

Ticket types for Email Security

Coro raises tickets for emails when it identifies the following security incidents:

- **Blocklisted sender**
- **Brand Impersonation**
- **Crowd Blocked Sender**
- **Domain Impersonation**
- **Email Phishing**
- **Forbidden Attachment Type**
- **Malware in email attachments**
- **Missing Required Authentication**
- **Reported by User**
- **Suspicious Content**
- **User impersonation**

Note

Each ticket raised for the types listed in this article includes **Findings** and **Additional Findings** sections. Use these sections to see details of the specific detectors that triggered the ticket, including an indication of the malicious content or authentication failure identified by the detector. For more information, see the **Using the ticket log**.

Blocklisted sender

Coro identifies that the sender's email address or domain is currently in the **Suspicious Content Blocklist**. The email is deleted for all recipients and the ticket is automatically closed by Coro.

Action	Outcomes
Re-open	Reopen this ticket for Admin user intervention and manual remediation.
Contact user	Coro sends an email to the recipient containing a message and the ticket info. An action: "Contact User" is recorded in the Ticket Log and Activity log.