Reporting a Missed Attack

https://campus.barracuda.com/doc/95263088/

Sometimes a suspicious message will get past Impersonation Protection. Should this happen, forward the suspicious message to the Impersonation Protection team so we can analyze it, learn from it, and improve Impersonation Protection for everyone.

Reporting a Missed Attack

Be sure to forward the email as an EML file, including any attachments, as described below. Forwarding the message inline or as a MSG file does not provide enough information to the Impersonation Protection Analysts Team.

To report a missed attack:

1. Open Outlook in a web browser. Usually, you will navigate to http://outlook.office.com/ and log in with your credentials for your organization.
2. Click **New Message**.
3. Locate the suspicious email in the Inbox.
4. Click the suspicious email and drag it into the new, blank message. It appears as an attachment.
5. Add the following information:
    - **To:** SentinelAnalysts_Team@barracuda.com
    - **Subject:** *Report Missed Attack*, or something similar
    - **Body:** Optionally, add a note to the Impersonation Protection Analysts Team to provide additional information or context.
6. Click **Send**.

The Impersonation Protection team will send you an email, confirming receipt of your submission. At this time, we are unable to follow up on individual submissions.

Why an Attack Might Be Missed

On somewhat rare occasions, an attack might pass by Impersonation Protection. Some of the reasons this might happen include:

- The attack might have come through on a mailbox that is not using Microsoft 365. For information on what is protected, see Getting Started.

- You recently purchased Impersonation Protection and it is still learning about your environment.
- Each user is treated as an individual, based on their individual attributes. The same email might have been considered an attack and blocked for one user, and allowed through for another user.
- The email might have been opened automatically in a mobile app before Impersonation Protection can get it from the main environment.
- Gateway policies or DMARC might not be configured properly. For more information, refer to the Domain Fraud Protection Background section of this document.
- Your Email Gateway Defense might have permissive inbound policies that allowed the email through. For information on updating your policies, refer to Inbound Filtering Policy in the Barracuda Email Gateway Defense documentation.