False Positives

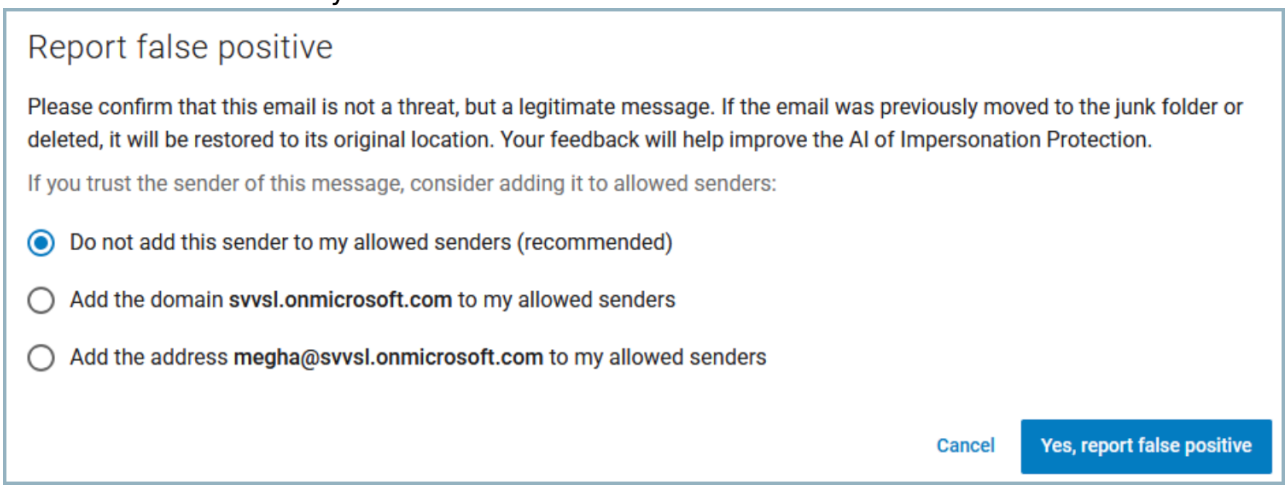
https://campus.barracuda.com/doc/13249/

If you receive an email that you believe is legitimate and not a malicious attack, you can report it as a false positive. This helps improve Barracuda AI, allowing it to better distinguish between legitimate emails and threats. When marked as a false positive, the email will be restored to its original location in the recipient's mailbox (i.e. the Inbox or a custom folder).

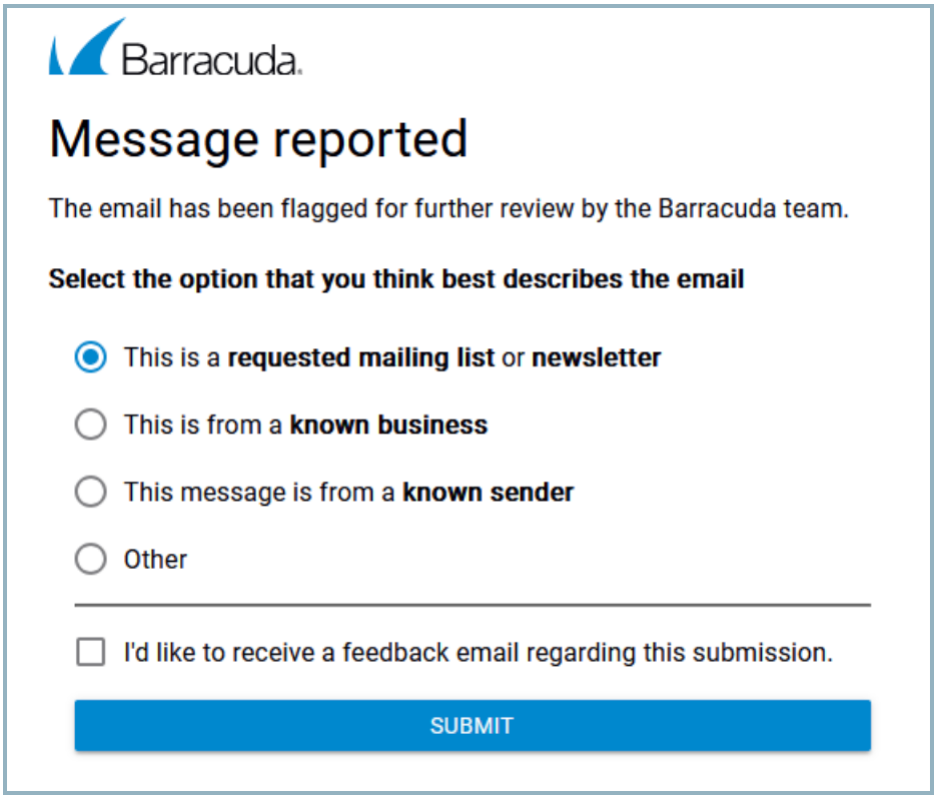
To report a false positive:

1. From the Impersonation Protection dashboard, locate the email in the **Spear Phishing Attacks** list. Click the More Details icon on the far right of the list to check the contents of the email.
2. If you think this email is not actually a threat, click the Report False Positive icon on the far right of the list.
3. Choose an action to take for this specific email. Then click **Yes, Report False Positive** to report the email.
   - **Do not add this sender to my allowed senders (recommended)** – The safest option, because future emails from this sender will still be reviewed and not allowed to bypass remediation.
   - **Add the domain to my allowed senders** – For all senders in a particular domain, not just a single sender.
   - **Add the address to my allowed senders** – For the single, individual sender who sent this email. This is the second safest option, because it only allows one individual sender to bypass remediation.

   Note that adding to your allowed senders list affects only the Barracuda allow list for Impersonation Protection and for Incident Response. It does not affect Microsoft 365 or Barracuda Email Gateway Defense.



4. To help the Barracuda team know why you think this email is a false positive, select the option that best describes this email. Select the **Other** option to enter a reason that is not already presented. Then click **Submit**.



5. The system displays a **Thank You** message, to let you know your information was received. Click **Close** to close that browser tab and continue working.

The system will learn, improving its AI, based on your input. Note that changes based on your feedback are not immediate.

You can also report false positives based on an account takeover alert. Refer to Account Takeover Alerts for more information.

Note that if you click **Delete All Attacks**, as described in Removing Attacks Found during a Barracuda Email Threat Scan, emails you reported as False Positives are not deleted.

Mistakenly Reporting a False Positive

If you mistakenly report an email as a false positive, there is no need to alert Barracuda.

You might want to take the following actions:

- **Move the email back to the Junk email folder** – If an email was previously moved to a user's Junk email folder or deleted through remediation, marking it as a false positive moves it back to the user's inbox or wherever they originally had the message. If the email is truly a threat, you will likely want to remove it from users' inboxes or custom folders. With Barracuda Networks' Incident Response, you can create an incident to remove the email from those

folders.
Barracuda Networks' Incident Response is available with all current Barracuda Email Protection plans. The legacy base level protection plan does not come with Incident Response.

- **Update the allowed senders list** – As part of the false positive report, you might have added the domain or address to the allowed senders list. If the email is truly a threat, remove the domain or address from the allowed senders list. Follow the instructions in How to Allow Senders to remove the erroneous entry.

Figures