False Positives

https://campus.barracuda.com/doc/80740499/

If you know that an incoming email is legitimate, and not actually a spear phishing attack, you can report it as a false positive. Reporting false positives helps to improve Barracuda Networks' artificial intelligence. Emails that you deem to be legitimate are also transferred from the recipient's Junk Email folder back into the recipients' inboxes, provided that the user did not delete or move those emails before you took action.

To report a false positive:

1. On the **RealTime AI** page, in the **Spear Phishing Attacks** list, locate the email you think was a false positive. 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 security evaluation.
   - **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 security evaluation.

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

Report False Positive

Confirm that this email was not a phishing attack, but rather a legitimate message. If the email was previously moved to the user's Junk folder, it will be returned to its original location. Your feedback will help improve Barracuda Sentinel's AI.

If you trust the sender of this message, consider adding it to allowed senders:

- ⦿ Do not add this sender to my allowed senders (recommended)
- ○ Add the domain **mssimply.apcprod01.prdexchangpe831.net** to my allowed senders
- ○ Add the address **ms-oxprotp@mssimply.apcprod01.prdexchangpe831.net** to my allowed senders

CANCEL   **YES, REPORT FALSE POSITIVE**

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:

- **Moving the email back to the Junk email folder** – If the email you marked as a false positive was previously moved to users' Junk email folders, as opposed to being deleted, marking it as a false positive moves it back to users' inboxes. If the email is truly a threat and you will likely want to remove it from users' inboxes. If you have Barracuda Networks' Incident Response, you can [create an incident](#) to remove the email from users' inboxes.
  Barracuda Networks' Incident Response is available with Barracuda Email Protection [Premium and Premium Plus](#) plans.
- **Updating 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.
- **Resend deleted mail with Email Gateway Defense** – If you are also using Email Gateway Defense, you can redeliver email that was deleted by Barracuda Impersonation Protection. For more information, refer to [Understanding the Message Log](#) in the Email Gateway Defense documentation.
  Note that Microsoft, by default, deduplicates emails with the same message ID. Emails you redeliver from your Email Gateway Defense Message Log can be silently dropped by Microsoft for deduplication.

Figures

1. moreDetails.png
2. falsePositiveReport.png
3. falsePositive.jpg
4. MessageReported1.png