## ← Case report for event ID: 1000

| ID | Alert rule | Description | Incident type | Severity level | Date and time detected |
|---|---|---|---|---|---|
| 1000 | Suspicious email from external domain. | A suspicious email was received from an external sender with an unusual top level domain. Note from SOC Lead: This detection rule still needs fine-tuning. | Phishing | Low | Nov 28th 2025 at 19:29 |

Alert details

datasource: email

timestamp: 11/28/2025 11:26:57.272

subject: Inheritance Alert: Unknown Billionaire Relative Left You Their Hat Fortunes

sender: eileen@trendymillineryco.me

recipient: support@tryhatme.com

attachment: None

content: A long lost billionaire relative has left you their secret hat empire To claim your inheritance send us your banking details immediately

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:** 11/28/2025 11:26:57.272
**Data Source:** Email
**List of Affected Entities:**
- **Recipient:** support@tryhatme.com
- **Sender:** eileen@trendymillineryco.me

**Description of Activity:** A suspicious inbound email was received from an external sender using an unusual top-level domain. The subject line and content indicate a phishing attempt involving fraudulent inheritance claims.
**Reason for Classifying as True Positive:**
- The subject line ("Inheritance Alert: Unknown Billionaire Relative Left You Their Hat Fortunes") is highly suspicious and consistent with common phishing lures.
- The body of the email requests sensitive banking details, a clear indicator of malicious intent.
- The sender domain (`.me`) is unusual and not associated with the recipient's business context.

**Reason for Escalating the Alert:**
- Although the detection rule requires fine-tuning, the indicators strongly suggest phishing.
- Escalation from low to high severity is warranted due to the direct request for financial information.

**Recommended Remediation Actions:**
- Block the sender domain and email address at the mail gateway.
- Conduct immediate user awareness reinforcement (e.g., pocket training or short post-shift briefing) to highlight this phishing tactic.
- Review and fine-tune detection rules to reduce false positives while maintaining sensitivity to similar phishing attempts.

**Does this alert require escalation?**

(•) Yes ( ) No

Save and close alert

Complete IR:

Time of Activity: 11/28/2025 11:26:57.272

Data Source: Email

List of Affected Entities:

Recipient: support@tryhatme.com

Sender: eileen@trendymillineryco.me

Description of Activity: A suspicious inbound email was received from an external sender using an unusual top-level domain. The subject line and content indicate a phishing attempt involving fraudulent inheritance claims.

Reason for Classifying as True Positive:

The subject line ("Inheritance Alert: Unknown Billionaire Relative Left You Their Hat Fortunes") is highly suspicious and consistent with common phishing lures.

The body of the email requests sensitive banking details, a clear indicator of malicious intent.

The sender domain (.me) is unusual and not associated with the recipient's business context.

Reason for Escalating the Alert:

Although the detection rule requires fine-tuning, the indicators strongly suggest phishing.

Escalation from low to high severity is warranted due to the direct request for financial information.

Recommended Remediation Actions:

Block the sender domain and email address at the mail gateway.

Conduct immediate user awareness reinforcement (e.g., pocket training or short post-shift briefing) to highlight this phishing tactic.

Review and fine-tune detection rules to reduce false positives while maintaining sensitivity to similar phishing attempts.

List of Attack Indicators:

Suspicious subject line with inheritance lure.

Sender domain (trendymillineryco.me) not registered or associated with legitimate business.

Email content requesting sensitive banking details.

Deceptive language designed to exploit urgency and curiosity.