

## What to Tell Your Users

Designed to be a turn-key solution for IT staff and end users alike, there is not much in the way of education or training required in order to successfully implement the OnlyMyEmail Business Spam Filtering service (MX-Defender).

Your average user will need no instruction whatsoever, but what follows are a few brief usage tips that you may wish to share with your end-users.

### Viewing/Retrieving Blocked Spam

An email “SpamReport” will be sent to each filtered address on a daily basis, though this feature may be deactivated from the Preferences menu within the Support site. These reports contain Subject line hyper-links from the previous day’s blocked emails that will allow your user to review any message deleted by our system.

Additionally, each SpamReport contains a link where users may generate an “On-Demand” report providing access to the current day’s deleted email as well.

When viewing an email we have deleted, clicking the “Resend” button will quickly re-deliver the original message.

Upon resending, a simple “Yes/No” option is provided that allows the user to request the sender be allowed to deliver messages to them in the future. Notice that such a decision by one end-user will not directly affect other users in your account. In effect, each user effectively trains the MX-Defender to meet their personal needs.

If you wish to filter these daily reports in any way (whether in your MTA or email clients) notice that the sending address will always be SpamReports@OnlyMyEmail.com

### Reporting Spam Messages

Each message we filter and then deliver as valid will contain an extra line at the very end of the email that will include a Spam Submission hyper-link. This link will always begin with a new line, stating:

*If this email is spam, report it here:*

Triggering this link will automatically open a new browser window (just like viewing emails from our SpamReports) where you can “click-to-confirm” that a spam message was delivered through our filters.

This feature may also be deactivated from the Preferences menu of the Support site.

### Outbound Emails

Unless you choose to host your email with us, the OnlyMyEmail MX-Defender is not involved or related to the sending of outbound email.

## **Inbound Emails**

There are a few specific rules and limitations that apply to emails delivered to your domain that are necessary in order to maintain the highest level of accuracy within the spam-filtering process.

**Size:** Email attachments are limited to 25 MB in size.

Should a user need to receive an email that exceeds this size, we suggest advising the sender to compress the file by first converting to a “zip” format.

Alternatively, there are many web sites on the Internet that allow users to upload large files and email links to the desired recipient, who may then download the attachment directly from the host Internet site.

**Subject:** Inbound emails must contain a “Subject”

Emails that do not contain any information in the “Subject” line stand a significant chance of being deleted as spam.

**Content:** Inbound emails must contain some content

This requirement is usually only an issue when a sender either:

- Uses email as though it were Instant Messaging, with the Subject line containing the entire message
- Sends an attachment with no other content within the body

Senders should be advised to include at least one “word” within the body of their emails. Notice that a sender who has configured an automatic “signature” for their email will not need to add any additional content.

**Recipients:** Inbound emails cannot contain more than 20 recipients destined for your domain.

If there is a need to send large volumes of email to your users, then senders should be advised to either:

- Send several emails with no more than 20 recipients per message
- Use a “list-server” that will send “individual” copies to each recipient
- Send email with a contact manager capable of sending individual copies to each recipient
- If the sender is internal to your organization, it is recommended that your email administrator configure your system to deliver such emails “locally” thereby bypassing our system entirely (and also speeding up delivery as well)

The above represents the only scenarios that have the potential to require any special end-user consideration when using the OnlyMyEmail MX-Defender to protect your domain. Feel free to distribute this document to your end users, or simply keep a copy on hand as a reference in case questions may arise.