

ThreatTest User Quick-Start Guide

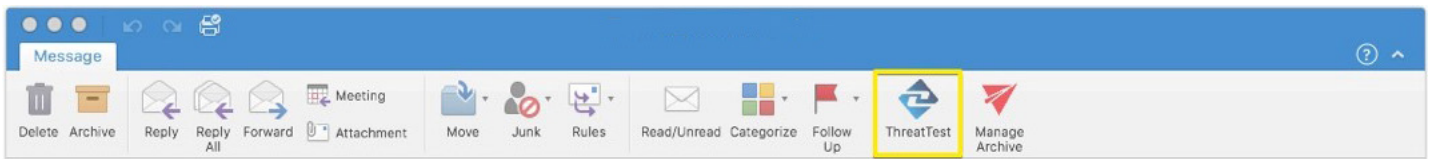


Welcome to EdgeWave ThreatTest!

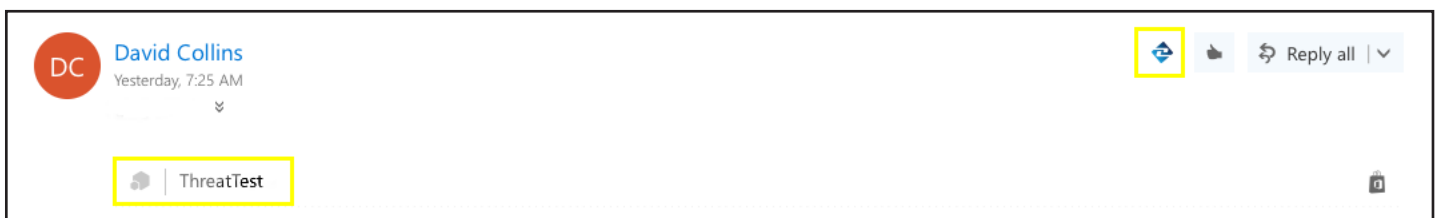
Your company has installed a cool, new tool – ThreatTest – to help you report suspicious emails that are in your inbox. With just one click of a button, you can help protect yourself and your company from spam, phishing, and other malicious attacks that come through your email inbox.

Confirming Activation:

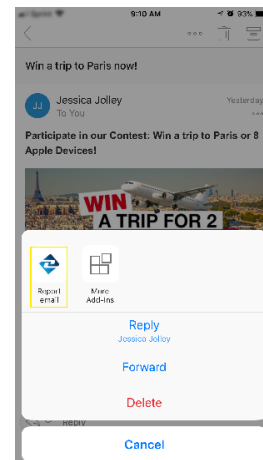
- 1 Your system administrator has likely already activated your ThreatTest account. The easiest way to tell is by looking in the Microsoft Outlook ribbon for the ThreatTest button.



- 1a ThreatTest is also available from Microsoft Outlook Web Access.



- 1b For mobile users (iOS and Android), ThreatTest is available when using the Microsoft Outlook app.





Using ThreatTest:

1 ThreatTest is all about making it easy for you to know if an email is good or bad. When you see a message that looks suspicious, report it via ThreatTest. To submit a message, open it or highlight it then click the ThreatTest button.

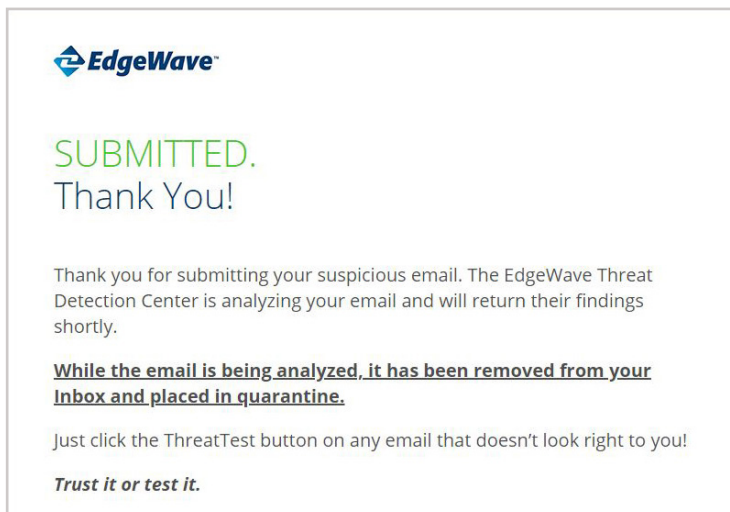
** do not click on any links within the message or open any attachments**

2 Once submitted the message will be moved to the EdgeWave ThreatTest folder to be held here while being analyzed. This folder is automatically created the first time you submit a message.

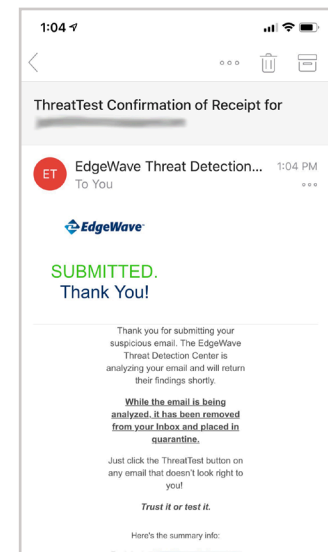
3 You will get a confirmation email showing the EdgeWave Threat Detection Center has received your message. You can also see the current status by selecting the submitted message from within the EdgeWave ThreatTest folder.

Examples of Suspicious Emails

- Unknown sender / unfamiliar email address
- Unexpected or strange subject line
- Includes unverified or unknown web links
- Request to download/open an unknown attachment (i.e. .txt or .doc)
- Contains bad grammar with obvious spelling errors



Microsoft Outlook Submission Notification



Microsoft Outlook Mobile Submission Notification