East of England Ambulance Service
NHS Trust

Coming soon – new email warning banners

An introduction to Egress Defend

Did you know that most cyber-attacks start with a phishing email? To bolster its defences against malicious inbound emails, the Trust has implemented the Egress Defend solution.

Egress Defend provides advanced detection capabilities that helps to stop phishing attacks. It also uses machine learning to evaluate context, relationships, and message content to prevent inbound cyber threats.

Please take the time to watch this short nano video for a glimpse of how Egress Defend will look and work to protect both you and the Trust. https://vimeo.com/727301059/037e9b99e7

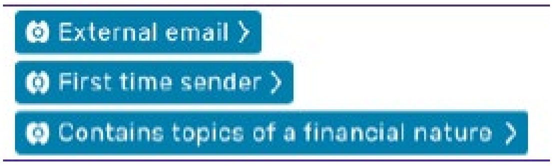
What's changing?

Once enabled, you will notice that emails received from outside of the Trust will have a coloured banner displayed on them. These banners will inform you of any potential threats and tell you how they have been classified. You can click on these banners to find out why an email was identified as being suspicious, this explanation page is referred to as the landing page.

Blue banner – informative

A blue banner is just for information purposes and is **not** associated with a threat being detected. It will indicate if any of the following have been identified.

- You have not received an email from this sender before.
- It has been sent from an external source (outside of the Trust).
- It contains financial or sensitive information.

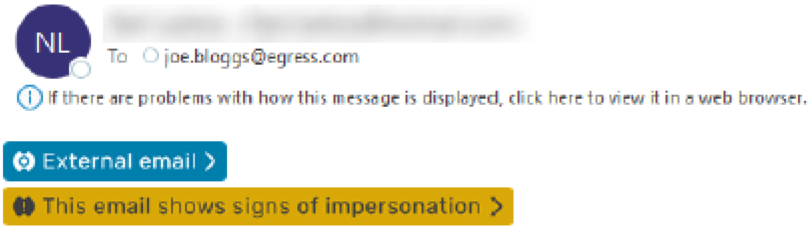

External email ›

First time sender ›

Contains topics of a financial nature ›

Amber banner – exercise caution

An amber banner indicates that ‘suspicious’ elements have been detected; this **could** be an indication of a phishing email or impersonation. You should exercise caution when interacting with this email and the sender.


NL [redacted]

To ○ joe.bloggs@egress.com

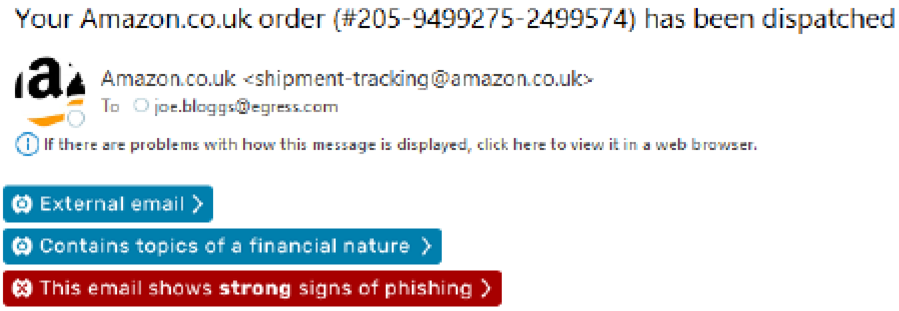
ⓘ If there are problems with how this message is displayed, click here to view it in a web browser.

External email ›

This email shows signs of impersonation ›

Red banner – high potential of danger

A red banner indicates that an email shows strong signs of phishing. This should be deleted.


Your Amazon.co.uk order (#205-9499275-2499574) has been dispatched

Amazon.co.uk <shipment-tracking@amazon.co.uk>

To ○ joe.bloggs@egress.com

ⓘ If there are problems with how this message is displayed, click here to view it in a web browser.

External email ›

Contains topics of a financial nature ›

This email shows **strong** signs of phishing ›

Link rewriting

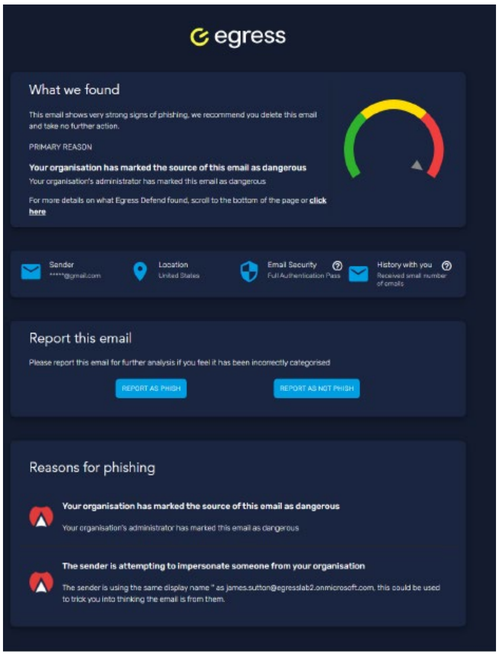
As a precaution, any links in emails you receive will automatically be rewritten to a secure landing page whilst checks are carried out. The landing page will show you the true destination of the link. For example, a link is displaying as Google.com but will actually take you to a different site, which may be trying to collect your username and password or encourage you to download malicious software.

You'll be able to continue from the landing page to the link destination at the touch of a button, if you feel it is safe to do so.

What should I do if I receive a suspicious email?

If you receive a suspicious email, you can report it via Egress Defend by clicking on the "Report as phish" button. This button is located on the landing page. You should then delete the email from your mailbox.

If you think that the email has been incorrectly classified, there is a button to indicate that the email is not a phish.



What we found

This email shows very strong signs of phishing, we recommend you delete this email and take no further action.

PRIMARY REASON

Your organisation has marked the source of this email as dangerous
Your organisation's administrator has marked this email as dangerous

For more details on what Egress Defend found, scroll to the bottom of the page or **click here**

Sender
*****@gmail.com

Location
United States

Email Security
Full Authentication Pass

History with you
Received small number of emails

Report this email

Please report this email for further analysis if you feel it has been incorrectly categorised

Reasons for phishing

Your organisation has marked the source of this email as dangerous

Your organisation's administrator has marked this email as dangerous

The sender is attempting to impersonate someone from your organisation

The sender is using the same display name " as james.sutton@egresslab2.onmicrosoft.com, this could be used to trick you into thinking the email is from them.

Egress Defend utilises both Artificial Intelligence and machine learning to improve its ability to detect threats, without registering false positives. Your interactions and categorisations help the system to identify the differences between safe email and significant threat.

For further information, please contact datasecurity@eastamb.nhs.uk.