

A Whitepaper of Email Marketing Webinar Questions & Answers:

How an Enterprise SPAM Filter Works – Questions & Answers



Introduction

This whitepaper is in a Question and Answer format and covers ‘how a spam-filter works’. The questions were asked during our live webinar **“Email Marketing 201: How an Enterprise SPAM Filter Works,”** which is also available on-demand at the URL below. In this webinar we follow an email message through the network of trials and tribulations it will encounter before final delivery (hopefully).

We explain the details of how a spam filter or blacklist determine if your email is acceptable or whether it is spam and headed for the SPAM folder (or simply dropped altogether.)

The on-demand webinar recording can be found on Pinpointe’s blog at:

www.pinpointe.com/blog/webinar-email-marketing-201-improving-email-delivery

The webinar and this Q and A whitepaper are intended as useful tools to help you understand why your otherwise good email might get blocked, even if you are doing everything correctly.

Q: FIRST - WHERE CAN I LEARN MORE ABOUT THE CAN-SPAM ACT?

You can check the FTC website at: www.ftc.gov/spam

Or call toll-free: 1-877-FTC-HELP (1-877-382-4357)

Q: WHAT IS AN “MTA” AGAIN?

MTA stands for ‘Mail Transfer Agent’. It’s a fancy word for an email server and more commonly means ‘outbound email server’ – as in ‘email server used to send email campaigns and automated emails.’

Q: WHAT ACTIONS CAN GET ME ONTO A BLACKLIST OR CAUSE A SPAM FILTER TO BLOCK OUR EMAIL?

Here are the main ways you can get onto a blacklist or have a spam filter block your otherwise good email campaigns:

- Send an email campaign that receives too many SPAM complaints. When recipients get your email they can click the ‘This is SPAM’ button on their email client. This registers with spam filters as a ‘vote’ that your email is spam. Too many complaints and your emails will start going into the SPAM folder or will be outright blocked. Unfortunately some ISPs like Aol.com encourage their users to click the SPAM button instead of unsubscribing, raising your spam rate. Many ISPs have a target complaint rate of less than 1 complaint per 1,000 emails sent.
- Send an email campaign to one or more ‘SPAM Honeypots’. (See the next question for a definition of a SPAM honeypot).
- Start sending a burst of emails from a newly configured email server at a new IP address. With spam filters, you are guilty until proven innocent. An IP address that has no email sending

history that all of a sudden starts spewing out thousands of emails will look like a spammer firing up a new bank of email spam cannons.

- Send an email campaign that has a high spam score (when analyzed by a spam content filter). If your email looks like spam content, some spam filters and blacklists will blacklist you for 48-72 hours.
- Register your email server with an IP address that is 'close' to other IPs that have been flagged as SPAM email servers. Yes, it matters what neighborhood you 'live' in. Some blacklists will add your email server to their blacklist if your 'neighbors' are known spammers. The logic is that either you may be associated with the spammer, or you are hosting your email at an ISP who is willing to host spammers, so you are guilty by association.
- Send emails to a list with a lot of hard bounces (invalid addresses). SPAM filters track the % of invalid emails you try to deliver. If your hard bounce rate is consistently high (greater than 15% for example), your email reputation will fall and you may be blacklisted for windows of 48 ~ 72 hours.
- Configure your email servers incorrectly. True spammers can be lazy and often do not configure their email servers correctly. Well, at least that is the opinion of most spam filters and blacklists, so if your equipment is not configured correctly, your emails may be blocked.
- Send email campaigns to general email lists and aliases such as support@, sales@, webmaster@, info@ and so on. These are often aliased to dozens or even hundreds of recipients and it is highly unlikely that a person will register on a website using such an address, so you are likely to irritate many recipients and generate spam complaints.

Q: WHAT IS A "SPAM HONEYPOT"?

There are blacklists that work directly with registrars to 're-cycle' domains when they expire. Send an email to an address at one of these domains and you will get stuck in their 'honeypot'. Some honeypot-based blacklists are more devious. They actually host websites with embedded email addresses. Utilities that crawl websites and parse out email addresses (which is illegal in the US anyway), will capture the honeypot addresses.

Blacklists that are based on honeypots use this logic. When a company goes out of business or a domain otherwise becomes invalid, you should not be sending emails to anyone at that domain anymore. If a company is out of business for say, 6 months, and you send an email there, then either a) you are not using good list management practices, and should be 'penalized' to clean up your act or b) you likely purchased or automatically generated the email address by combing websites for email addresses.

Q: DO "SPAM HONEYPOTS" ACTIVELY SUBSCRIBE WITH BOGUS DATA TO E-MAIL LISTS?

No; however malicious hackers and bots sometimes crawl sites and may register email addresses on signup forms that are from a dead domain that could coincidentally, have been 'harvested' by a honeypot blacklist. This is one of the reasons to use double-opt-in forms on your website to validate that the email addresses used are valid.

Q: CAN I GET A LIST OF SPAM HONEYPOTS SO I CAN AVOID THEM?

We all wish! No. This would defeat the purpose – if blacklists made their honeypot addresses visible or available, any spammer would just use these addresses as suppression list and avoid the honeypots. These addresses are always changing as blacklist managers/vendors are constantly registering new domains.

Q: WHAT IS ‘WARMING UP’ AN IP ADDRESS?

SPAM filters often assume a sender is guilty until proven innocent. An IP address that has no email sending history all of a sudden starts spewing out thousands of emails, it will look like a spammer firing up a new bank of email servers. To reduce the impact on deliverability, slowly ramp up the email volume over a 60 day window and actively monitor main blacklists. If you get on a blacklist (and your email and list were legitimate), request removal immediately with an explanation that your email server and IP allocations are new. If you are managing email in-house, register the IPs with feedback loops at the major ISPs. (Email Service Providers like Pinpointe will do this for you.)

Q: MY EMAIL SERVER’S IP ADDRESS IS SHARED WITH OTHER SENDERS. WILL THE OTHER COMPANIES ON THIS IP ADDRESS IMPACT MY EMAIL SENDING REPUTATION?

If your (outbound) email servers are using a shared IP address, it is possible that other customers on the same IP address will impact your email sending reputation. But before you run out and get dedicated IPs, there are a few caveats:

- First, you need to be sending a high enough volume. If your volume is not at least 100,000 emails / month, most spam filters and blacklists will not be able to assess your sending reputation. Having a blank reputation can impact your deliverability as much as having a slightly negative reputation.
- If you do get a dedicated IP address, know that when first sending from your ‘virgin’ IP, deliverability will be impacted for the first 2-3 months. See the ‘warming up an IP address’ question, since many spam filters assume you are guilty until proven innocent.
- If you are using an ESP, discuss the option with them. Most credible Email Service Providers will monitor your sending habits and sending statistics (we need to do this to protect our customers and our network from both ‘unknowing’ and unscrupulous spammers). Based on your campaign statistics, you are likely to be ‘grouped’ onto an IP or IP range with other companies that have a very similar reputation. Although one company can still impact another’s reputation, the likelihood is much lower.

Q: WHAT ARE THE BEST PRACTICES IN REDUCING BOUNCE RATES?

Ideally, remove contacts that have not received an email in more than 9-12 months – see the explanation for ‘SPAM honeypots’ above. Use valid contacts who have opted to receive your emails. Also if you have received a ‘soft bounce’ error for an email address after 4-5 attempts, it is best to remove that address from your list. Most ESPs (Email Service Providers) do this automatically.

Send to your clients / email contacts more frequently – at least once a month if possible (assuming you have newsworthy information to send). Most Email Providers automatically remove the invalid email addresses that accumulate each month as people change jobs and move.

Q: DO BOUNCE RATES IMPACT EMAIL REPUTATION AND DELIVERABILITY?

Yes. Some SPAM filters track information on your % of delivery to invalid addresses (hard bounce rates) over time. If hard bounce rates are consistently high, (15% or more for example), then your email reputation will fall and you will be blacklisted.

Q: WHAT DO YOU THINK ABOUT SENDING REENGAGEMENT EMAILS TO THOSE WHO HAVE NOT OPENED AN EMAIL IN 3-6 MONTHS?

This is an excellent idea and many ESPs recommend doing this. If you send the re-engagement letter (or variations) 2-3 times – it is a good idea to consider removing contacts who have never opened any email campaigns.

Q: HOW CAN I CHECK TO SEE IF MY COMPANY IS ON A BLACKLIST?

There are several tools on the Internet that you can use to check the more important SPAM blacklists. Here are two tools that you can use to check several public blacklists simultaneously:

www.mxtoolbox.com

www.dnsstuff.com

Pinpointe's blog entry below includes a more comprehensive list of spam blacklists that you can check in order to see if your IPs (or domain) are on a spam blacklist:

www.pinpointe.com/blog/how-do-i-know-if-im-on-a-spam-blacklist

Q: TO CHECK REPUTATION, WOULD YOU CHECK THE ESP'S IP ADDRESS OR IS IT OUR IP ADDRESS REGARDLESS OF WHETHER WE USE AN ESP?

Check the IP address of the email servers that are sending your email. If you are using an ESP, ask the ESP for the IP addresses that your account is using or sharing. If you are sending emails from your own in-house servers, ask your IT team for the IP address of your outbound email servers.

Note that there are also blacklists that are based on your 'top level domain'. This is the domain that is used to send your emails. If you are using an ESP you can ask what your sending 'top level domain' is, or you can forward an email to yourself and check the email header (or ask IT to help you determine this).

Q: HOW CAN YOU TELL WHAT PERCENTAGE OF YOUR EMAILS MAKES IT TO THE INTENDED RECIPIENT?

Unfortunately you cannot tell with 100% certainty which emails are getting to the inbox for a host of reasons. First, email servers are not always consistent in the response codes that they return (to the sending email server), so your email may receive a return code of 'OK', when in fact the local inbox email filter decided to place your email into the spam folder. Some SPAM filters always return an 'OK' status regardless of whether your email was dropped, blocked or delivered. The philosophy is that – providing

response information only helps spammers to improve their ability to penetrate or trick the email filter or email blacklist. Also, the decision to deliver your email to the recipient's inbox or spam folder is partly dependent on the recipient's own personal email filter settings and address book.

That said, there are services like www.returnpath.com and www.emailreach.com (a service managed by Returnpath) that can provide you with accurate statistics as to whether your email is being accepted by inboxes at yahoo.com, gmail.com etc. These services monitor test inboxes across multiple networks. When you send a test email, the service checks whether your email was delivered to the inbox or spam folder.

Q: WOULD WE IMPROVE OUR RESULTS IF WE CHANGED OUR IP ADDRESSES EVERY 6 MONTHS?

This would almost always harm your reputation, unless you are a spammer. Spam filters and blacklists accumulate historical email delivery information for the IP address of your sending email server(s). Over time, if you are sending relevant, high quality permissions based email, your reputation will *improve* over time. On the other hand, if your practices include purchasing large cheap lists, or not maintaining your lists by removing unsubscribers and hard bounces, your reputation will go from bad to worse. In this case, you might improve your email reputation by moving to a new IP address but if your company is not employing good practices, you will simply burn through new IP addresses every 6 months, which may upset your ISP enough to consider terminating your service.

Q: HOW DO YOU REPAIR YOUR EMAIL REPUTATION IF IT HAS BEEN DAMAGED BY POOR SENDING PRACTICES?

If you have damaged your sending reputation as a result of poor sending practices, poor list hygiene practices and sending repeatedly to purchased lists and non opt-in contacts, then clearing your reputation can take 2-3 months. Some recommendations:

- Of course – the first step is to clean up your sending practices and send only to customers and prospects that have requested that you send emails, because otherwise, you will find yourself right back where you started.
- Practice good list hygiene. Be sure all bounces and unsubscribed contacts are immediately and permanently removed from your list (most email providers do this automatically).
- Check all available blacklists and request removal.
- Consider requesting new IP addresses. If your sending volume is > 200,000 emails per month you may qualify for a dedicated IP; otherwise, you may not have enough email volume for spam filters to establish a sending reputation for you. Note – a brand new IP address will require 2-3 months to 'warm up' – your deliverability will be lower initially. Refer to 'Warming up IP addresses' in this Q and A.
- Consider an email practices 'audit' from <http://www.senderpath.com>.

Q: WILL MY EMAIL SPAM SCORE BE AFFECTED IF I SEND EMAILS THAT ARE ONLY IN TEXT FORMAT (OR ONLY IN HTML FORMAT)?

Yes. Spammers often send only text or only HTML versions of their emails, so spam filters often increase your spam score if you send only a text version or only an HTML version of your email. For more information about how content impacts delivery, check for our webinar: Email Marketing 101 which is available on-demand at:

www.pinpointe.com/blog/webinar-email-marketing-tips-to-improve-email-responses

Q: WHAT ADVANTAGES ARE THERE FOR HAVING A DEDICATED IP WITH A MTA

A dedicated IP address means that you are in charge of your own email sending reputation, for the most part. Other senders can have limited impact on your delivery. Again there are caveats read 'Warming up your IP addresses.' Your reputation can still be impacted by others:

- If your IP addresses are close (numerically) to other IP addresses that are used by spammers or companies with high spam complaint rates, your email reputation may be impacted (guilt by association).
- If your emails contain URLs that might be associated with domains reported as 'spamvertized' sites, then links in your emails to these sites will impact deliverability
- If your ESP is using a common 'return-path' email address for multiple customers and if the ESP does not closely monitor (and cancel) spammers, then once customer can still impact another's reputation. Note though, that this is unlikely with reputable ESPs.

Q: WHAT IS THE DIFFERENCE BETWEEN A "HARD BOUNCE" AND "MAIL BLOCK"?

A hard bounce occurs when there is a permanent failure. The most common hard bounce occurs when sending to an invalid or inactive email address or a domain that is no longer in operation. A "Mail Block" indicates that your email has been blocked by the recipient's spam filter.

Q: WHAT DOES "LOCAL POLICY VIOLATION" MEAN?

A recipient's email server may reply with an error code or message 'Local Policy Violation' in the response code text. This usually indicates that your email has been blocked by the recipient's spam filter. Note that this is not a message that you receive directly; it is a message that is communicated from the recipient's email server to your sending email server. An ESP might provide this information in the reporting statistics.

Q: DOES PINPOINTE RATE LIMIT WHEN SENDING EMAIL CAMPAIGNS?

Yes. Pinpointe throttles email send rates for each customer in order to protect customers and Pinpointe from a rogue spammer who might sign up and immediately fire off a large spam campaign. Slower sending rates also generally improve deliverability. Our backend servers also throttle the aggregate outbound traffic to certain domains that are known to accept email at a slower rate.

Q: IS THERE A PLACE WHERE YOU CAN PREVIEW MY EMAIL CAMPAIGN IN MULTIPLE CLIENTS?

Yes. Pinpointe’s email service includes an email preview tool which shows how your email will display in various email clients. The previewer checks the email campaigns HTML code against the supported code for each email client and reports warns of possible html coding errors.

We also include a SPAM check tool that will review your email for spam phrases that might increase the chance of your email being blocked based on the content. The checker provides specific feedback so you can modify / edit the email so you can reduce your spam score.

Another excellent tool is www.litmus.com. For a fee, an email can be previewed in dozens of email clients.

Q: I HAVE RECIPIENTS THAT BLOCK MY EMAIL NO MATTER WHAT. I HAVE DONE EVERYTHING. WHY IS THIS?

Assuming you have verified that your email spam score is low and that your email servers are not on any blacklists, it is still very common to experience some email being blocked by spam filters. Some IT organizations set their spam firewalls to very conservative settings, often unknowingly creating more problems for end users, since a higher percentage of valid email may be blocked. In this case your options are:

- Contact the end customer directly and request that they add your email address to their address book. Local inbox settings usually over-ride general settings and this should permit your email to get through
- If the recipient is getting your email but it consistently ends up in the spam folder, have the recipient click ‘this is not spam, and request they add you to their address book (above).
- Contact the recipient and provide the IP addresses of your outbound email server (if you are using an Email Service Provider (“ESP”), ask the ESP what IPs you are assigned. Provide these IPs to your recipient and ask them to request that their IT department add the IPs to the corporate whitelist / non-blocklist.
- Otherwise, consider removing these contacts from your list. Note that, if a recipient’s email filter responds that your email is being blocked after multiple campaigns, most Email Services Providers, like Pinpointe, will automatically remove the contact from your list or flag the address as undeliverable after some number of failed ‘soft bounce’ attempts. Pinpointe for example flags email addresses as undeliverable after 5 ‘soft bounce’ or ‘email blocked by sender’ response codes.

Q: ARE EMAILS THAT ARE SENT THROUGH OUR ESP ‘ON BEHALF OF’ US HURTING OUR OPEN RATES? THE ‘SEND-FROM’ ADDRESS THAT DISPLAYS FOR RECIPIENTS IS: MYCOMPANY@MAIL.VRESP.COM.

Some ESPs do not permit you to use your own actual email address as the send-from email address and others do. Pinpointe permits you to use your own send-form email address so our domain does not appear in the recipient’s inbox. There are trade-offs with respect to how ESPs have to manage our services and configure servers. It is possible that a small number of recipients may choose to not open

the email because the above send-from address makes your email appear like a bulk email instead of a personalized email message sent directly from you (or your CMO.)

IF I HAVE RECIPIENTS IN MY LIST THAT NEVER OPEN MY EMAIL, DO THESE NON-RESPONDERS AFFECT MY SENDING REPUTATION?

At present, probably not. However if you have contacts in your email list that have not opened a single email of yours in 6-12 months, why do you want to keep sending to them? You might be better off sending a final re-engagement campaign to these unresponsive contacts (see earlier question) and deleting contacts who do not respond.

Q: YOU USED THE TERMS B2B AND B2C - WHAT DO THESE MEAN?

"B2B" means 'Business to Business' - as in businesses communicating with other businesses, whereas "B2C" means 'Business to Consumer'.

Q: WHAT IS MULTI-PART VS. HTML-ONLY?

A: Multi-Part means that, when your email is sent, it is 'packaged' with both an HTML version - for email clients who prefer to open HTML emails, and a Text version, which will be opened on many PDAs, handhelds and where people have set their preferences to only read 'text' versions of email. Most emails are sent in Multi-Part format. Spammers on the other hand rarely take the time to create Multi-part versions and more often will send only HTML or only Text versions.

Q: HOW MANY LINKS CAN I USE IN MY EMAIL? WILL TOO MANY LINKS GET MY EMAIL TRIPPED UP BY A SPAM FILTER?

A: Based on analysis of our B2B customer data, adding more links will almost always improve response rates. Key points to consider:

- Try to include a link within your initial opening paragraph (Read More.. for example). This can increase overall click rates by 12-15% and is virtually always the top-clicked link of a campaign.
- Do you know where the second best performing link is? In the 'P.S. or Footer section! Don't be afraid to 'advertise' or promote below your signature.
- Work more links into your campaigns. Our analysis shows that campaigns with more links produced higher total click response rates while *not* increasing the unsubscribe rate. 15-20 links in a campaign is not unreasonable.

Pinpointe Questions

Q: ARE ANALYTICS AND E-MAIL DEPLOYMENT HELP, REPORTS AND E-MAIL EFFECTIVENESS METRICS INCLUDED IN THE MONTHLY PRICING PACKAGES FOR PINPOINTE'S EMAIL SERVICES?

A: yes, advanced reporting, help and effectiveness metrics are all standard features. If you would like to learn more, or to schedule a live 1 on 1 demonstration of Pinpointe, please contact us at: 408-834-7577, Option #2 (Sales); sales@pinpointe.com.

Q: WHAT SETS PINPOINTE APART FROM LOW END SOLUTIONS LIKE CONSTANT CONTACT?

A: Pinpointe offers the following advanced features and services:

- Pinpointe services B2B customers.
- **Pinpointe Professional** edition is a powerful full-featured email system with WYSIWYG editor, spam checker, email previewer and more.
- **Pinpointe Enterprise** edition is for larger enterprises who need 5 ~ 250 users (seats) and send 300,000 emails – 10M+ emails /month.
- Pinpointe transparently integrates with Google Analytics, so all of your campaigns can be tracked, monitored and analyzed within Google analytics.

Q: WHAT IS PINPOINTE'S PRICING?

Pinpointe's pricing is based on the number of emails sent per month. We offer some of the industry's most competitive pricing and the industry's most feature-rich email service. There are no contracts, up front fees or long term commitments.

For the latest pricing please check www.pinpointe.com/get-started.

About Pinpointe

Pinpointe is a leading provider of on-demand email marketing automation software based in the heart of Silicon Valley, California. As former High Tech B2B marketers, we've been in your shoes. Our team has a passion for helping B2B marketing professionals communicate with existing customers, and target new prospects through behavioral targeting, improved segmentation and message personalization.

Other Resources

If you're a Business to Business marketer and are want to stay on top of the latest marketing trends, tips and best practices, then please sign up for our twice-a-month Tips 'n Tricks notes. Once or twice a month we'll send you a briefing with tips and tricks. We'll also include a link so you can op-out or update your preferences, any time.

Pinpointe Site: www.pinpointe.com

Pinpointe support Blog: www.pinpointe.com/blog

Contacting Pinpointe

Pinpointe sales and support are available from 8am to 6pm PST, M-F. We can be reached at:

(800) 557-6584 or (408) 834-7577, Option #2

General Information: info@pinpointe.com

Sales: sales@pinpointe.com

Twitter (Tips): @Pinpointe (www.twitter.com/pinpointe)

Please feel free to pass this handy pdf on to all your friends and enemies.

PUBLISHED BY: Pinpointe On-Demand, Inc. www.pinpointe.com

© 2011, Pinpointe On-Demand, Inc. All Rights Reserved. No part of this publication may be reproduced or transmitted in any form without the written consent on Pinpointe On-Demand, Inc. Pinpointe, Pinpointe On-Demand Inc and the Pinpointe logo are trademarks of Pinpointe On-Demand, Inc.