Fight Spam and Protect Your Privacy by Disabling Remote Content in Apple Mail

We all hate spam. No, not the disturbingly delicious canned meat. I'm talking about email spam. Despite continued improvements in spam detection and filtering, it's almost unavoidable these days, and while you likely won't ever be able to stop it completely, there *are* steps you can take to minimize it. One of those steps is disabling remote content in the OS X Apple Mail app. Here's why and how to do it.

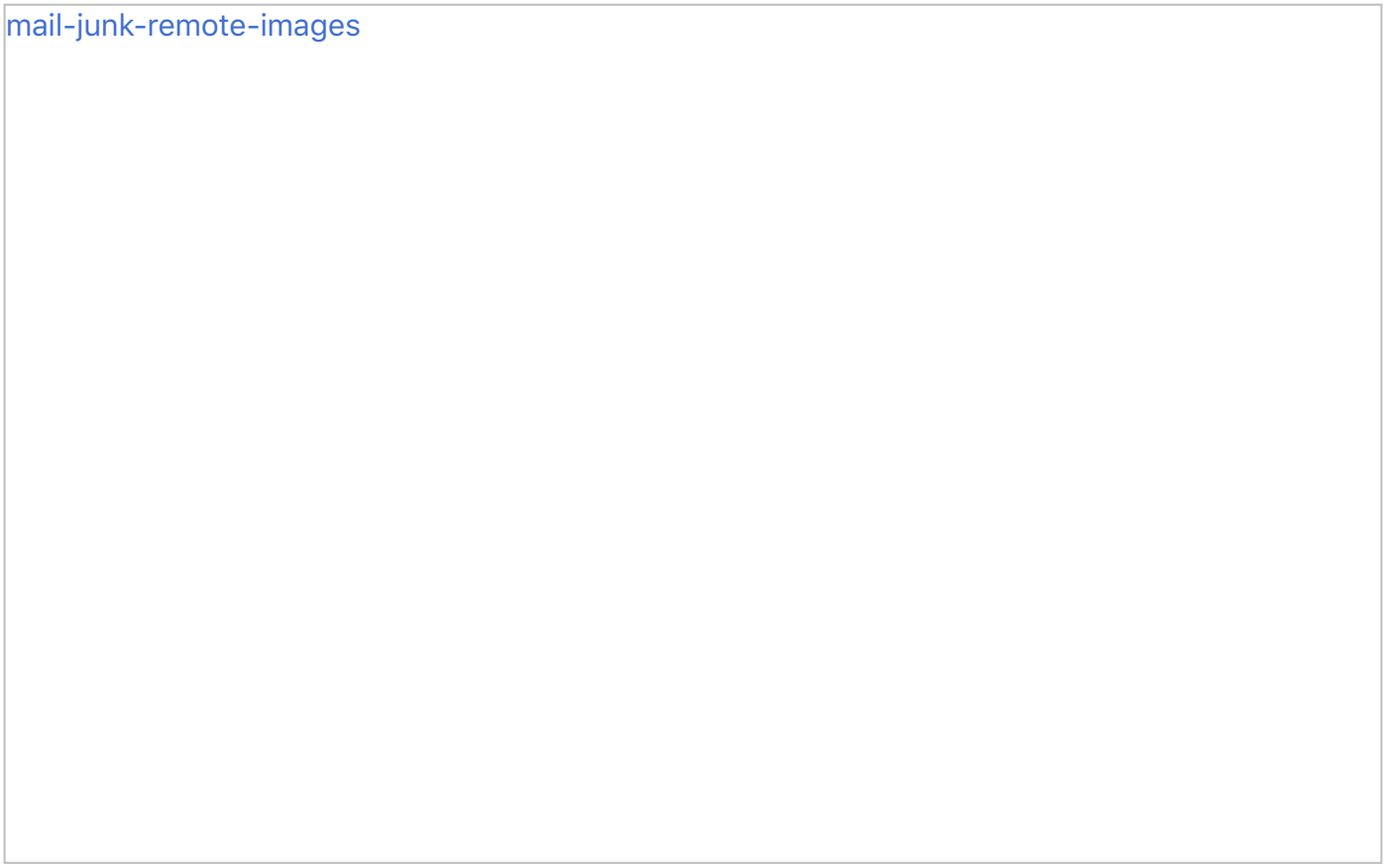
First, a little background. The immoral jerks behind spam email often send out millions of messages at a time, frequently "guessing" at email addresses

from popular domains such as Gmail, Yahoo, and iCloud. From a spammer's perspective, for example, it's a safe bet that "bob@yahoo.com" is a real email address, and when you have powerful modern computers and scripting software, you can just as easily generate "bob2@yahoo.com," "bob1980@yahoo.com," and so on, with virtually endless variations. The spammer will eventually end up with a huge list of potential victims, but one that's filled with email addresses that don't actually work.

In terms of the huge numbers that spammers deal with, such a list is still relatively valuable, even if only one out of a thousand addresses is real and actively used by the account holder. But narrowing down that list to maximize the number of "real" email accounts can be extremely lucrative to spammers, both for their own criminal marketing ambitions as well as for increasing the value to potential buyers of that list.

So spammers often employ several tactics to try and confirm that email addresses in their system are real and in active use. The first and most obvious tactic is of course attempting to trick the recipient into acting on the spam email's offer, by enticing the recipient into clicking on a link to "buy" a product, receive a "discount," or provide personal information in some other way. Hopefully, most experienced email users have by now learned to be wary of such offers.

The second method is a little more devious: offering an "unsubscribe" link. Real companies are required by various laws and regulations to offer email recipients a safe way to remove themselves from a legitimate mailing list, and spammers take advantage of this requirement to trick users into clicking on an "unsubscribe" or "remove me from this list" link.



This spam email is using all three tactics, including the dangerously fake unsubscribe button.

At best, clicking a link like this confirms to the spammer that your email address is real and that you actively use the account. At worst, it takes you to a phishing page in an attempt to ascertain your personal information, or takes you to a hijacked website that will try to infect your computer with malware. In any event, *never* click the "unsubscribe" links in suspicious email messages. Doing so will only ensure that you receive even *more* spam.

Once again, hopefully most users are already aware of the unsubscribe trick, and a day will come when such a tactic is no longer effective for the spammers. But there's still a third tactic that's less obvious: remote images and content.

You see, once upon a time email was just plain text with no formatting, images, or other fancy features. But as the needs and desires of Internet users grew, so too did users' expectations for email, and today's email is

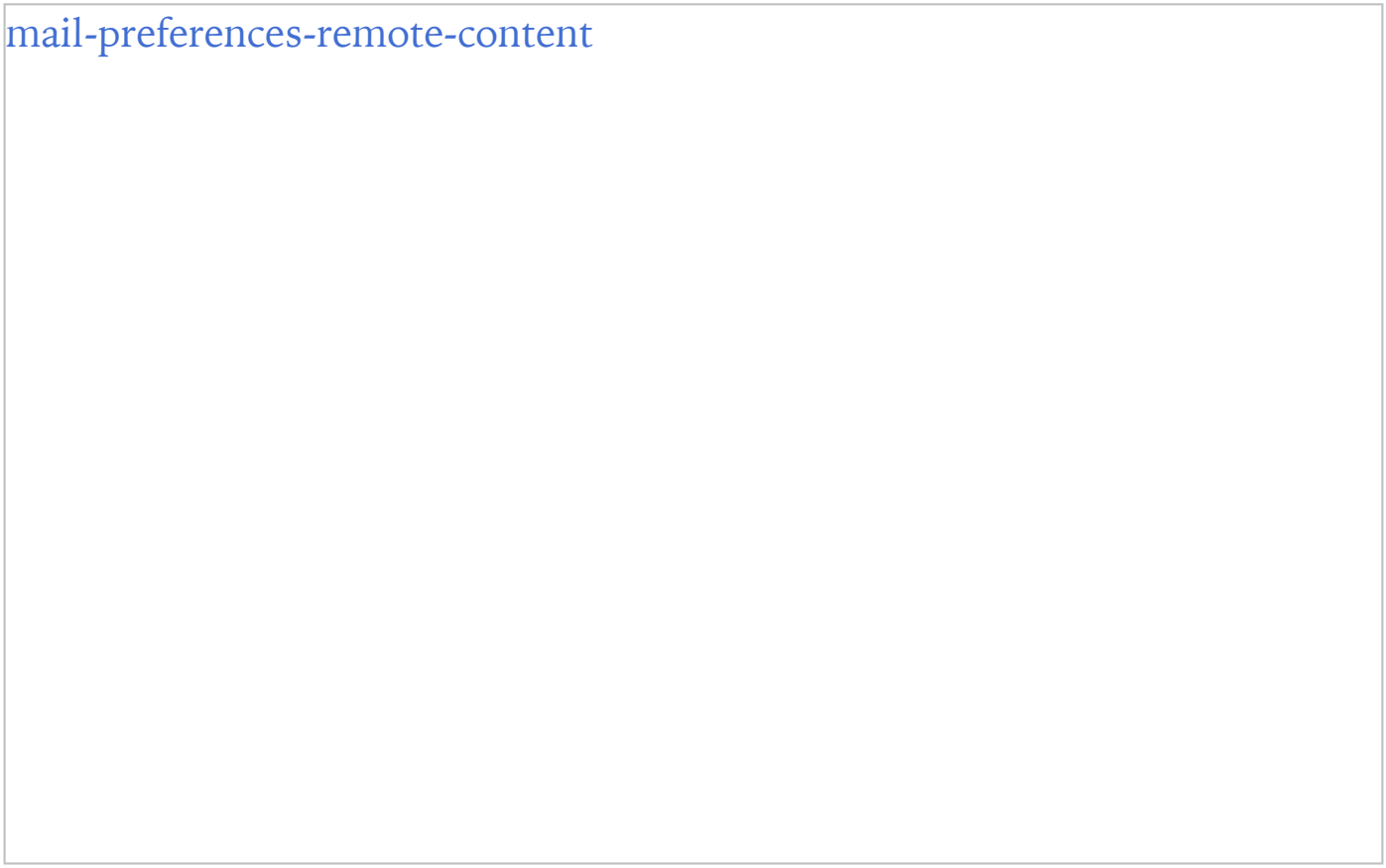
available in full HTML, with links, images, text formatting, and code. The problem is that the code that displays images or content in your email is hosted on an offsite server. When you receive an email from Amazon.com, for example, the Amazon logo and product images aren't attached to the email, they're stored on Amazon's servers, and when you open the email to view it, a little bit of code in the email message makes a call to the Amazon servers and displays the intended images. This is all seamless to the user, but there are some important privacy and security implications here, especially when it comes to spam.

An example of an email with remote images disabled (left) and enabled (right).

Using remote images and content lets legitimate companies and users keep email messages small, and allows for more useful formatting. But spammers and other online bad guys can use remote code to tell if you've received their email. Unlike our Amazon example, a spammer will use tracking code that

associates your specific email address with a link to a remote image on the spammer's server. If you even *open* a spammer's email that contains images, the spammer instantly knows that your email address is valid and that you saw the spam email. Even worse, the spammer will also be able to learn important information about you, such as your IP address, which for most users reveals their general geographic location.

Just like the first two tactics above, this proves you're a real person, and gives the spammer far more information about you that you ever intended to provide. It's even more insidious, however, because the user doesn't even have to do anything other than open the email message, which may not always be easily identifiable as spam *until you open it*. Thankfully, you can mitigate this risk fairly easily in most modern email applications, including Apple Mail, by preventing the automatic loading of remote images and content.



Launch Mail in OS X and go to **Mail > Preferences > Viewing**. Find the box labeled **Load remote content in messages** and **uncheck** it. This stops Mail from automatically loading images and other remote content when you first open an email message. Instead, you'll see a new bar at the top of each email that contains remote content, asking you if you'd like to "Load Remote Content" (you can see examples of this prompt in the screenshots above). Just click on that button once you're sure that the email is legitimate, and you'll see the remote images and formatting appear in the message.

Note that Apple Mail doesn't save or remember your choice, so you'll need to choose to load remote content each time you open an email message, even if you had previously elected to load remote content on that same email.

The potential downside to disabling remote content is that emails from legitimate senders won't render properly unless you click "Load Remote Content" for each message, but considering the increasingly disruptive spam problem, such a drawback is arguably a small price to pay for decreased risk. Disabling remote images and content in Mail won't eliminate spam entirely, but it's an important step in the greater battle against this terrible practice.

Although this tip focused on Mail for OS X, you can achieve the same result in Mail for iOS by going to **Settings > Mail, Contacts, Calendars** and turning off "Load Remote Images." Other email apps such as Outlook and Thunderbird have a similar feature, although both prevent remote images from unknown senders by default.