

Understanding and Maximizing Deliverability

Strategies for Success in Permission-Based Email Marketing

Executive Summary

Permission-based email has matured as a communication channel. It has become a cost effective, measurable, and personalized way to build and maintain a relationship with customers. However, the inevitable abuses of email have forced ISPs and other hosted email vendors to take drastic measures to protect their users.

These measures have impacted the effectiveness of both legitimate and illegitimate email. Deliverability (the ability to deliver a message to a recipient's inbox) remains a primary concern of permission-based email marketers (see sidebar). Despite the claims of many email industry vendors, there is no simple fix to secure optimal deliverability. No brother-in-law working for an ISP, signature on your email, or secret handshake will address all of a sender's deliverability challenges.

Optimizing email deliverability requires a combination of tactics, some of them implemented by an email sender and some by their Email Service Provider.

An email gets blocked in only a few different ways: an ISP refuses the email from a suspicious sender, an ISP/user filters an email with suspicious content, an ISP/user refuses a sender's email based on a published list of offenders, or a technical problem interrupts an email's delivery. Unfortunately, each one of these scenarios can be triggered by one of many different reasons.

Improving deliverability requires a thorough understanding of these reasons and a careful analysis of their relationship to a given situation. A strategy for improving deliverability could include a change to basic business processes, a partnership with a specialized vendor, or even some email recipient psychology.

The most effective strategy will be one that is tied closely to a specific email sender's circumstances.

All email marketing users, in partnership with their Email Service Providers, should design and implement a balanced deliverability plan. They should take care to address not only the technical details of deliverability but also the traditional marketing practices of protecting a customer relationship and ensuring that content is both targeted and relevant.

Valuable Permission-Based Email Marketing

In it's simplest sense, the difference between spam and legitimate commercial email is *permission*. However, even a sender with permission can send emails too frequently, emails with content that is irrelevant to a given recipient, or content which is just plain boring and repetitive. Successful email marketing depends on a sender's ability to protect the permission they have received, and to deliver information that is valued by the recipient.

Table of Contents

Growing Challenge of Deliverability.....	2
Common Causes of Deliverability Issues.....	3
Strategies for Improving Deliverability.....	5
Blue Sky Overview.....	9

Growing Challenge of Deliverability

Deliverability (the ability to deliver a message to a recipient's inbox) has been a top concern of email marketers for several years now. This has happened as ISPs and hosted email vendors, in protecting their users from spam, have also been blocking and filtering a considerable amount of legitimate commercial email.

Deliverability is deceptively complex, leading many marketers to under-invest in the day-to-day processes that drive its successful execution. Many in house users in particular suffer from exceedingly poor deliverability—sometimes without even knowing it.

Deliverability Rates

According to a recent study in the marketing publication ClickZ, Q1 2005 gross deliverability of legitimate commercial email was only 92.5 percent. Of greater interest was the deliverability to the inbox which only ranged from 78 to 88 percent. That means that 10 to 20 percent of legitimate email was not arriving in the recipient's inbox.

Contrary to popular belief, the B2B segment of email marketing is equally vulnerable to these challenges. According to Jupiter Research, the average B2B delivery rate is only 89 percent, excluding bounces. MarketingSherpa's Email Marketing Metrics Guide estimates that 14 percent of B2B emails are bounced. Even with legitimate B2B marketing emails, nearly one fifth are never received.

Growing Popularity

Complicating the efforts of ISPs and email marketers alike, the past several years have brought unprecedented growth in the volume of email campaigns. The growing popularity of email as a customer relationship tool, and the proven value that it can deliver through cost-effective and personalized marketing, has brought greater scrutiny on the process and practices of vendors and email senders alike. The deliverability battle is one that is well worth fighting.

Common Causes of Deliverability Issues

Delivery really begins when a receiver grants permission to a sender to send them email. At this point the sender and receiver become partners in communication. The recipient is the sender's ally should an ISP, spam filter, or blacklist prevent the delivery of a message.

The technology and uses of email are constantly changing. New causes of deliverability trouble continue to arise regularly. At the moment, some of the primary causes of deliverability problems for permission-based email include ISP-blocking and content filters.

Blocking by an ISP

ISPs have taken an increasingly active role in preventing their users from sending and receiving unwelcome email.

- **ISP blocks incoming mail** – This is by far the most common form of ISP blocking. Many ISPs maintain an internal blacklist of IP addresses that are denied incoming connections. An IP address ends up on the blacklist as a result of frequent ISP-customer complaints about traffic from the particular address. The largest source of these complaints is from the “This is SPAM” button that has become a standard feedback loop for the customers of most hosted email vendors.

In addition to spammers, legitimate email senders often fall victim to “This is SPAM” when their content is poor, they send too often, or they in some other way irritate the email recipient (See “Target the Recipient”). Forced to handle a daily load of hundreds of thousands of complaints, ISPs often take the drastic measure of blocking a sender's entire IP range without any notification. The best defense against this is to maintain a close relationship and feedback loop with the ISP (See “Protect Your Reputation”).

- **ISP blocks outgoing mail** – In this instance, an ISP actually blocks its own customer's outgoing traffic to another ISP. Although this is rare, with most ISPs focusing their attention on incoming traffic, it can happen. This tactic may grow more common as ISPs are increasingly held accountable for the manner in which their customers use their services. The growing prevalence of whitelists and third-party reputation audits and certifications is making it much easier to determine whether an ISP is effectively responding to complaints against its customers.

Content Filters

Although content filters exist in a variety of forms, they all examine the contents of an email in an attempt to evaluate its legitimacy. While many content filters add value to a great number of users, they are all subject to an inherent limitation: determining whether an email is spam remains a very subjective process. One recipient's spam is another recipient's legitimate advertisement.

- **Distributed content Filters** – A number of third-party anti-spam vendors help ISPs and customers manage the growing flood of unsolicited email. Postini, Symantec's Brightmail, and other vendors in this field use blocking systems that generate and constantly tune complex content analysis rules that scan email messages, generate message "signatures" or patterns for violating emails, and then distribute those signatures to all of the vendor's clients.
- **ISP content filters** – ISPs often create and adapt their own content filters. Each ISP's filter is different but they all scan for a variety of typical spam characteristics. As spammers evolve, so do these filters. Many can learn to detect new patterns such as the practice of inserting characters in words that would normally trigger a block. SpamAssassin is a good open-source example of how these content filters operate.

- **User content filters** – Almost every email client now provides some form of junk mail filter. While Microsoft Outlook's filter simply searches for offensive keywords and phrases, more powerful filters can be configured and can run from a user's desktop.

Other Common Causes of Deliverability Problems

- **Public blacklists** – The universal backlash against spam has led to the development of several publicly accessible blacklists and whitelists. These lists are often maintained by volunteers and are sometimes used by smaller ISPs and companies, those without a dedicated email administrator. Some widely used lists include Mail Abuse Prevention System (MAPS), SpamCop, Spamhaus, and Spam Prevention Early Warning System (SPE)WS. The criteria for these lists vary greatly, ranging from very reliable to downright casual, depending on the desires and the skills of the list owner.

To avoid interfering with normal email usage, the users of these lists must carefully select the public blacklist organization that most closely matches its own email policy and usage.

- **User lists** – Recent upgrades to email applications, including AOL, MSN, Yahoo!, and Outlook, allow users to create their own lists of allowed and blocked addresses and domains. Some more sophisticated email clients even contain a challenge/response system to query non-whitelisted senders for an authorization code or other type of confirmation.
- **Message bounces** – A “soft” bounce is an email message that gets as far as the recipient’s mail server before being turned back. This could occur because the recipient’s mailbox is full or there is a block against the email sender or IP address. A “hard” bounce is an email message that has been turned back because the recipient’s address is invalid.

Strategies for Improving Deliverability

There is no panacea for optimizing deliverability. As email changes, so do the abuses and the tools for protecting against those abuses. Accompanying these changes, there is a natural evolution in the best practices for preventing permission-based email from being mistaken for spam.

Improving deliverability requires a multi-faceted and constantly changing strategy. The basic elements of this strategy include: permission, complying with content and design standards, targeting the recipient, intelligent processes, proving your identity, and protecting your reputation.

Permission

Permission is the foundation of email marketing. Not only does it have an enormous impact on the deliverability of a piece of email, permission also has legal and ethical considerations.

The “N” in “CAN-SPAM Act of 2003” stands for “Non-Solicited” – permission is the point when email becomes solicited. Failure to capture and track permission can not only annoy the recipient and damage the reputation of the sender, it can result in large legal costs and fines.

- **Double opt-in subscription** – A single opt-in subscription merely requires a subscriber to fill out a form or make a request. A double opt-in subscription also confirms that request. The most common way to confirm the subscription is with an email describing the subscription and requesting the subscriber to validate by responding or clicking on a hyperlink. Many marketers resist moving to a double opt-in process for fear of losing new subscribers. However, a well executed double opt-in strategy will deter very few subscribers beyond those who didn't actually want to subscribe in the first place.

The benefits of the double opt-in strategy include a list with fewer unintentional subscribers, fewer bounced emails due to address input errors, and a strong process and audit trail to use to defend against any spam complaints.

- **Track and Store** – Capture key pieces of data during the opt-in process. You should be able to easily store the date, time, subscriber's IP address, and the source of the subscription. Store this information like you do your tax and employee information.
- **No Trickery** – A common ploy to get a person to subscribe is to pre-check the "subscribe" box on a user form. Although this may lead to a higher number of initial subscribers, it will invariably result in a subscriber list tainted with people who have unintentionally opted in. Not only will subscribers be less responsive to emails sent to this list, some may not recall subscribing at all, resulting in a spam complaint. The CAN-SPAM Act requires messages without affirmative consent to include a notice that the email is an advertisement or promotion. Don't jeopardize your marketing efforts and your brand reputation with processes that blur the line between solicited and non-solicited email.
- **Easy Updates** – Include a prominent “update your address or preferences” link. Approximately one third of an average email list's recipients churn each year as a result of address changes. Make it easy for your customers to stay with you.

Content and Design Standards and Best-Practices

Like permission, the content and structure of your email has an immediate and dramatic affect on the deliverability of an email.

- **Basic HTML Standards** – One of the dirtiest tricks in a spammer's arsenal is the use of invalid or broken HTML code to hide an email's true contents. When you use HTML in your messages, go out of your way to ensure that it is error-free and that it follows World Wide Web Consortium (W3) HTML guidelines. Don't be mistaken for a spammer because of unchecked HTML.
- **Poor Design** – Amateurish content and spam-like keywords or formatting will make you look like a spammer to ISPs and recipients alike. Both will filter, block, or blacklist you as a result. Get help if you don't have the inhouse skills to add some polish to your formats and content.
- **Preview Pane** – Preview panes are growing more prevalent, allowing many users to screen an email's content without opening the message. Make sure that your message has impact even if only the top portion is visible. Consider including teaser text and an HTML header that will display if a recipient has images disabled.
- **Message Content Checker** – Many email solutions have built-in content checkers that estimate the likelihood of a message being filtered. Use these tools. Although they are at best an approximation, they will help to screen for problems that have gone unrecognized during the writing and design process.
- **Compelling and Branded Subject Line** – Many subscribers receive several hundred email messages a day and much of that is spam. Make sure that, as recipients scan their inboxes, your message is easily recognized. Consider branding your subject line and reinforcing it in the sender name. For example, send your email from "Acme Newsletter" with a subject including "Acme News Update" at the beginning. Although this uses valuable subject line space, it will clearly identify your message and reduce the chances of being missed, filtered, or unopened. Experiment to determine what is received best by your recipients.

- **Content Filtering** – Although no one can be expected to keep up with the latest tricks of spammers and the resulting changes in content filtering, anyone sending email should be familiar with the different kinds of filters and the content that is high risk. Keep current by reviewing your bounce messages and by tracking the bounce and open rates for different messages.

Target the Recipient

Another strategy for improving deliverability moves beyond getting an email into the inbox. Targeting the recipient includes tactics for getting the subscriber to actually open and read a message. It has more to do with psychology and your customer relationship than it does with email systems and technology.

- **Friendly Sender Name** – The sender name should be recognized and expected, and should be consistent from one email to the next. When scanning overloaded inboxes, recipients see the sender, subject, or both. Consistently using a sender name that is simple and recognizable will foster trust and familiarity with your subscribers. Take care in your choice of a sender email address as well since some large email clients display the name *or* the email address but not both.
- **Mail Regularly** – Send at least once every 30 days in order to keep your list current. If you wait longer, you will begin to experience deliverability problems resulting from changing email addresses and subscriber preferences. If you have already waited too long, consider re-soliciting permission before beginning a more frequent email send.
- **Personalization** – The greater the relevance and personalization of your messages, the better the chance that they will be recognized and appreciated by subscribers. Track click-through activity in order to segment your lists by subscriber interest and then send messages with subject lines and content that targets those individual interests.

- **Manage Subscriber Expectations** – Make sure that recipients aren't surprised by what they receive or how often they receive it. During email sign up, indicate the frequency, email type, the content of mailings, and the value proposition of anything you intend to send. Summarize key information in a welcome message and provide a link to your privacy policy.

Improve Your Process

The execution of your email marketing strategy and the internal processes that you use will determine whether your email gets delivered. ISPs and content filters cannot measure good intentions, only results.

- **List Hygiene** – Lists of incorrect or outdated addresses affect the delivery, click, open, and return rates of both current and future email campaigns. Their high bounce rates become suspicious to ISPs and often result in your future messages being blocked or routed to junk folders as well.

Provide a one-step, web-based unsubscribe process to keep subscriber profiles current. Automate the response to email address changes and remove addresses if they hard-bounce more than once. A few unhappy subscribers can quickly damage the deliverability of entire email campaigns.

- **Monitor Your Delivery** – Review your delivery reports during and after each send in order to detect problems. Monitor the feedback and reply mailboxes associated with your email application. If possible, set up filters to intercept automated challenge-response programs that intercept and detain your email until you verify your identity.
- **Proofing and Testing: Content** – Always send a test of your message to yourself, to co-workers, and if possible, to a larger test list across the domains of your primary recipients. These tests or proofs help to uncover mistakes, missed changes, broken links, incorrect image paths, and potential blocking or filter problems.

For high volume campaigns, you may want to send a test message to a small percentage of your overall list in order to test several content versions and to identify any delivery problems.

- **Proofing and Testing: ISP/Domain** – Set up a test account at major ISPs and in several email clients, platforms, and web browsers. Another option is to use a delivery-monitoring service. Compare the open, delivery, bounce, unsubscribe, and spam complaint rates between your tests and actual campaigns in order to validate the quality of your testing.
- **Send Time** – Avoid all similarities with spam. Spam is often sent in the middle of the night – so you shouldn't. Adjust your send time to your readership. Do they check email when they get to work or when they get home? Ideally, you want to schedule your send so that your message is the last email received before your recipient checks their email. It will be at the top of their inbox.
- **Send Slowly and Confidently** – Again, avoid similarities with spammers. Some email systems shovel as many messages as possible through one connection, almost like putting 1,000 email addresses in the "To" field. This looks just like a spammer who wants to get as many messages sent before being blocked by the ISP. Instead, throttle your email send rate to no more than 2500 messages per minute. Take care not to send so quickly that you interfere with your ability to receive bounced emails and other traffic.

Prove your Identity

As the cat and mouse game of domain and content blocking has grown tiresome, anti-spam efforts have shifted towards reputation checking and management. In many cases, the accreditation of the sender now counts more towards the deliverability of a message than does the email's content.

- **Authentication Methods** – Currently, no single authentication method applies to all ISPs and senders. Some of the more common methods (and leading users) include Sender Policy Framework (AOL), Sender ID (MSN/Hotmail), and DomainKeys (Yahoo!). These authentication keys also protect you from spammers who try to impersonate your sender information in an attempt to gather confidential information from your customers and subscribers (known as *phishing*).
- **Reverse DNS** – Make sure that your outgoing mail IP has a reverse DNS (RDNS) properly set up. This allows a receiving email server to see who owns the IP trying to connect to it. Leaving the RDNS blank will make you look like a spammer who is trying to hide their identity.

Protect Your reputation

ISPs, accreditation agencies, independent blacklist operators, and others judge, block, and filter your messages based on your reputation. This reputation depends almost entirely on how much email you bounce, how many spam complaints you generate, and how well you respond to complaints.

- **Business Process** – Since your reputation is based on your email history, you must track all aspects of your email process and then respond quickly to issues as they arise. Pay special attention to your opt-in process, list hygiene, content testing, delivery tracking, complaints response, and your published privacy policies.
- **Monitor Bounces** – ISP/domain bounces are one of your most reliable forms of feedback. Make sure that you accept and monitor these bounces as part of a larger relationship with the primary domains of your recipients. Many email systems have a tendency to reject bounce messages, a sure way to generate suspicion at an ISP or domain.
- **The Whitelists** – Get listed on the whitelists of those ISPs that have them. This does not guarantee deliverability but it does help to cover

up the occasional deliverability problem with the users of the whitelist.

- **Reporting** – Segment your reports by ISP/domain, looking for unusual bounce, unsubscribe, spam complaint, or open activity. Since the largest ISPs (AOL, EarthLink, MSN/Hotmail, and Yahoo!) and many smaller service providers use different procedures to accept and reject email, you must track your performance with each.
- **Get others to vouch for you** – As anti-spam efforts have moved away from domain and content blocking, reputation management and accreditation groups have become more important for getting your email delivered. A third party, such as Habeas or Bonded Sender, examines your list, permission, subscription, delivery, and privacy practices and then provides an accreditation if you pass. Accredited senders are often automatically placed on ISP-accepted whitelists, allowing their email to bypass a portion of normal filtering.
- **ISP/Domain Relationships** – Develop a relationship with the anti-spam official at the primary domains of your recipients. They can help you resolve any issues before they escalate. If you use an email service provider, find out who handles ISP relations and work through this person to track and resolve any problems. Sort your subscriber database by domain to see which companies are a significant part of your list, and then check your delivery and open rates with each.
- **The Blacklists** – Regularly check for your IP addresses on the main blacklists. It can take some time to get your name removed from a list so catch the errors soon and start the protest process quickly. At www.DNSstuff.com, you can check whether anyone is blacklisting your IP address.
- **Monitor spam complaints** – Even the best permission marketers receive spam complaints. Track the number of complaints for each mailing to establish a baseline level. Then, look for mailings with complaints that exceed this norm and try to determine what caused the problem.

Blue Sky Overview

Blue Sky Factory is a leading provider of email marketing software and solutions. Their on-demand services and personalized support help customers of all sizes get the most out of permission-based email marketing. Blue Sky Factory has been exceeding customer expectations and experiencing a year-over-year revenue growth rate of nearly 100% for several years.

Founded in 2001 and headquartered in Baltimore, Blue Sky Factory is proud to work with some of the world's leading advertising agencies, public relations firms, interactive shops, and with a variety of direct clients. Its combination of self-serve and managed service solutions ensure that each customer receives the optimal level of support, even as their needs change. Blue Sky Factory's staff of technology, database, creative, and marketing experts help to optimize each marketing effort.

Publicaster ASP, Blue Sky Factory's web-based email marketing platform, combines a simple user interface and a robust feature set to help organizations of all sizes to manage their own email marketing campaigns. Publicaster ASP includes a high speed delivery engine and detailed, real-time tracking and reporting metrics.

Blue Sky Factory also offers a fully managed solution. Their online marketing professionals can work with your team to create the best email strategy for your organization's goals and objectives. Blue Sky professionals are available to handle the strategy and design, set up and quality assurance, distribution, and the tracking and reporting of your email marketing initiatives.

Find out why companies like Under Armour, Weber Shandwick Worldwide, and Texas Instruments rely on Blue Sky Factory for their email marketing needs.

Blue Sky Factory, Inc.

1010 Hull Street
The Tide Building
Suite 200
Baltimore, MD 21230

Phone: 410.230.0061

Toll Free: 866.216.BLUE (2583)

General info: info@blueskyfactory.com

Sales: sales@blueskyfactory.com

Technical support: support@blueskyfactory.com