Email Warning Banner Messages

https://campus.barracuda.com/doc/25225/

This article refers to capabilities currently available as a beta release and will be gradually rolled out to customers.

Phishing scams are typically fraudulent email messages appearing to come from legitimate senders (for example, a university, an Internet service provider, a financial institution). These messages usually direct you to a spoofed website or otherwise get you to reveal private information such as logins, passwords, or other sensitive data. This information is then used to commit identity and/or monetary theft.

The **Inbound Settings > Anti-Phishing > Email warning banners** setting alerts users about the types of potential threats that may exist within a given email. Notification banners will display if there are any potential threats identified in the email.

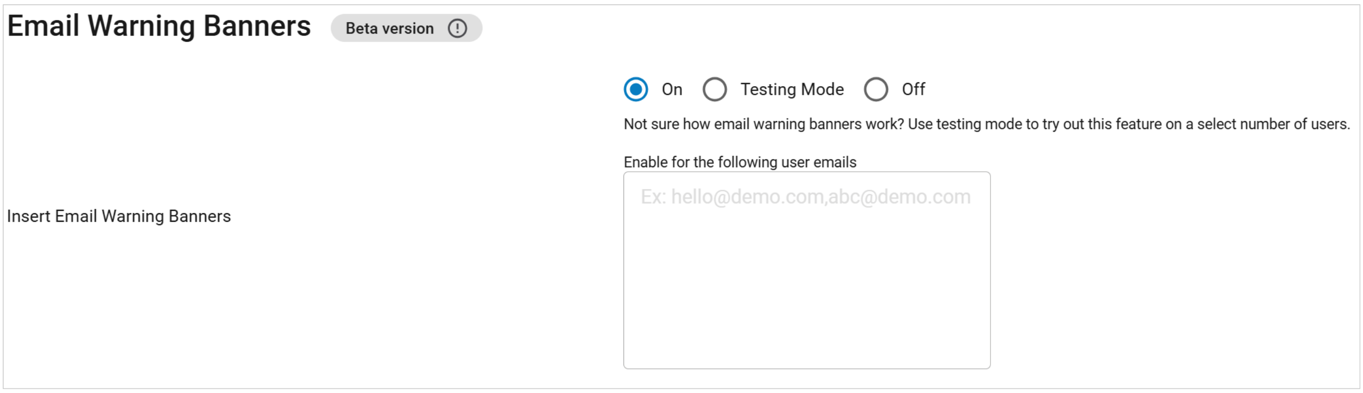
Note that these settings apply to all domains you have verified in Email Gateway Defense for processing mail. You are unable to change these settings for a specific domain.

Choose from the following options to set the notification banners:

- **On** – Notification banners are turned on for all inbound email traffic.
- **Testing Mode** – Notification banners are turned on only for a select set of users. Banners are applied to emails that contain the trial user email addresses in the To, Cc, or Bcc fields. Email addresses must be valid email users in the Email Gateway Defense user list. Enter the desired user email addresses separated by commas.

Note that users other than those in the trial user group may also see a notifications banner in the email. For example, a user `jsmith@contoso.com` is added as a trial user for email warning banners. `jsmith` is bcc'd on an external email to `jdoe@contoso.com`. The recipient of that email `jdoe` will also see the external sender warning banner, even though they are not part of the trial user group.

- **Off** – Notification banners are turned off for all inbound email traffic.



Email Warning Banners Beta version

Insert Email Warning Banners

● On ○ Testing Mode ○ Off

Not sure how email warning banners work? Use testing mode to try out this feature on a select number of users.

Enable for the following user emails

Ex: hello@demo.com,abc@demo.com

Note: Email warning banners are not applied to any emails from the Message Log with the Delivery Status of **UI Delivered**. This can include messages that were previously blocked/quarantined or system generated emails such as user quarantine digests.

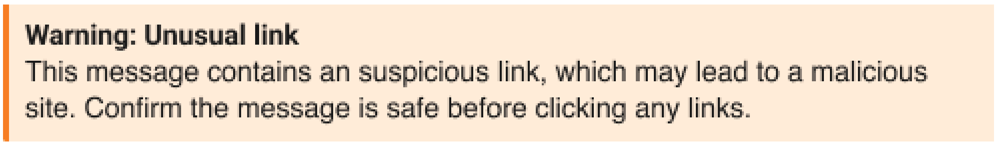
Types of Notification Banners

The following are the types of email warning banners used in Email Gateway Defense.

Unusual link

This email contains an external link to a domain you have not seen previously in communication from this sender. Confirm the message is safe before clicking on any links.

After you have interacted with a sender a few times, Email Gateway Defense will recognize the sender as a legitimate contact and will no longer display the warning banner because you have now established a history of communication and trust with the sender.

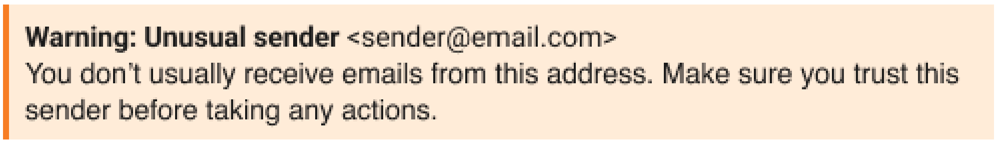


Warning: Unusual link
This message contains an suspicious link, which may lead to a malicious site. Confirm the message is safe before clicking any links.

Unusual sender

This email was sent by a sender that has never sent an email to this recipient before. Confirm you trust this sender before taking any actions.

After you have interacted with a sender a few times, Email Gateway Defense will recognize the sender as a legitimate contact and will no longer display the warning banner because you have now established a history of communication and trust with the sender.

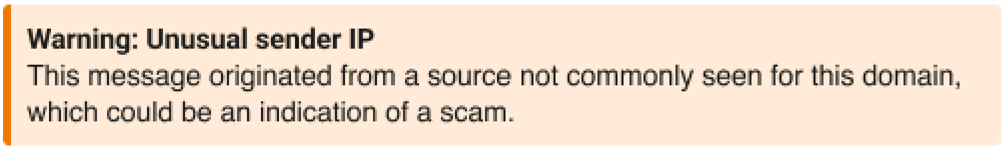


Warning: Unusual sender <sender@email.com>
You don't usually receive emails from this address. Make sure you trust this sender before taking any actions.

Unusual sender IP

This email sent from a sender IP that has never sent an email to this recipient before.

After you have interacted with a sender a few times, Email Gateway Defense will recognize the sender as a legitimate contact and will no longer display the warning banner because you have now established a history of communication and trust with the sender.

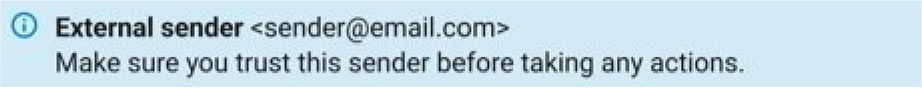


Warning: Unusual sender IP
This message originated from a source not commonly seen for this domain, which could be an indication of a scam.

External sender

This email was sent by an external sender. The banner includes the Header From address. Confirm you trust this sender before taking any actions.

Note: The external warning is added to inbound email.



External sender <sender@email.com>
Make sure you trust this sender before taking any actions.

Notification Banners Determination

The data used to evaluate suspect emails is based on a rolling 30 day window of email data seen by Email Gateway Defense. Thus, banner insertion behavior can be summarized as follows.

For a new sender:

- Day 1 – Notification banner
- Day 2 – No emails from this sender
- Day 3 – Notification banner
- Day 4 – No notification banner because Email Gateway Defense has seen that sender within 30

days
- Day 29 – No notification banner

Because Email Gateway Defense has seen the sender within the rolling 30 day window, the recipient will not see any new notification banners for that sender.

The same logic will apply to URLs and IP addresses.

Notification Banners Exemptions

Notification banners are exempt under the following conditions:

- SPF has passed (Unusual IP exemption).
- IP is listed in the SPF Exemptions by IP Address or IP Exemption policies (exempt from Unusual IP).
- Sender is in the Sender Policies Exemption list (exempt from Unusual Sender).
- URL is in the Intent Domain Policies Exemption list (exempt from Unusual URL).

Note that there can be conditions where one notification banner type is exempt, but another applies.

For example, if the email passes SPF check but the sender is new to the recipient, the notification banner will be applied for Unusual Sender. After you have interacted with a sender a few times, Email Gateway Defense will recognize the sender as a legitimate contact and will no longer display the Unusual Sender notification banner because you have now established a history of communication and trust with the sender.

Figures