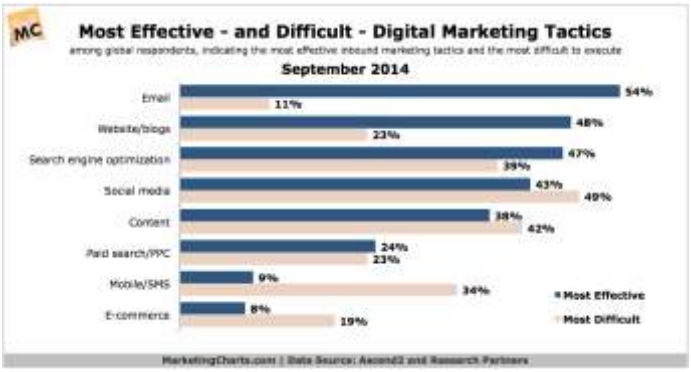
SPAN
GLOBAL SERVICES

Email Deliverability

Email Deliverability

An email marketing campaign will only be successful when all the emails make it to the inbox of the prospects. This is commonly known as 'email deliverability' and plays a vital role in determining the success of your campaigns. Email is still regarded as the most effective digital marketing strategy.



The most common issue faced today by marketers using email is email deliverability. Email deliverability commonly refers to the issues involved with getting your emails delivered to the recipient. New online marketers often wonder what could be the issues with delivery of emails. After all, it takes just a click to send an email to a customer's inbox. However, when marketing emails are sent to hundreds of recipients, not all of them receive the message. In fact, it is likely that many of the prospects will not receive your message at all.

> Over 65% of marketers in US strongly agree that email deliverability is the greatest challenge in email marketing.

There are 2 major reasons for emails not getting delivered: Bounces and Spam issues. This whitepaper aims to talk in-depth about both these issues and what preventive measures can be taken to control them.

What are Email bounces?

Bounces are emails that are returned to the sender. The email is sent properly, but technical issues prohibit it to enter the sender's inbox. Bounces are broadly classified into 2 major categories, hard bounces and soft bounces.

Hard Bounces – This refers to the permanent technical problems with the recipient's address. For instance, the email address itself does not exist. This will also take into account typos and formatting errors in the address bar. For example, if an email is sent to john@yahoo instead of john@yahoo.com, it will be considered a spam email and bounced back to the sender.

The next is non-existent address – this is similar to the previous issue, the only difference being the address is imaginary or fictitious. This can occur when people change their jobs, switch over domains etc.

Some amount of hard bounces is inevitable with any email campaign. But hard bounces can be fatal to your campaigns' success if you ignore them and keep sending emails to those addresses. Such practices can trigger the SPAM filter and label you as a spammer. Immediately remove all hard bounces from your database and CRM system to avoid further deliverability issues.

Soft Bounces – This are caused due to the temporary technical problems with delivering the email. For instance, if the internet suddenly goes off, emails sent at that particular time will bounce back. A full inbox, very large message, or an abandoned mailbox will cause a soft bounce.

Soft bounces are often kept on hold and treated later. The system tries to deliver the message for a few times, but gives up after a certain time. Senders usually get a bounce message in such cases. Sometimes, this is sent many days after the email was sent for the first time.

Misleading Bounces - Many domains and ISPs don't adhere to existing standards at all. In many cases, they deliberately block emails and cite vague reasons for causing a block in delivering the message.

The table below shows some common bounce codes and their interpretation.

codes	reference
500	Syntax error, command unrecognized
501	Syntaxerrorinparametersorarguments
502	Commandnotimplemented
503	Badsequenceofcommands
504	Commandparameternotimplemented
211	System status, or system help reply
214	Help message
220	<domain> Service ready
221	<domain>Serviceclosingtransmissionchannel
421	<domain>Servicenotavailable,closingtransmission channel
250	Requested mail action okay, completed
251	Usernotlocal;willforwardto<forward-path>
450	Requestedmailactionnottaken:mailboxunavailable [E.g.,mailboxbusy]
550	Requestedactionnottaken:mailboxunavailable[E.g., mailboxnotfound,noaccess]
451	Requestedactionaborted:errorinprocessing
551	User not local; please try <forward-path>
452	Requested action not taken: insufficient system storage
552	Requested mail action aborted: exceeded storage
553	Requested action not taken:mailbox name not allowed [E.g.,mailbox syntax incorrect]
354	Start mail input; end with <CRLF>.<CRLF>
554	Transaction failed

Common methods of spamming

According to Wikipedia, SPAM is the use of electronic messaging systems (including most broadcast media, digital delivery systems) to send unsolicited bulk messages indiscriminately.

There are several criteria that an ISP considers while reporting spam against an email. Spamming proves to be economic for advertisers as it involves no operating costs. There are numerous spammers across the web and pose a serious threat to honest online advertisers. As a result Internet Service Providers (ISP) have formulated several measures to check the increasing rate of spamming.

Let us know some common methods of email spamming used by the major ISPs and servers.

Blacklisting – ISPs use this technique to identify which emails from a particular address should be blocked. Such lists would contain domains or IP addresses of known or expected spammers. If spam emails are sent from a domain continually, it might be blocked permanently. Also, constant spam complaints may cause domains to be on the blacklists. Sometimes, blacklists also contain email service providers who are into opt-in marketing.

Listed below are a few types of blacklists:Internet Service Providers (ISP) have formulated several measures to check the increasing rate of spamming.

Public Blacklists: Several organizations like MAPS and SpamCop keep lists of IP addresses linked to suspected or known spammers, and make them public for ISPs and others to use in screening outspam.

Fingerprinting/Spam Traps: Such systems work by filtering spam messages. These messages are then matched against the creative that generated spam complaints or were delivered to spam trap addresses. Bright mail is the most common fingerprinting/spam trap system.

Server Configuration: Here, the email addresses are blacklisted due to faulty server configuration. They are also responsible for you being labeled as spam. Not having a reverse DNS, having open relays or proxies can create an email block.

Volume Cap: Email addresses are blacklisted when they send too many emails in too short a time. Some ISPs, like, may shut down sending connections when resource demand gets too high. Be careful of your number of connections or messages per connection so they don't exceed their thresholds.

Challenge Response: Some ISPs ask for a challenge message. This is just to prove that the sender is a real person. Having your address included in the recipients' 'allowed' list is beneficial to combat this. Failing to respond favorably might cause the email address to get blacklisted.

Content Filters – This method is purely based on the content of the emails. Emails containing 'spam' terms in the body can get filtered by the ISP. Here, the entire

domain or IP address is not blocked, but that particular email is. Though it might seem less serious, it can affect a major percentage of emails if continued unchecked. Emails with near-identical subject lines are detected and destroyed. Spam filtering software identifies words, phrases, and patterns that are likely to trigger filters. They also take into consideration text formatting; such as the use of ALL CAPS, excess use of bright colors, picture images or very large fonts.

Volume Filters - Most of the prominent ISPs trigger volume filters for emails that exceed the stipulated maximum rate. Industry based or categorized mailing invariably has large percentage of users with common major ISPs like Yahoo and MSN. Sophisticated mail servers these days bounce email from mass mailing campaigns. Servers show up on your report as if the email didn't exist. This has lead to email service providers and email tools reporting a lot more bounces while the emails actually exist. This problem is also because of the type and the number of emails of emails you have sent to that server.

Custom Filters – Often, the corporate networks and ISPs set their own rules for filtering emails. They use spam complaints and refer to blacklists for this purpose. Sometimes, a threshold or 'spam point' is set for any email to be deliverable. Not matching up to that cut-off will result in the email to be bounced back. Sometimes other criteria like unknown user rates or server configuration issues are also considered. They are alternatively called Private Blacklists.

Stringent SPAM Laws – They restrict the legality and processes involved in sending Unsolicited Commercial Email (UCE). The service providers are not accountable to guarantee delivery of all messages. In fact, ISPs are provided the right to filter and block any email that may seem necessary according to their policies.

The problem is that these filters block not only spam, but also permission-based email as well. The law doesn't allow ISPs to discriminate whether the email was permission-based or unsolicited. They can block any incoming bulk emails simply on the basis of a single complaint.

Why do ISPs block emails

There are several issues that can negatively affect the deliverability rates of emails. There are many among these which are unpredictable and not under the full control of the marketer. Recent studies have shown that reputed ISPs are stricter with commercial emails than with personal ones. It is important for every marketer to know what triggers an email block and make necessary changes to their campaign.

Some important reasons why ISPs block emails are:

Spammy Looking Content – An ISP will consider any incomplete or doubtful information as 'spammy' content. For example, unknown addresses in the 'From' field, misspelled subjects, subject line written in caps etc.

There are many words that are often identified as SPAM (listed later in this whitepaper). Though these words become indispensable sometimes, use them with great caution in your emails (especially in the subject line) if you must.

Spam Complaints – Too many spam complaints adversely affect the sender reputation of an IP address and its email deliverability. This is the most common factor that ISPs consider while filtering emails. If you receive spam complaints from recipients, figure out what's wrong with your emails. Rectify those and make sure you do not get frequent complaints.

Invalid Email Address – If an IP address continually sends emails to invalid addresses, it might get listed as a spammer. The ISP can also filter the future emails sent from that IP address. So, even if you have an opt-in list, make sure all of them are valid addresses to ensure smooth deliverability.

Technical Issues – These include errors such as incorrectly formatted headers, no reverse DNS, PTR records setup and can cause the ISP to block the email. These are easy to fix but not doing so might pose a serious threat to your campaigns.

Email Header - This can be listed under Reason 4(Technical Issues), but listing it as a separate reason altogether would stress its importance.

The header of the email is like an introduction to what is

there inside. Now, for the email to be delivered, the recipient's server must accept the email's header. In short, the sender's mail server identity should be identical to that of the domain name. This will help the spam filter to know that the sender is authentic.

Thus, a forged sender identity would result in the email to be blocked. False email headers are sometimes a big concern for major ISPs and malicious senders might as well be prosecuted.

> On an average 19.2% marketing emails are blocked by ISPs.

HTML Code – Emails can be sent in HTML format but a wrong code can block an email. Any HTML error, however simple should be avoided at all costs. Some of them are:

- Not including plain text version
- Not adding Alt+Text for graphics
- Containing dead links in HTML

Consider using validators to check HTML emails before sending. This will act as a re-checking tool and enhance the deliverability.

Email Shooting Speed - Sending large chunks of emails too frequently will have a negative impact on your sender reputation. This might also result in increasing number of spam complaints. If the frequency is too high and there are too many complaints (Refer reasons 1 & 2), the email account might be shut down by the ISP.

Poor Links/Image Paths – Any link from a blacklisted domain can be the reason for filtering. However, the same email without links can be delivered successfully. Hence, the links that are included in emails must be working fine.

Inclusion of images can enhance an email's look and feel. But, confusing and unclear image paths can be a deliverability issue. Image paths must be easy to read. It must not disguise what's inside and conform to the anti-spam filters.

List Hygiene – Old and unappended email list mostly trigger problems. If you are using a list that is couple of months old, your address can be blacklisted. Abandoned email addresses must be found out and deleted from the list. Consider frequent list appending to maintain a clean, hygienic list.

Marketing experts opine that even if a list is 100% opt-in, it is sure to have some spam complaints and bounce-backs. The reasons listed above are the most common ones that cause ISPs to initiate a block. Not rectifying these can generate other serious blocks in email deliverability.

How to improve Email Deliverability?

All online marketers today face the challenging issue of getting spammed. The causes of an email labeled as spam are several. The least an email marketer can do is to keep the email campaigns within the spamming parameters of the ISP. Email marketing vendors often offer deliverability services that can help you minimize any potential issues regarding spam.

Here are some ways how you can ensure successful email deliveries:

Check Bounce-back Rates - These are emails that are returned as undelivered and the most common factor that affects deliverability. To avoid this:

- Have your lists properly filtered and get rid of any invalid email addresses.
- Reduce your bounces by correcting formatting errors like invalid addresses, domains and typos.
- Look for missing @ signs or missing domain names and fix them at the earliest. Another reason for a bounce-back is that the recipients have changed their addresses or moved to a new domain.
- Request your ESP to get you granular delivery reports to manage your lists.
- Confirm email addresses by sending welcome emails to all the recipients on the list.
- Make sure you update your lists timely and incorporate changes in addresses to avoid frequent bounce-backs.
- Carry out a test email campaign to identify any basic errors.
- Bounces can purge an email address, hence set a bounce threshold for a given period of time.
- Monitor your delivery rates by categories such as

- domain names, time of sending and other criteria. Track them and if you see a negative pattern in the deliverability rates, call an expert for help.
- Make sure you update your lists timely and incorporate changes in addresses to avoid frequent bounce-backs.

Avoid Sharing IP Address While Executing Campaigns - If the other senders on that IP address are spam listed, then you have a high chance of your email not hitting the right inbox. If you have a robust email list as your prospect, try investing in a unique IP address. This can add to the deliverability rate and also your reputation. Many email service providers can provide you with an IP address.

Request Recipients To Recognize Your Email Address - Sometimes, major ISPs and spam filters place bulk emails into the spam folders unless the recipient has marked the email address as safe. Ask your subscribers to mark your email address as 'safe' or 'allowed' when opting in for your newsletter list and when confirming their subscriptions. This will help you avoid being a spammer.

When you're using an opt-in list, let your subscribers know what you will be offering. This will increase the reputation of your products and also retain the prospects on your opt-in list.

Get Help With Email Spoofing - ISPs these days can identify if a particular email is sent by a legitimate address or from a fake one by spammers. Check if your email service provider has:

SPF (Sender Policy Framework) – This is a standard with technical methods that help sender address spoofing.

DomainKeys – This adds an encoded digital signature in the emails and help ISPs establish that the sender address is genuine.

Enable Your Prospects To Unsubscribe Promptly - Allow your prospects to opt-out whenever they wish to. By not doing so, you could be listed as a spammer. Also review your opt-out procedure. Make sure it's not too lengthy and has clear instructions as to what a subscriber ought to do in order to opt-out.

You might get more spam complaints simply because the opt-out procedure in place is complicated and it is easier to click the Spam button than unsubscribe.

Write To-The-Point Subject Lines - Your subject line should be to-the-point and not off-content. Questionable content in the headlines can block your emails and put them straight to the junk folder.
Keep Your Lists Updated - This cannot be stressed more, but list hygiene is a highly important factor affecting email deliverability. Databases should not contain old records. They should be verified monthly

Write To-The-Point Subject Lines - Your subject line should be to-the-point and not off-content. Questionable content in the headlines can block your emails and put them straight to the junk folder.

Keep Your Lists Updated - This cannot be stressed more, but list hygiene is a highly important factor affecting email deliverability. Databases should not contain old records. They should be verified monthly and any expired listing should be immediately replaced with the fresh one. and any expired listing should be immediately replaced with the fresh one. Immediately delete a recipient's name upon request.

Keep spam at a bay

Here are a few tips that will help you keep the most dreaded SPAM at bay:

Get Whitelisted - Each ISP has different rules in place to detect SPAM. It is a good idea to get white listed with major ISPs like Yahoo, Hotmail, AOL, MSN etc. White listing will prevent the filters from blocking any message from your email address. Most of your emails will get through the inbox and this will help unnecessary filtering of legitimate emails.

Follow The Laws – Make sure your campaigns are fully CAN-SPAM compliant. If you send to other countries, comply with their SPAM rules, too. Keep yourself abreast with the latest regulations and laws.

Hire A Vendor – This will make your task several times easier. Most email campaign vendors have deliverability specialists that are capable of taking care of SPAM and deliverability issues. Even if you carry out a campaign yourself, consult the experts when you encounter deliverability issues. The service providers are technically equipped to identify deliverability issues and fixing them.

Implement authentication methodologies while executing a

campaign. Also, meet your ESP's deliverability team regularly to discuss data and metrics.

Adjust To SPAM Filtering Rules – Mark your email campaigns against the filtering rules. This process will show you where exactly you need to tweak your campaign. Seek good relationships with the ISPs to understand their filtering policies better.

Use Double Opt-in Lists – Also, known as confirmation opt-ins, double opt-in lists are a safe way to execute an email campaign. Here the recipients receive an automated response from the list service prompting them to click on a given URL to confirm their subscriptions. They will be considered opt-ins only when they click on that link.

Pay Heed To Spam Complaints – Pay utmost importance to the spam complaints received by you. Firstly, delete the email addresses that have reported spam against you. You can also create an exclusion list and put such addresses into them for future reference.

Manage Your Unsubscribe Requests - Give due importance to the unsubscribe requests and do not continue persuading them to still stay opted-in. this can affect your reputation adversely and you can be listed as spam. Also, send them a confirmation that they have been unsubscribed.

Knowing the root causes of delivery issues should help an online marketer know where they are going wrong. However, regular monitoring of email deliverability rates is important because the rules around delivery change daily. Many companies make the mistake of investing too little staff or budget resources for deliverability – the basic factor that determines the success of email programs.

Words That Trigger SPAM

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
Apply Online	Free preview	mail
As seen on	Free priority mail	Outstanding values
Billing address	Free quote	Pennies a day
Auto email removal	Free sample	People just leave money
Avoid bankruptcy	Free trial	laying around
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

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	Increase traffic	Reply remove subject
any other offer	Insurance	Requires initial investment
Cancel at any time	Investment decision	Reserves the right
Can't live without	It's effective	Reverses aging
Cash bonus	Join millions of Americans	Risk free
Cashcashcash	Laser printer	Round the world
Casino	Limited time only	S 1618
Cell phone cancer scam	Long distance phone offer	Safeguard notice
Cents on the dollar	Lose weight spam	Satisfaction guaranteed
Check or money order	Lower interest rates	Save $
Claims not to be selling	Lower monthly payment	Save big money
anything	Lowest price	Save up to
Claims to be in accordance	Luxury car	Score with babes
with some spam law	Mail in order form	Section 301
Claims to be legal	Marketing solutions	See for yourself
Claims you are a winner	Mass email	Sent in compliance
Claims you registered with	Meet singles	Serious cash
some kind of partner	Member stuff	Serious only
Click below	Message contains disclaimer	Shopping spree
Click here link	Money back	Sign up free today
Click to remove	Money making	Social security number
Click to remove mailto	Month trial offer	Stainless steel
Compare rates	More Internet traffic	Stock alert
Compete for your business	Mortgage rates	Stock disclaimer statement
Confidentially on all orders	Multi level marketing	Stock pick
Congratulations	MLM	Strong buy
Consolidate debt and credit	Name brand	Stuff on sale
Stop snoring	New customers only	Subject to credit
get it now	New domain extensions	Supplies are limited
Special promotion	Nigerian	Take action now
Copy accurately	No age restrictions	Talks about hidden charges
Copy DVDs	No catch	Talks about prizes
Credit bureaus	No claim forms	Tells you it's an ad
Credit card offers	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
Dear somebody	No fees	refund!
Different reply to	No gimmick	They're just giving it away
Dig up dirt on friends	No inventory	This isn't junk
Direct email	No investment	This isn't spam
Direct marketing	No medical exams	University diplomas
Discusses search engine	No middleman	Unlimited
listings	No obligation	Unsecured credit/debt
Do it today	No purchase necessary	Urgent
Don't delete	No questions asked	US dollars
Drastically reduced	No selling	Vacation offers
Earn per week	No strings attached	Viagra and other drugs
Easy terms	Not intended	Wants credit card
Eliminate bad credit	Off shore	We hate spam
Email harvest	Offer expires	We honor all
Email marketing	Offers coupon	Weekend getaway
Expect to earn	Offers extra cash	What are you waiting for?
Fantastic deal	Offers free (often stolen)	While supplies last
Fast Viagra delivery	passwords	While you sleep
Financial freedom	Once in lifetime	Whom really wins?
Find out anything	One hundred percent free	Why pay more?
For free	One hundred percent	Will not believe your eyes
For instant access	guaranteed	Winner
For just $ (some amt)	One time mailing	Winning
Free access	Online biz opportunity	Work at home
Free cell phone	Free consultation	
Free DVD	You have been selected	
Free grant money		
Your income		

Conclusion

Good deliverability rates are a result of proper bounce management and keeping away from spam. A proper email deliver review will help any marketer know at what rate their emails are getting delivered. Advertisers today need lots of clever practices to have their emails delivered at the right inbox. How it is achieved is a matter of patience, trial and a little bit of investment.

SPAN
GLOBAL SERVICES

Span Global Services
848 N. Rainbow Blvd.
Suite#5439 Las Vegas, NV 89107

USA: 877- 837-4884
Canada : 877-452-2061
UK : +44 (0) 800 088 5015

info@spanglobalservices.com

Span Global Services is a leading provider of digital marketing and data-driven services. The brand's forte lies in its data intelligence, which holds the largest intellectual mapping available in the industry. As an expert B2B marketing solutions provider, Span Global Services specializes in customized services using the latest business models in online marketing, search marketing, and innovative data strategies. It is the world's only social verified and email verified data provider today. With nearly a decade's expertise in digital marketing, its business intelligence enables companies to utilize the intellectual online marketing strategies along with data insights, market reports, and IT support services. Consulting, Marketing, or Outsourcing solutions — Span Global Services is the most preferred choice.