How to Use Quarantine Reports

Quarantine reports help you review and manage emails that have been flagged and quarantined for your protection. These reports are automatically emailed to users and include direct links to release, allow, block, or delete messages—without needing to log into a separate portal.

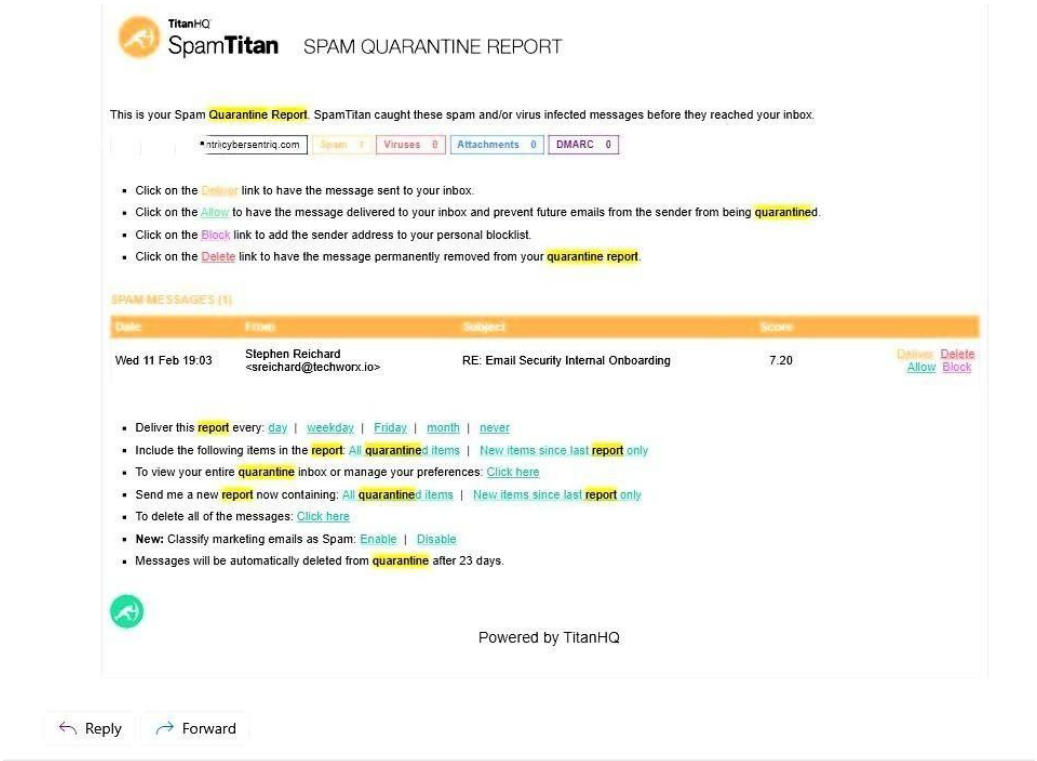
What Is a Quarantine Report?

A quarantine report is an email sent to you on a scheduled basis that contains:

- A list of emails currently held in quarantine
- Actions you can take on each message (such as **Release**, **Allow**, **Delete, or Block**)
- Secure, time-sensitive links for managing those messages These links allow you to take action

  directly from the report itself.

Note:
Quarantine report links are tokenized for security. By default, each link expires **7 days** after the report is generated.



When Are Quarantine Reports Sent?

Quarantine reports are generated **nightly**, but will only be sent to you if all of the following conditions are met:

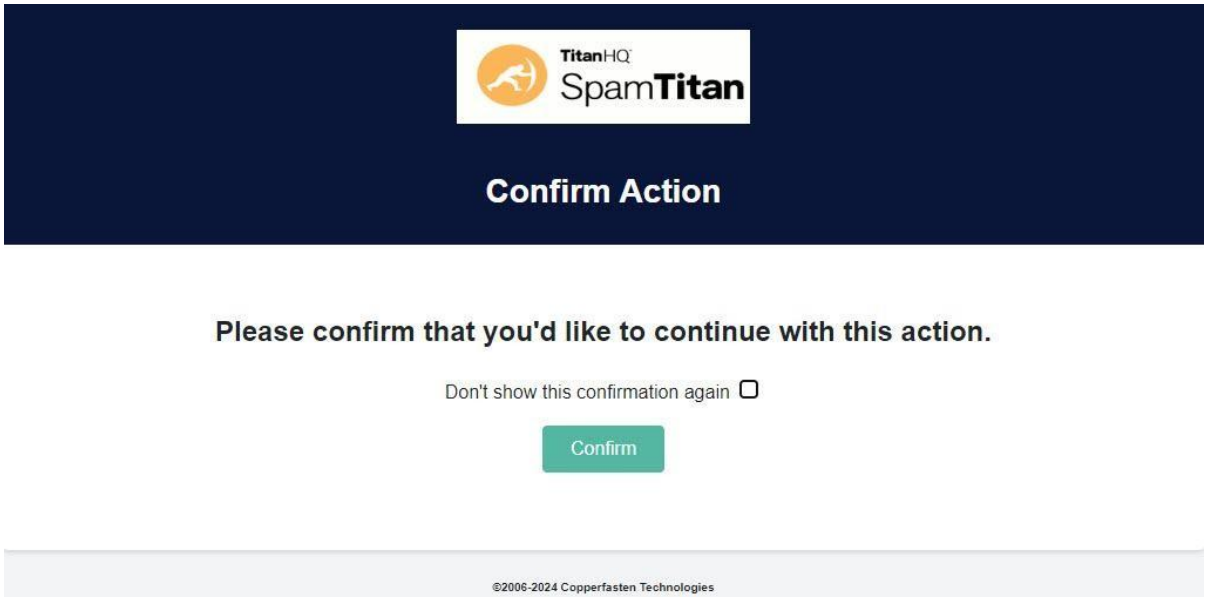
1. **Quarantine reports are enabled** by your domain admin. ○
   Default setting: Disabled
2. **You have quarantined email** waiting to be reviewed.
3. **Today matches your report schedule.**
   - For example, if you or your admin set reports to send weekly on Fridays, you will only receive them on Fridays—*not daily*.

Using the Links in Your Report

When you click any action link in your quarantine report (such as "Release" or "Delete"), you'll see a confirmation pop-up asking you to verify the action.

You can choose:

- **Continue** to complete the action
- **Cancel** to go back
- Or check **"Don't show this confirmation again"** if you prefer to skip the pop-up in the future



System-Detected Threat

WARNING Spam, malware or phishing has been detected. Our AI is always learning, report feedback with the TitanHQ Outlook Add-In. Powered by TitanHQ™.

- A **warning** banner is applied to an email if spam, malware, or phishing has been automatically detected by PhishTitan.
- This email is visible in the Incident list, on the Resolved tab.
- If auto remediation is enabled, this email is moved to the user's Junk folder.

Admin-Remediated Threat

WARNING Spam, malware or phishing has been detected. Our AI is always learning, report feedback with the TitanHQ Outlook Add-In. Powered by TitanHQ™.

- A **warning** banner is applied to an email an administrator has manually remediated.
- This email is visible in the Incident list, on the Resolved tab.
- Email is moved to the user's Junk folder.

No Threat Detected

SAFE Your Administrator has marked this email as clean. Powered by TitanHQ™.

- If an email is considered clean and no threat has been detected, a **safe** banner is applied.
- If manual remediation is enabled, this email remains in the user's Inbox.
- If auto remediation is enabled, this email is moved from the user's Junk folder to the Inbox.

Exploited Domains

ALERT Our analysis shows that this is a suspicious domain as it is frequently used in phishing attacks. Be careful with this email. Powered by TitanHQ™.

- If Exploited Domains is enabled, an **alert** banner is added to emails from domains known to be frequently used in phishing attacks.
- It is a reminder to users to stay vigilant, even if the content of an email does not look suspicious.
- Exploited Domains setting default is disabled. Banner is applied to Exploited Domains regardless of whether manual or auto remediation is enabled.
- Mails are delivered to the user's Inbox.

Anti-spoof

ALERT Display name spoofing has been detected. Be careful with this email unless you know it is safe. Powered by TitanHQ™.

- When Anti-spoof is enabled, manipulated display names are checked, and if detected, an **alert** banner is added.
- It is a reminder to users to stay vigilant, even if the content of an email does not look suspicious.
- Anti-spoof default setting is disabled. Banner is applied to anti-spoof mails regardless of whether manual or auto remediation is enabled.
- Mails are delivered to the user's Inbox.

Graymail / Marketing Mail

INFO Our analysis indicates this is graymail (legitimate, opted-in, bulk mail). Be careful with this email unless you know it is safe. Powered by TitanHQ™.

- If Graymail is enabled, it is treated as malicious, and an **information** banner is added to alert customers and users.
- Banner is applied to graymail regardless of whether manual or auto remediation is enabled.