

In keeping with industry standards regarding e-mail security, RMA had implemented state-of-the-art e-mail filtering solutions to protect its network, members, and partners. Every attempted connection to our network is carefully monitored and either accepted or denied, depending on the content and the connecting server's credentials.

If you are experiencing problems sending e-mail to RMA, we suggest that you forward this document to your Internet Service Provider (ISP) or your internal Information Technology (IT) staff. There are several reasons why you or your company may not be able to communicate with RMA via e-mail. These reasons are explained in greater detail below.

Reverse DNS lookup

RMA uses reverse DNS (Domain Name Service) lookups to prevent spammers from connecting to our network. A connecting mail server's identity is looked up or verified by our server before the e-mail is accepted. DNS works like a telephone cross-reference directory, where a number can be looked up by providing a person's address. Most spammers cannot provide this information because they are constantly roaming from ISP to ISP in hopes of spreading their message without detection.

In conjunction with the reverse DNS lookup procedures, RMA uses Internet available blacklists to make our servers aware of "known spammers." These services provide a continually updated list of "known spammers."

If your Internet DNS is not configured correctly, your server will not be permitted to communicate with ours. The correct DNS configuration must contain a PTR (Pointer) record listing your connecting mail server's IP address. This PTR record means that your server can be reverse looked up in the Internet domain name service. All mail servers connecting to RMA must be configured correctly with this entry. If you have questions regarding this configuration, please contact your ISP or your internal IT department. They will be able to verify that they have configured these settings correctly.

An example of a mail server conversation and how reverse lookup is performed:

You send e-mail to someone at rmahq.org (or rmahq.com). Your mail server makes a connection to RMA's mail server and says helo abc.com (helo is spelled this way between mail servers speaking **SMTP**, Simple **M**ail **T**ransfer **P**rotocol, and **abc.com** is an example of what your domain may be called).

RMA's server then begins the process of verification to ensure that your server is legitimate. The IP address (a unique number assigned to any device connecting to the Internet) of your mail server is taken and an attempt is made to reverse lookup the number and get the name of the

server that is connecting. This is done using the Internet Domain Name Service (DNS). An Internet domain known as in-addr.arpa exists to resolve an IP address into a **Fully Qualified Domain Name**. If your mail server were called **mail.abc.com**, this would be its **FQDN**. If your ISP has not listed the IP address and name of your mail server in this in-addr.arpa domain, the lookup will fail. Your ISP must configure the proper record in your domain's DNS records to correct this problem.

If this process fails, RMA's server assumes that your mail server is not legitimate and disconnects from it, terminating the "conversation." The sender of the message would then receive a message explaining that their transmission failed. This message does not come from RMA but from the sender's own mail server telling them that the message was not delivered. If this should happen, do not delete this message. Forward it to your ISP or IT staff. It will help them resolve the issue.

Example: Your company, yourcompany.com, would like to send a message to RMA; yourserver.yourcompany.com connects to RMA's mail server. Your server's IP address is 1.2.3.4. RMA's mail server takes this number (IP address) and tries to do a reverse lookup on it by asking what name (yourserver.yourcompany.com) is associated with the IP address of 1.2.3.4. The answer does not have to be yourcompany.com; it could be yourisp.com but it must resolve, or answer, with some Internet domain name. If there is no entry in the in-addr.arpa domain (reverse lookup of the IP address) the connection is terminated and the message is denied.

The pointer record must be configured by your ISP.

Blacklists

A server will normally be blacklisted when it is configured incorrectly and allows other Internet mail servers to relay mail through it. An example of this would be to mail a letter to a friend and have them mail it to a third person so that the third person does not know it came from you. If you receive a non-delivery report telling you that your mail was not delivered for this reason, you must contact your ISP or IT department and provide them with this information. They must then contact the service that has blacklisted your domain and take appropriate steps to have it removed. Please do not delete the non-delivery message because it will be useful to your technical support department.

An example of how your server can be blacklisted:

Certain organizations on the Internet compile lists of known spammers and organizations that have been known to relay spam. These organizations, known as blacklist services, constantly test and monitor mail servers on the Internet to see if they are facilitating spam delivery. If your server has been known to relay spam by these organizations, your server(s) will be blacklisted. If you are listed, it is the responsibility of the blacklisted party to correct these misconfigurations. Then, to have your servers removed from blacklist, you must contact the blacklisting organization. The blacklisting organization will then test your server to see if it is configured properly and, if so, will remove it from the list.

Sometimes it is difficult to convince these services to remove your domain name from their list. But unless you can convince them, no one using their services will be able to accept mail from you. If your domain name is on any list that RMA uses, we cannot do anything to resolve the problem until you are removed from their list.

RMA uses the following Blacklist servers:

Bl.Spamhaus.Org
Rbl.Spamcop.Net

Here is an example of how a hacker can relay spam through your “third party” mail server without you knowing it. A hacker’s Internet domain is abc.com. The hacker creates a message to send to someone at xyz.com. He then sends the message to the address at xyz.com using mail.def.com as his mail server; that way, when it gets to xyz.com, no one will know that it was sent from abc.com. This is called relaying. If a mail server is configured incorrectly, it may be open to hackers attempting this procedure.

It is RMA's policy to respond to all communications in a timely manner. If you send e-mail to an RMA staff member and do not hear back in a reasonable timeframe, please contact that individual by telephone. In addition, if you receive any return e-mail from either our mail server or your mail server, please keep the message and forward it to your ISP or IT staff. This will help them resolve the issue.

Filtering

All incoming mail is carefully filtered. If the content is legitimate, it is automatically passed on to the intended recipient. However, if it is deemed to be spam or inappropriate, we isolate it for further review and may discard it.

In addition, any attachments with an .exe file extension will not be allowed through. These executable files generally are the source of viruses and worms. In regards to all other attachments, RMA’s policy regarding e-mail attachments is very liberal. We accept attachments up to a file size of 20MB. If you have a file that is larger, you will need to save it to disk or CD-ROM and mail it to RMA.

What to do?

We suggest that you forward this document; along with any e-mail error messages, you may have received, to your IT staff to see if they can help resolve the issue.

If you are still experiencing problems and are unable to send e-mail to RMA, please contact us at Ineedsupport@mailhelp.rmahq.org. Please indicate in the subject line that your e-mail is for IT support in regards to your continuing problems. You may also send any e-mail intended for an RMA recipient to the address listed. Please indicate in the subject line that the e-mail is intended for delivery to a specific person at RMA.