RIGHT NOW®

BEST PRACTICES IN EMAIL MARKETING

Get Delivered, Get Read, and Get Results

BEST PRACTICES IN EMAIL MARKETING:
Get Delivered, Get Read, and Get Results

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Email is a maturing, but still effective business communication channel. Whether you are innovating or duplicating what's always worked in the past, technology, audience expectations, and CAN-SPAM compliance are creating a constantly changing email landscape.

Email marketers need to stay abreast of these changes in order to be consistently successful. Used effectively, email marketing is a cost-effective and personal way to reach both customers and new audiences. But the power of email can work against you as well. Email marketing can squander your budget if you target the wrong people or don't get through to the right ones.

This paper reveals best practices for email marketing in 2009. You'll learn about deliverability, response solicitation, understanding your audience, your businesses reputation, ISPs, address acquisition, and much more.

But, it all boils down to the two major issues that confront email marketers:

- Email that does not get delivered
- Failing to elicit a response

Email not getting delivered is a symptom of SPAM, and may result in getting flagged as SPAM. In addition, low response rates can be the result of several factors including: poor audience definition, bad mailing lists, poor content, and unclear call to action.

This paper outlines email marketing best practices and guidelines to help ensure both high deliverability and high effectiveness. We've collected these best practices from many businesses across several industries.

The most creative campaign is useless if it doesn't reach the right audience. This paper will not only help you hit your target, it gives you the information you need to deepen your customer relationships and build your brand.

THE CHANGING EMAIL LANDSCAPE

Thanks to new anti-SPAM laws and ongoing efforts by vendors and marketers who have worked to ensure credibility, consumers can trust their email. But, it's critical that email marketers stay abreast of evolving trends and technologies because what worked a year ago may not work today.

One important trend is that Internet Service Providers (ISPs) have emerged as a kind of meta-audience, which email marketers must understand and cultivate relationships with. ISPs now serve as gatekeepers who decide which emails get through and which do not.

Once you've gotten your message through, you still combat the email overload your recipient may be experiencing. Permission-based marketing offers guidelines for opt-in programs based on the simple and proven premise that people will read what they ask for—and tend to delete or flag as SPAM what they have not requested.

Understand ISPs as a Meta-Audience

Since ISPs now act as gatekeepers, it's critical to build your reputation by establishing the credibility of your domain name and the deliverability of your recipients' addresses. You'll want to test your email to smaller audiences before you execute a major campaign. This will allow you to begin establishing what amounts to a credit rating on sites like Senderscore.com, which ISPs use as a barometer of a sender's reputation.

To establish your company as a legitimate email marketer with ISPs, follow these eight guidelines:

1. Establish email accounts with the free email providers. Use Yahoo, Gmail, AOL, etc. to start building your deliverability rating and to test sample lists.

2. Create seed lists to test mailings. Try before you fly. What you are after prior to an actual email campaign is a well-vetted list of people who have opted-in to receive your information. You may have "warm leads" from other marketing initiatives, if not, you will have to build your own list.

3. Warm up your IP address. This builds your reputation with ISPs. The process involves sending small amounts of email through a new-unused IP address in order to establish a positive deliverability reputation. This takes several weeks, so plan ahead.

   If you want to warm your own IP, don't send to your entire mailing at once. Break it into smaller "chunks." Give ISPs a chance to see the types of messages that are coming through and let them establish a sending reputation. If you give the ISPs a chance to get to know you and the type(s) of email you are sending, it will give them a chance to gradually establish a sender reputation for you, which will work to your advantage. Our suggested model, using a total universe of 200,000 as an example for multiple mailings is:

   - First send – 2000 names (or one percent of your list)
   - Second send – 10,000 names (five percent)
   - Third send – 20,000 (10 percent)
   - Fourth send – 40,000 addresses (20 percent)
   - Fifth send – 80,000 (40 percent)
   - Sixth send – remainder of list

Carry out these six sends over a period of five days. Follow the same process for a few weeks while your IP Reputation builds.

4. Honor abuse reports. Treat them like unsubscribe requests. Set up and monitor accounts such as abuse@yourdomain.com or postmaster@yourdomain.com.

5. Be aware of ISPs' acceptable use policies. Stay up-to-date with the various ISP policies to ensure your emails get delivered now and in the future.

6. Implement a thorough SPAM complaint, bounce, or reply emails resolution process. To ensure clean contact lists and prompt follow-up of legitimate customer replies, implement a process to handle "out of office" replies, unsubscribe requests, SPAM complaints, and general replies.

7. If you plan to use a branded domain (e.g. @yourcompanyname.com), publish your authentication. This practice helps ensure good delivery rates and reputation. Authentication does require some action by your IT staff to implement. There are two categories of email authentication technologies:

   - SPF/Sender ID: These are complementary email authentication technologies that designate permitted senders to send email originating from your domain. Mismatched or incorrectly specified SPF/sender records will cause negative delivery reputation and poor delivery rates.

   - DK/DKIM: This stands for Domain Keys/Domain Keys Identified Mail, two email authentication technologies that designate email as originating from an authorized email delivery provider through use of cryptographic signatures. Unsigned or incorrectly assigned signatures will cause negative deliverability reputation and poor delivery rates.

8. Do not attach Word or other documents. Many ISPs now identify attachments as SPAM. And if they haven't, some users have blocked it from their inboxes to save storage. Include links to sites where people can download information instead.

Acquire Email Addresses the Right Way

Rates of return on email campaigns correspond directly to the quality of email recipients. If your organization harbors any old notions of buying mass mailing lists and sending out vast, indiscriminate marketing pitches via email, blow those notions up now! In this era of permission-based marketing, it's critical that your audience opt-in to receive the information from you. Make opting-in very easy with highly visible single-click options—and unsubscribing should be that easy too.

To make sure you're acquiring email addresses the right way, follow these four guidelines:

1. Send email only to those who have opted-in. Again, the idea is simple; people are overloaded but they will generally read what they've asked for.

2. Obtain opt-in permission via common methods. These include single opt-in, double opt-in, or confirmed opt-in (see glossary for detail on these terms). Be sure your marketing automation provider delivers the tools to easily track who asked for what,

and when. Not only is this critical to communicate effectively with customers, but you can learn a lot about how to influence them by noticing their communication preferences. Remember that you cannot send email to customers requesting permission to send them email.

3. Do not purchase or rent mailing lists. Beware the SPAM Trap! Found in most purchased or rented lists, SPAM Traps are "triggered" to cause email to be treated as SPAM. Having such a trigger in your mailing is a red flag for ISPs. The quality of purchased or rented lists is unverifiable, even from providers who say they've gotten people to opt-in, so they are better avoided. Some ISPs will also have what is known as "Honey Pot Traps" these are email addresses that the ISPs are aware have been inactive for at least 12 months and therefore they may consider emails to those accounts as SPAM.

4. Always be up-front. State clearly what the contact is opting-in for. After gaining their permission, the credibility of your brand and the quality of their customer experience hinges in part on giving them what they thought they were receiving. Do not be misleading.

Do the Inside Work

Marketers do not work alone. Define the internal dependencies on which the success of your email campaign depends. Ensure that all customer touchpoints within your organization—such as customer support or sales—know about upcoming campaigns.

Remember, many customers are touching or being touched by other facets of your organization—maybe even within marketing; increase your success by being consistent across all channels.

Using CRM applications, many marketers today make it a standard practice to check whether there's an open customer support incident before sending out proactive emails. Similarly, some customer support organizations share incident information with marketing so they can follow-up with timely emails regarding upgrades or new programs.

To make sure you're doing your inside work, follow these three guidelines:

1. Ensure cross-organizational support for and knowledge of email campaigns.

2. Make sure you have the reporting tools in place to support campaign goals. This means you need a marketing automation application that tracks intended action completion, such as a form submittal, form download, or purchase. Integration between your web and email marketing tools is vital here.

3. Review invalid contact reports. Stand by the integrity of your mailing list at all times. Be aware of how many contacts are invalidated with each mailing. Some undeliverables may be inevitable, but a high volume suggests the need to reevaluate or clean up your list.

Content is King

Once you've followed these best practices to ensure that your messages get through, content is king. We'll leave the copy to you, but here are some content guidelines:

1. Remind the contact why they are receiving this email. Include a link to opt-out and to update their profile information. Have both of these at the top of the email.

2. Ask contacts to add the "from" address to their address book. This ensures consistent delivery.

3. Use a consistent look-and-feel. The basic formatting of your email marketing messages is not the place you want to differentiate yourself. As with a business letter, putting things where people expect them speeds expedition of requested actions and ultimately supports better rates of return. A common look-and-feel provides a consistent customer experience and should include spaces for: email opt-in, email format correction, add-to-address book, company website and contact information, relevant copyright references, opt-out, privacy policy, profile update, and "reply-to" policy if different from the "reply-to" address.

4. Include your privacy policy. Tell contacts how their profile information will and will not be used. Assure contacts that their information will never to rented or sold unless they specifically opt-in to partner email programs.

5. Allow contacts to easily update their profiles. Have information already filled in, so contacts can simply enter a cursor to type in a new address, information about their internet connection, and so on.

6. Ensure the "from" and "reply-to" addresses make sense to your contacts. A clear "from" address increases recognition of the message to recipients and ISPs.

7. Make the "subject" line and body copy sensible and intuitive. State up-front any terms or special conditions, such as with an offer or promotion. AVOID special characters or jumbles of letters and numbers as these can identify your mail as SPAM. Consider that commonly-known acronyms in your industry may be senseless jumble to an ISP.

8. Avoid CAPs, special characters, and certain words. These are common flags for SPAM. Avoid profanity. See the "SPAM Flags" list just prior to the glossary at the end of this paper.

9. Ensure your content is internally approved by all necessary stakeholders, including the legal department.

10. Target your campaign to specific audiences. The narrower the better. By tracking demographics, previous campaign history, offer acceptance, and interests stated in the customer's profile, over time you should be able to deliver increasingly timely messages demonstrating ever-greater levels of specificity. Herein lays the real beauty of email marketing—greater personalization made possible by increasing customer intimacy.

11. Balance images and text. Pleasing graphic design still applies; you want your message captivating but not distracting, and easy to read.

12. Use test cells to optimize mailings. Test randomly selected segments of your audience to try out different approaches. For example, try different subject lines or body copy to different groups of the same or very similar audiences.

13. Test email content for SPAM identification. RightNow's CAN-SPAM checker makes this simple; we can recommend third party solutions as well.

14. Include the physical postal address of your organization within your email. All emails governed by CAN-SPAM must contain a physical address or valid P.O. Box of your organization.

A NOTE ABOUT LEGAL COMPLIANCE

Ensure compliance with SPAM laws. Legal definitions and penalties vary internationally, so consider this if your email campaign crosses borders. It is important to stay abreast of current and pending legislation. RightNow ensures ongoing CAN-SPAM compliance of our own email marketing tools through our hosted delivery model. Good sites to monitor rules and regulations include www.spamlaws.com and www.findlaw.com.

Ongoing commitment to effective email marketing practices can improve your customer's experience and allow you as a marketer to better understand your target audience. While specific best practices may continue to evolve, the maturity of this industry and the SPAM laws that guide it mean that marketers can plan on using email as a powerful marketing tool for sometime to come.

SPAM FLAGS

To maximize email deliverability, AVOID the following words and/or phrases in your email subject line.

DO NOT USE ALL CAPS
50% Off
100% Free
Act Now
All New
Amazing
As Seen On
Buy Direct
Cash Bonus
Call Now
Credit
Compare
Collect
Contains $$$
Don't Delete
Discount
Double Your Income
Earn $$$
Easy Terms
Excessive $ or !
E.X.T.R.A. Punctuation
Free
Information You
Join Millions
Million Dollars
No Cost
Now Only
Order Now
Opportunity
Promise You
Please Read
Removes
Requested
Subscribe Now
Special Promotion
Save Up To
Satisfaction Guaranteed
Serious Cash
You've Been Selected
Why Pay More

GLOSSARY

Abuse Reports – any email received by an ISP or organization indicating SPAM has been received. ISP-generated abuse reports are very serious, and may adversely affect deliverability to that ISP if corrective action is not taken.

Branded Domain – an internet domain name uniquely associated with your organization.

CAN-SPAM – United States legislation governing commercial email communication, and regulated by the United States Federal Trade Commission. CAN-SPAM legislation applies to any email address you send to residing within the United States.

Deliverability – the overall process of ensuring that your email arrives in its intended recipient's mailbox.

DKIM – DomainKeys Identified Mail: like DomainKeys, an email authentication technology that uses cryptographic signatures to determine which emails have originated from a particular organization. DKIM differs from DomainKeys primarily in the email headers used to generate the cryptographic signature.

DomainKeys – an email authentication technology that uses cryptographic signatures to determine which emails have originated from a particular organization.

"From" Address – in an email, the field that indicates who the email is from. This should always be a valid email address.

IP Address – the unique network address of a machine or service on the internet. Email reputation and authentication services observe email arriving from a particular IP address, and associate reputation by the IP address.

ISP – Internet Service Provider. An organization that provides internet services to its customers that usually include email. Yahoo, AOL, and Hotmail would all be considered ISPs, as would one's high speed broadband provider.

Opt-In: Single, Double, Confirmed explicit permission given by your contacts to receive emails from you. For single opt-in, a contact gives you an email address and indicates that he or she is willing to receive communications from you. For double opt-in, a contact responds positively to your email confirming that they indeed signed up to receive your communication. This is also referred to as closed-loop opt-in or confirmed opt-in. All email you send should be to contacts that have participated in one of these processes and have indicated that they wish to receive email from you.

Privacy Policy – a document that expresses to your contacts how their personal information will be used.

Reputation – the collected information about an organization's email sending patterns. Reputation is adversely affected by how responsive an organization is to complaints, how many complaints are received as a percentage of total emails received, and how many emails are delivered to non-existent email addresses. A poor email reputation will result in fewer emails being received and viewed. Reputation is usually maintained at an ISP level, and also shared via services like SenderScore and Microsoft's SNDS.

Response Rates – in an email campaign, a positive action observed in response to your email. Includes links followed from your email, but would not include views observed from your email.

Sender-ID – like SPF, an email authentication technology that identifies IP addresses authorized to send email on behalf of a particular organization. Sender-ID and SPF differ primarily on the components of email they observe to determine authentication.

SPAM – any unwanted email received, as defined by the recipient.

SPAM Trap – an email address that is not associated with any person. Email received at this address is almost certainly SPAM, because no one could have given opt-in permission for that email address. Several large ISPs take inactive email addresses and turn them into SPAM Trap addresses. Spam Trap email will seriously affect an organization's email reputation in a short amount of time.

SPF – an email authentication technology that identifies IP addresses that are authorized to send email on behalf of a particular organization. SPF defines policies about how email should be handled for a particular domain name.

Template – a consistent document format in which particulars related to the campaign may be added without substantially changing that format. Incorporate "look" as well as placement of particular content items like unsubscribe links and mailing addresses are usually provided through the use of templates.

Test Cells – a set of known good email addresses maintained by your organization through which proofs of your emails are sent, which your organization monitors for deliverability and rendering.

Warming IPs – the process of sending small amounts of email through a newly used IP address in order to establish positive deliverability reputation. IP addresses are warmed over several weeks. We recommend the following methodology:

First send: 2000 well-qualified contacts
Second send: 10,000 contacts
Third send: 20,000 contacts
Fourth send: 40,000 contacts
Fifth send: 80,000 contacts
Sixth send: All remaining contacts.

.....

ABOUT RIGHTNOW

RightNow (NASDAQ: RNOW) delivers the high-impact technology solutions and services organizations need to cost-efficiently deliver a consistently superior customer experience across their frontline service, sales, and marketing touchpoints. Approximately 1,900 corporations and government agencies worldwide depend on RightNow to achieve their strategic objectives and better meet the needs of those they serve. RightNow is headquartered in Bozeman, Montana.

For more information, please visit www.rightnow.com.