Retruster  
Email To Send To New Users

short line

*Subject*: Announcing Retruster for Outlook

The add-in “Retruster” has just been deployed to all users’ Outlook. No action is required of you.

Retruster helps you identify suspicious or fraudulent emails.

**This has been deployed in our organisation because:**

* Email fraud and particularly phishing (the attempt to obtain sensitive information by disguising a fraudulent email to look like a trustworthy one) is on the rise
* Retruster helps keep you protected against email fraud
* While trying as much as possible not to interrupt your workflow

**How Retruster works:**

* If an email shows signs of suspicion, a tag is added to the email
* This is similar to a Microsoft Outlook “category”, yet does not interfere with existing categories
* Users can click the Retruster button in the Outlook ribbon (that’s the top bit) to see more information
* Take extra care when dealing with an email that has been marked as suspicious
* If in doubt, check the sidebar
* Always be careful clicking links and responding to emails

**FAQ**:

1. *I received a suspicious email: what do I do?*

Generally speaking, nothing. Do not click on any links or reply to the email. Notify your administrator immediately.

2. *I received a normal email that has been marked as suspicious – why?*

Sometimes email senders are not technically set up correctly, which makes their emails seem suspicious. Sometimes even major companies slip up here. Therefore it is possible that the email is legitimate, even if it has been marked as suspicious. In all cases, stay alert.

3. *What are some of the common reasons an email is marked as suspicious?*

**1. First-time email**

You could get an email that looks like it's from someone you regularly correspond with, yet is a cleverly disguised phishing attempt. Retruster will alert you if this is the first time you've received an email from this sender. This does not mean it’s definitely suspicious – it just helps to make you aware.

**2. Suspicious routes detected**

Retruster will alert you if an email suddenly comes via a different route than expected. This is a common indicator of a fraudulent email.

**3. Reply-to doesn't match sender**

You get an email from Bob, but your reply goes to Jane. This is a common trick used by fraudsters.

**4. Missing protocols**

Legitimate organizations have protocols in place to prevent fraudulent use of their domains (you may have heard of SPF, DKIM and DMARC for example). If these are missing, it’s an indicator that the email can be a fake.

Other warnings might highlight a sender impersonating a common website or domain, or impersonating your own website or domain.

**Note**

• Many legitimate emails from large companies (especially marketing emails) can show some of the signs of “fraud”, such as poorly set up email records

• You will still be warned about these – as they can be easily faked, and rather safe than sorry

• Caution is urged even when seeing an email that hasn’t been marked as suspicious

In all cases, it’s recommended to stay alert. Wishing you safe emailing!

**Images**

These images may be helpful in understanding Retruster.

*1. Examples of the Retruster button in the Outlook Ribbon, in different Outlook versions:*

