Handling Email Attachments with Mimecast

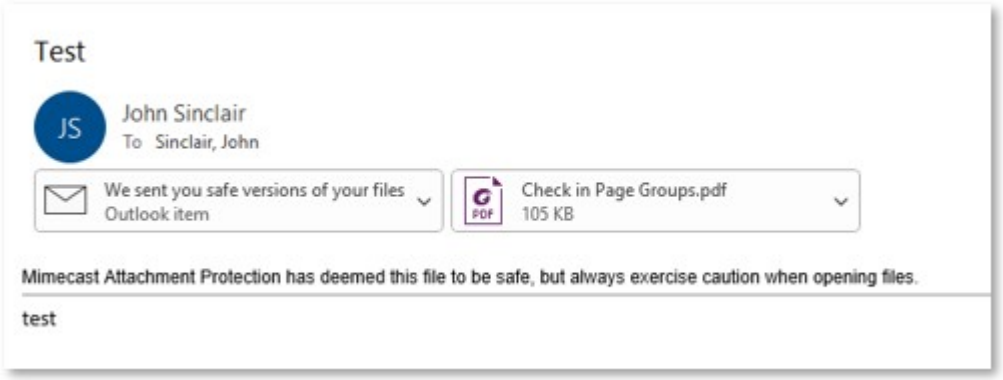
Eric Ruthenberg - 2023-07-14 - Comments (0) - General

There are many ways of delivering malware and viruses via email attachments. **Mimecast** handles these attacks by scrubbing the original file for any malicious content and then converting all attachments to a safe PDF format.

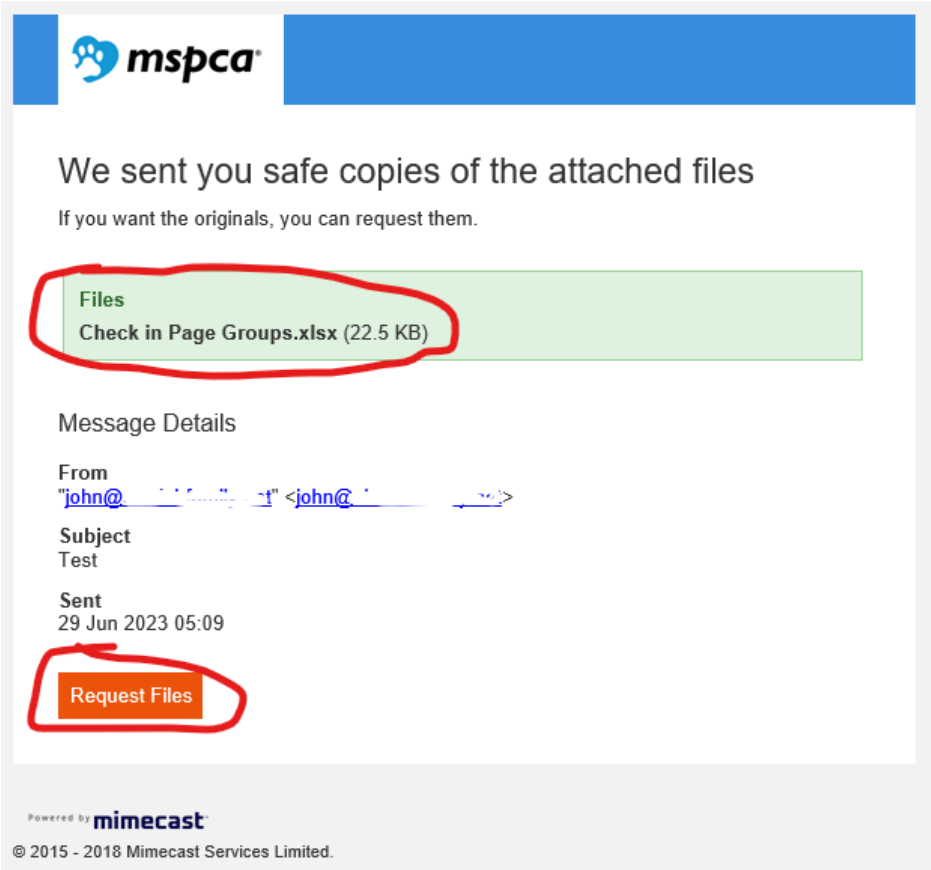
For all emails that contain attachments you will now be presented with a “safe file” first. The “safe file” is a .pdf version of the attachment that was sent to you. If that version is sufficient for your purposes, there is no action needed. If you require the file in its original format there will always be the option to request that file right from the email in which the transcribed file was provided.

For example, if you were sent a word document that you need to edit, you will first receive the document in a .pdf format immediately, then you can request the original word version by clicking on the link within the email. It will take a few minutes to receive the original file.

Below is an example of an email that was sent with an Excel attachment, and how the corresponding Mimecast alerts appear:



As you can see, there is an additional message titled “We sent you safe versions of your files” – this is the message that will contain the link for receiving the original file. Upon opening that message, you will see the following:



As highlighted, the message will list the file name(s) of the original file(s), as well as a “Request Files” button to request the delivery of the original files.

If the PDF version is not sufficient for your needs, please click the “Request Files” button and the original files will be delivered to you in a matter of minutes.