Case report for event ID: 1005

ID	Alert rule	Description	Incident type	Severity level	Date and time detected
1005	Suspicious Attachment found in email	A suspicious attachment was found in the email. Investigate further to determine if it is malicious.	Phishing	Low	Nov 28th 2025 at 19:39

Alert details

datasource: email

timestamp: 11/28/2025 11:37:05.272

subject: FINAL NOTICE: Overdue Payment - Account Suspension Imminent

sender: john@hatmakereurope.xyz

recipient: michael.ascot@tryhatme.com

attachment: ImportantInvoice-Febrary.zip

content: URGENT: Your account is 30 days past due and will be suspended today unless immediate payment is processed. Legal action will commence if payment is not received within 24 hours. Open the attached invoice immediately to view payment options and avoid legal consequences.

direction: inbound

Incident 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: 11:18:19.544
When: 12/01/2025

List of Affected Entities:
Who:
sender: leonard@fashionindustrytrends.xyz
recipient: yani.zubair@tryhatme.com

Reason for Classifying as True Positive:
Why:
- The email provides phishing content that attracts recipients to click an untrusted link.
- The email shows signs of fake business (impersonation)

Reason for Escalating the Alert:
- The email sender needs to be blocked
- The email domain needs to be blocked

Does this alert require escalation?

(●) Yes ( ) No

Complete IR:

Time of activity: 11:18:19.544
When: 12/01/2025

List of Affected Entities:
Who:
sender: leonard@fashionindustrytrends.xyz
recipient: yani.zubair@tryhatme.com

Reason for Classifying as True Positive:
Why:
- The email provides phishing content that attracts recipients to click an untrusted link.
- The email shows signs of fake business (impersonation)

Reason for Escalating the Alert:
- The email sender needs to be blocked
- The email domain needs to be blocked

Recommended Remediation Actions:

- Pre-shift meeting about how to identify, handle, and report phishing emails.
- Pocket Training about how to identify, handle, and report phishing emails.

List of Attack Indicators:
- Impersonation
- Email guarantees non-realistic offers.