of your email message's nature

Make your unsubscribe link easy to find.

8. Random sample list testing-

Test ideas and options as variables before sending to your entire list:

It is beneficial to test your message's image placement, call to action placement, length of copy, and verbiage for subject lines, from-names, and from-email addresses. An often-overlooked value of having a large list is that you can afford to test your different ideas through random-sample testing. For example, if you can't decide between two options for a subject line, random-sample testing will indicate which one inspires more opens.

Exercise in Random-Sample Testing

You may have 2 versions of a message.

1. A brief message that bullet points your value and call to action for your recipients.
2. Another message on the same topic that is written in essay style.

How do you know for certain which one will inspire more clicks to your landing page?

You may have 2 versions of a message:

1. A message with no images.
2. A message with a nice graphic header and a few product images.

How do you know which one will inspire more opens (preview pane) and click-through's to your landing page?

There are no limits as to what you can test, though it is advised to limit testing to one variable at a time for simplicity.

Test variable 1 by sending a message containing the variable to a random sample of your list (no more than 5% of your list).

Test variable 2 by sending a message containing this variable to an additional random sample of your list (no more than 5% of your list). Make certain that this list excludes emails tested from variable 2.

Send the top performing variable to the remainder of your list (Be certain to exclude the emails you have already tested).

For this to work properly you must use random sampling. This is a great way to take advantage of your large list and make scientific decisions about what ideas to utilize.

Key Points:

1. Random Sample tests are a great way to make solid decisions about ideas to implement.
2. Testing variables (that you'll use in your emails) is a great way to increase your ROI from every send to your list.