Marketing Cheat Sheet

Email Deliverability

What is Email Deliverability?

Email deliverability is the ability of an email message to reach the intended recipient's inbox, which is affected by spam filters, client-side filters and junk folders. It refers to the rate of success of deliverability, where the recipient does not report the email as spam or unsubscribe. It also refers to the management, procedures and technologies surrounding this process.

Coding for Email Deliverability

- Make sure to use clean and efficient HTML. Properly close HTML tags to avoid undesirable email rendering.
- Don't embed CSS in header tags, as many email clients strip these tags from the email.
- Use an HTML validator to guarantee your message uses correct HTML.
- Include a text version along with the HTML version to ensure readability from clients that can't receive HTML messages.

Subscription Best Practices

- Sign up for ISP feedback and receive instant notification of subscriber complaints.
- Use the highest permission standard you can support, such as double opt-in. At a minimum, use confirmed opt-in.
- Provide subscribers with detailed sign-up options so they have a clear idea of what they will receive. Some new subscribers drive complaints because they aren't receiving the content they wanted or expected.
- Give clear instructions on adding your email to their address book, both on the sign-up page and in your welcome email.

Email Deliverability – Analyst Facts

"77% of deliverability is based on sender reputation."
– Return Path, 2008

"The presence of a just one spam trap can drop your deliverability rating by up to 53%"
– Return Path's Reputation Benchmark Report, 2009

"Costs of incorrectly blocked opt-in email will rise to $419 million in 2008."
– Jupiter Research

"Sender Score reputation score closely correlates to delivered rates. Senders with a Sender Score of 72 had, on average, delivered rates of 87%. Compare that to senders with a Sender Score of 26 who average a delivered rate of 23%."
– Return Path's Reputation Benchmark Report, 2008

Glossary Terms

Authentication – Technical standards through which ISPs and other mail gateway administrators can establish the true identity of an email sender

Blacklist – A list of IP addresses believed to send spam

Bounce – A message that is returned to the sender because it was not deliverable

Cascading Style Sheet (CSS) – Controls the design and format of a document written in HTML

Deliverability – The ability of an email message or campaign to reach the intended recipient's inbox, which is affected by spam filters, client-side filters and junk folders

Delivery Status Notification (DSN) – Also known as "bounce message", a system that informs the sender of a delivery problem

DNS Records – The database records stored in the domain name system

DomainKeys Identified Mail (DKIM) – A method for email authentication that allows an organization to take responsibility for a message in a way that can be validated by a recipient

Domain Name System – A naming system for computers connected to the Internet or private network

Email Service Provider (ESP) – A company that provides email services, including batch email and email marketing

Internet Protocol Address (IP Address) – A number assigned to each computer or network in order to distinguish each network interface and networked device

Internet Service Provider (ISP) – Sometimes referred to as Internet access provider (IAP), gives customers access to the Internet

ISP Feedback – When the ISP forwards complaints of recipients to the organization that sent the email

List Fatigue – A condition producing diminishing returns from a mailing list whose members are sent too many offers, or too many of the same offers, in too short a period of time

Phishing – Sending email that claims to be from a legitimate organization to trick recipients into providing personal information

Role Accounts – An email account that is associated with a department, office, position or task

Seed Email Accounts – Accounts created by a monitoring service with each of the ISPs

Sender Policy Framework (SPF) – An email vailidation system that is used to prevent spam

Sender Score – An indication of the trustworthiness of an email source

Spam Traps – Old inboxes that ISPs reactivate specifically to trap spammers. Because these addresses have never been registered to receive email, any mail that lands in the trap inbox is labeled as spam

Spoofing – A fraudulent email activity in which the sender address and email header are changed to look as though the email originated from a different source

Design for Deliverability

- Avoid Flash and JavaScript. Flash doesn't work consistently in most email clients and JavaScript is usually disabled as a security precaution.
- Don't embed your text and graphics in a single image. The email should not contain attachments or large images. These are things that are commonly used by spam and will go directly to junk folders.
- Check to see how your email will render in each ISP. If your recipients cannot make sense of the email, they will most likely call it spam.
- Use "absolute" links. Be sure to code your links so the email client can recognize where it is going. If you do not do this, links and images are more likely to break.
- Do not link images used elsewhere. Because of human error, it's best to not use images that are linked somewhere else on your website. The web designer could replace or delete these images, causing them not to display.

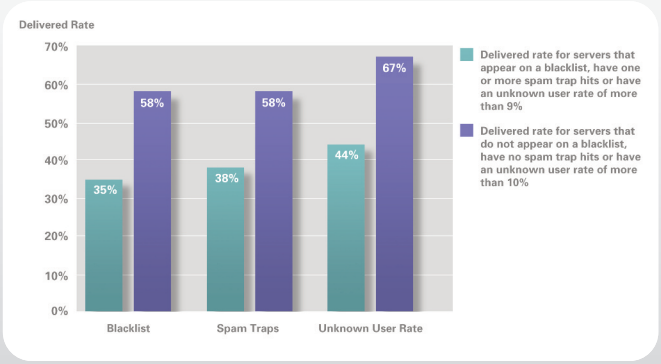
Top Data Measured by ISPs

- **Volume:** Spammers have high numbers of total email. If your company has a high volume of email, make sure your complaint, hard bounce and spam trap hit rates are low.
- **Complaint rates:** This is the amount of times email recipients hit "report spam" when they receive your emails. Small increases or decreases can dramatically affect your inbox performance.
- **Bounce rate:** A bounce is caused by a non-existent or unknown address. By lowering this rate you can increase your chances of maintaining your reputation.
- **Spam trap hits:** Spam traps are old inboxes that ISPs reactivate specifically to trap spammers. Because these addresses were never registered to receive mail, any email that lands in this inbox is marked as spam. Poor list hygiene leads to inclusion of spam trap addresses on a mailing list.
- **Authentication:** Authentication lets the ISP know that the sender is who they say they are. With the help of your IT department you can take steps to further authenticate your IP.

Top Resources

- MAAWG: www.maawg.org
- Email Experience Council: www.emailexperience.org
- Return Path's Resource Section: www.returnpath.net/blog/whitepapers.php
- Deliverability Blog: www.deliverability.com
- DKIM: www.dkim.com
- SenderID: www.microsoft.com/senderid
- SPF: www.openspf.org

Spam Traps, Blacklists & Unknown User Rates Impact Delivered Rates



The Super Six: Best Practices That Will Make You More Successful with Email Marketing – Return Path

How to Keep Your Lists Clean

- Learn how your server processes bounces. Regularly clear out role accounts, clearly non-used addresses and addresses with errors.
- Quarantine new data until you send a welcome message to avoid adding a bad address to your campaigns.
- Make it easier for customers to update their information. At the point of unsubscribe, offer change of address and frequency options.
- Regularly email your lists. Lists that aren't emailed frequently are more likely to increase bounce rates and have old addresses that are now spam trap addresses.
- Establish a time where you remove inactive records if they have not responded to anything sent (e.g. 1 year, 6 months, 90 days).

Authentication Best Practices and Benefits

In order to clearly differentiate yourself from spammers, take steps to protect your brand by incorporating sender authentication technologies.

- Research and find the authentication scheme that best suits your organization's needs. (DKIM, SenderID or SPF)
- Identify the machines that send email for your organization and record the IP addresses and sending domains for each.
- Create and publish authentication records.
- Test your authentication records by publishing records in "test" mode. This will determine if you've missed identifying mail servers in your inventory.
- Regularly monitor your IP addresses.