Threat Actor Identification Activity in Pioneer Webmail

Cybercriminal activity continues to be on a massive rise in this digital age. One of the most common ways these threat actors steal data and information is through phishing. Phishing emails and texts typically tell a story that brings forth a sense of urgency for the end-user to react immediately through a sudden course of action.

4 signs of a phishing email are as follows:

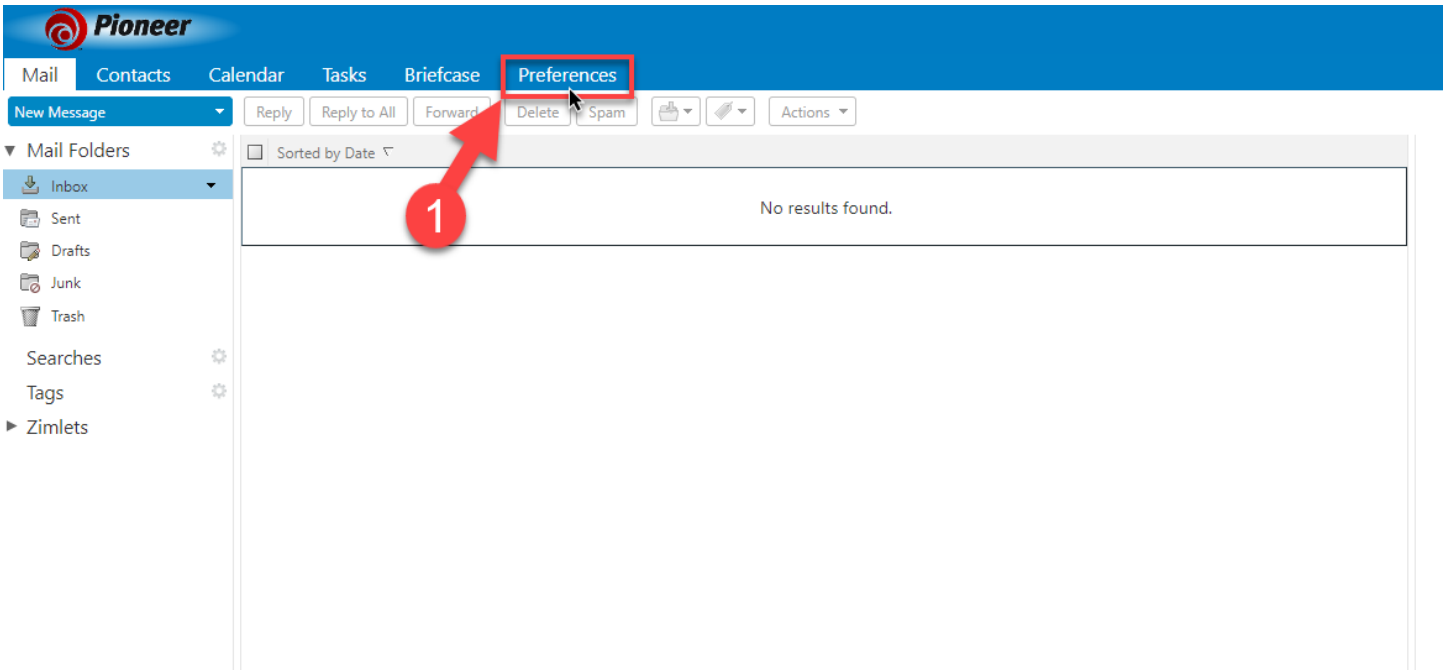
1. An unfamiliar greeting
2. Email addresses or domains that do not match
3. Misspelled words or bad grammar
4. Urgency – "*IMMEDIATE ACTION REQUIRED*…*ACT NOW* by a specific date/time…. etc."

We encourage Pioneer email customers to continue to be diligent and aware of these types of phishing email tactics. Please mark these as spam and/or delete them as necessary when you see them. If you are concerned that you may have entered any information through a phishing email that may have been obtained by a threat actor, we ask that you call Pioneer technical support immediately so we can assist you in changing your email password. We can also answer any questions you have about the legitimacy of any email you receive.

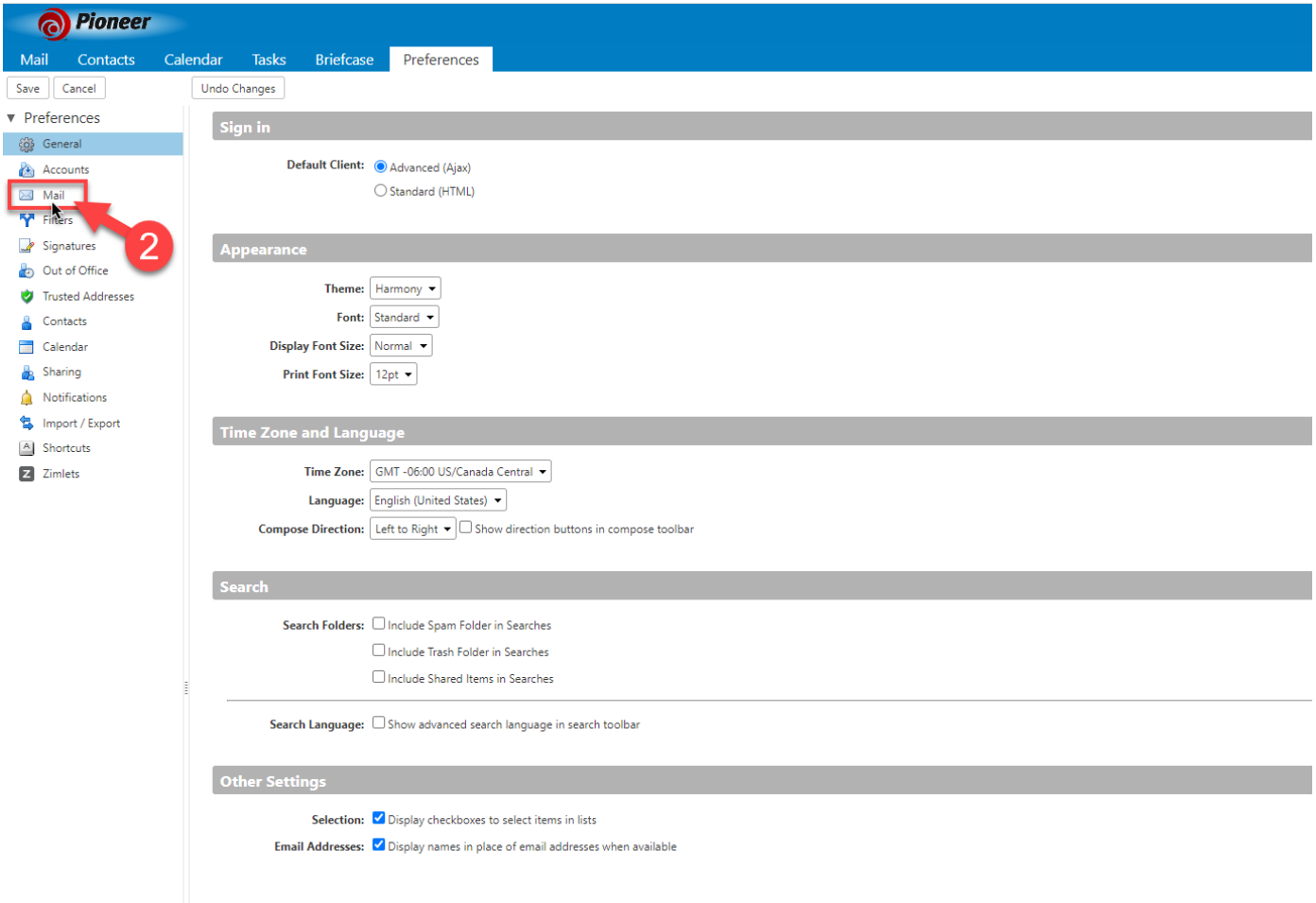
In this document example, we will be showing you exactly how these cybercriminals operate after immediately gaining access to a victim's email. This document explains their methodology of navigating to the "Preferences" of a customer's email account and manipulating and setting up "Incoming Mail Forwards" to their email account. They also create various "Mail Filters" to hide the email activity that typically follows, as they begin to infiltrate and collect data from the various services associated with your email address. When these cybercriminals do this, it means that even if you change your email password, they may still have a form of access to your incoming mail that is being forwarded/filtered from your account back to theirs.

It is highly recommended that you, the rightful email owner, not only change your email password if you suspect foul play, but also to navigate through these preferences/settings to make sure there is no suspicious activity listed and identify and remove any suspicious activity promptly. Checking these webmail preferences from time to time is highly recommended!

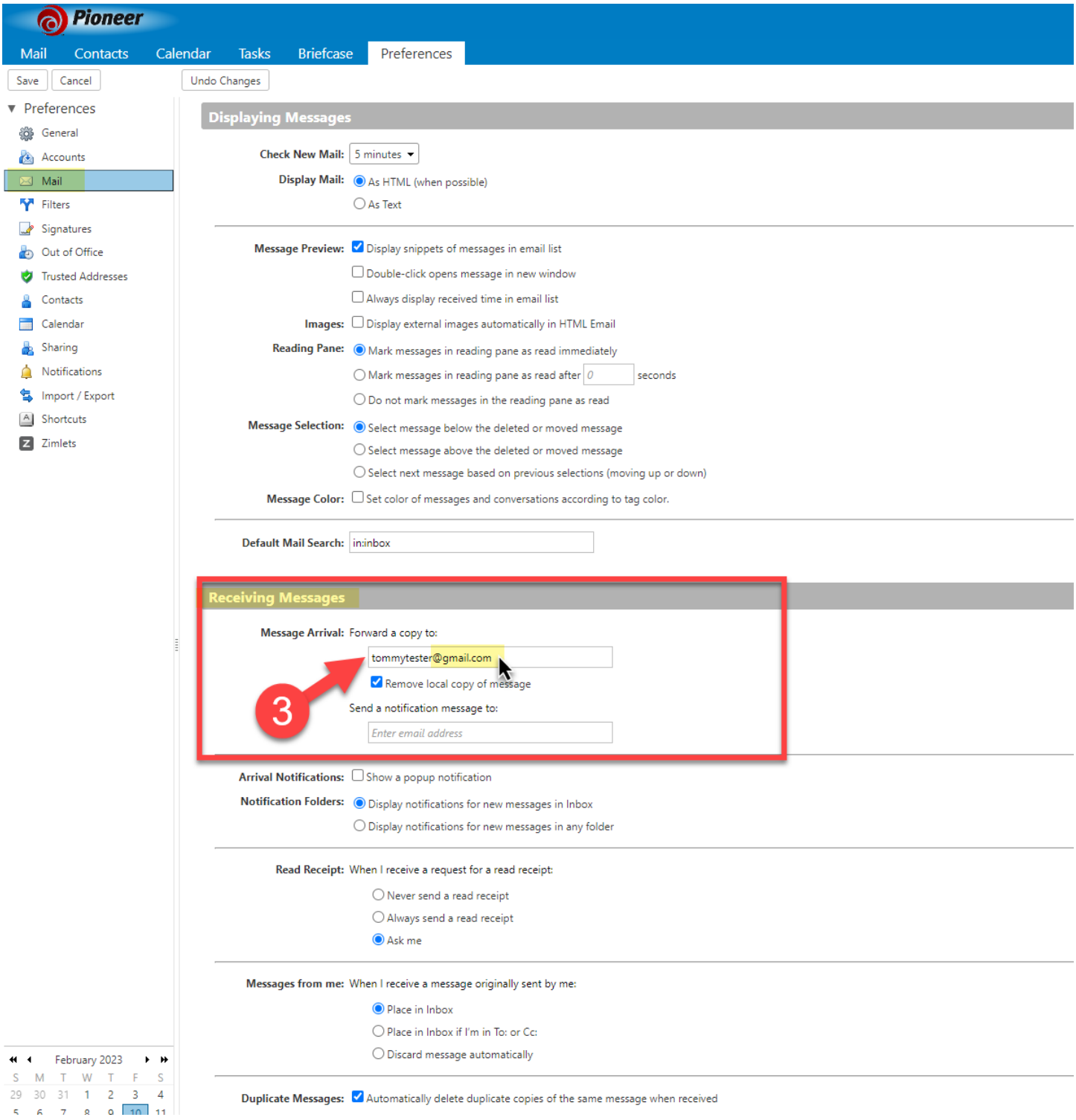
1. While in your Pioneer Webmail (https://mail.pldi.net/) , find and click on **Preferences.**



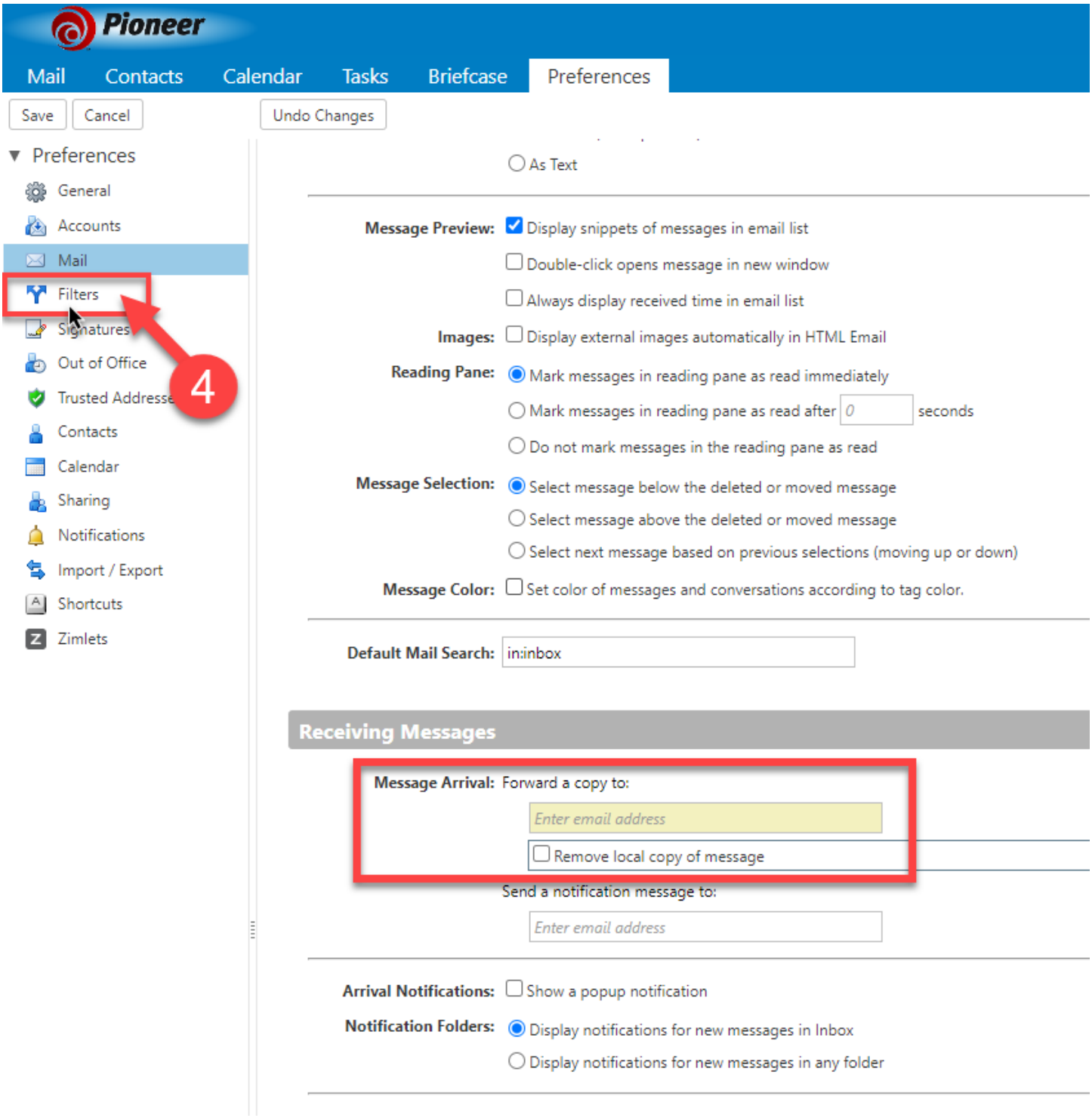
2. In preferences you will see many options. On the left-hand side click on **Mail**.



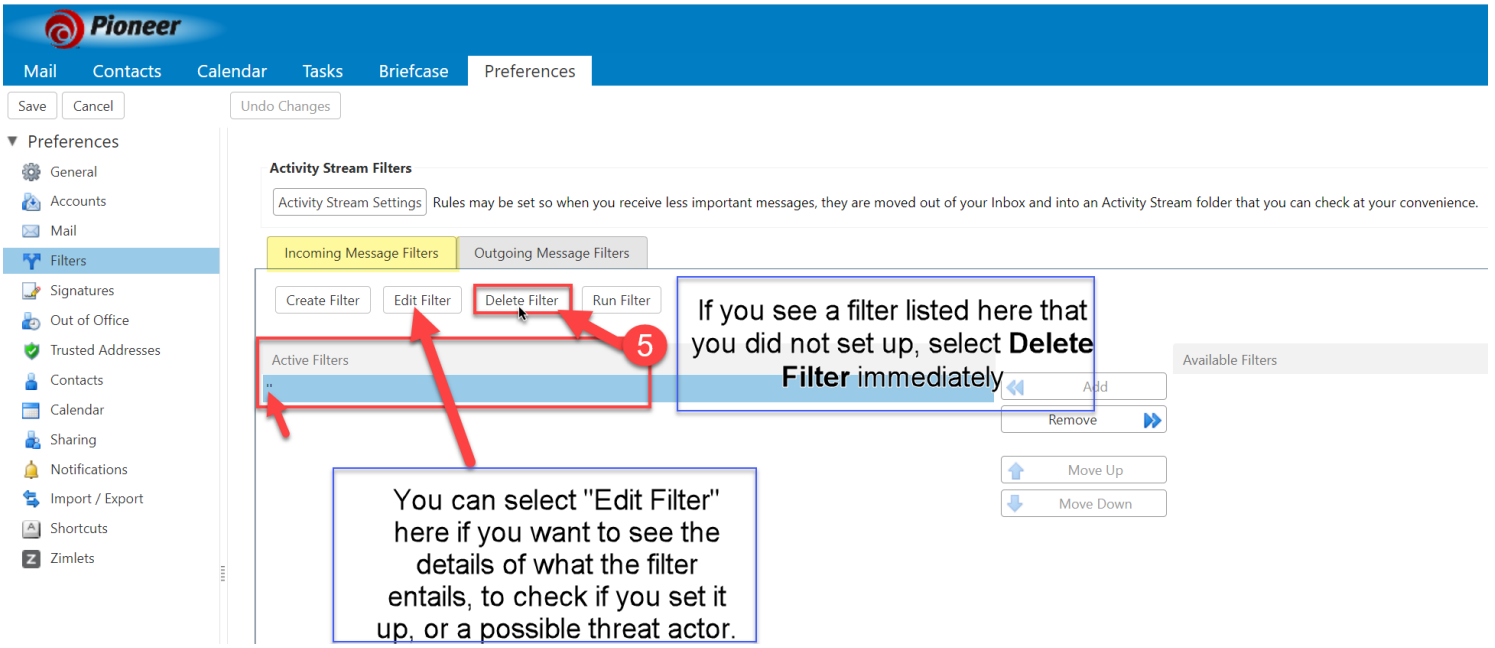
3. Under Mail, look under “Receiving Messages” and look in the field for **Message Arrival: Forward a copy to:** If you see an email here that you obviously do not recognize, remove it immediately! (*If you see nothing here continue to Step #4*)



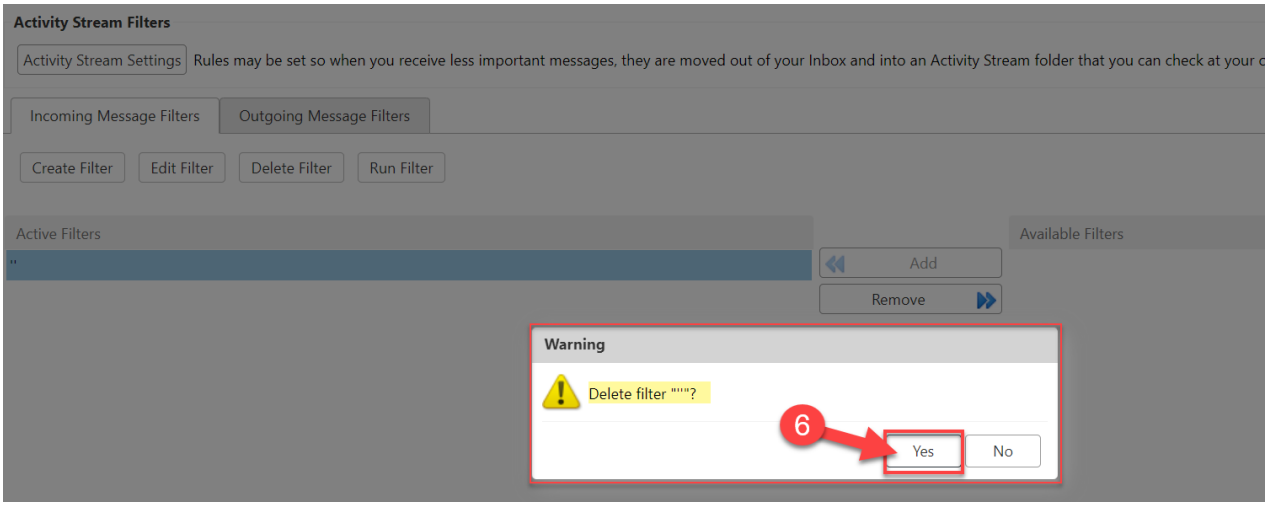
4. After you have removed the suspicious forwarded email address, navigate to the left-hand side, and select **Filters.**



5. While in Filters, please look for anything suspicious under the “Active Filters” column. The threat actor typically comes here and sets up a mail filter on your account that has keywords in it such as “Bank, banking, amazon, password…etc”, this tells the server to filter out any email that contains those words and immediately deletes it and moves it to trash, or to move it into another folder they are monitoring inside your mailbox. This happens right under the nose of the rightful email account owner. Also, most of the time, these cybercriminals will name the filter in just symbols instead of words to make it harder to notice this suspicious activity. If you notice a filter that you did not setup, select it and click **Delete Filter.**

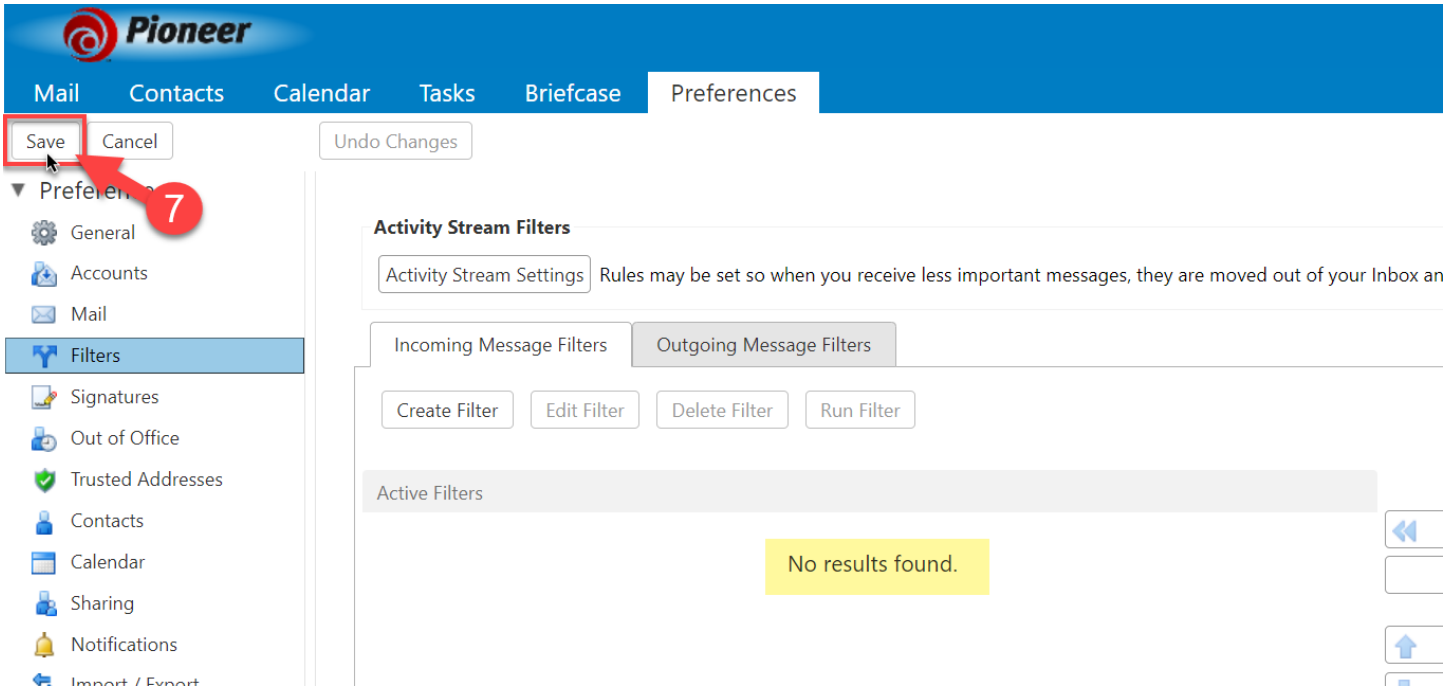


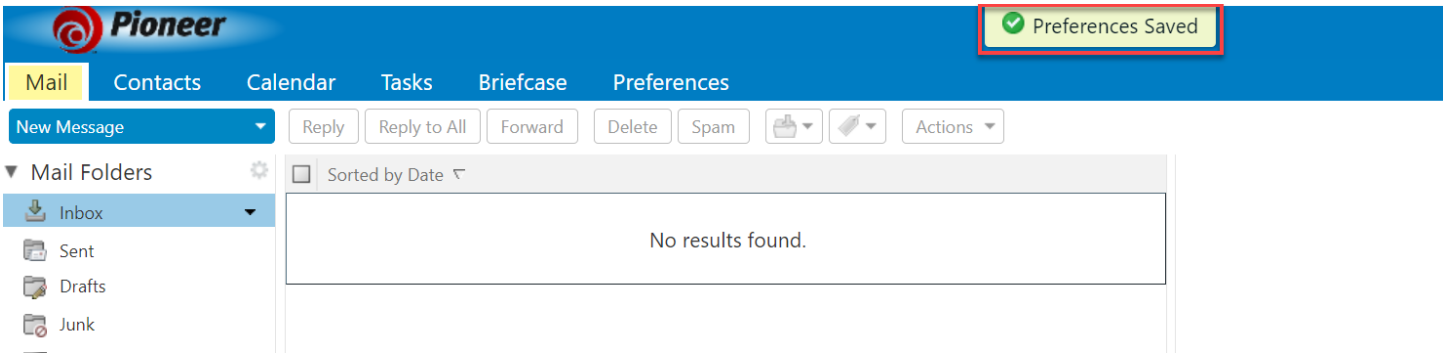
6. A confirmation box pops up with a Warning of the filter name in question. Click **Yes**.



If you did select and delete a filter, you should see a green confirmation box at the top that says **Filter Deleted**.

7. Lastly, before navigating away from Preferences always click **Save** to ensure all the changes you reviewed and made are successfully saved.





As always, if you are concerned that your email account has been compromised, feel free to reach out to our technical support team at 1-888-782-2667 or you can submit a SmartHub ticket for our support team to call you back directly. We would be happy to help you with this process or any other questions or concerns that you have. Our customers' security and well-being are very important to us!