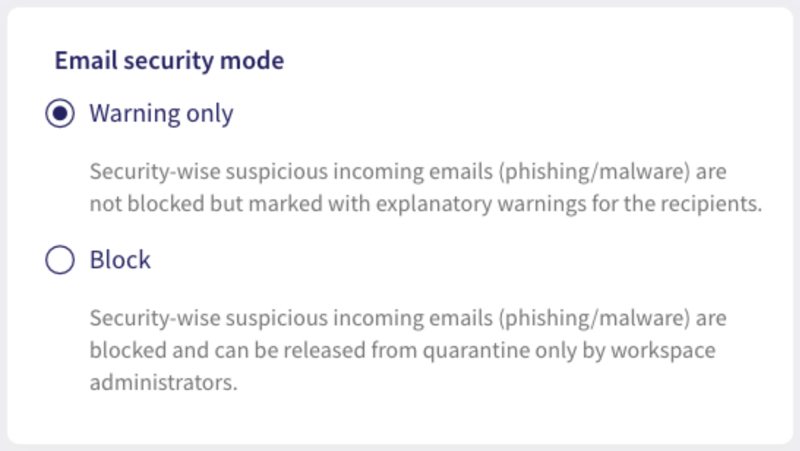
How Coro handles malicious email

Coro's Inbound Gateway offers two configurable outcomes when potentially malicious email is encountered. Such emails can be either:



Email security mode

● Warning only

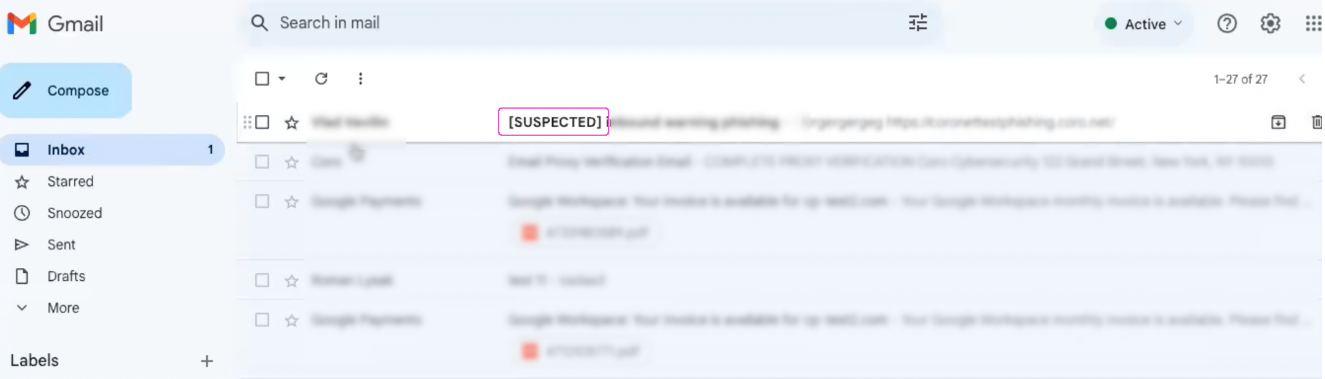
Security-wise suspicious incoming emails (phishing/malware) are not blocked but marked with explanatory warnings for the recipients.

○ Block

Security-wise suspicious incoming emails (phishing/malware) are blocked and can be released from quarantine only by workspace administrators.

- **Warning only**: Emails are sent on to intended recipients as normal, with a warning indicator **[SUSPECTED]** added to the email subject line.

  For example:

  Admin users can inspect tickets raised to identify a suspicious email; however, this is for information only and no further remediation actions are available as the email has already been forwarded. Ticket actions might be limited to retrospective operations such as adding the sender or sender's domain to an allowlist or blocklist for future remediation decisions.

- **Block**: Emails are blocked from end recipients and remain in Coro's dedicated secure quarantine storage pending remediation.