



Email Delivery

Are my emails reaching the intended audience?

If you send regular emails to your customers and/or prospects the bad news is that not all of your emails are making it to your intended recipients, even if you have accurate email addresses. Chances are that ISP SPAM filter software, SPAM-blocking email servers, and email content filters are roadblocks to your emails.

Research studies show that opt-in emails are erroneously bounced or SPAM blocked at the rate of 15% to as high as 41% (according to Mail.com). According to Email Delivery monitoring firm "Returnpath" approximately 20 % of all email gets blocked or filtered by ISPs and corporate system administrators.

Essentially, 15% to 41% of the email you send to people who have requested it (as information relevant to them) does not reach them. Just by choosing the wrong words or phrases, sending the wrong type of attachment or sending in volume, your email can be classified under "Junk" and end up filed in a virtual rubbish bin.

There is no implied responsibility on behalf of any service provider to guarantee delivery of all messages. In fact, ISPs are provided the right to filter and block email any way they deem necessary according to their policies. The problem is that filters block not only SPAM, but also permission-based email as well. And the law doesn't burden ISPs to discriminate whether the email was permission-based or unsolicited. They can block incoming bulk email simply on the basis of a single complaint.

Delivering even an opt-in email to a recipient's inbox, can be a daunting task due to the number of potential points of failure.

How to improve Deliverability?

Every company sending large volumes of commercial or transactional email struggles with a hidden issue: email deliverability. Whether email is sent in-house or through an ESP, non-delivery erodes response rates and campaign effectiveness.

Companies that are inexperienced with email marketing could see as high as 50% of their emails bounce. Listed below are hints & tips on what you can do to get your email into more inboxes. By following the recommendations listed below you will achieve over 85% email delivery rates.

To determine how email deliverability affects your email campaigns, there are several things you need to do:

1. Understand the factors that contribute to blocking & filtering
2. Monitor your campaign delivery to learn the extent of problems
3. Uncover the root causes of your specific issues
4. Ensure your technical infrastructure meets required standards
5. Build relationships with ISPs to help resolve delivery issues

There are six primary filtering methods used by ISPs and corporate system administrators as they deal with the deluge of SPAM hitting their servers.

1. **Blacklists:** Several organisations such as SpamCop keep lists of IP addresses linked to suspected or known spammers, and make them public for ISPs and others to use in screening out SPAM. ISPs and some corporate system administrators also keep their own list. These are typically based on complaints received from subscribers, but they can also be based on other criteria like unknown user rates and server configuration issues.
2. **Fingerprinting/SPAM traps:** These systems work by filtering known SPAM messages after matching them against creative that has either generated previous complaints, or was delivered to SPAM trap addresses. The "From" address can also influence this.
3. **Machine Learning-based Content Filters:** These filters block based on words and phrases. Machine learning filters can be based on the content in the email body or header. SPAMAssassin is an example of one of these filters.
4. **Server Configuration:** Certain server configurations open you up to instant blocking. These include not having a reverse DNS, or having open relays or open proxies. Make sure your IT dept know all the ins and outs to setting up your email server, including the rules around authentication.
5. **Volume Cap:** Some ISPs may shut down sending connections when resource demand gets too high. Be mindful of your number of connections or messages per connection so they don't exceed their thresholds. Emails that exceed the allowed maximum rate trigger volume filters at most of the large & prominent ISP's. This problem is also because of the type of email you have sent and the number of emails you have sent to that server. An option is to try and send text emails to new lists as an initial introduction and follow that with an HTML newsletter.
6. **Challenge Response:** Some systems require a reply to a challenge message, which basically proves you are a real person. Having your email or domain in the recipient's "allowed sender" list prevents this challenge requirement.

Complaints:

The number of people who complain to ISPs and SPAM watch groups about your email can be detrimental to your email campaigns. The first line of defense is to make your email so relevant that it is at the opposite end of the SPAM spectrum.

According to a recent DoubleClick study, 72% of people think that hitting the "this is SPAM" button in their email client is the best way to unsubscribe from a list. This means that every time your customers decide they don't want your email, you are susceptible to complaints at the ISP level – and the ISPs make this easy with very prominent "report SPAM" buttons.

You can minimize complaints by following best practices. Make sure you keep track of your complaints and correct issues causing them. Companies following standard opt-in and privacy guidelines can continue to experience optimal delivery rates.

Some resources available to help you keep track of complaints to ISPs are:

AOL Feedback Loop

<http://postmaster.info.aol.com/fbl/index.html>

United Online Feedback Loop

<http://www.unitedonline.net/postmaster/whitelisted.html>

SPAMCop

<http://www.SPAMcop.net/fom-serve/cache/94.html>

Abuse.net

<http://www.abuse.net/addnew.html>

Knowing the root causes of delivery issues should help you prevent them. However, you still need to monitor your email deliverability rates religiously because the rules around delivery change daily. Many companies make the mistake of investing too little staff or budget resources for deliverability – yet it controls the performance of email campaigns.

To reach full delivery, you should:

Monitor: The best way to determine whether you have an issue is to use a seed-list based monitoring service that tracks your true delivery rates across all the major ISPs. You should not just use your bounce codes to determine problems – some mail goes missing, or it might be delivered to the bulk folder, and you'd never know without a service in place to tell you.

Analyse: When your results show less than 100% delivery, it is time to work out why. Your internal or external delivery team needs to look at every aspect of the email in question, and email campaigns as a whole.

Is the program configured correctly? Did the content trigger blocking? Were there list issues contributing to blocking?

Resolve: Build relationships with ISPs so that when problems occur, you have someone to call to help fix them. While there is no magic number to dial, ISP representatives can provide vital clues to the issue at hand, and requirements to fix the issues. You should have a dedicated resource for ISP relations.

Optimise: Use the data from all sources to correct the problems that are leading to your email deliverability problem. Simply by tweaking a list, creative, or server configuration, your email delivery performance can improve – and you will see a direct correlation to response. Again, the deliverability landscape is complex, with hundreds of triggers. If you stay engaged with your delivery, you can continually improve your delivery rates and program performance.

“Bounce rates in 2007 were 12-25% higher on new email lists than house files”

A verified new email list doesn't necessarily mean you can reach all those addresses immediately. Newly imported lists have lower deliverability than existing in-house lists due to the nature of how email servers are programmed to deal with new email from mail servers. When an email campaign is sent to a new list in bulk you tend to see 12% to 25% increase in bounce rates because of the various email blocks and message rules on the email servers, which haven't yet white-listed you. We recommend sending emails in smaller volumes to new lists (no more than 1000 emails at a time) to get the best delivery rates. Also, try keeping the emails to less than 5 contacts per company so that your email is not flagged as SPAM.

Unknown Users:

ISPs block domains in part based on the number of “unknown user” errors generated when sending large broadcasts of emails. Keeping your email list clean and current will help lower the percentage of bad addresses on your list resulting in “unknown user” codes at ISPs.

You should remove all bad addresses from your database promptly and:

- Run your file through a list hygiene service.
- Require double entry of addresses for accuracy.
- Check addresses for RFC compliance & ISP standards.
- Send a welcome message and pull bounces off immediately.

Content:

Make sure your content is free of SPAM filter triggers before you send a campaign. Test creative before sending campaigns.

You can't assume that avoiding words like “free” will ensure your delivery. Sometimes the most innocuous words – and uncommon ones – can trip up your best efforts. The only way to ensure that your content doesn't trigger a block is to test it in a “SPAM lab” such as SPAM Filter Monitor, and correct all issues that are preventing delivery before you hit the send button.

Investigations show that emails with near-identical subject lines to several employees are detected and 'junked' or bounced as undeliverable. The logic used by SPAM filtering software is to identify words, phrases, and patterns that are likely to trigger filters. Content filters focus on promotional, phrases such as “work from home”, “guaranteed income”, or even phrases such as “click here” and “unsubscribe.” They also assign points to text formatting that is indicative of SPAM, such as the use of ALL CAPITAL LETTERS, excessive use of bright colors, images or very large fonts.

Content to avoid

Here is a list of 250 words and phrases from top SPAM filter lists. It is not complete. We have left out porn trigger words. Most SPAM filters work on a point system, so that the occurrence of just one “SPAM phrase” might not trigger rejection - except some which the filter considers notorious. SPAMAssassin 2.43, for example, assigns default points for these top offenders, as follows:

Reverses ageing	3.37
'Hidden' assets	3.28
stop snoring	3.26
Free investment	3.19
Dig up dirt on friends	3.12
Stock disclaimer statement	3.04
Multi level marketing	3.01

Compare rates	2.83
Cable converter	2.75
Claims you can be removed from the list	2.70
Removes wrinkles	2.69
Compete for your business	2.57
free installation	2.51
Free grant money	2.50
Auto email removal	2.36
Collect child support	2.33
Free leads	2.29
Amazing stuff	2.26
Tells you it's an ad	2.21
Cash bonus	2.20
Promise you ...!	2.15
Claims to be in accordance with some SPAM law	2.11
Search engine listings	2.09
free preview	2.07
Credit bureaus	2.03
No investment	2.01
Serious cash	2.00

Even if you don't use these notorious phrases, other SPAM words can add up. Here are some to be aware of in your email communications.

4U	Free hosting	Online pharmacy
Accept credit cards	Free installation	Only \$ / £
Act now! Don't hesitate!	Free investment	Opportunity
Additional income	Free leads	Opt in
Addresses on CD	Free membership	Order now
All natural	Free money	Order status
Amazing	Free offer	Orders shipped by priority mail
Apply Online	Free preview	Outstanding values
As seen on	Free priority mail	Pennies a day
Billing address	Free quote	People just leave money laying around
Auto email removal	Free sample	
Avoid bankruptcy	Free trial	

Be amazed	Free website	Please read
Be your own boss	Full refund	Potential earnings
Being a member	Get paid	Print form signature
Big bucks	Get started now	Print out and fax
Bill 1618	Gift certificate	Produced and sent out
Billion dollars	Great offer	Profits
Brand new pager	Guarantee	Promise you ...!
Bulk email	Have you been turned down?	Pure profit
Buy direct	Hidden assets	Real thing
Buying judgments	Home employment	Refinance home
Cable converter	Human growth hormone	Removal instructions
Call free	If only it were that easy	Remove in quotes
Call now	In accordance with laws	Remove subject
Calling creditors	Increase sales	Removes wrinkles
Cannot be combined with any other offer	Increase traffic	Reply remove subject
Cancel at any time	Insurance	Requires initial investment
Can't live without	Investment decision	Reserves the right
Cash bonus	It's effective	Reverses aging
Cashcashcash	Join millions of Americans	Risk free
Casino	Laser printer	Round the world
Cell phone cancer scam	Limited time only	S 1618
Cents on the dollar	Long distance phone offer	Safeguard notice
Check or money order	Lose weight SPAM	Satisfaction guaranteed
Claims not to be selling anything	Lower interest rates	Save \$ / £
Claims to be in accordance with some SPAM law	Lower monthly payment	Save big money
Claims to be legal	Lowest price	Save up to
Claims you are a winner	Luxury car	Score with babes
Claims you registered with some kind of partner	Mail in order form	Section 301
Click below	Marketing solutions	See for yourself
Click here link	Mass email	Sent in compliance
Click to remove	Meet singles	Serious cash
Click to remove mailto	Member stuff	Serious only
Compare rates	Message contains disclaimer	Shopping spree
Compete for your business	Money back	Sign up free today
Confidentially on all orders	Money making	Social security number
Congratulations	Month trial offer	Stainless steel
Consolidate debt and credit	More Internet traffic	Stock alert
Stop snoring	Mortgage rates	Stock disclaimer statement
get it now	Multi level marketing	Stock pick
Special promotion	MLM	Strong buy
Copy accurately	Name brand	Stuff on sale
Copy DVDs	New customers only	Subject to credit
Credit bureaus	New domain extensions	Supplies are limited
Credit card offers	Nigerian	Take action now
	No age restrictions	Talks about hidden charges
	No catch	Talks about prizes
	No claim forms	Tells you it's an ad
	No cost	Terms and conditions

Cures baldness	No credit check	The best rates
Dear email	No disappointment	The following form
Dear friend	No experience	They keep your money -- no refund!
Dear somebody	No fees	They're just giving it away
Different reply to	No gimmick	This isn't junk
Dig up dirt on friends	No inventory	This isn't SPAM
Direct email	No investment	University diplomas
Direct marketing	No medical exams	Unlimited
Discusses search engine listings	No middleman	Unsecured credit/debt
Do it today	No obligation	Urgent
Don't delete	No purchase necessary	US dollars
Drastically reduced	No questions asked	Vacation offers
Earn per week	No selling	Viagra and other drugs
Easy terms	No strings attached	Wants credit card
Eliminate bad credit	Not intended	We hate SPAM
Email harvest	Off shore	We honor all
Email marketing	Offer expires	Weekend getaway
Expect to earn	Offers coupon	What are you waiting for?
Fantastic deal	Offers extra cash	While supplies last
Fast Viagra delivery	Offers free (often stolen) passwords	While you sleep
Financial freedom	Once in lifetime	Who really wins?
Find out anything	One hundred percent free	Why pay more?
For free	One hundred percent guaranteed	Will not believe your eyes
For instant access	One time mailing	Winner
For just \$ / £	Online biz opportunity	Winning
Free access		Work at home
Free cell phone		You have been selected
Free consultation		Your income
Free DVD		
Free grant money		

UNSUBSCRIBE Terminology to Use

"Click here to Unsubscribe" is a commonly SPAM blocked set of words and should be avoided. Instead, use:

"Use this link to remove your email from the database and to stop receiving future emails from us" or

Please reply to this email with subject "Change Email Preference" to stop receiving emails from us in the future.

Solutions?

SPAM is universally recognized as an industry wide crisis on the Internet and experts representing all areas of knowledge are working together to come up with a solution. We practice only permission-based, opt-in email marketing and enforce it with our clients and partners. Since current SPAM filtering software blocks many legitimate emails as well, we've taken several steps to ensure our clients achieve the highest possible delivery rates.

Whitelists

Key ISP's offer white list relationships, to ensure emails sent via a recognised system reach the intended audience. Get listed on the "white list" for major ISP's, such as AOL, Juno, Yahoo, Compuserve, NetZero, and others. A white list status allows mail sent to be appropriately delivered to customers without the potential for filtering.

What we do...

Our team consists of professionals who are educated in best practice email marketing and understand how to avoid filtering, the foremost of which is writing good copy. The overall cost of SPAM is now estimated at over \$10 billion annually, and we are fully aware that it is now more important than ever to prevent valid emails from being falsely labeled as SPAM.

Apart from the best practice email marketing rules above, make sure you:

- Avoid ALL CAPITAL LETTERS
- Avoid excessive punctuation
- Avoid excessive use of "click here," \$, £, and other symbols
- Avoid words like Free, Guarantee, SPAM, Credit Card & various parts of the anatomy etc.
- Use simple, easy to follow unsubscribe instructions

Summary

Email deliverability needs full focus. Make sure that you are tracking delivery, testing for SPAM filters and ISP blocking before a large broadcast and are reacting to all changes that need to be made, in particular, data cleansing of bouncebacks. It might be complicated, but it is a necessity for successful email campaigns in today's email climate.

Glossary

- **Email Blocking** - Email blocking occurs when the receiving email server (e.g. Yahoo!, AOL, Hotmail etc.) prevents an inbound email from reaching the inbox of the intended recipient. Most of the time the sender of the email receives a "bounce" message notifying the sender that their email has been blocked.
- **Filters** - Filtering" is a technique used to block email based on the content in the "from:" line, "subject:" line, or body copy of an email. Filtering software searches for key words and other indicators that identify the email as potential SPAM. This type of blocking occurs on a per email basis.
- **False Positive** - A false positive occurs when a legitimate permission-based email is incorrectly filtered or blocked as SPAM.
- **Blacklist** - It is common for an ISP to use a blacklist to determine which emails should be blocked. Blacklists contain lists of domains or IP addresses of known and suspected spammers. Unfortunately, these blacklists also contain many legitimate email service providers. Just a few complaints can land an email service provider or IP address on a blacklist despite the fact that the ratio of complaints to volume of email sent is extremely low.
- **Whitelist** - A whitelist is the opposite of a blacklist. Instead of listing IP addresses to block, a whitelist includes IP addresses that have been approved to deliver email despite blocking measures. It is common practice for ISPs to maintain both a blacklist and a whitelist. When email service providers say they are "whitelisted" it means that their IP addresses are on a specific ISP's whitelist and are confident that emails sent using their service will be delivered.