FAQ

Question: What happens if I don’t read this document?

Answer: When we cut over to the new spam scanning service, you will no longer be able to send email using CMS mail infrastructure, and if you forward email from your CMS/CS/ACM address to a mail address somewhere else, you will find some confusing messages sent to your destination address. You may wind up with some mail in a quarantine that you don’t know how to access. Your incoming mail server settings will not change.

Question: What is Can-It Pro?
Answer: Can-It Pro is the new spam scanning service replacing Maia Mailguard, our former spam scanning service.

Question: Why are we switching?
Answer: Maia Mailguard is a fairly complex system made of multiple moving parts. It has gone from being under active development to being unacceptably out of date. While we have a general commitment to using Free and Open Source software, spam scanning is regarded as a highly critical service which requires a reliable vendor. This has become a big enough complaint that we are initiating this change a year before our projected end-of-lifecycle for the existing spam scanning service.

Question: What does this mean for me?
Answer: First and most importantly, you should wind up getting a *lot* less spam. Second, it depends on a couple of factors.
- If you currently send mail using CMS, you will need to reconfigure your email client to send mail using the new spam scanning service, which will replace the existing outgoing mail server “mailhost.cms.caltech.edu”. Instructions on how to do that are below.
- If you use both a usuário@cms.caltech.edu and a usuário@cs.caltech.edu or a usuário@acm.caltech.edu email address, you will have to make some additional changes, see also below.
- The new system is no longer opt-in. You are required to funnel email through Can-It Pro, especially if you use your usuário@cms.caltech.edu as a placeholder address which forwards email to some other email domain

Question: What if I really, really want to make sure certain emails don’t get caught in the spam quarantine?
Answer: You can add individual email addresses or email domains (such as cms.caltech.edu, caltech.edu, or gmail.com) to a whitelist, which will ensure that any email that has a “from” address matching those parameters sails through the spam scanning service. Instructions on how to do this are below. However, since email is not authenticated, that also means that anyone who forges that email address will be able to send you spam and it will pass straight through the filter. The risk involved here is highly user-dependent. Everyone on campus has
received a phishing email from a forged techsupport@caltech.edu address at one point or another, so you can see the potential danger here of simply whitelisting “caltech.edu” email addresses.

As a reminder, the technical staff will never ask for your account password in email, nor will we point you to a web form that requires your password for administrative purposes. Our password expiration notifications will always look the same, and they will remind you to log in, interactively, using the SSH protocol. Any message that is alleged to be from the CMS systems administrators that asks for your password is guaranteed to be a phishing attack.

**Question:** Wait, that means if I have people emailing me at my cms.caltech.edu address and it forwards to my gmail address, that I have *two* spam queues to check! Isn’t there another way?

**Answer:** Unfortunately, no. If we simply forward all mail that is addressed to your username@cms.caltech.edu address to your gmail address, you will indeed only have one spam queue. But the consequence of that is we will be forwarding a corpus of mail that is roughly 99% spam, and 1% legitimate mail. We have done this in the past, and what winds up happening is that the destination email service adds our mail service as a “suspected sender of spam” to various real-time block list services on the Internet, which means they no longer accept mail forwards for your alias… and they also contribute to blocking CMS mail functionality for the rest of the department.

**Question:** What about the folks who have old email addresses, either ACM or CS or CMS ones, but no longer have CMS accounts?

**Answer:** Equally unfortunately, we will have to have some defaults set in place to cover all of those addresses, and the users (no longer having accounts) will not be able to change their preferences, or access their quarantine, so the mail will simply be discarded. This means that mail that looks sufficiently “spam-like” will just disappear. Their choice is either to accept that we pre-screen some of the mail and reject it, or to discard their old CMS/CS/ACM alias. The faculty who possess CS/ACM email addresses but no longer have CMS accounts are an exception. We can make some changes to their account as site administrators and allow certain lists of addresses through un-scanned if this is deemed necessary.

**Instructions for End Users**

*Changing Your Outgoing Mail Server Settings*

Starting with the beginning, we need to reconfigure your outgoing mail server settings to connect to the new mail system.

The SMTP server name will remain the same (“mailhost.cms.caltech.edu”). The SSL certificate will remain the same. All you need to do is change your outgoing mail port from port 25 to port 587. If you’re using Thunderbird, you do this by choosing the Tools Menu, and selecting “Account Settings”. This will open the “Account Settings” window. On the left, you will see a box with entries for your CMS account, and at the bottom of the list there will be an entry for “Outgoing Server (SMTP)”. 

When you click on that, you’ll see the right side of the window change to show all of the outgoing mail servers you have saved in your account profile. One of them should be named “CMS” or “mailhost.cms.caltech.edu” (you may have only one). Select that and choose “Edit”.

The SMTP Server window will open. All you need to do is change the “Port:” entry to 587. The Connection security remains at “STARTTLS”, Authentication method remains as “Normal password”, and the User Name is your CMS account name (the Description field can be blank, it isn’t necessary).
When you send your first email after changing this setting, you will get a pop-up warning that the certificate belongs to a “mailhost”, but the machine name is not “mailhost”. This is normal, as “mailhost” is a CNAME. You can accept this certificate, select “store this certificate permanently”.

**Logging into Can-It Pro**

Like Maia, Can-It has a web interface for managing both your preferences and your spam/ham queue. Like Maia, Can-It uses a mix of set rules, real-time block lists, whitelists, blacklists, and a Bayesian database to score messages as “potential ham” (legitimate mail) and “potential spam”. Once the accrued score of a mail passes over your threshold for “considering a message to be spam”, it will be either tagged or put into a quarantine.

By default, the system is set to quarantine suspected spam when the spam score is 4.5 or greater. The lower you make your “spam threshold”, the fewer spam messages will get through to your INBOX… but the higher the likelihood that you will catch legitimate mail in your spam filter. The technical staff use a spam threshold score of the default and “3”, respectively, for reference.
The Can-It Pro web site is: http://canitpro.cms.caltech.edu Your login is your full email address (username@cms.caltech.edu), and your password is your CMS password:

![Image of login screen]

Note: Cookies must be enabled in your browser to log in.

After you log in, you will be taken to the Can-It Pro Home Screen:

![Image of home screen]

You can easily add individual senders or domains to your whitelist from this screen.

To get to your individual settings, you click on the Preferences link:
Which will take you to the page where you can see your preferences.

The first thing to do, if you have a CS or ACM legacy email address, is to add that address to your username@cms.caltech.edu stream so that you only have to manage one set of spam settings.

Click on the “My Addresses” link:

And in the next window, add your CS or ACM address (or both, if you have them), and click “Add Addresses”:

Next, if you want to change your Quarantine Settings, click on the Quarantine Settings link:
The Quarantine Settings page is too large to show in one picture. The areas that most people will be concerned about are the “Filter Settings”, the “Tag Settings”, and the “Auto-Whitelist” feature.

The default spam threshold is “4.5”, this is located in the “Filter Settings” section. You can change that to lower or increase the default threshold:

![Filter Settings Table]

The “Tag Settings” section is used if you don’t want to quarantine messages at the spam filter, but instead have them delivered to your INBOX and use your email client’s rules to filter out potential spam messages. Some people prefer to have their spam mail delivered, but simply marked as “likely spam”. You can change that setting in the “Tag Settings” section:

![Tag Settings Table]

Finally, by default Can-It Pro uses an auto-whitelist feature. This means that if someone sends you a message that is mis-identified as spam, and you rescue it out of your spam queue, the “from” address will be automatically added to your whitelist, for 180 days. You can change these settings in the Auto-Whitelist Section:

![Auto-Whitelisting Table]

Finally, the Can-It Pro system has excellent online documentation, which can be accessed on virtually every page by clicking on the Online Documentation link: