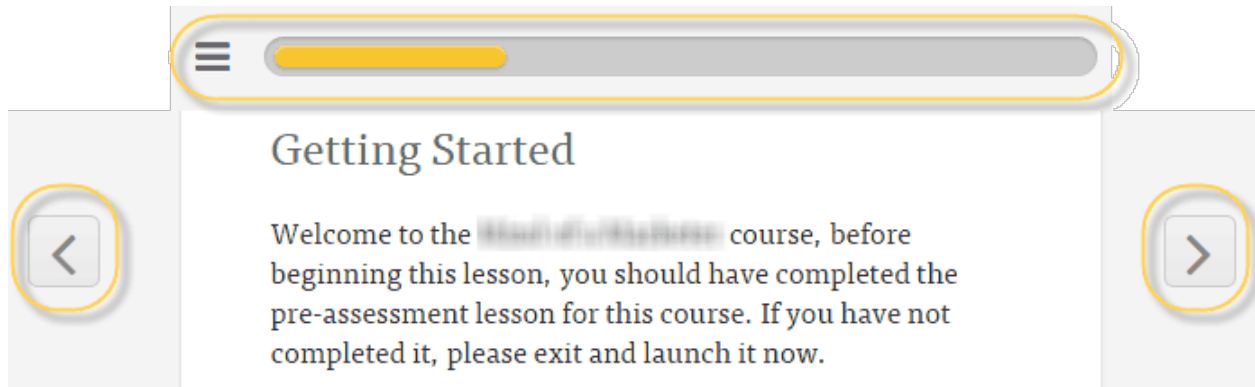


# Sender Reputation and the Inbox (Lesson)

## Getting Started

Welcome to the Sender Reputation and the Inbox course, as you move through this course you will find navigation buttons, use the following as your guide:

**Previous**, **Next** and **Progress Bar** -- you will find each of these on every page.



Caption: Click to enlarge

When watching videos, use the **Enter Full Screen / Exit Full Screen** option in the lower right corner of the video window for a better viewing experience.



**Course Duration:** This course will take you approximately 35-40 minutes to complete.

### **Course Overview**

This course contains educational information related to sender reputation and email deliverability. We will present the factors that make up and have a direct impact on email sender reputation, sender score, deliverability and inbox placement.

The goal of this course is to ensure that everyone has a basic understanding of the concepts presented, including those new to the email industry.

### **Objectives**

At the end of this course, participants will be able to:

- \*Describe the purpose of Sender Score
- \*Describe how Sender Score is determined
- \*Define sender reputation
- \*Describe how sending practices and recipient responses impact sender reputation
- \*List the major factors that influence sender reputation
- \*Describe how each factor impacts sender reputation
- \*Describe why sender reputation is important

### **Introductory Video**

This introductory video talks about sender reputation and email deliverability -- some of the factors that make up and have a direct impact on email sender reputation, deliverability and inbox placement.



## Your reputation is your most important asset

If your emails are routinely blocked, marked as spam, or delivered to unused mailboxes, they're damaging your reputation.

A diminished reputation hurts more than just your pride. It means you're spending more money to get the same results getting to the inbox.

A good reputation is the only reliable way to reach the inbox, and a good reputation starts with knowing where you stand.



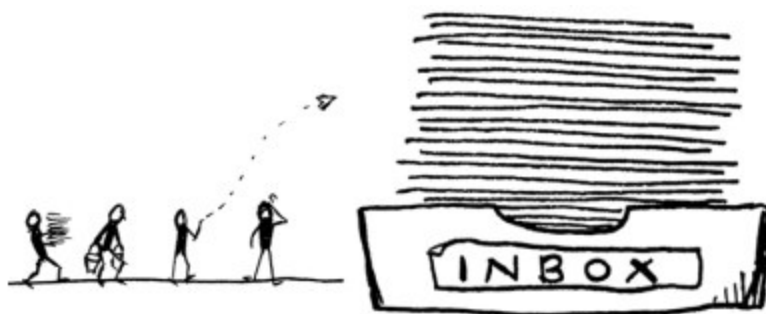
Caption: Click to enlarge

## Getting to the Inbox

Marketers sometimes overlook how tough it can be to get their email into their subscribers inbox, so the question is of course, what stops your email from getting delivered?

Recognizing that reputation is one of the many moving parts involved in email deliverability, it's also good to know that Return Path's **Sender Score** gives you insight into your reputation.

Today, it's your sending practices that play the major role in determining whether or not your email makes it to the inbox.

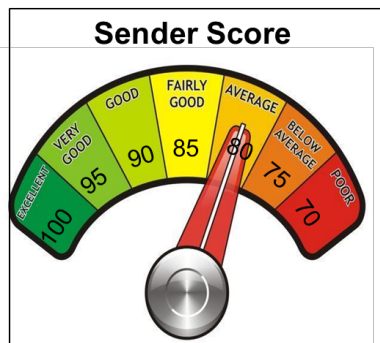


## What is Sender Score?

Your **Sender Score** is like your Credit Score, it's an indication of your trustworthiness. And just like a bank would use your credit score to determine if they would give you a loan, Mailbox Provider's use the metrics in Sender Score when deciding whether or not to place a sender's email in the inbox.

A Sender Score for your sending IP(s) is generated by Mailbox Providers, filtering companies and email users - all who contribute to your overall Sender Score. Their input, combine with a formula developed by Return Path, is how your score is generated.

Your score can tell you the most important factors needed to improve delivery rates. The factors used in determining your Sender Score are similar to those used by email networks and Mailbox Providers to determine your **Sender Reputation**, and include things like complaints, spam traps, unknown users and blacklists.



Caption: Click to enlarge

## Sender Score Continued

Because email networks and Mailbox Providers use the same factors to determine your Sender Reputation, you should first monitor your Sender Score to gauge where you are in the reputation spectrum and then analyze the factors that impact your reputation so you can maintain it.

1. Monitor your Sender Score to gauge where you are
2. Analyze the factors that impact your reputation
3. Maintain (maintain, maintain)

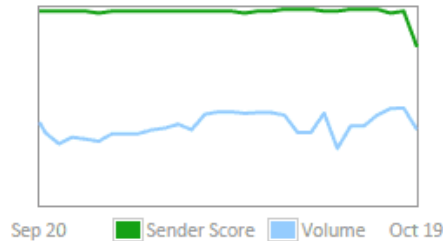
## Sender Score Metrics for 96.47.30.7

80

Hostname ::  
giltgroupe.outbound.ed10.com  
Very High Volume Sender ?

✓ Return Path Certified ?  
✓ Return Path Safe ?

[Whois Lookup](#)



Caption: Sender Score example as displayed in Return Path's Reputation Monitor

### What is Sender Reputation?

**Sender Reputation** is the ranking that Mailbox Providers give your sending IPs and domains. Your reputation is also based on your sending behavior and Mailbox Providers take all of this into consideration when determining if your email should be sent to the inbox, the spam folder or block it completely.

Your sender reputation changes depending on your sending habits and the responses of your recipients, meaning, your reputation could change after each email you send.

Ultimately your Sender Reputation = your Sender Score

### Knowledge Checks

#### Some of factors that determine sender score are:

Complaints, spam traps, **segmentation**, unknown users

Complaints, spam traps, **seeding**, filters

\*Complaints, spam traps, blacklists, unknown users

Complaints, spam traps, unknown users, **seeding**

#### A Sender Score is based on:

\*Sending IP(s)

Sending IP(s) and domain(s)

Sending domain(s)

#### To gauge where you are in the reputation spectrum, you should:

Analyze, monitor and maintain

\*Monitor, analyze and maintain

Maintain, analyze and monitor

## Did not use

### A Sender Reputation is based on:

Sending IP(s)

\*Sending IP(s) and domain(s)

Sending domain(s)

---

### Factors that Influence Reputation

There are several factors that have an impact on your sender reputation and will be discussed in the following sections:

- Complaints
- Unknown Users
- Spam Traps
- Blacklists
- Filters
- Infrastructure and Authentication
- Volume
- Engagement
- Content

### Why is Sender Reputation Important?

Because Mailbox Providers need to fight spam and provide good inbox experiences for their customers, they need to make tough choices about whose email to filter.

*Mailbox Providers use reputation as the most important factor for why email does or doesn't get delivered.*

Poor reputation can lead to your email being delivered to the spam folder and if you don't fix issues with your reputation, Mailbox Providers will scrutinize your email ever more closely -- potentially blocking it from your subscribers.



[6 Dos and Don'ts When Sending Business Emails](#), Graham Winfrey

### Knowledge Checks

**Your Sender Reputation has nothing to do with your sending behavior**

True

\*False

**The better your reputation, the less likely your email will be delivered to the inbox**

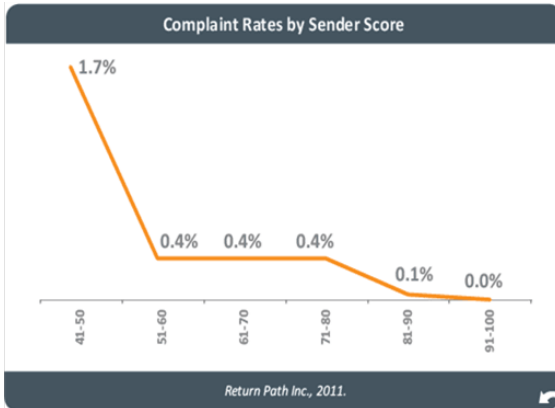
True

\*False

---

### Your Reputation Holds the Key

The crude, content-based tools that Mailbox Providers once used to counter the “spam crisis” are no longer the main factor in determining whose mail gets through. Mailbox Provider relationships aren’t that important any more, either. It’s your **Sending Reputation** that drives deliverability, and your reputation is all about your numbers.



Caption: Click to enlarge

## Data That Drives Deliverability

A Return Path study found that:

*77% of delivery problems were based on sender reputation*

That reputation is based on:

- Complaints
- Unknown Users
- Spam Traps
- Blacklists
- Filters
- Infrastructure and Authentication
- Volume
- Engagement
- Content

## Complaints

**(What)** Complaint rates show how often your subscribers complain to Mailbox Providers, hitting the “report spam” button when they receive your message.

*47% of subscribers use the **spam** button to unsubscribe*

**(So What)** If Mailbox Providers believe your complaint rate is too high, they will filter your email to the spam folder or block it. Subscriber complaints can cause major reputation issues.



Monitoring **Feedback Loops** allow you to identify where the complaints are coming from, then do something about them and learn how to make changes to stop them in the future.

**(Now What)** Sign up, monitor and analyze data from feedback loops for trends, such as date, time, source and demographics. Taking action on this information allows you to maintain a good Sender Reputation.

	49,112,414	144,446	0.29%
WEEKDAY	SENDS	COMPLAINTS	COMPLAINT RATE
SUNDAY	6,133,897	13,000	0.21%
MONDAY	5,744,281	20,758	0.36%
TUESDAY	7,386,666	20,538	0.28%
WEDNESDAY	5,854,336	28,293	0.48%
THURSDAY	7,361,944	26,942	0.37%
FRIDAY	8,753,814	19,822	0.23%
SATURDAY	7,877,476	15,093	0.19%

Caption: Analyze Complaints for Trends

### Knowledge Checks

**If Mailbox Providers believe your complaint rate is too high they are less likely to...**

Filter your email to the spam folder

Block your email

\*Send your email to the inbox

**After signing up for feedback loops, you should:**

Do nothing

\*Monitor and make changes

Monitor the reports

**Feedback loops provide information around which reputation factor?**

\*Complaints

Spam traps

Unknown users

Volume

## Unknown Users

**(What)** An **Unknown User** is an email address that is invalid. If an Unknown User shows up on your list, you know that the email address has either been returned as a permanent failure (address does not exist) or has been abandoned – either way, it is not a valid email address.

The good news is that Mailbox Providers let you know when you send to an unknown user via a message that includes a bounce code. The not-so-good news is that this indicates to Mailbox Providers that you have poor data practices. Be sure to immediately remove these unknown users from your list

```
Reporting-MTA: dns; qmta10.emeryville.ca.mail.comcast.net[76.96.30.18]
Received-From-MTA: dns; omta17.emeryville.ca.mail.comcast.net [76.96.30.74]
Arrival-Date: Wed, 07 Aug 2013 03:40:56 +0000

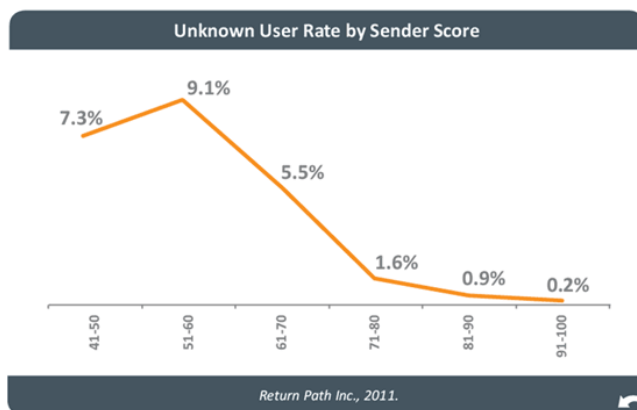
Final-recipient: rfc822; recip123@mac.com
Action: Bounced
Status: 5.1.1
Diagnostic-Code: smtp;550 5.1.1 Recipient address rejected: User unknown.
Last-attempt-Date: Wed, 07 Aug 2013 13:20:11 +0000
```

Caption: Example of a hard bounce code

## Unknown Users Continued

**(So What)** Maintaining an accurate subscriber list is an email best practice. While Mailbox Providers are tolerant of an unknown user rates of about 10%, anything beyond this threshold can result in delivery performance issues.

If you're not monitoring your bounce codes and removing unknown users from your active list, you'll be considered a sender with poor data practices and could be perceived as a spammer. And worse news yet, if you decide not to take action on your unknown users, once the Mailbox Provider converts them into a spam trap and stops sending you unknown user error codes, the time and resources involved in identifying and removing spam traps becomes significantly more intensive. And too many spam traps hits can get you blacklisted!



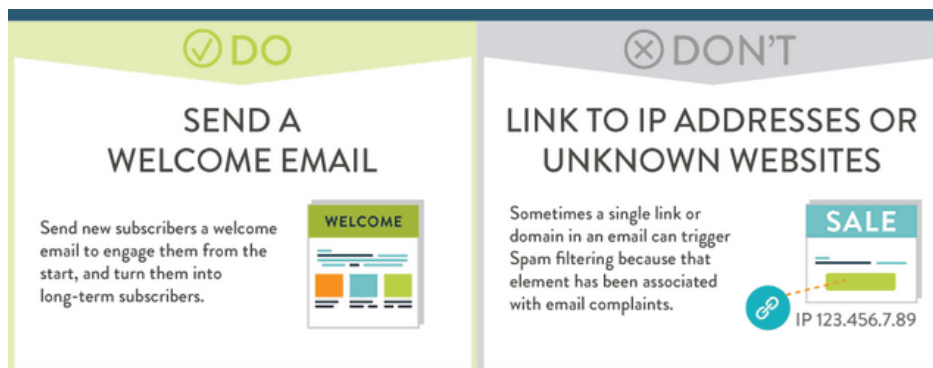
Caption: Click to enlarge

## Unknown Users Continued

**(Now What)** Okay, so before we get carried away detailing all the bad things that can happen if you don't do something with unknown users, here's a few ideas for you to prevent or eliminate them from your list:

- On the registration form, require recipients to enter their address twice to ensure accuracy
- Send a welcome message to everyone who registers and pull any bounced addresses off your list immediately
- Keeping your lists clean means you need to engage in ongoing list maintenance, such as monitoring the age and activity of your data and re-engage and/or remove inactive addresses.

All of these will not only lower your bounce rate, they also reduce the chance that your email will get caught in a spam trap.



[6 Dos and Don'ts When Sending Business Emails](#), Graham Winfrey

## Knowledge Checks

An **Unknown User** is not:

An email address that is invalid

An email address that is a permanent failure

An email address that has been abandoned

\*An email address that you use for promotional email

Mailbox Providers let you know when you send to an unknown user via:

A blacklist

A complaint

\*A bounce code

A feedback loop

An unknown user rate above \_\_\_\_\_ can result in delivery performance issues

5%

\*10%

15%

50%

Once the Mailbox Provider converts an unknown user into a spam trap all of the following occur except for (select one):

The Mailbox Provider stops sending you unknown user error codes

\* The effort involved in identifying and removing spam traps remains unchanged

Too many spam traps hits can get you blacklisted

One way to lower your bounce rate is to send a welcome message to everyone who registers.

\*True

False

---

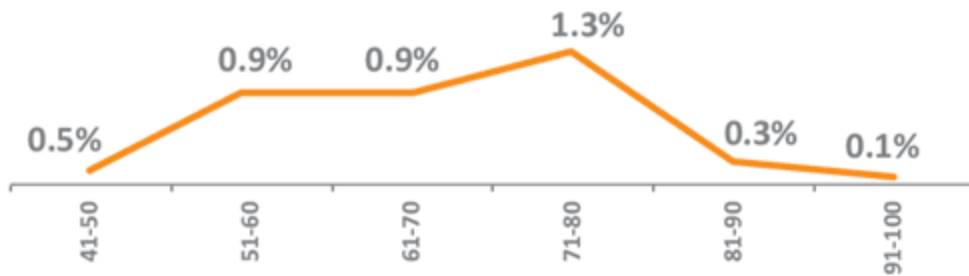
### Spam Traps

**(What & So What)** If you are not already familiar with spam traps, there are two kinds: recycled and pristine. **Spam Traps** are email addresses that are activated for the sole purpose of catching senders with poor data quality and illegitimate data collection practices. So, of course, its no surprise that aged and inactive addresses are the primary reason why most senders have Unknown Users and Spam Traps in their lists.

**(So What).** So, what's the big deal of hitting a spam trap here or there you ask? Well, there are several problems associated with spam traps that can significantly impact your deliverability:

- Spam traps can reduce your sender score and decrease your inbox placement rates
- Mailbox Providers will lower your sending reputation
- Your mailing IPs and/or domains may become blacklisted

## Spam Trap Rate by Sender Score



Return Path Inc., 2011. ↶

Caption: Click to enlarge

### Spam Traps Continued

**(Now What)** We know the last thing marketers want to do is remove emails address from their list, but chances are if you have inactive users on your list, some of them could be spam traps.

Once you figure out which email address are spam traps and remove them from your list, it's all good news! Not only should this have a *positive* effect on your reputation, it can also benefit your active subscribers by ensuring your messages reach their inbox. And you know what this means - more opens, clicks and conversions!

Inbox Percent			
Sender Score	Gmail	Hotmail	Yahoo
0 to 50	26.35%	34.51%	46.61%
51 to 60	29.53%	29.77%	51.99%
61 to 70	32.09%	36.31%	55.85%
71 to 80	38.61%	41.20%	62.46%
81 to 90	62.31%	61.39%	79.71%
91 to 100	81.09%	79.71%	89.89%

Caption: Sender Score and Average Inbox Placement Rate

## Knowledge Checks

### Spam Traps are:

Email addresses that no longer exist

Email addresses consumers use to sign up for promotional email

Role accounts that belong to large groups in an organization

\*Email addresses that are activated for the sole purpose of catching senders with poor data quality and poor data collection practices

### Select from the list the two types of spam traps:

\*Recycled and pristine

Reused and pristine

Recycled and perfect

Reused and primary

The #1 reason spam trap addresses are on a mailing list is poor list hygiene

\*True

False

When you purchase an email address list, they never contain spam trap addresses

True

\*False

You will automatically be removed from blacklists if you manage spam trap hits

True

\*False

---

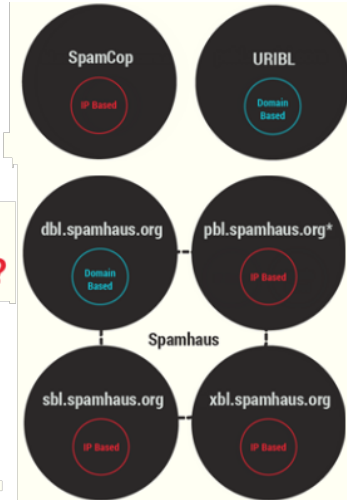
## Blacklists

**(What)** Even if you know how awesome your email is, Spam Filters may not agree. If you are not following best practices, you always run the risk of being blocked. Blacklists are private and public lists of IP addresses and domains that have been reported and listed as “known” sources of spam.

Blacklists use specific criteria to determine if IPs or domains are hitting a lot of spam traps, sending questionable URLs and receiving lots of complaints. The tricky part is that each mailbox provider uses a different combination of these lists to make decisions about which senders to block.

A few of the most reputable blacklists include [SpamCop](#), [Spamhaus](#) and [URIBL](#).

## What are the most common blacklists?



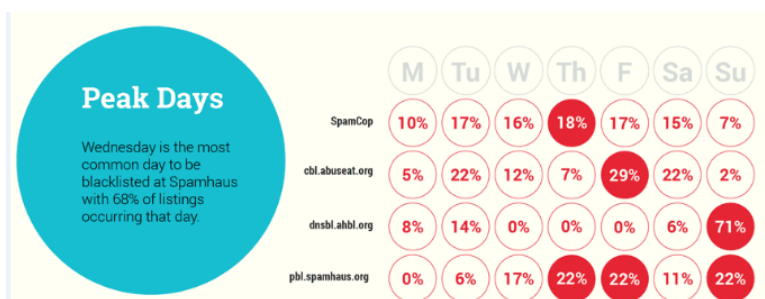
Caption: Click to enlarge

### Blacklist Continued

**(So What)** If your IP address or entire server gets on a blacklist, all of the email sent from that IP address or server gets **blocked**, which means your email never made it, not to the Inbox and not even to the spam folder.

And because each mailbox provider uses a different combination of lists to make decisions about which senders to block, you might get flagged at Hotmail but not at Yahoo.

**(Now What)** Don't let all of your hard work be for nothing, follow best practices (such as including unsubscribe options and double-opt in) and stay off the blacklists.

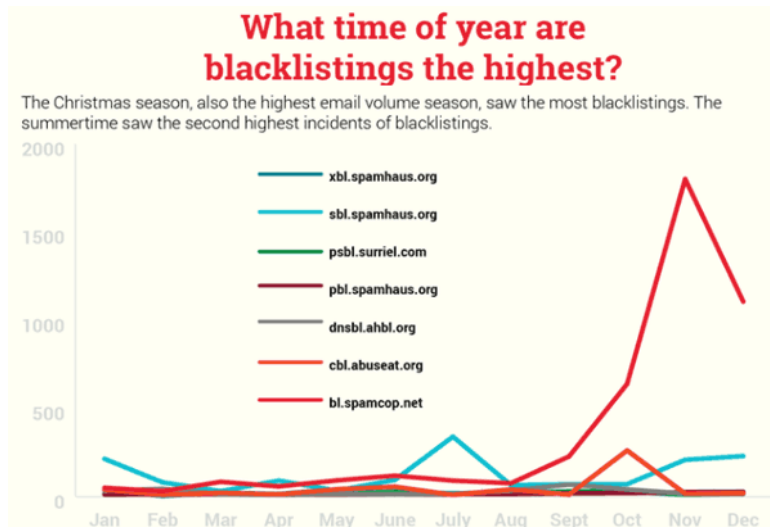


Caption: Peak blacklist days

## Real World -- Seasonal Trends

Blacklisting rates increase dramatically during the holiday season with **more than 49% of blacklistings taking place in November and December.**

The summer months produce the second highest volume of commercial email as well as the second highest blacklist rate.



Caption: Click to enlarge

## Knowledge Checks

### Blacklists are:

Lists of private IP addresses and domains only accessible by the top Mailbox Providers

\*Lists of IP addresses and domains that have been reported and listed as known sources of spam

Lists of private and public IP addresses and domains that are not authenticating

Lists of private and public IP addresses and domains not using DMARC

### The following can be blacklisted:

IPs

Domains

\*IPs and Domains

### Select how a Mailbox Provider makes decisions about which senders to block:

They all use one universal blacklist

\* They all use a different combination of private and public blacklists

They all use the same combination of private and public blacklists



## Filters

**(What) Filters** are processing email according to specific criteria based on patterns found in spammy content or computer viruses. That sounds easy enough, right? Not so quick. What is considered spammy often changes because filters change based on subscribers feedback, for example marking email as spam. All kinds of things get analyzed through filters:

- Formatting
- Content
- Coding
- Images
- From: name
- Sender IP addresses
- Domain
- Reputation

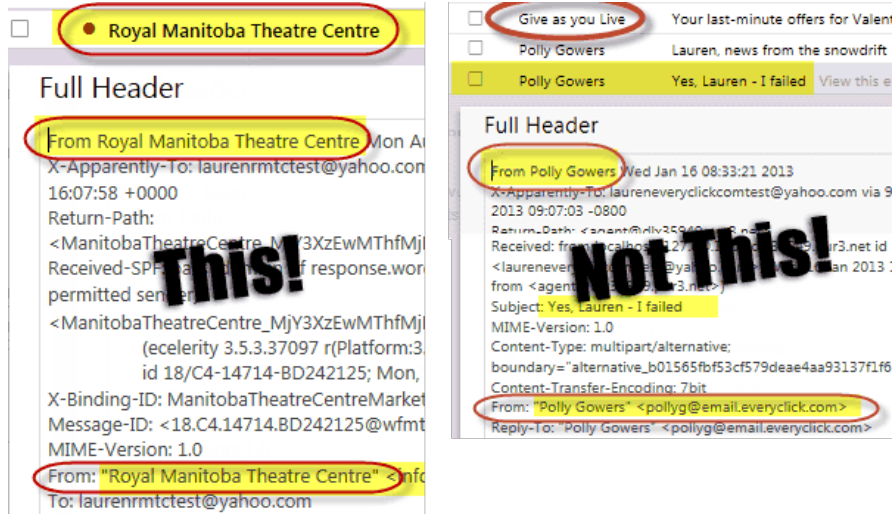


Caption: Click to enlarge

## Filters Continued

**(So What)** The more suspicious activity that is revealed on your IP's, the higher chance that your Sending Reputation will suffer. So don't be *that guy*, don't let your messages get blocked before they've had a chance to make it to the inbox.

**(Now What)** As a sender you should always follow email best practices, including infrastructure, privacy policies, and permission and consent disclosures. Following best practices keeps your Sender Reputation in good standing, ensuring the email you send makes it to the inbox of the people who want it.



Caption: Click to enlarge

## Knowledge Checks

### Filters are:

A process using a domain to identify patterns associated with spammy content or computer viruses

\*A process in which emails are identified as spammy in nature according to specific criteria based on patterns

A process using images to identify patterns associated with spammy content or computer viruses

A process in which emails are identified to be spammy in nature according to the content

### What is considered spammy often changes because:

Filters change based on subject lines

\*Filters change based on what subscribers mark as spam

Filters change based the content of an email

## Infrastructure/Authentication

**(What)** Are you who you say you are? That is a good question. In a time when phishing and spoofing are common occurrences, its really important that both your infrastructure and authentication are set up properly to make sure others know who you are.

**Email Infrastructure** is a term for how computers, networks and servers all work together to send email over the Internet, and that includes *your* email. When you are properly **authenticated**, you are identifying yourself as a legitimate sender.

**(So What)** You might be thinking, wow, that sounds kind of technical, I just need to send email to my customers.


Trust me, nothing destroys your brand and reputation quicker than someone **spoofing** (changing the sending name and / or address in an email message so that it looks like it came from another address) and **phishing** (authentic looking email to trick recipients into giving out sensitive personal information) the customers who trust you.

### Infrastructure/Authentication Continued

**(Now What)** Here are a few concepts that you should be mindful of, depending on if you are working with your IT department or your ESP:

- Once your authentication is set up, you must keep your records up-to-date for SPF, Sender ID, Domain Keys and DKIM
- Do you have functioning reply-to and return path addresses?
- Make sure you have a configurable sending speed and volume (allowing only so many messages at a time)

```
Return-Path: <[REDACTED].5766@envfrm.[REDACTED].com>  
Received-SPF: pass (domain of envfrm.[REDACTED].com  
designates [REDACTED] as permitted sender)  
X-YMailISG: [REDACTED]
```



Caption: Example of partial SPF record

### Knowledge Checks

#### Email Infrastructure is:

A term for how networks and servers work together to send email over the Internet

A term for how email is sent over the Internet

\*A term for how computers, networks and servers all work together to send email over the Internet

#### Spoofing is:

Changing the sender's domain key in an email message so that it looks like it came from another address

\*Changing the sending name / and or address in a message so that it looks like it came from another address

Changing the sender's DKIM in an email message so that it looks like it came from another address

**Which of the following is NOT an example of phishing:**

An email that looks to be from a reputable brand that is trying to trick you into giving out your login information

An email that looks to be from a reputable brand that is trying to trick you into giving out your social security number

\*An email from a reputable brand that is really asking you to fill out a survey about their customer satisfaction

An email that looks to be from a reputable brand that is trying to trick you into giving out your banking information

When you are properly **authenticated**, you are identifying yourself as a legitimate sender.

\*True

False

Your sender reputation is directly linked to the quality of your infrastructure.

\*True

False

---

**Volume**

**(What)** Think about the holidays and how many more emails get sent. A lot of retailers struggle with how many emails to send and on which days, all vying to get customer purchases at the busiest time of the year. **Email volume** is the total amount of email sent and there are several factors that influence and determine how much email you can send successfully, and yes, Sender Reputation is one of them.

**(So What)** One key in the volume metric is consistency, Mailbox Providers like to see smooth broadcast activity, rather than spikes. If your email volume sending changes and Mailbox Providers see large spikes of volume, they might think those large spikes are spam.

Remember that everyday activities can have an effect on the volume of your sends and thus your Sender Reputation, such as purchasing a list or mergers, both can conceivably double the volume of email sends. A brand new IP address can also have an impact on the number of emails you are trying to send.

**(Now What)** Find the balance and find what works for your customers. Send subscribers only what you promised to deliver at sign-up. Also consider offering a preference center where your subscribers can easily choose the email they want to receive and when.

**Knowledge Checks**

**Email volume is determined by total amount sent**

\*True

False

### **In regards to sending volume, which factor has the most effect on your reputation?**

Seasonality

\*Consistency

IP management

Purchasing Email Lists

A best practice is to set up a preference center where subscribers can choose the email they want to receive and when.

\*True

False

---

### **Engagement**

**(What)** Marketers define **engagement** as how active their subscribers are and if they are interacting positively or negatively with their emails. We typically think of measuring engagement through things like opens, clicks, and conversions. We hope that high engagement means marketing efforts are working and translating into higher return on investment (ROI).

**(So What)** Engagement data plays an important role in determining the placement and positioning of emails. It's being used both to influence inbox positioning (how high up the inbox) as well as inbox placement (inbox vs spam). With low engagement, emails are more likely to be sent to the spam folder.

Even though engagement data is great for marketers to measure how effective their programs are, Mailbox Providers don't care how many clicks or conversions you get. Mailbox Providers only care about their users which happen to be your subscribers -- are they showing signs of subscriber fatigue and are they marking your mail as spam?

### **Engagement Continued**

**(Now What)** Email marketers who follow best practices (including using the double opt-in method of collecting subscribers and good list hygiene practices), and who have the best sender reputation metrics will get the best results from their recipients who interact and engage with their email programs.

## Knowledge Checks

### Engagement is not:

The activity level of subscribers

The negative or positive interaction of subscribers

\*Opens, clicks and conversions

Inbox or spam folder placement can be affected by engagement levels

\*True

False

### With low engagement levels, email are more likely to:

Get delivered to the Inbox

\*Get delivered to the Spam folder

Senders with the best reputation metrics often have low engagement levels from subscribers with their email programs

True

\*False

---

## Content

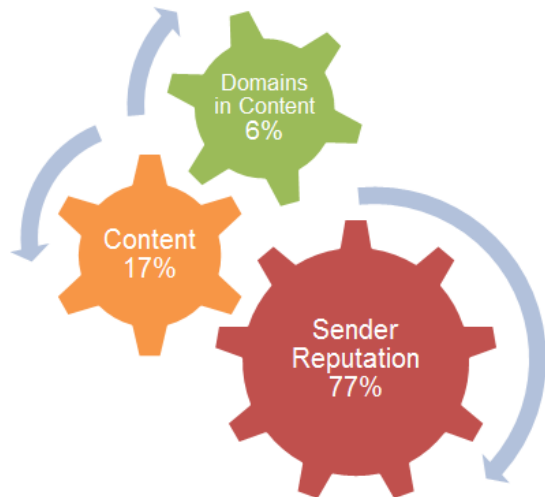
**(What)** As a successful email marketer, you need to walk in your subscribers' shoes. You see what they see, you know how they respond and have learned how they tick in order to maximize your email ROI.

**Content** includes things like your subject line, the text, words, phrases, images, links and header information within the email itself.

**(So What)** Content filters can block or quarantine messages with specific words or phrases or even unique patterns of letters or numbers. So, how important is email content filtering today? Research shows us that focusing on keywords is mostly a myth, what we found is that your Sender Reputation is the reason 77% that your email is getting caught by spam filters, compared to your content at 17%.

## Content Continued

**(Now What)** So now we know, content is important, but not as important as your Sending Reputation. If you're mailing any third party links, like including referral links or mentioning another website, make sure they have a good reputation or you could be guilty by association!



77% of your email is getting caught by spam filters because of your reputation, not your content

### Knowledge Checks

#### Content includes things like:

Header information, images and From: name

\*Text, subject lines and header information

Subject lines, header information and coding

#### Research shows us that focusing on keywords is mostly a myth

\*True

False

#### Which is the most significant reason why email is caught by spam filters?

Content

\*Sender Reputation

Keywords

Subject lines

#### Third party links, like referrals or other websites, are always safe and reputable

True

\*False

## Wrap-Up

Your reputation is your most important asset and a good reputation is the only reliable way to reach the inbox. A good reputation starts with knowing where you stand. Not only is **Sender Score** an indicator of trustworthiness it also helps identify the most important factors that can improve delivery rates.

Today, **Sender Reputation** plays the biggest role in determining whether or not your email makes it to the inbox. A bad reputation can land your emails in the spam folder, a reputation that continues to get worse might cause Mailbox Providers to simply block your emails entirely, so they never reach subscribers.

It's important to understand the many factors that have an impact on deliverability and reputation. Knowing the factors allows you to gain a better understanding of what and how you can strive to implement best practices and continue to be able to make it to the inbox of your subscribers who want and engage with your messages.

---

### Test Feedback Questions:

Based on what you've just read about <topic here>, what are the key points?

Why is this information important for you to know?

How would you use this information in your job here at Return Path?

Was the amount of information covered too much, too little or just right? Too much, Too little, Just right

What would you add or take away?

Other feedback?

After reviewing the course objectives, did this course address these?

What content needs to be added or deleted to address these better?

What did you learn from this course?

What did you like best about this course?

What did you like least about this course?

Who would you recommend take this course?

Do you have suggestions for how to improve this course?

Other comments?