Advanced Email Security powered by INKY Help Guide

Advanced Email Security powered by INKY is a legacy product and is no longer sold. This guide contains archived Help content for Advanced Email Security powered by INKY to help answer questions. However, it's no longer being updated as of December 2023.

To find answers in this guide:

- Select any title in the Contents to go directly to a specific Help article.
- Use the **Find** function (**Ctrl + F** for Windows OR **Command + F** for Mac) in your browser to search the PDF for specific keywords.

Contents

What is Advanced Email Security?

Email is essential for any business. It allows you to communicate with employees and vendors and keeps your team connected on important projects. However, sometimes attackers take advantage of your reliance on email by impersonating others to steal your information or for other malicious reasons.

That's where Advanced Email Security comes in. Advanced Email Security protects against cybersecurity threats, including spam, malware, and phishing attacks. It's cloud-based email security that works on any email client, on any device, and displays warning banners directly in messages so you're always one step ahead of attackers.

Who needs Advanced Email Security?

Advanced Email Security is useful for anyone who uses email, especially businesses that want to protect their day-to-day operations from disruptions or threats. Email attacks are becoming increasingly sophisticated, which makes them harder to detect. Advanced Email Security identifies potentially harmful email so you can best protect yourself and your business.

It also includes encryption, which is a critical requirement for businesses in regulated industries, like financial services, insurance, and real estate. For example, if an attorney sends a contract to their client, and the message is sent unencrypted (in plain text), it could be at risk of being intercepted or misdirected. Advanced Email Security protects email communication and helps businesses avoid a potentially serious data breach.

How does Advanced Email Security work?

Advanced Email Security uses computer vision, artificial intelligence and machine learning to detect and protect against malicious email. Advanced Email Security is constantly learning to improve its threat recognition and identify suspicious emails.

Some of Advanced Email Security's protection technology includes:

- Text analysis models to identify if the sender is legitimate and prevent scams. This includes checking the company logo to determine if it's a forgery or uses brand-impersonation techniques.
- Social graphing to alert you of text-based phishing emails. It determines if a sender is legitimate to stop impersonation attempts.

- Color-coded warning banners on incoming emails that include guidance on how to safely treat the email.
- A dashboard where admins can control Advanced Email Security and manage their warning banners.
- Reporting and visualization tools so you have a complete understanding of all email activity.

Advanced Email Security integrates with Microsoft 365, so you have organization-wide security that doesn't slow down mail delivery. All incoming email is automatically checked by Advanced Email Security, and you can track all blocked threats.

What are Advanced Email Security's limitations?

Advanced Email Security works on any email client and any device, including mobile, but there are some limitations to keep in mind:

- Encrypted outbound messages must be less than 75 MB, including attachments.
- Replies in the encryption portal must be less than 75 MB, including attachments.
- Encrypted messages will be retained for 30 days.
- Emails and domains added to Allow or Block lists can't be deleted but can be disabled.

Advanced Email Security has no send rate limits and no recipient limitations. Microsoft 365 limitations still apply.

Sign in to Advanced Email Security

The Advanced Email Security add-on protects against cybersecurity threats, including spam, malware, and phishing attacks. Admins can either sign in directly to Advanced Email Security or through the Email & Dashboard, but users can only sign in directly. (In your Email & Office Dashboard, on the Advanced Email Security page, admins are listed under **Admin accounts with advanced email security login access**).

Sign in directly to Advanced Email Security

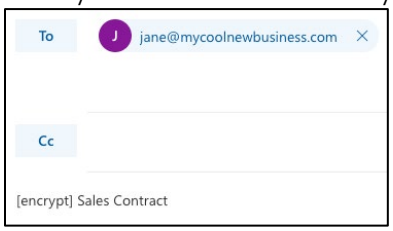
1. Go to Advanced Email Security. Select **Sign in using Microsoft account**.
2. Use your Microsoft 365 email address and password. You'll be taken to your dashboard.

Sign in through the Email & Office Dashboard

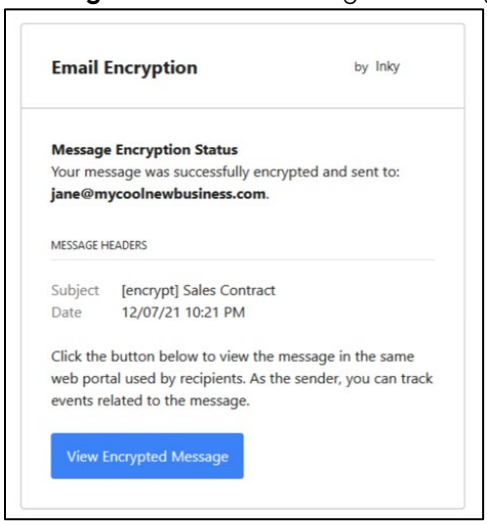
1. Sign in to your Email & Office Dashboard.
2. Select **Add-Ons**.
3. Under **Advanced Email Security**, select **Manage**. You'll be taken directly to your dashboard and won't need to enter your credentials.

Send an encrypted message

To encrypt an email, add **[encrypt]** or **(encrypt)** at the beginning of the subject line. This works on any email client and on any device.



After sending the message, you'll receive an email confirmation. Select **View Encrypted Message** to see the message. You might need to sign into the encryption portal.



The email expires after 15 days, and the recipient cannot forward or save it (but they can download attachments from the email).

Note: If you get a response to your encrypted message, it'll be delivered to your inbox, even if it's from a user outside of Microsoft 365. If the message size is greater than 20 MB, you'll receive an email notification to sign in to INKY and view the response in your message list.

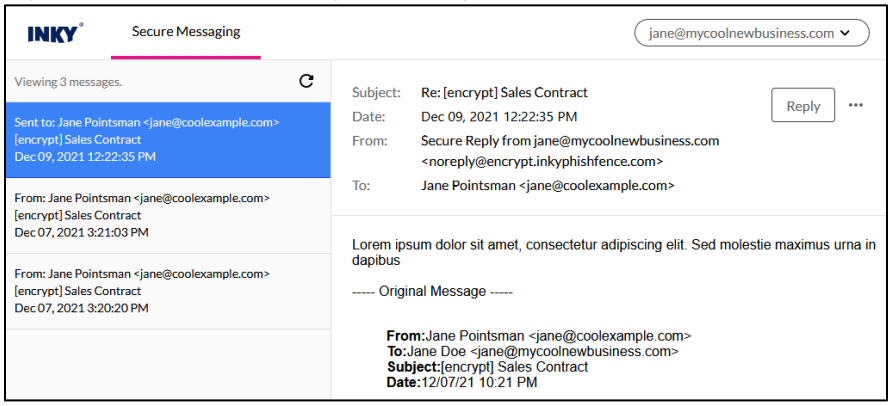
View an encrypted message that was sent to you

When you're the recipient of an encrypted message, you'll receive an email notification addressed from Proofpoint Essentials on behalf of the sender. To access the message, select **View Encrypted Message**. You'll need to sign into the encryption portal.

To sign in with an existing email account, select **Sign in with Microsoft** or **Sign in with Google**. Or you can select **Sign in with email** to receive a link in your email. This option allows you to sign in without using a password.

Note: If you receive an error after you select **Sign in with Microsoft** or **Sign in with Google**, you might be signed into an email address that isn't the intended recipient.

You'll see a list of sent and received messages, sorted by date, on the leftmost side when you're signed in. Select a message to decrypt it and view it. To send a response, select **Reply**.



Limitations for encrypted messages

Keep the following limitations in mind when sending and receiving encrypted messages with Advanced Email Security powered by INKY:

- Encrypted outbound messages must be less than 75 MB, including attachments.
- Replies in the encryption portal must be less than 75 MB, including attachments.
- By default, Advanced Email Security keeps encrypted messages for 30 days.

Microsoft 365 limitations also still apply.

What are quarantined emails in Advanced Email Security?

Advanced Email Security scans your incoming messages for malware and phishing. Suspected messages are stored outside of your mailboxes, or quarantined, so they can be evaluated without putting your users at risk of malware or phishing. When a message is quarantined, it isn't delivered to your Inbox or Junk folders.

How does Advanced Email Security decide to quarantine a message?

There are multiple levels of malware and phishing. When Advanced Email Security is confident that a message contains malware or phishing (like in the form of a link or attachment), the message is quarantined. Messages with other types of malware or phishing get routed to your Junk folder.

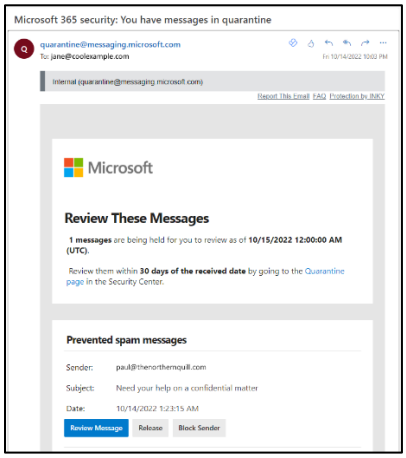
Where do messages get quarantined?

Advanced Email Security puts messages in the Microsoft 365 quarantine. From there, you can decide if the message should be released and delivered to the mailbox or deleted. By default, quarantined messages are only viewable by admins.

How do I know a message was quarantined?

With Advanced Email Security, users and admins will receive an email every 3 days notifying you of newly quarantined messages. Users can't take any action on quarantined messages, but admins can review, release, and block the sender of them directly in the email.

Note: If you're expecting a message and it doesn't show up in your mailbox or a quarantine notification, then an admin can verify if it was quarantined by running a message trace (the status will show as **Quarantined**).



How long does a message stay quarantined?

Messages are quarantined for 15 days, and then the message expires. After a message expires in quarantine, it can't be delivered to a mailbox.

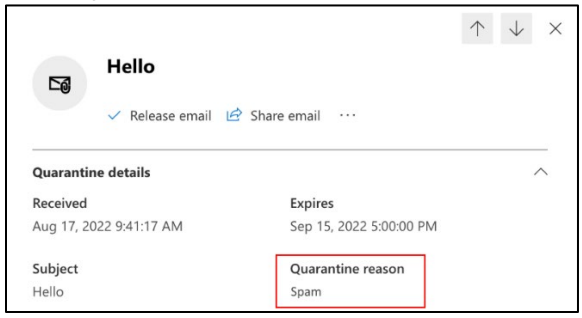
Release or delete a quarantined message

Messages are quarantined when they're suspected of containing malware or phishing. After a message is moved into Microsoft 365's quarantine, you can review it and then decide what do to with it, like release or delete it.

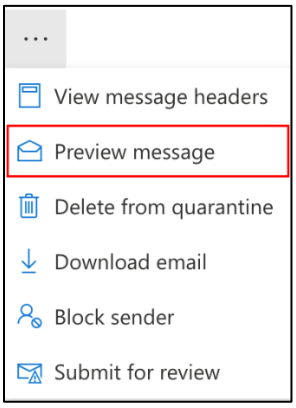
1. Sign in to the Microsoft 365 Defender Portal. Use your Microsoft 365 email address and password.
2. After the **Quarantine** page loads, verify that the **Email tab** is selected. You'll see a list of messages that are quarantined.

   Note: Only admins can preview, release, and view *all* types of quarantined messages. If you do not see the message you're looking for in your list, you may need to ask an admin to manage it for you.

3. From the list, review the details of a specific message:
   - **Find out why the message was quarantined**: Select a message to open the message details. You'll see a **Quarantine reason** listed.



- **Preview the message**: After viewing the message details, select the **More** menu, and then select **Preview message** to see the actual message that was sent.

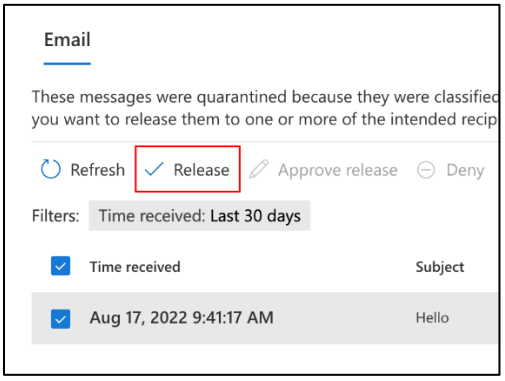


After you've previewed a message, you can release it or delete it from quarantine.

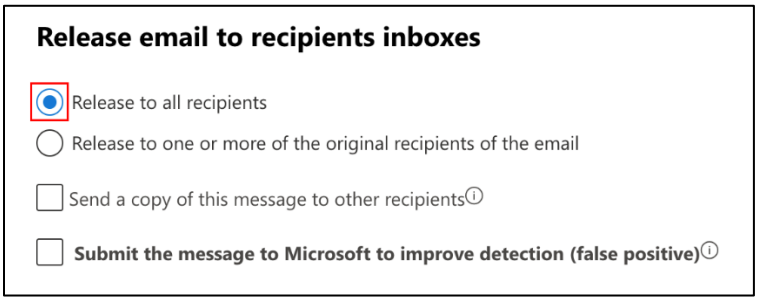
Release a message from quarantine

Customize how a message is released to its intended recipients.

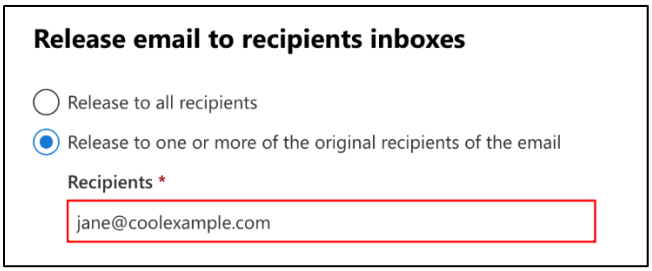
1. To release a message from quarantine, select the message, and then select **Release**.



2. Choose whether to **Release to all recipients** or **Release to one or more of the original recipients of the email**.

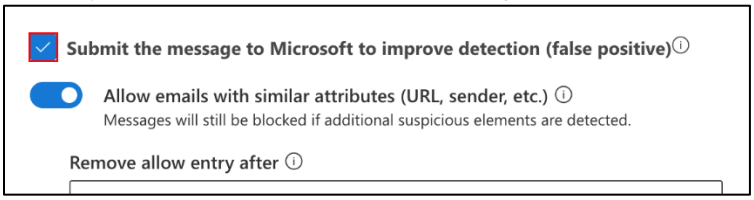


- If you choose **Release email to one or more of the original recipients of the email**, enter the email address for each recipient.

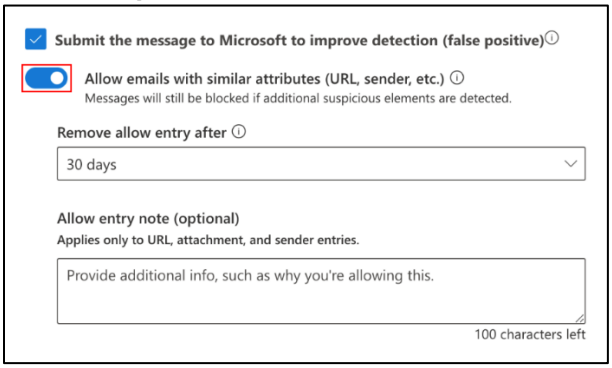


3. (Optional) To send the message to another recipient, select **Send a copy of this message to other recipients**, and then enter the email address for each recipient.

4. (Optional) If the message was incorrectly sent to quarantine, select the checkbox next to **Submit the message to Microsoft to improve detection (false positive)**. Or, if the message was incorrectly sent to quarantine by *Advanced Email Security*, report the message as **Safe** after it's delivered to your mailbox.



   - If you choose to submit the message to Microsoft, turn on the **Allow messages with similar attributes (URL, sender, etc.)** toggle to temporarily prevent similar messages from being quarantined. The following options will be available:
     - **Remove allow entry after**: Select how long you want to allow messages like this. Select **1 day** to **30 days**. By default, 30 days is selected.
     - **Allow entry note (optional)**: Enter a description for the allow.

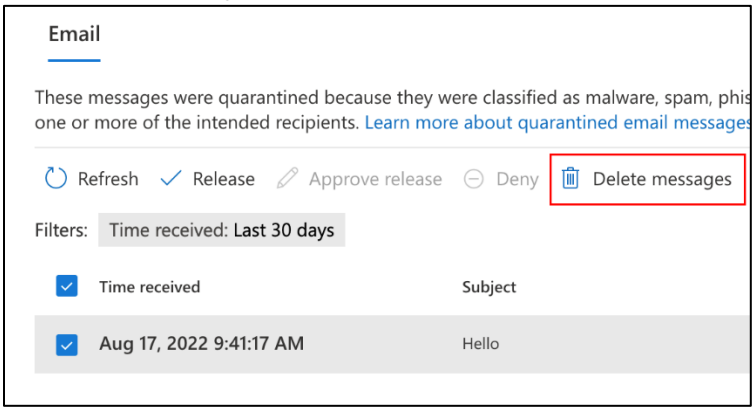


5. When you're finished, select **Release message**.

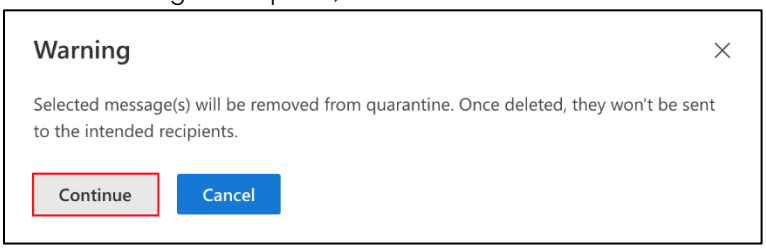
Delete a message from quarantine

Remove a quarantined message with no further action.

1. Select the message from the list, and then select **Delete messages**.



2. In the warning that opens, select **Continue**.



The message is immediately deleted without being sent to the original recipients.

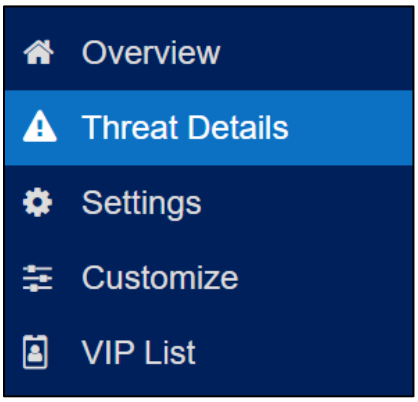
In the ... **More** menu, you can take other actions, like sharing or downloading the quarantined message or blocking the sender.

Allow list or block list

With Advanced Email Security, all incoming email is flagged with a banner informing the recipient of its threat level. You can view all received emails on your **Threat Details** page, where you can filter out dangerous emails or disable warnings for trusted senders. If you trust the message, add it to your Allow List to prevent similar messages from being flagged. Otherwise, add it to your Block List so similar messages always get a warning.

Note: We recommend adding the email to your allowed list instead of the domain unless you're certain the domain can be trusted. Once the domain is added, Advanced Email Security won't know if the domain was spoofed and can't warn you about compromised email.

1. Sign in to Advanced Email Security. Select **Sign in using Microsoft account** and use your Microsoft 365 email address and password.
2. Select **Threat Details**.



3. Use the menus to sort your results using some or all the following categories:
    - **Minimum Threat Level**: Filters messages with Neutral, Caution, or Danger banners.
    - **Reason**: Filters by a specific type of warning, such as a misleading link or suspicious URL.
    - **Reported Messages**: Filters by messages included or not included in user reports. Not selecting this filter displays all messages.
    - **Message-ID**: Filters to a specific message by its unique ID (located in the email header).
    - **Recipient Email Address**: Filters messages to those received by a specific email address.
    - **Filter by Selected Date Range**: Confirm the box is checked to filter messages received within a specific time period. In the bottom left corner, select the start and end dates to choose your date range. Uncheck the box to remove this search criteria.

Note: Try setting the threat level to Danger and reported messages to those included with user reports. This will show you the emails that need the most amount of tuning. You can then filter to the lower threat levels as needed.

4. Select **Refresh List**.
5. You'll see a list of all messages that meet your filter criteria. Select a message, then select **Allow List Actions** or **Block List Actions** located below its banner. Emails and domains added to Allow or Block lists can't be deleted but can be disabled.

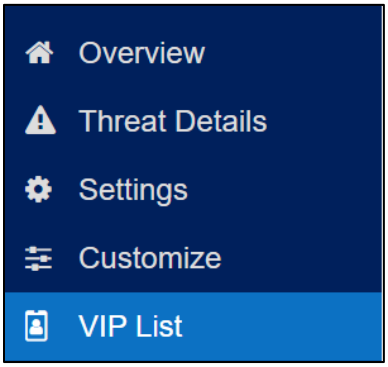
Note: Your available actions are based on the type of threat and might differ depending on the messages.

6. Under **Remediation**, delete a message from the mailbox if it shouldn't be accessed by a user.
7. Under **User Reports**, provide feedback on misclassified messages to INKY. Select ✔ green check, to confirm the user report is correct, or select ✖ red X, to reject it.
8. If the email was miscategorized, under **Report Feedback**, select **Report This Email** to make a policy change, like adding the sender address as a trusted sender.

VIP spoofing protection

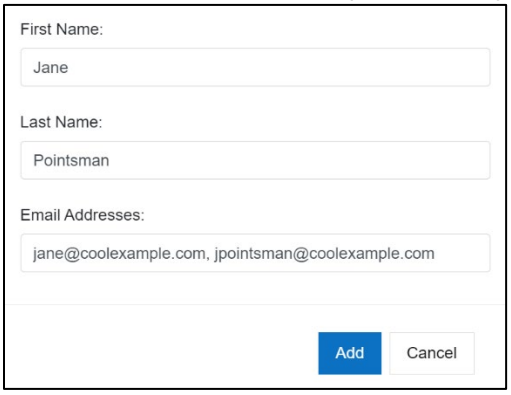
Add names and email addresses of executives, commonly spoofed employees, or important external contacts to your **VIP List**. If an incoming email appears to come from one of these people but is from an impersonator, Advanced Email Security will alert you that it's a spoofed VIP.

1. Sign in to Advanced Email Security. Select **Sign in using Microsoft account** and use your Microsoft 365 email address and password.
2. Select **VIP List**.



3. In the upper-right corner, select the checkbox to **Enable VIP spoofing checks**.

4. To add a VIP, select **Add Person**, enter the contact details, and select **Add**. You can add multiple email addresses by separating them with commas.



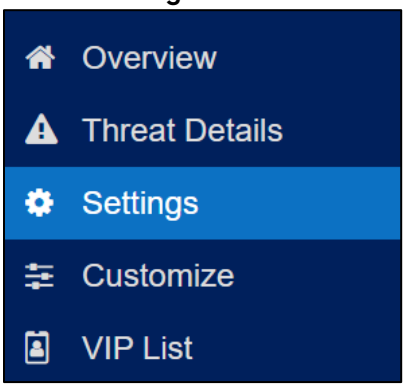
Note: It's good practice to add all the VIP's personal and business email addresses. That way, if they send an email from any of their personal emails, it won't be flagged as spoofing.

5. (Optional) Add multiple VIP contacts with a CSV file. Select **Import CSV**, then **Continue**. Then choose and open your CSV file.

Link rewriting

When you select a link you've received in an email, Advanced Email Security checks the URL in real-time to help ensure it's safe. By default, link rewriting is enabled for your organization when you add Advanced Email Security (and we recommend leaving it enabled), but you can customize your options if needed.

1. Sign in to Advanced Email Security. Select **Sign in using Microsoft account** and use your Microsoft 365 email address and password.
2. Select **Settings**.



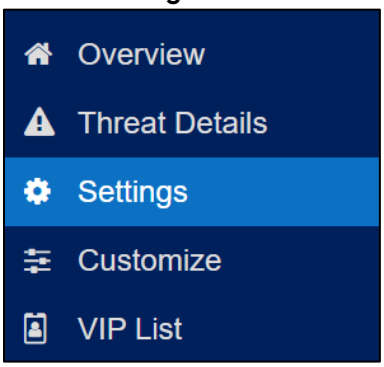
3. Go to the Link Rewriting section.

4. (Optional) By default, INKY rewrites all links. To disable link rewriting for your organization, clear the checkbox.
    - To exclude URLs from specific senders, select **0 exceptions**, enter the sender's details, and then select **Save**.
5. (Optional) By default, INKY won't allow users to proceed to a site it classifies as dangerous. To allow users to proceed, clear the checkbox.
6. (Optional) By default, INKY requires users' confirmation before continuing if a URL or message is classified as harmful or dangerous. To change when confirmation is required, select your desired option:
    - Next to **Trusted 3rd Party / Internal mail**, select when to require confirmation for links from trusted senders and other users in your organization.
    - Next to **External mail**, select when to require confirmation for links and messages sent from addresses outside of your organization.
7. At the bottom of the page, select **Save Changes**. Changes can take up to an hour to take effect.

Trusted third-party senders

If you use a third-party to send messages on behalf of your users, such as an email marketing product, Advanced Email Security might flag these messages as internal-sender spoofing. To prevent these warnings, add any third-party senders to your Trusted Third-Party Senders list.

1. Sign in to Advanced Email Security. Select **Sign in using Microsoft account** and use your Microsoft 365 email address and password.
2. Select **Settings**.



3. Next to **Domain mapping**, enter the sender's domain name (use a comma to separate multiple domain names).

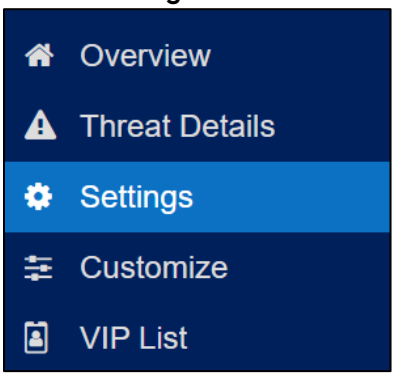
4. Select the checkbox to **Treat messages sent by these third parties as internal mail**.

5. At the bottom of the page, select **Save Changes**. Changes can take up to an hour to take effect.

Spear phishing protection

Advanced Email Security continuously learns and makes predictions to prevent spear phishing, targeted attacks impersonating an individual or business you trust. After you've had Advanced Email Security for a week or two, the technology will have established patterns to prevent spear phishing. At that time, enable spear phishing warnings so you know if an email is trying to trick you into doing something harmful.

1. Sign in to Advanced Email Security. Select **Sign in using Microsoft account** and use your Microsoft 365 email address and password.
2. Select **Settings**.

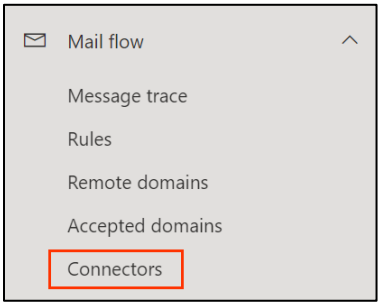


3. Select the checkbox under **Spear Phishing Protection**.
4. At the bottom of the page, select **Save Changes**. Changes can take up to an hour before they take effect.

Check connectors in Microsoft 365

If your email account was compromised, you'll need to check for malicious connectors that can affect your ability to send and receive messages. You need admin permissions to check connectors. For more info, see admin roles from Microsoft.

1. Sign in to the Exchange admin center. Use your Microsoft 365 email address and password.
2. Select **Mail flow**, and then select **Connectors**.



3. If you don't recognize any connectors listed, select a connector, and then select **Delete**.

> **Note:** There will be multiple encryption connectors, like IPW and OBC-VPC-O365-RETURN for your Advanced Email Security powered by INKY.

4. To delete the connector, select **Confirm**.

What do the banners from Advanced Email Security mean?

With Advanced Email Security, all incoming email is flagged with a banner or tag informing you of its threat level. This strengthens your security by making it easier to identify and report potentially malicious content. There are different types of banners or tags that warn you of possible email threats.

Neutral (gray), caution (yellow), and danger (red) are all possible threat categories.

A neutral (**External**) banner means that the message came from an external sender but does not appear to be a threat.

A **Caution** banner means that Advanced Email Security found something unusual in the email. It might not be considered dangerous, like when you receive email from a first-time sender, but the message should be treated with caution.

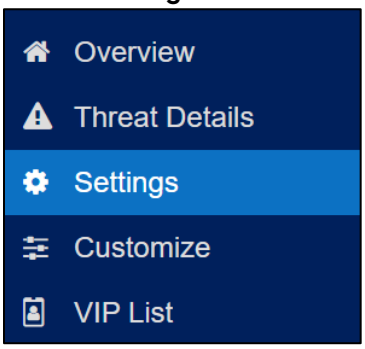
A **Danger** banner means that Advanced Email Security believes the message is suspicious and could be a phishing attempt. Possible reasons for this banner include brand impersonations, blacklisted phishing URLs, or attempts to spoof mail so it looks like it came from an internal company account. Your security team or email administrator can configure your server to automatically quarantine these dangerous emails.

If the email includes a suspicious link that you or another user opened, Advanced Email Security will stop you from continuing to the malicious site.

Customize my banners in Advanced Email Security

You can change how much detail is shown, and even suppress certain banner types on messages.

1. Sign in to Advanced Email Security. Select **Sign in using Microsoft account** and use your Microsoft 365 email address and password.
2. Select **Settings**.

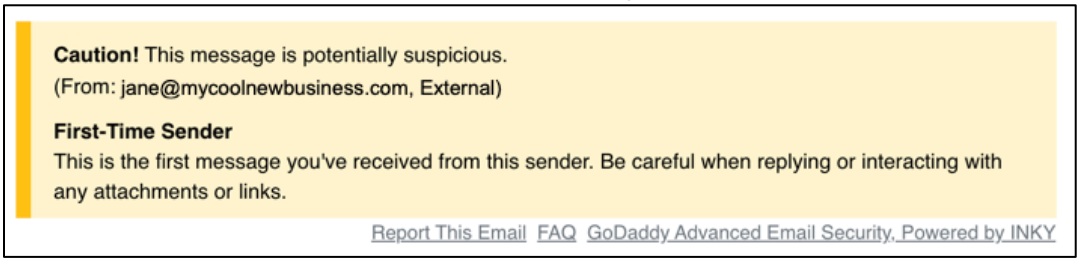


3. Under **Banner Format**, choose your preferred format:

- **Minimal**: Lists the threat type found in the message and a **Details** link for more information. This format is selected by default.

- **Minimal (all links inside color banner):** Like Minimal but includes the footer links inside the banner

- **Verbose:** Includes the details within each message



- **Micro**: Doesn't show any threat information. The user will need to use the Details link in the footer for specific threat information.

4. Under **Customize Which Banners To Include**, manage the settings for your banners, including when to display them on messages:
    - **Trusted 3rd Party / Internal Mail:** Choose which banners appear on email received from addresses within your organization or on your trusted third-party senders list.
    - **External Mail:** Choose which banners appear on email received from addresses outside of your organization.
5. If you suppressed any banners in the previous step, confirm the checkbox next to **Always include the "Report This Email" link** is selected, even if no banner is included. This allows users to report messages even when there isn't a banner.
6. At the bottom of the page, select **Save Changes**. Your banner changes will be saved. They can take up to an hour to take effect.