



## ***PerfectMail*** **User Guide**

Version: 3.5.0  
May 18, 2012



# Contents

<b>1 Copyright Notice.....</b>	<b>1</b>
<b>2 Welcome to PerfectMail™.....</b>	<b>3</b>
2.1 Live Filtering.....	3
2.2 Quarantines = E-mail Uncertainty.....	3
2.3 E-mail Recovery.....	4
<b>3 Understanding E-mail.....</b>	<b>5</b>
3.1 E-mail Structure.....	5
3.2 E-Mail Addresses and Delivery.....	5
3.3 Envelope Abuse.....	6
3.4 A Definition of Spam.....	6
<b>4 Our Philosophy on E-mail Security.....</b>	<b>9</b>
<b>5 How It Works.....</b>	<b>11</b>
5.1 Basic Setup.....	11
5.2 Scoring Spam.....	11
5.3 Anti-Spam Tests.....	12
5.4 Rejecting Spam.....	12
<b>6 E-Mail and Anti-Spam Concepts.....</b>	<b>15</b>
6.1 Real-Time Block Lists.....	15
6.2 Grey-Listing.....	15
6.3 Anti-Virus.....	15
<b>7 Frequently Asked Questions.....</b>	<b>17</b>
7.1 Why does an e-mail get Deferred.....	17
7.2 A Spammer Is Using My E-mail Address!.....	17
7.3 Receiving e-mail not addressed to me.....	17
7.4 SPF Rejects.....	18
7.5 My Outbound E-mail is RBL Listed!.....	18
7.6 Why am I still receiving Spam?.....	20
7.7 A legitimate message was tagged [SPAM?].....	20
7.8 E-mail Backscatter.....	21
<b>8 Getting Help.....</b>	<b>23</b>
<b>9 Glossary.....</b>	<b>25</b>
<b>10 Contact Information.....</b>	<b>27</b>



# 1 Copyright Notice

This document is copyright © 1999-2010 by PerfectMail™ Inc. All rights reserved.

This document may be freely redistributed as long as it remains intact. You may quote from this document with appropriate attribution, which must include: the author's full name, PerfectMail™ and, if quoted electronically a hyperlink to PerfectMail™'s web site (<http://www.PerfectMail.com>). PerfectMail™, PerfectArchive™, and PerfectReplay™ are trademarks of PerfectMail™ Inc.

This document may contain proprietary notices, trademarks or copyrighted materials belonging to third parties. Any reference to third party information in no way infers endorsement or association between our company and that party. All such references are for information purposes only. Any terms or conditions of third party intellectual property must be followed.



## 2 Welcome to PerfectMail™

Welcome to the *PerfectMail™ Anti-Spam Solution*. PerfectMail is a server product that filters e-mail *before* it reaches your Mail Server. We provide a flexible solution that works with all SMTP based e-mail products; including Microsoft Exchange™, Lotus Domino™, Novell GroupWise™, Sendmail™, QMail™, etc. PerfectMail™ is a complete server product that can be installed on most modern hardware and virtualized environments.

Our focus is on *business e-mail*. Our mantra is: **No False Positives!**

### 2.1 Live Filtering

*PerfectMail™* is a *live filtering solution*. E-mail is actively filtered, in real-time, during transmission. The e-mail transmission results in either an *accept* or *reject* status.

- *Accepted* e-mail is always delivered to the recipient... always!
- *Rejected* e-mail is always rejected during transmission.

Rejecting e-mail during transmission has some significant benefits for our customers. We accept or reject a message during the SMTP exchange between mail servers. This means we can leverage the existing e-mail infrastructure to *guarantee* the sending server receives the *rejection status* and associated *rejection message*. This is not a *Delivery Status Notification* but an actual *SMTP response*.

The result is **E-mail Delivery Certainty**. The sender can always be certain if an e-mail destined for a *PerfectMail™* server was delivered. If it is accepted, it is *always delivered*. If it is rejected the sender *always received the rejection message*.

Caveat: While we can guarantee the sending server receives the rejection message; we can't control what that server does with it. Most will faithfully pass this rejection message back to the sender; though we have seen instances where this has not happened.

### 2.2 Quarantines = E-mail Uncertainty

A *quarantine* is a holding area for e-mail. Anti-spam filters use quarantines when they cannot decide what to do with an e-mail. This creates a problem of **E-mail Delivery Uncertainty**. The anti-spam solution is uncertain about the *disposition* of the e-mail (spam or legitimate?) and the sender and recipient are uncertain about the delivery of the e-mail.

*"Where is my e-mail from ... ???"*

*"Why did ... not receive my e-mail???"*

Because *PerfectMail™* is a *live filtering* solution it eliminates the problem of e-mail uncertainty. If PerfectMail accepts the e-mail, it is delivered. If PerfectMail rejects the e-mail, this is done during message transmission - **guaranteeing** the sending server receives the reject status, which is then passed to the sender.

Requiring users to check a quarantine for messages is a false economy. The user still needs to review their spam messages and they may have to do it using a separate application or website! All the quarantine has done is added a layer of complexity to checking e-mail. **Many users will not check their personal quarantine - EVER.** Messages held there are forever lost.



PerfectMail offers the benefit of having **no quarantine**. Our uncertainty rate is small enough that simply forwarding messages with uncertain dispositions removes the need of a quarantine. The trade-off is having a couple of spam messages in your in-box. This compromise ensures **no e-mail gets lost**. That is **e-mail certainty!**

## 2.3 E-mail Recovery

Rather than having a *quarantine*, PerfectMail™ has a short term message storage facility where it keeps a copy of **all e-mail** that has passed through it, including a copy of most of the e-mail that PerfectMail *rejected*.

Not only can you release messages that may have been inadvertently rejected, but you can also resend messages that may have been lost for some other reason.

In fact, if you lose your *whole mail server* you can recover your e-mail by using the *PerfectReplay™* feature to simply re-transmit any lost e-mail activity.

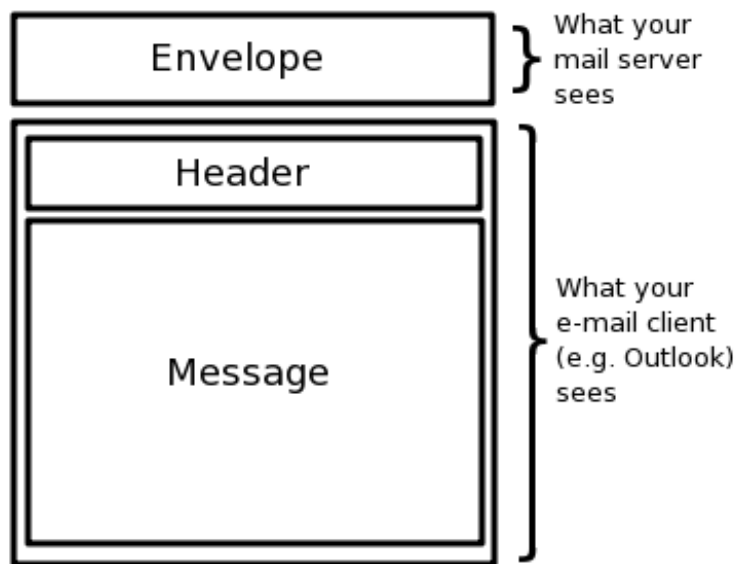
If your mail server does stop functioning, PerfectMail will identify and spool up your e-mail and automatically forward it to your mail server when it comes back up. Then if necessary, you just replay the lost time period. Easy!

## 3 Understanding E-mail

It's important to have a clear understanding of what e-mail is, or more specifically how it is structured. The concepts referred to in this section will be used throughout this document. Many of the idiosyncrasies of spam result directly from the structure of an e-mail. This is also the starting point for the development of the many **anti-spam tests** used by *PerfectMail™*.

### 3.1 E-mail Structure

E-mail is actually composed of two main elements: the *envelope* and the *data* sections. The *data* section is further divided into the e-mail *header* and e-mail *body* or *message*; which may be comprised of different alternative formats and contain embedded images and other elements; as well as e-mail *attachments*.



If we focus on the two main elements, the *envelope* and the *data* sections you can think of an e-mail like a conventional written letter.

The *envelope* contains addressing and delivery information. Your e-mail server uses the *envelope* to decide how an e-mail should be forwarded or delivered. It ignores the actual *message*.

When you view an e-mail using your mail App (e.g. Microsoft Outlook™), you are seeing the *data* section comprising the *header* and actual *message*; the envelope has been stripped away. Liken this action to a receptionist who has taken the letters from their envelopes, put those letters on your desk and discarded the envelopes.

### 3.2 E-Mail Addresses and Delivery

The *envelope* is used, and only used, for message delivery, just like a written letter.

The e-mail *header* is made up of what we like to think of as the delivery information: the From, To, Subject, Date, etc. But this simply is not the case. The delivery information is contained in the *envelope*, which has been discarded. The *header* information is simply information displayed as a courtesy to the recipient.

**The information in the *envelope* and the *header* are completely unrelated!** For legitimate messages the *header* will contain the original delivery information, but this is simply not something that is enforced.

### 3.3 Envelope Abuse

Spammers make use of the inconsistency between the *envelope* and the *header* to try and side-step spam filters. They do many things to push the boundaries of what is acceptable in e-mail. This is why you can receive emails that look like they were addressed to someone else, or no-one at all. In fact, you can put any e-mail address in the *header*!

So why don't we just block this sort of e-mail? Unfortunately, many legitimate e-mail clients also push the boundaries of what is acceptable in e-mail and the spammers take advantage of these issues. Also, this technique is commonly used by distribution lists and newsletters. You may often see text such as "undisclosed-recipients". This technique is so widely used that we cannot block these sorts of messages.

(PerfectMail™ adds a score for mismatches between the e-mail *envelope* and *message headers*, but this alone is not enough to reject a message.)

### 3.4 A Definition of Spam

The word *spam* as applied to e-mail means Unsolicited Bulk Email ("UBE").

Unsolicited means that the Recipient has not granted verifiable permission for the message to be sent. Examples include: first contact inquiries, job inquiries, sales inquiries, etc.

Bulk means that the message is sent as part of a larger collection of messages, all having substantively identical content. Examples include: subscriber newsletters, customer communications, discussion lists, etc.

The technical definition states a message is spam only if it is both *unsolicited* and *bulk*.

Spam is an issue about consent, not content. Whether the UBE message is an advert, a scam, porn, a begging letter or an offer of a free lunch, the content is irrelevant; if the message was sent unsolicited and in bulk then the message is spam.

Spam is not a subset of UBE. It is not "UBE that is also a scam or that does not contain an unsubscribe link". All email sent unsolicited and in bulk is spam.

This distinction is important because legislators spend inordinate amounts of time attempting to regulate the content of spam messages, and in doing so come up against free speech issues.

Important facts relating to this definition:

1. The sending of *Unsolicited Bulk Email* ("UBE") is banned by all legitimate Internet service providers worldwide.
2. Real-time Block Lists are used by hundreds of millions of Internet users to reject emails identified as spam. These lists are based on the internationally accepted definition of spam as *unsolicited bulk email*. Therefore anyone sending UBE on the Internet, regardless of whether the content is commercial or not, illegal or not, needs to be fully aware that they will lose their Internet access if they send UBE and they will be placed on the Real-time Block Lists.
3. All a spammer has to do is **GET YOUR PERMISSION** and they can spam you with impunity.

The last point above is currently a huge issue. All the spammers have to do is to get your e-mail address and

permission, then they can spam you with impunity. At PerfectMail™ we call these spammers "industrial spammers" or "spamvertizers". They are by far the biggest problem we are now encountering.

While they technically gain impunity by skirting the law, at PerfectMail™ we expand our definition of spam to include messages where the sender attempts to hide who they are or where they are coming from.



## 4 Our Philosophy on E-mail Security

We take a different view of e-mail than other anti-spam solutions. Our primary focus is not simply blocking unwanted messages, but allowing legitimate messages through.

An e-mail security product should be safe, secure and reliable. PerfectMail™ is based on the following principles:

### 1. Legitimate mail must get through

PerfectMail's first goal is to identify and accept legitimate e-mail. Our unique approach ensures we have extremely low false positive ratings. *Business e-mail must get through!*

### 2. E-mail servers must be protected

E-mail is business-critical. Mail servers are under constant attack from spammers, hackers and other rogue entities. Using PerfectMail as the first point of contact, you effectively insulate your e-mail server from the Internet.

Using PerfectMail also reduces the amount of traffic that reaches your mail servers. That means a lower load for your servers; and lower costs for your organization. At many of our sites, PerfectMail's *Return on Investment* is high enough to cover cost within a few months.

### 3. Spam should be stopped at the edge of your network

You have three opportunities to block spam & viruses: at the edge of your network, on your mail server and on the PC Desktop. Malicious e-mail poses a significant risk to your company's infrastructure; it needs to be blocked as soon as possible. PerfectMail acts as an e-mail firewall, protecting your servers and desktops at the edge of your network.

### 4. Information is power

PerfectMail includes powerful reporting and search tools to show exactly what is happening with your e-mail systems. We provide metrics so you can monitor your infrastructure and make better decisions to ensure you are getting the best return on investment.

### 5. Anti-spam solutions should free your users

Your anti-spam solution should be accurate and effective, without requiring constant attention from administrators and users. Using adaptive techniques PerfectMail is able to self train, freeing up your administrators and users to be more productive. PerfectMail watches your e-mail traffic and learns who you are, who you know and what you do. Your anti-spam solution should not be more onerous than the problem it's trying to solve.

### 6. E-mail addresses belong on your website

*Make it easy for your customers to contact you: Put your e-mail addresses on your website!* While spammers do harvest e-mail addresses from web sites, PerfectMail makes it safe again. We have tools that identify spammers who gather e-mail addresses from your website - and we stop them.

*At PerfectMail we list our e-mail addresses on our website. See if our competitors do that!*

### 7. Any solution must be compatible with all mail servers

PerfectMail acts as an e-mail relay. By filtering e-mail at the protocol level, PerfectMail is compatible with all mail servers, including:

- ◆ Microsoft Exchange™
- ◆ Lotus Notes™
- ◆ Novell GroupWise™



- ◆ Sendmail™
- ◆ and many more

#### 8. Let you choose your delivery platform

PerfectMail gives you the power to choose how to implement your e-mail security solution. We deliver our product in several ways to give you the most flexibility.

- ◆ *Deploy PerfectMail on your own hardware* - Leverage your existing infrastructure by deploying on: [IBM™](#), [Dell™](#) and [HP™](#); or build your own server.
- ◆ *Deploy PerfectMail as a Virtual Machine* - Virtualization has many benefits for your organization. PerfectMail is developed and delivered on VMware's virtualization products.
- ◆ *Order a hosted solution* - Have your e-mail filtered at our Class A data center. We'll give you all the benefits of PerfectMail and we'll take care of the server.

## 5 How It Works

### 5.1 Basic Setup

PerfectMail™ works as a server based e-mail *filter and relay* solution. Setup your PerfectMail server on the *edge* of your network, just behind your firewall.

**Internet <=> Firewall <=> PerfectMail <=> Mail Server**

PerfectMail™ is a **live filtering solution**. It filters e-mail in real-time during the actual e-mail exchange.

When an e-mail message arrives at your PerfectMail product, it is subject to our suite of validation and verification tests; many unique to PerfectMail. The result is one of three decisions: *Accepted*, *Tagged* (uncertain), or *Rejected*.

Depending on your configuration the messages may be rejected at your PerfectMail server or simply scored and filtered later.

### 5.2 Scoring Spam

Each e-mail is assigned a numerical *score*, generated by our anti-spam engine. The initial score of a message is "0". We use many techniques to scan each message to see how "spammy" it is. The cumulative value of each test becomes the *spam score* of the message.

We have two thresholds, defined for each domain, that determine what happens to each message. The more *spammy* a message is, the higher the score. If the score reaches the *tag threshold* the e-mail will be tagged. If the score reaches the *reject threshold* the e-mail will be rejected.

Similarly, we look for evidence that the message is legitimate, reducing the spam score. Thus, the *spam score* can be a positive or negative number. The higher the number (positive) the more spammy it is; the lower the number (negative) the less spammy.

Tests that result in a high impact are examined first: virus scanning, black/white listing, sender history, etc. These tests take precedence; they can set the message result by themselves and may cause other tests to be skipped.

Some very expensive tests can get very good information about the sender; but they are done last and only if the test can change the disposition of the message.

We examine the traffic patterns between the sender and recipient. For legitimate senders, as their traffic history accumulates, their *spam scores* drop until the sender becomes *implicitly white listed*. This ensures their messages will never be blocked in error.

If the message is not *accepted* or *rejected* by the high impact tests, it is then classified based on its spam score and the Tag and Reject thresholds defined for the recipient.

PerfectMail™ uses three categories when scoring messages:

#### Accept

After being thoroughly scrutinized, the message was deemed wanted and is immediately forwarded to the intended recipient(s).

#### Reject

Messages that are rejected typically contain any of: unwanted content, obfuscated text, misleading or inaccurate e-mail header and/or envelope information, references to spam-friendly networks or other criteria that strongly indicates spam. As a result, PerfectMail™ refuses the message with an appropriate explanation to the sender. Reject messages are customizable so that in the unlikely chance the message was rejected in error, the sender can contact you by other means (phone).

**Tag**  
PerfectMail™ tags messages that score above the Accept threshold but below the Reject threshold. We "Tag" the subject line of the message [SPAM?] and deliver it to the recipient. The user does not need to check a separate quarantine. Typically less than 1% of all messages are tagged.

**Note:** Messages containing viruses, unwanted file attachments, or known Phishing (fraudulent) messages are always rejected.

## 5.3 Anti-Spam Tests

PerfectMail™ uses a variety of anti-spam tests:

- Sender Reputation
  - ◆ Real-time Block Lists
  - ◆ Black/White lists
  - ◆ Real-time dynamic sender behavior analysis
- Historical Information
  - ◆ Past server and sender behavior
  - ◆ Analysis of e-mail traffic patterns
- Server Analysis
  - ◆ Sending server analysis
  - ◆ Sending address verification
  - ◆ DNS configuration validation
  - ◆ Server profiling and identification
- Sender Intention Checks
  - ◆ Test for sender/origin obfuscation
  - ◆ Phishing attempt identification
  - ◆ Recipient validation
  - ◆ Spam Traps
- Content Scanning
  - ◆ Anti-virus scanning
  - ◆ Dangerous attachment filtering
  - ◆ E-mail structure analysis
  - ◆ Content black listing and watch words
  - ◆ Anti-obfuscation engine
  - ◆ OCR analysis
  - ◆ Adaptive content filtering

## 5.4 Rejecting Spam

On any type of *reject*, a message delivery failure is *immediately* returned to the sending mail server. This occurs during the actual e-mail transaction which ensures a guaranteed delivery to the sending server.

Because PerfectMail™ never *accepted* the e-mail, the *responsibility* for dealing with that e-mail lies with the sending server. This behavior is markedly different from many *delivery failure* messages which are generated after a message has been accepted, scanned, then deemed to be spam.

This is a subtle difference but an important one. This ensures the *responsibility* for the e-mail lies with the sending server. We avoid the potential responsibility for such messages and avoid any legal requirements for storage, archiving, etc. that may otherwise be implied.

Further, many *delivery failure* messages are sent to spammers who do not accept them. This can literally choke your e-mail infrastructure with garbage messages that will never be sent.



## 6 E-Mail and Anti-Spam Concepts

### 6.1 Real-Time Block Lists

Real-time Block Lists (RBL) are databases of IP addresses of verified spam sources and spam operations (including spammers, spam gangs and spam support services). These lists are the result of the combined multinational effort to eradicate spam.

PerfectMail™ subscribes to several high quality RBL services along with its own proprietary services.

If your e-mail peers are being rejected due to RBL sites, then there has been some issue with their servers. To stop the messages being blocked, they either need to fix the problem and get de-listed; or you can add their domain to the *No Host Checks* table in the user interface.

### 6.2 Grey-Listing

*Grey-listing* is a technique where incoming e-mail messages are temporarily delayed before being accepted. This can be an effective technique in blocking spam. Here's how *grey-listing* works in PerfectMail™.

*Grey-listing* forces a delay in the message delivery. It forces the sending server to try to resend the message at a later time, usually within 10 to 30 minutes. The *grey-listing* scheme makes use of normal e-mail server behavior. This sort of thing happens quite often with mail servers.

PerfectMail performs its normal analysis of the e-mail. If the score of the message is higher than your tag threshold and the sender has never before sent you a good message, this message is temporarily delayed. This is not a "real" failure. The server says, "I can't receive that message right now, try again later." Most spam engines will not come back, while all legitimate mail servers will. After 3 minutes or 3 attempts to send the message (whichever comes first) the message will be accepted.

PerfectMail has a module that maintains an ongoing list of all machines that have been *grey-listed*. It double checks to ensure the message will come through without too much delay.

*Grey-listing* may also be used on messages that appear to be newsletters or spamvertising. These two types of e-mail are extremely similar and hard to distinguish. If the score is high enough or if specific triggers are found in the message these types of e-mail will be *grey-listed*. Newsletters are not usually time sensitive. Still, after a few messages are exchanged, *grey-listing* will no longer occur for the sender.

If delaying messages becomes an issue, you can turn off *grey-listing* on the *Web Based User Interface (Web-UI) Filter Setup* page.

### 6.3 Anti-Virus

Anti-Virus software examines your e-mail for known rogue software, including computer viruses, worms and dangerous files. Additionally our anti-virus engine has been leveraged to identify known phishing scams and social engineering scams. All such content has the potential to harm your users and your company.

Additionally, PerfectMail™ lets you filter out e-mail attachments which may be dangerous to your users.

PerfectMail offers professional grade anti-virus filtering with ClamAV. To stay up-to-date, your PerfectMail product checks for virus signature updates automatically every ten minutes.



**Important:** PerfectMail anti-virus filtering cannot replace your *desktop anti-virus software*. Sometimes e-mail can contain *web links* to viruses and executable files that PerfectMail simply can't block. We check all *web links* against a list of known malware sites, but this kind of filtering is far from perfect. You still need to rely on your *desktop anti-virus software* to analyze and block viruses and malware at the desktop.

## 7 Frequently Asked Questions

### 7.1 Why does an e-mail get *Deferred*

E-mail deferral occurs when a message (usually outgoing) cannot be immediately handed off to the next relay host. It is quite common to have messages queued as "deferred" as remote mail servers may not be available for any number of reasons: network traffic congestion, service outages, server load, DNS hiccups, grey-listing, etc.

Sometimes *spam* and *delivery notification messages* will get stuck in the queue as well. Spammers send a lot of e-mail, but rarely accept return e-mail, including bounce messages. These messages can get stuck in the queue. PerfectMail™ has automated processes that clean out such messages on an hourly basis.

### 7.2 A Spammer Is Using My E-mail Address!

E-mail is very prone to this sort of thing. When an e-mail is crafted, you can say you are anyone you wish! Spammers take advantage of this to give themselves more credibility and deflect bounce messages to other people.

The best way to block this sort of thing is using Sender Policy Framework (SPF). SPF is implemented as a DNS entry for your domain. It specifies what hosts are valid for sending mail for your domain. Any other host should be considered a hoax.

You can get more information on crafting an SPF Record by going to <http://www.openspf.org/>. On this page there is a section called "Deploying SPF", with a web form for crafting an SPF record (currently set to example.com). Use this to craft an SPF record for your domain.

Many e-mail hosts and even anti-spam filters are not making use of SPF records, so there will always be a number of false messages being delivered; but this is the best method available to us at this time.

### 7.3 Receiving e-mail not addressed to me

E-mail is actually composed of two elements. The envelope and the actual e-mail. Think of it like a conventional letter.

The envelope contains the addressing/delivery information. Your mail server looks at the envelope to decide where the e-mail should go, but will ignore the actual e-mail content. The actual e-mail content contains the e-mail headers (including From: To: Subject:, etc), message body and any attachments.

Your e-mail client displays only the actual e-mail content; the envelope has been stripped away. Liken this to a receptionist taking your letters from their envelopes, putting those letters on your desk and throwing away the envelopes.

This is why you can receive emails that look like they were addressed to someone else or no-one at all. If you received the e-mail, then be assured your e-mail address appeared on the envelope.

Why don't we just block all of this type of e-mail? Well, this technique is commonly used by distribution lists and newsletters. You may often see text such as "undisclosed-recipients". This technique is so widely used that we cannot block these sorts of messages.

## 7.4 SPF Rejects

Message Example:

```
550-5.1.1 SPF Block: YOUR DNS says [192.168.1.13] can't send mail(ID:115I924U002784))
```

This sort of reject message occurs when a sender is blocked because of an SPF failure. Sender Policy Framework (SPF) is a great method for verifying the authenticity of e-mail. E-mail is very prone to spammers spoofing other peoples e-mail addresses. When an e-mail is crafted, you can say you are anyone you wish! Spammers take advantage of this to give themselves more credibility and deflect bounce messages to other people.

The best way to block this sort of thing is using Sender Policy Framework (SPF). SPF is implemented as a DNS entry for your domain. It specifies what hosts are valid for sending mail for your domain. Any other host should be considered a hoax.

Many e-mail hosts and even anti-spam filters are not checking SPF records, so there will always be a number of false messages being delivered; but this is the best method available to us at this time.

Some domains are having problems with their SPF records. We've seen instances where domains are not fully specifying all the machines that send e-mail for that domain.

If you are receiving these errors chances are the computer you sent the message from is not registered in the SPF record for your domain.

This sometimes happens when people send e-mail from their "Home Computer" using their "Work E-mail Address". The e-mail address you used is fine; but the "Work" domain doesn't accept your ISP's IP number (Bell, Sympatico, Rogers, Telus, etc.) as a valid relay host for their domain. If this is the case, make sure you configure your "Home Computer" to use an appropriate e-mail address. If you want people to reply to your "Work E-mail Address", then use this as the "Reply-To" in your e-mail setup.

E-mail may also get blocked when using e-mail relay sites, such as Yahoo Groups. This occurs when the relay site forwards your e-mail using your original e-mail address as the sender address. If your SPF record does not record the relay site as a valid source of e-mail for your domain, your messages will likely be blocked. This situation is best fixed at the recipient site. Add whitelist entries for relay-sites you want to accept mail from.

In general: These issues lie with the sender and their domain administrators; but life is not always that simple. If this is presenting problems you can do the following:

- Contact the sender and tell them there is a problem with their SPF record.
- White list their IP number or Domain.
- Tell the support staff at PerfectMail. We maintain a list of common relay domains that are not SPF checked.
- Or if this is a big problem, turn off SPF filtering in the Global Settings page.

You can get more information on crafting an SPF Record by going to <http://www.openspf.org/>. On this page there is a section called "Deploying SPF", with a web form for crafting an SPF record (currently set to example.com). Use this to craft an SPF record for your domain.

## 7.5 My Outbound E-mail is RBL Listed!

There are many RBL services available on the Internet. If your mail server becomes listed by one of the RBL services you need to go to the website for that particular RBL service. Most RBL sites will provide a look-up page to check if your mail server is listed. Most will also provide a web page for de-listing your mail server.

It's unlikely you were listed without reason. Use the web-tools provided by the RBL site to find out why you were listed. Common reasons are:

- Your mail server has a configuration error that makes it vulnerable to attack.
- Your mail server has been hijacked by a spammer
- A PC in your organization has a spam-virus.
- Your users may be blasting out marketing e-mail that might get reported as spam
- Your server was listed in error.

Once you have solved the problem, visit the RBL service again and ask to have your mail server removed from their block list.

It's important to fix any problems. Repeated listings may find your server permanently listed with an RBL site.

A RBL reject message looks like this:

```
From: Mail Delivery Subsystem <mailer-daemon@recipientDomain.com>
Date: Nov 21, 2006 4:46 PM
Subject: Delivery Status Notification (Failure)
To: theSender@senderDomain.com
```

This is an automatically generated Delivery Status Notification

Delivery to the following recipient failed permanently:

```
recipient@recipientDomain.com
```

Technical details of permanent failure:

```
PERM_FAILURE: SMTP Error (state 9): 550 5.1.1 <recipient@recipientDomain.com>... RBL Block:
spamhaus.org 1.2.3.4
```

Note the IP address above. This is the IP address of the blocked mail server. SpamHaus is the only external RBL service PerfectMail uses. You can query SpamHaus directly by entering the following URL into a web browser (for the above example):

```
http://www.spamhaus.org/query/bl?ip=1.2.3.4
```

To see if you are listed in any of 250+ other popular RBL list sources, please try the following query:

```
http://www.dnsstuff.com/tools/ip4r.ch?ip=1.2.3.4
```

If your IP address is on SpamHaus' RBL lists, please follow the instructions on SpamHaus' web site to remove your IP address. Please keep the following in mind:

- It may take a day or more from the time you ask to have your site removed to the time your mail server is removed from a black list. Consequently, you need to act quickly to ensure minimal interruption to your e-mail service.
- Do not remove your site from a black list unless you are certain that you are no longer forwarding spam. Most black list sites have a 3 strikes rule. They will let you remove yourself 3 times without question. After that, you will have to prove that you are no longer a spam source.
- Mail servers, and antispam products, use many different black lists to determine if a message may be unwanted. Removing yourself from SpamHaus is necessary but may not be enough to fully unblock your server.

- Most mail servers use some sort of RBL protection. If you do not get your server off of popular RBL lists, you will not be able to send mail to most businesses and about 50% of the rest of the Internet.

## 7.6 Why am I still receiving Spam?

There are a number of reasons why the amount of Spam you receive does not go down immediately after implementing PerfectMail.

Here are the most common reasons along with suggestions on how to fix the problem:

- You may be receiving e-mail from unprotected mail accounts. It is quite common for people to have multiple e-mail accounts. Modern mail clients (e.g.: Outlook) can poll for mail from many sources and consolidate it into a single in-basket. PerfectMail will block Spam from your protected accounts but not from unprotected accounts. If all of your e-mail accounts are on local servers, then you can solve the problem in one of 2 ways:
  1. Be sure that PerfectMail filtering is configured for all of your domains. To do this, create domain records in PerfectMail for all local mail servers and all of their respective domains. Be sure to indicate that each domain has filtering enabled (Domains -> Your Domain -> Filtering Enabled is checked).
  2. Ensure that all mail is directed to your PerfectMail server. This may involve updating DNS mail exchanger (MX) records so that they direct mail to your new PerfectMail server or changing the SMTP port forwarding rules at your firewall to direct all traffic to your PerfectMail appliance.
- You may be receiving e-mail from remote mail servers. PerfectMail can only protect e-mail traffic directed to local mail servers. Often people use a mix of e-mail accounts on both local and remote mail servers. PerfectMail cannot protect remote mail servers or popular Web based mail services like HotMail, MSN or Yahoo Mail.
- You may have insecure mail relays. PerfectMail can be told to accept all e-mail from a trusted source. If this trusted mail server also accepts mail from the Internet, then you are providing a back door through which Spam may arrive. To solve this problem, ensure that your internal trusted mail relays do not accept e-mail directly from the Internet. Stated another way, all internal relays must be outbound only mail relays, not inbound mail relays.
- Spammers may continue to use your old IP address. A common implementation strategy is to provide PerfectMail with a new IP address and then redirect e-mail to the new address via DNS MX record updates. This strategy works well for legitimate senders but may result in no immediate decrease in Spam.

Our research has shown that Spam engines do not do DNS queries for each message they send. Instead, they query DNS once and then remember (cache) the answer - sometimes for months. Since DNS queries take time and mail servers rarely change IP addresses, caching IP addresses helps Spammers send out much higher volumes of junk mail.

Often the old IP address is still a legitimate pathway to your mail server. If true, and spammers have cached your mail servers' IP address, then Spam will continue to show up in your inbox.

You can solve this problem by migrating all of your domains to PerfectMail as quickly as possible. Once this is done, configure your firewall to shut down mail handling on the old IP address.

Another solution is to configure your local mail server so that protected domains may only communicate with the mail server from the IP address assigned to PerfectMail (as that is their only legitimate pathway). The local mail server should not accept SMTP traffic for protected domains directly from the firewall.

## 7.7 A legitimate message was tagged [SPAM?]

PerfectMail prepends the phrase [SPAM?] to messages that score above the Tag threshold but below the Reject

threshold. This is intended to indicate that PerfectMail was uncertain as to the real disposition of the message (wanted or unwanted) and so it chose to forward the message with a warning to the recipient.

There are a number of things you can do to address this situation:

- Nothing. PerfectMail will continue to watch your e-mail traffic and record activity between you and your senders. If a sender continues to e-mail you from the same location, with the same e-mail address, then PerfectMail will quickly recognize a 1-way mail relationship and will score messages more favorably. The result is that the [SPAM?] warning usually goes away on its own within a few days to weeks. This works especially well for e-mail newsletters and other 1-way correspondence.
- Reply to the Sender. When you reply to the sender, PerfectMail assumes that you are giving the sender implicit permission to continue sending you e-mail. This behavior is in line with e-mail Best Practices, as users are strongly encouraged to never reply to Spammers or opt out of Spam mail. It usually takes just one reply to cause PerfectMail to drop the [SPAM?] warning. (Note: You must reply from your original e-mail account, not an e-mail relay account. If your mail, once it is filtered, is relayed to a new e-mail address then PerfectMail will not handle the return message.)
- White-List the Sender. The last, and least desirable, alternative is to find the sending server's e-mail address and add it to PerfectMail's white list. This will cause PerfectMail to automatically accept everything (except Viruses and unwanted attachments) from that server. This step can only be performed by the PerfectMail administrator.

## 7.8 E-mail Backscatter

*E-mail backscatter* are the incorrectly addressed bounce messages sent by mail servers generally as a side effect of spam activity. You may receive *Bounce* or *Delivery Status Notification* messages for e-mails that you did not send.

Spammers will use various tools to harvest legitimate e-mail addresses from the Internet. They use these as the *From:* address for spam to make their messages appear to originate from the legitimate e-mail addresses; possibly fooling recipients and anti-spam filters. Due to the design of SMTP mail, recipient mail servers receiving these forged messages have no simple standard way to determine the authenticity of the sender. If a mail server initially accepts the spam, then later refuse and bounce the message, the bounce message will be sent to the (potentially forged) address in the *From:* header.

Because PerfectMail filters during the e-mail message exchange it avoids the problem of backscatter. It returns SMTP mail status messages directly to the connected server, rather than sending a separate bounce message.

There are currently no reliable methods of eliminating spammer generated backscatter. At PerfectMail we continue to investigate this issue and will implement solutions as they become available.



## 8 Getting Help

If you're having problems with your e-mail, contact your local e-mail support personnel. They have more information and the tools to diagnose and remedy your problems.

If your support personnel need assistance they can contact our support staff at PerfectMail™.



## 9 Glossary

### AfriNIC

AfriNIC is the Regional Internet Registry (RIR) for Africa.

### APNIC

APNIC is the Regional Internet Registry (RIR) for the Asia/Pacific region.

### ARIN

American Registry for Internet Numbers. The Regional Internet Registry (RIR) providing services for Canada, many Caribbean and North Atlantic islands, and the United States.

### DNS

Domain Name System (DNS) stores and associates many types of information with domain names; most importantly, it translates domain names (computer hostnames) to IP addresses. It also lists mail exchange servers (MX) accepting e-mail for each domain.

### DNSBL

DNS Black List. Any Black List that is implemented using DNS services. For example, the Spamhaus RBL list.

### DROP

Don't Route Or Peer is an advisory "drop all traffic" list consisting of stolen 'zombie' netblocks and netblocks controlled entirely by professional spammers. DROP is a tiny sub-set of the SBL designed for use by firewalls and routing equipment. DROP is maintained by spamhaus.org.

### FQDN

Fully Qualified Domain Name. An unambiguous domain name that absolutely specifies the machine's name within DNS. For example, mailserver.foo.com.

### IMAP

Internet Message Access Protocol (RFC 1064) is an application layer Internet protocol that allows local clients to access e-mail on a remote server.

### LACNIC

LACNIC is the Regional Internet Registry (RIR) for Mexico, Central and South America.

### MTA

Mail Transport Agent. A term for programs that send and receive e-mail between servers using the SMTP protocol.

### PBL

The Spamhaus PBL is a DNSBL database of end-user IP address ranges which should not be delivering unauthenticated SMTP email to any Internet mail server except those provided for specifically by an ISP for that customer's use. The PBL helps networks enforce their Acceptable Use Policy for dynamic and non-MTA customer IP ranges. PBL is maintained by spamhaus.org.

### POP or POP3

Post Office Protocol is a protocol used by mail clients for fetching e-mail from a mail server.

### Reverse DNS

A process to determine the hostname or host associated with a given IP address or host address.

### RIPE

RIPE is the Regional Internet Registry (RIR) for Europe and the Middle East, including Greenland and Russia.

### RIR

Regional Internet Registry. Five Regional Internet Registries exist: ARIN, RIPE, APNIC, LACNIC, AFRINIC. Each RIR provides services related to the technical coordination and management of Internet number resources within its service region.

### ROKSO

The Register of Known Spam Operations (ROKSO) database collates information and evidence on known professional spam operations that have been terminated by a minimum of 3 Internet Service Providers for spam offenses. ROKSO is maintained by spamhaus.org.

### SBL

The SBL is a real-time database of IP addresses of verified spam sources and spam operations (including spammers, spam gangs and spam support services), maintained by the Spamhaus Project team and supplied

as a free service to help email administrators better manage incoming email streams. SBL is maintained by spamhaus.org.

Spam

E-mail that is both unsolicited by the recipient and sent in substantively identical form to many recipients. Two categories of spam exist: unsolicited bulk e-mail (UBE) messages and unsolicited commercial e-mail (UCE). UBE is bulk blasting of e-mail in contravention of anti-spam laws (e.g. CAN-SPAM Act). UBE spammers promote unethical, illegal and/or immoral activity and may also use spam to commit fraud (identity theft). UCE is e-mail used as a marketing tool. Senders must clearly identify themselves and maintain an opt-out capabilities.

Spam Traps

Spam Traps are *fake e-mail addresses* that are used to catch spammers.

SPF

Sender Policy Framework is an extension to the SMTP. SPF allows software to identify and reject forged addresses in the SMTP MAIL FROM header. This strategy helps defend against e-mail spam. SPF is defined in Experimental RFC 4408.

SMTP

Simple Mail Transfer Protocol is the de facto standard for e-mail transmissions across the Internet. Formally SMTP is defined in RFC 821 as amended by RFC 1123. The protocol used today is also known as ESMTP and defined in RFC 2821.

SSL

Secure Sockets Layer (SSL) is an encrypted protocol designed to enable applications to transmit information back and forth securely. Applications that use the Secure Sockets Layer protocol inherently know how to give and receive encryption keys with other applications, as well as how to encrypt and decrypt data sent between the two.

XBL

The Spamhaus Exploits Block List (XBL) is a real-time database of IP addresses of illegal 3rd party exploits, including open proxies (HTTP, socks, AnalogX, Wingate, etc), worms/viruses with built-in spam engines, and other types of trojan-horse exploits. XBL is maintained by spamhaus.org.

Warez

Is copyrighted material traded in violation of copyright law. The term generally refers to illegal releases by organized groups, as opposed to peer-to-peer file sharing between friends or large groups of people with similar interest using a Darknet.

## 10 Contact Information

PerfectMail™ is developed and distributed by **PerfectMail** (789852 Ontario Inc.).

If you have any questions please don't hesitate to contact us. You can reach us between 9:00am and 6:00pm EST, Monday to Friday.

**Mailing Address:**

PerfectMail;  
15 Claypine Trail  
Brampton, Ontario  
Canada L6V 3L8

**Web Site:**

<http://www.PerfectMail.com>

**E-mail Addresses:**

Sales: [sales@PerfectMail.com](mailto:sales@PerfectMail.com)

Support: [support@PerfectMail.com](mailto:support@PerfectMail.com)

**Phone Numbers:**

Office: +1 905 451 9488

Toll Free: +1 888 451 3131

Facsimile: +1 905 451 7823

