← Case report for event ID: 8815

ID	Alert rule	Description	Incident type	Severity level	Date and time detected
8815	Inbound Email Containing Suspicious External Link	This alert was triggered by an inbound email contains one or more external links due to potentially suspicious characteristics. As part of the investigation, check firewall or proxy logs to determine whether any endpoints have attempted to access the URLs in the email and whether those connections were allowed or blocked.	Phishing	Medium	Nov 30th 2025 at 12:17

Alert details

datasource: email

timestamp: 11/30/2025 04:14:36.186

subject: Your Amazon Package Couldn't Be Delivered – Action Required

sender: urgents@amazon.biz

recipient: h.harris@thetrydaily.thm

attachment: None

content: Dear Customer,\n\nWe were unable to deliver your package due to an incomplete address.\n\nPlease confirm your shipping information by clicking the link below:\n\nhttp://bit.ly/3sHkX3da12340\n\nIf we don't hear from you within 48 hours, your package will be returned to sender.\n\nThank you,\n\nAmazon Delivery

direction: inbound

Incident report

Edit report

Incident classification

(●) True positive ( ) False positive

Case report

Please write a detailed report on the steps taken to analyse and contain this incident, including all relevant information and the rationale for its closure.

Time of activity: 11/30/2025 04:14:36.186

List of Affected Entities:
sender: urgents@amazon.biz
recipient: h.harris@thetrydaily.thm
attachment: None
Link : bit.ly/3sHkX3da12340

Reason for Classifying as True Positive:
- The email contains an unsafe link that directs the user to a potential phishing website
- The website does not provide an appropriate URL based on the email intent
- Email is generic - authentic email address consumers with their names or usernames.

Reason for Escalating the Alert:
- The user may have added the work email in a phishing / unsafe website that may lead to wider phishing email activities (receiving).
- The user may have used the work address as the delivery address

Does this alert require escalation?

(●) Yes ( ) No

Complete IR:

Time of activity: 11/30/2025 04:14:36.186

List of Affected Entities:
sender: urgents@amazon.biz
recipient: h.harris@thetrydaily.thm
attachment: None
Link : bit.ly/3sHkX3da12340

Reason for Classifying as True Positive:
- The email contains an unsafe link that directs the user to a potential phishing website
- The website does not provide an appropriate URL based on the email intent
- Email is generic - authentic email address consumers with their names or usernames.

Reason for Escalating the Alert:
- The user may have added the work email in a phishing / unsafe website that may lead to wider phishing email activities (receiving).
- The user may have used the work address as the delivery address

Recommended Remediation Actions:
- User policy reminder
- pre-shift meeting or pocket training about proper use of work email and how to identify and deal phishing emails.

List of Attack Indicators:
- Social Engineering tactic: Urgency
- Suspicious link included in the email asking for valuable information (Address)