HARMONY

01 July 2025

# AVANAN

User Guide

CHECK POINT™

# Table of Contents

# Email Security Portal

The **Email Security Portal** provides you with a user-friendly interface to handle emails flagged as suspicious or potentially harmful, allowing you to manage them proactively while ensuring a secure environment for your email communications.

In the Email Security Portal, you can preview the quarantined emails, restore them, or submit a restore request for them - all in accordance with your organization's policies.

## Benefits

- Proactive Management: Handle suspicious emails proactively.
- Enhanced Security: Reduce the risk of phishing and malware.
- User Empowerment: Take immediate action without IT support.
- Efficient Filtering: Quickly find and manage specific emails quarantined emails.
- Trust Management: Add trusted senders to improve email delivery.
- Clear Status Tracking: Track the status of your restore requests easily.

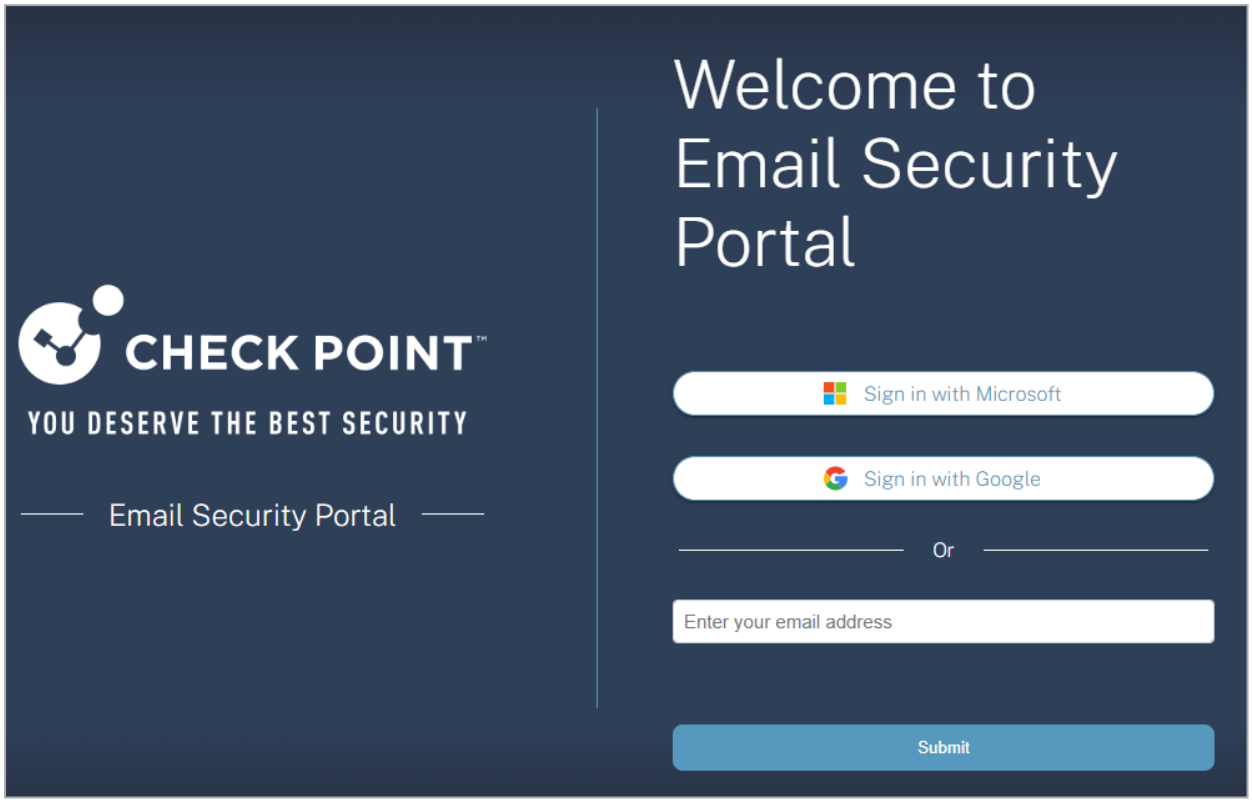
## Accessing the Email Security Portal

Depending on your organizational policy, you can access the Email Security Portal using any of these authentication methods:

- **Microsoft login**
- **Google login**
- **One-time password via email**

**To log in to the Email Security Portal:**

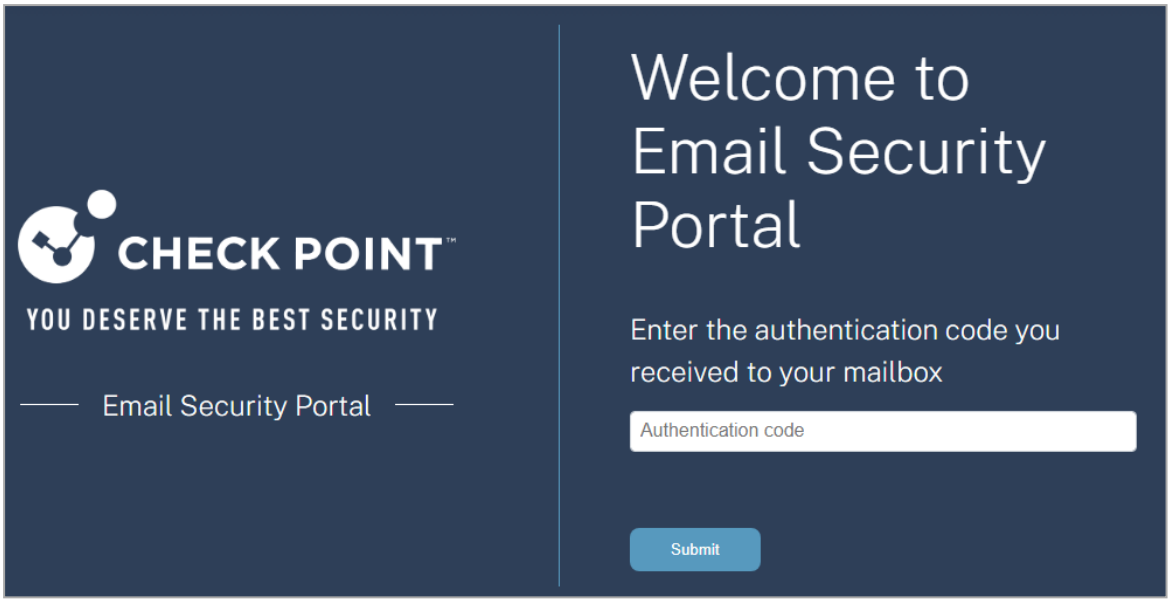
1. Access the Email Security Portal using .




2. To sign in using Microsoft credentials:
   a. Click **Sign in with Microsoft**.
   b. Follow the on-screen instructions and sign in with your organization's Microsoft credentials.
3. To sign in using Google credentials:
   a. Click **Sign in with Google**.
   b. Follow the on-screen instructions and sign in with your organization's Google credentials.
4. To sign in using one-time password through email:
   a. In the **Enter your email address** field, enter your organizational email address.
   b. Click **Submit**.

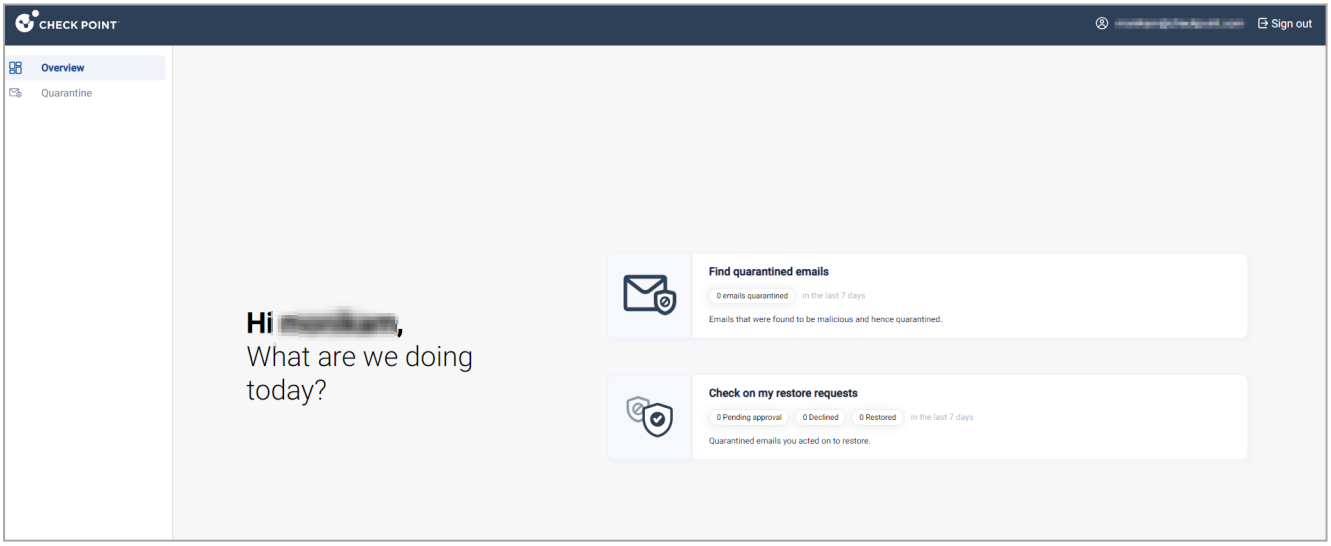
   The system sends a verification code to your organizational email address.

c. In the **Enter the authentication code you received to your mailbox** field, enter the verification code you received to your organizational email address.




d. Click **Submit**.

After successful authentication, the **Overview** page appears.




# Viewing Quarantined Emails

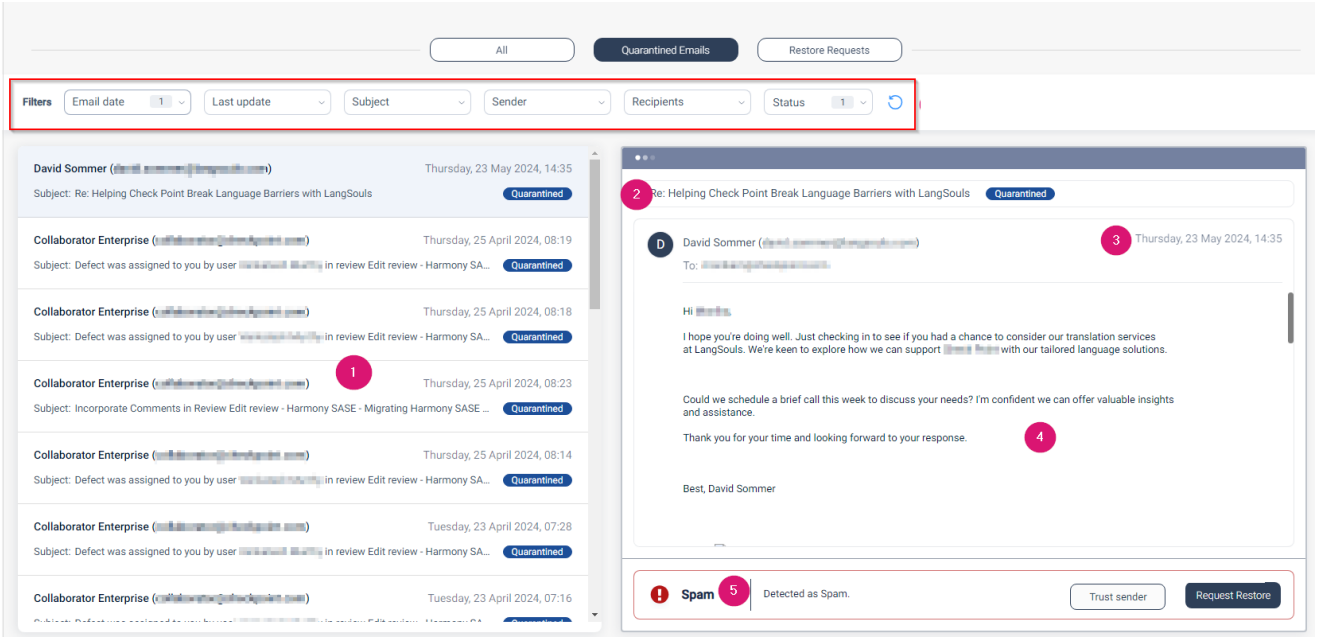
The **Quarantined Emails** page shows all the quarantined emails.

**Note** - You can view only a preview of the quarantined emails.

- By default, the portal shows the images as icons only. If your organizational policy allows you to view the images, **Display images** option appears at the top-right corner of the previewed email. To view the images, click **Display Images**.
- All the links are disabled in the preview.

To view the **Quarantined Emails** page, do one of these:

- In the **Overview** page, click **Find quarantined emails**.
- From the left navigation panel, click **Quarantine** and select the **Quarantined Emails** tab.




| Legend | Item | Description |
|---|---|---|
| 1 | Quarantined emails | All quarantined emails that you can take action on. |
| 2 | Email Subject | Subject of the email. |
| 3 | Date and Time | Day, date and time the email was received. |
| 4 | Email body | Body of the email. |
| 5 | Threat Category | Category of the quarantined email, such as malware and phishing. |

<table>
<tr><th>Legend</th><th>Item</th><th>Description</th></tr>
<tr><td>6</td><td>User Actions</td><td>Shows the available user actions for the email.
<table>
<tr><th>Action</th><th>Description</th></tr>
<tr><td>Restore</td><td>Allows you to restore the email yourself without an administrator's approval.</td></tr>
<tr><td>Request Restore</td><td>Allows you to request to restore an email and an administrator must approve to restore the email.</td></tr>
<tr><td>Trust Sender</td><td>Allows you to add a sender to the Trusted Senders list.<br>When you add a sender to the Trusted Senders list, the emails from the sender will be delivered to your mailbox instead of moving to the spam folder.<br>Note - These emails might still be flagged as phishing or containing malware and quarantined.</td></tr>
</table>
Note - Availability of these options depends on your organizational policies.</td></tr>
</table>

<table>
<tr><th>Legend</th><th>Item</th><th>Description</th></tr>
<tr><td>7</td><td>Filters</td><td>Available options to filter the emails.
<table>
<tr><th>Filter Type</th><th>Description</th></tr>
<tr><td>Email date</td><td>Shows all relevant emails matching the selected date or date range.</td></tr>
<tr><td>Last update</td><td>Shows all emails matching the status update date.</td></tr>
<tr><td>Subject</td><td>Shows all emails matching the text entered in the Subject field.</td></tr>
<tr><td>Sender</td><td>Shows all relevant emails from senders matching the text entered in the Sender field.</td></tr>
<tr><td>Recipients</td><td>Shows all emails matching the text entered in the Recipient field.</td></tr>
<tr><td>Status</td><td>Shows all emails matching the selected status:<ul><li>All - Emails that are quarantined, pending, declined, or restored.</li><li>Pending - Emails that are pending for administrator's approval.</li><li>Quarantined - Emails that are quarantined.</li><li>Declined - Emails that are requested for release from quarantine, but are declined by the administrator.</li><li>Restored - Emails that are restored to the mailbox.</li></ul></td></tr>
</table></td></tr>
</table>

# Restoring Quarantined Emails

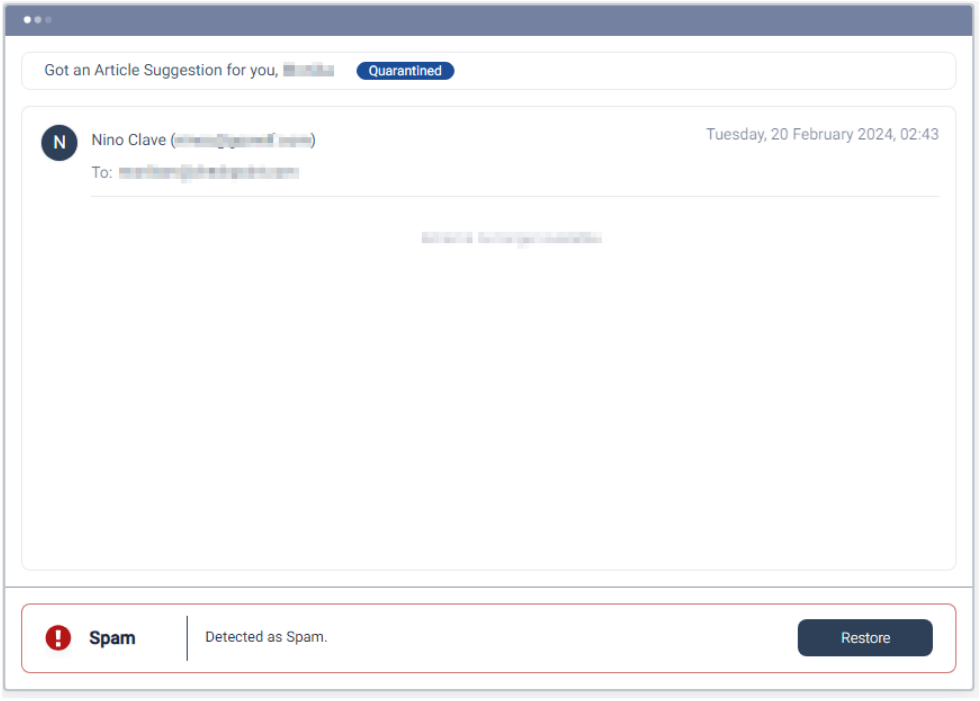
Based on the threat category of an email, your organizational administrators would have configured policies that allows you to restore the email yourself or require administrator's approval for restoration.

- **Restore** - Allows you to restore the email yourself without an administrator's approval.
- **Request Restore** - Allows you to request to restore the email. The email will be delivered to your mailbox only when it is approved by an administrator.

# How to restore emails that do not need an administrator's approval

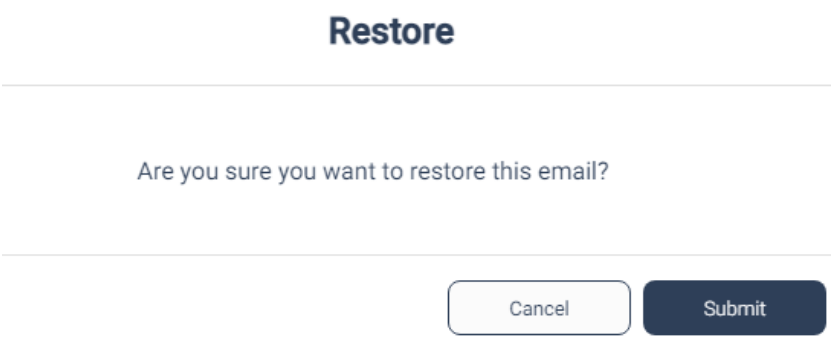
For emails that do not need an administrator's approval, the **Restore** option appears. To restore these emails:

1. Select the email you want to restore.



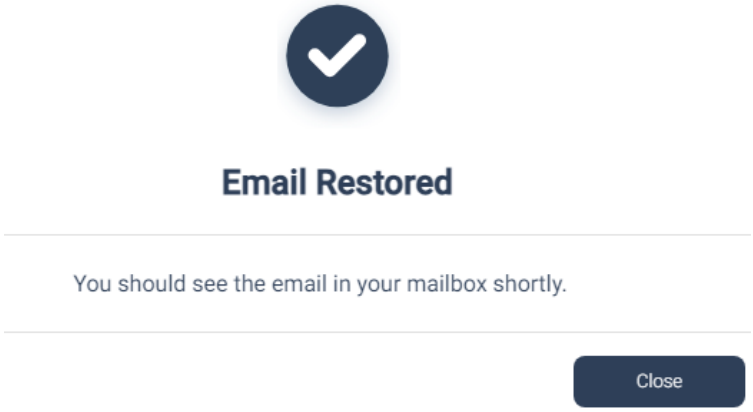

2. Click **Restore**.

   The **Restore** window appears.



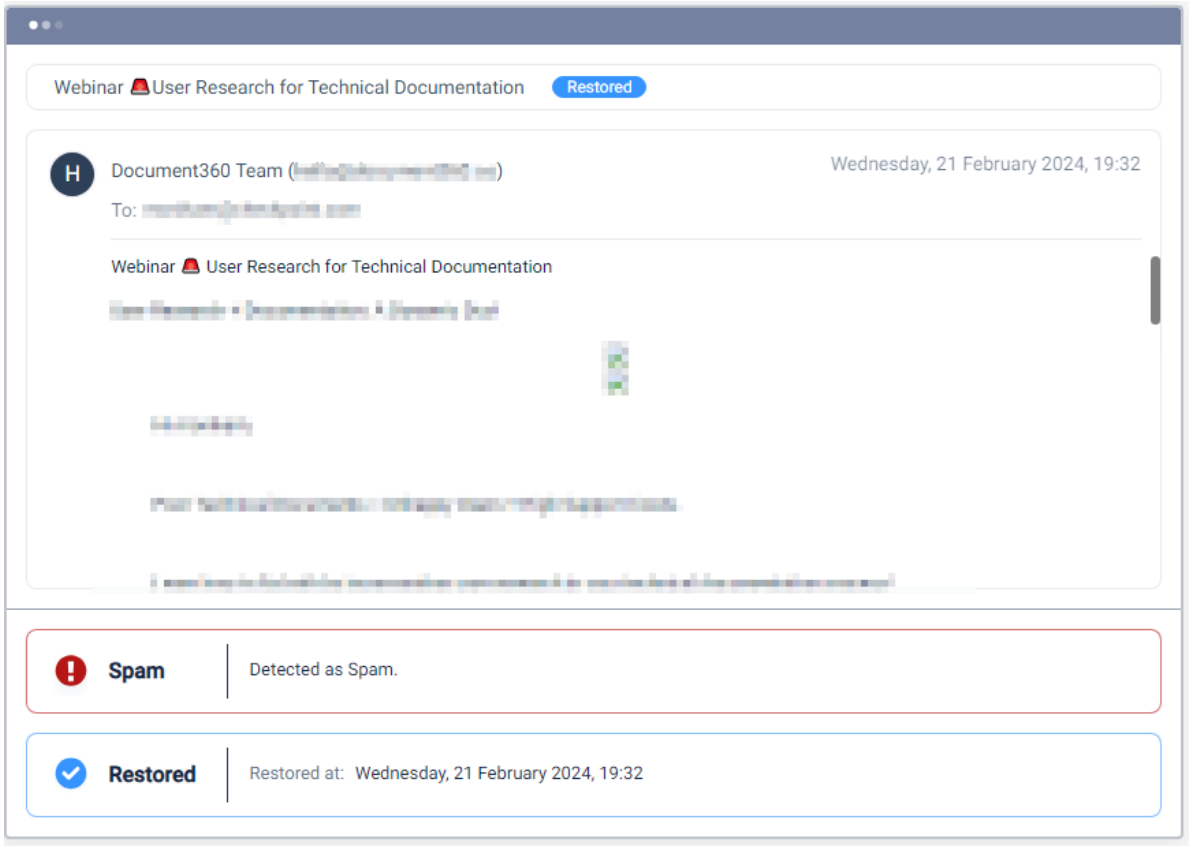

3. Click **Submit**.

   The email gets restored to your mailbox.




4. Click **Close**.

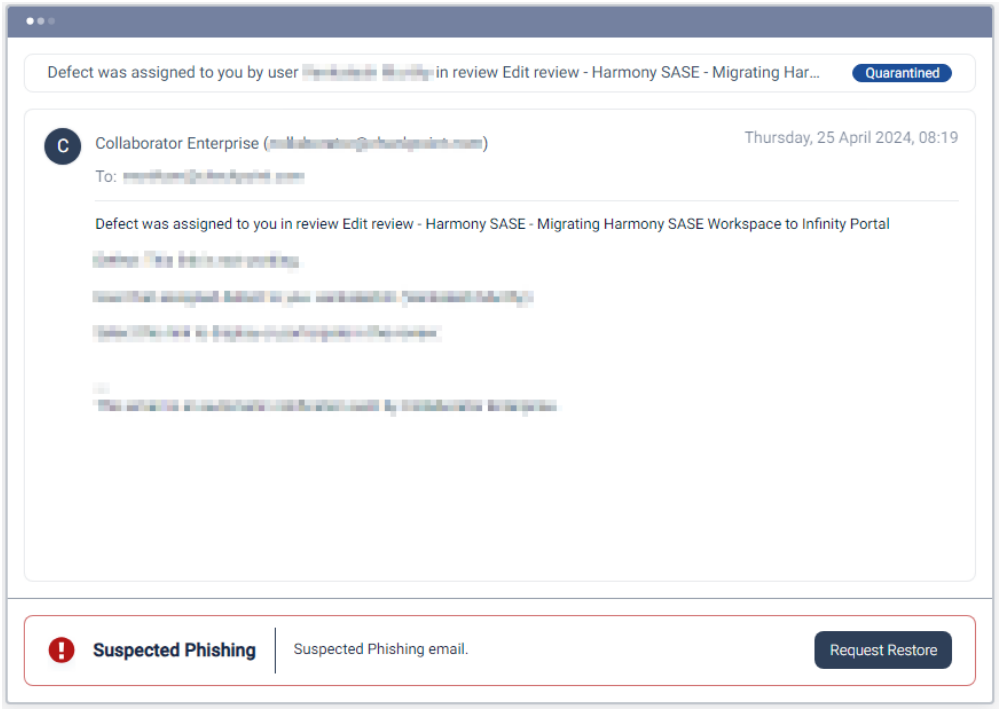
   Once restored, the email status changes from **Quarantined** to **Restored**.




## How to restore emails that need an administrator's approval

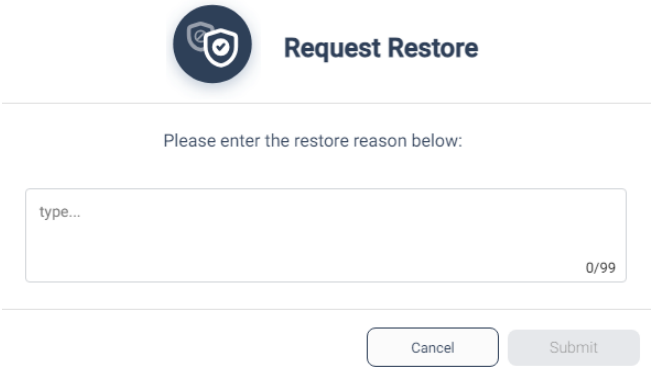
For emails that need an administrator's approval, the **Request Restore** option appears. To restore these emails:

1. Select the email that you want to restore.

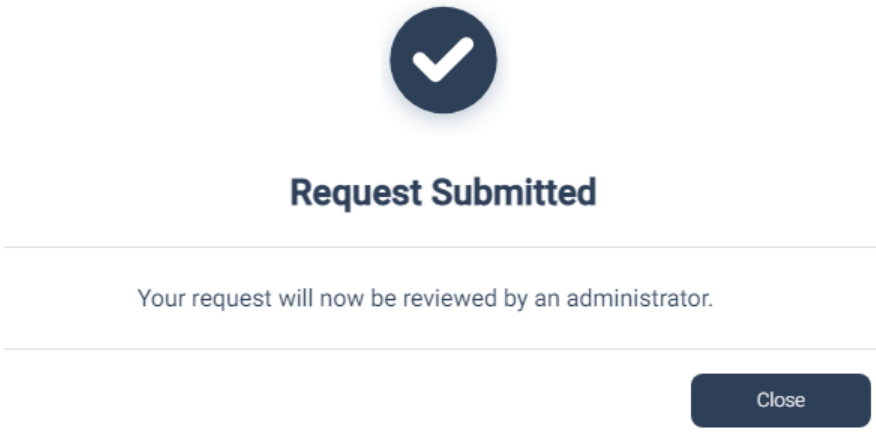



2. Click **Request Restore**.

   The **Request Restore** window appears.



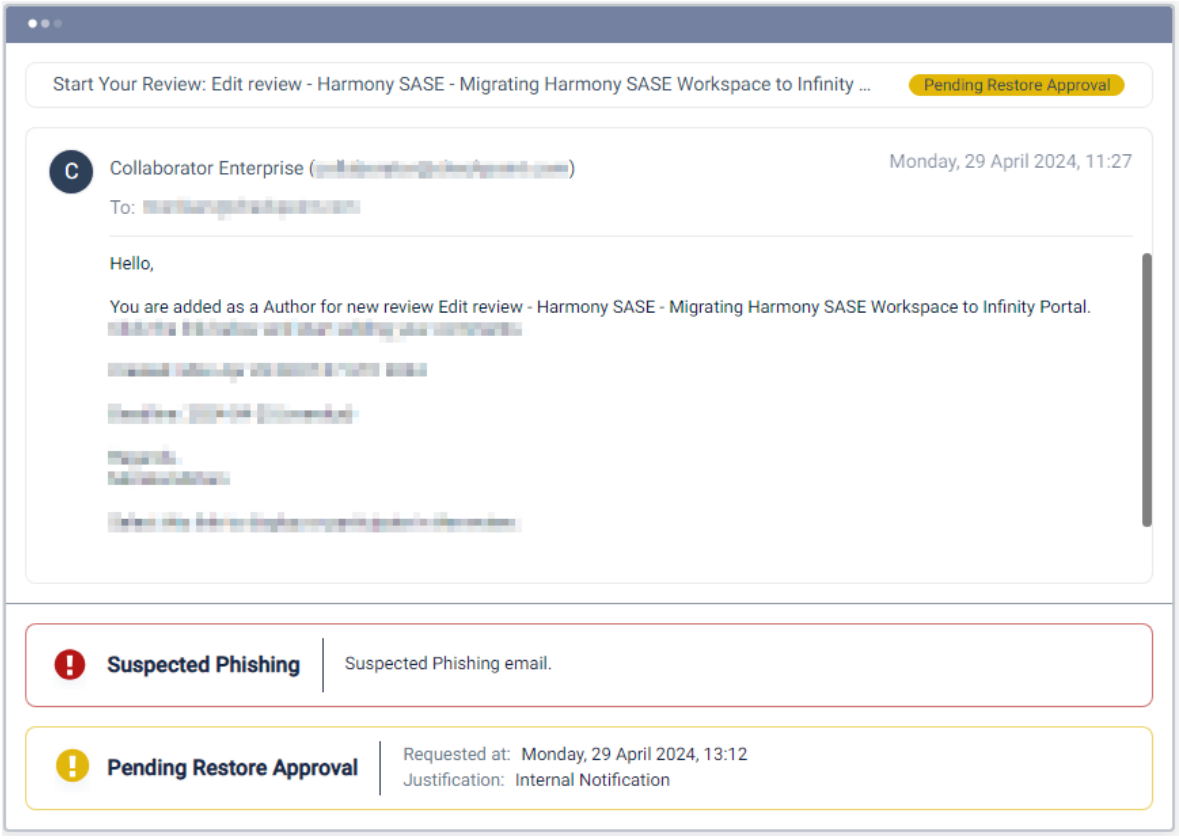

3. In the **Please enter the restore reason below** field, enter your justification for restoring the email.
4. Click **Submit**.



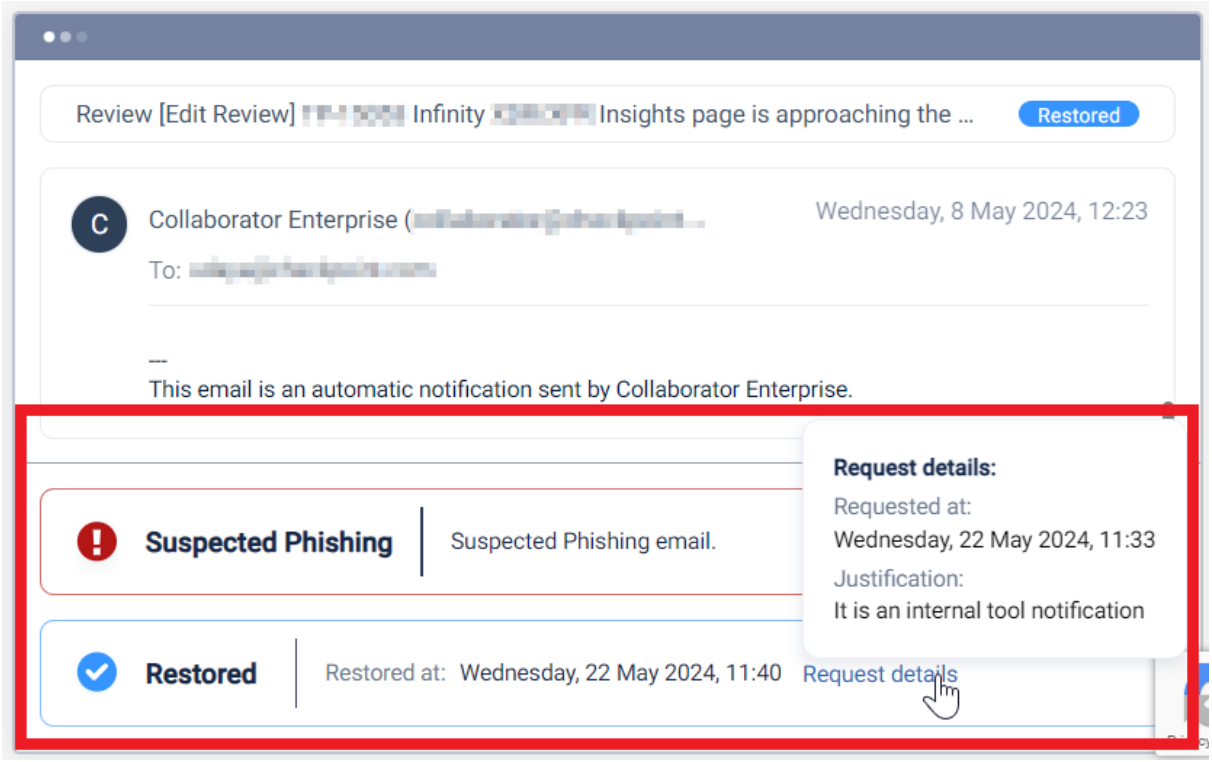

The system sends a request to the administrator for review.

5. Click **Close**.

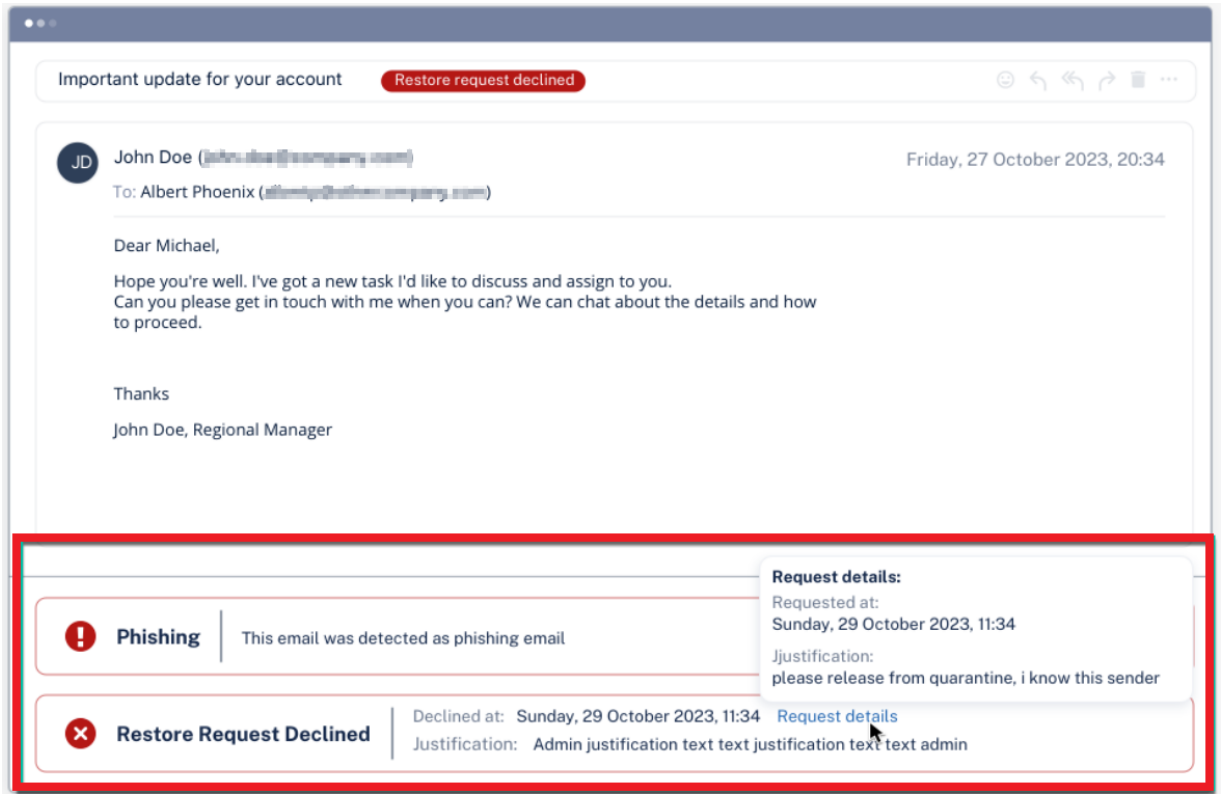
   The email status changes from **Quarantined** to **Pending Restore Approval**.




If the administrator approves the request, the email is restored to your mailbox and the email status changes to **Restored**.




If the administrator declines the request, the email status changes to **Restore Request Declined** and the system shows the reason for declining the request.

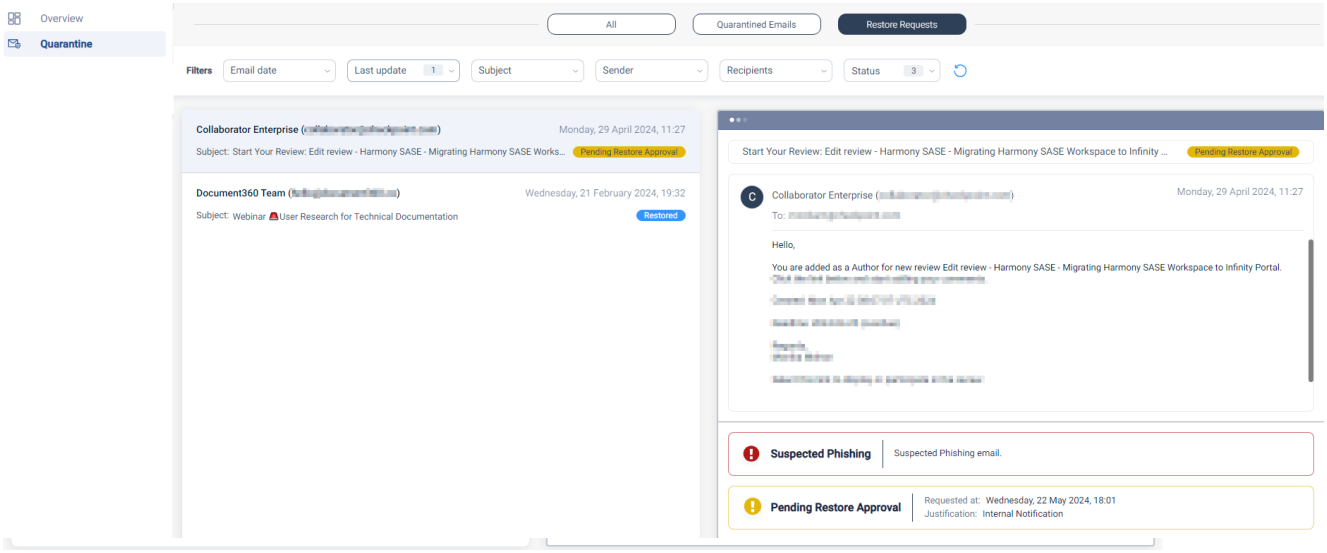


# Viewing the Status of Restore Requests

This page shows the status of restore requests that have been declined, awaiting approval (pending), or have been successfully restored.

To view the **Restore Requests** page, do one of these:

- In the **Overview** page, click **Check on my restore requests**.
- From the left navigation panel, click **Quarantine** and select the **Restore Requests** tab.



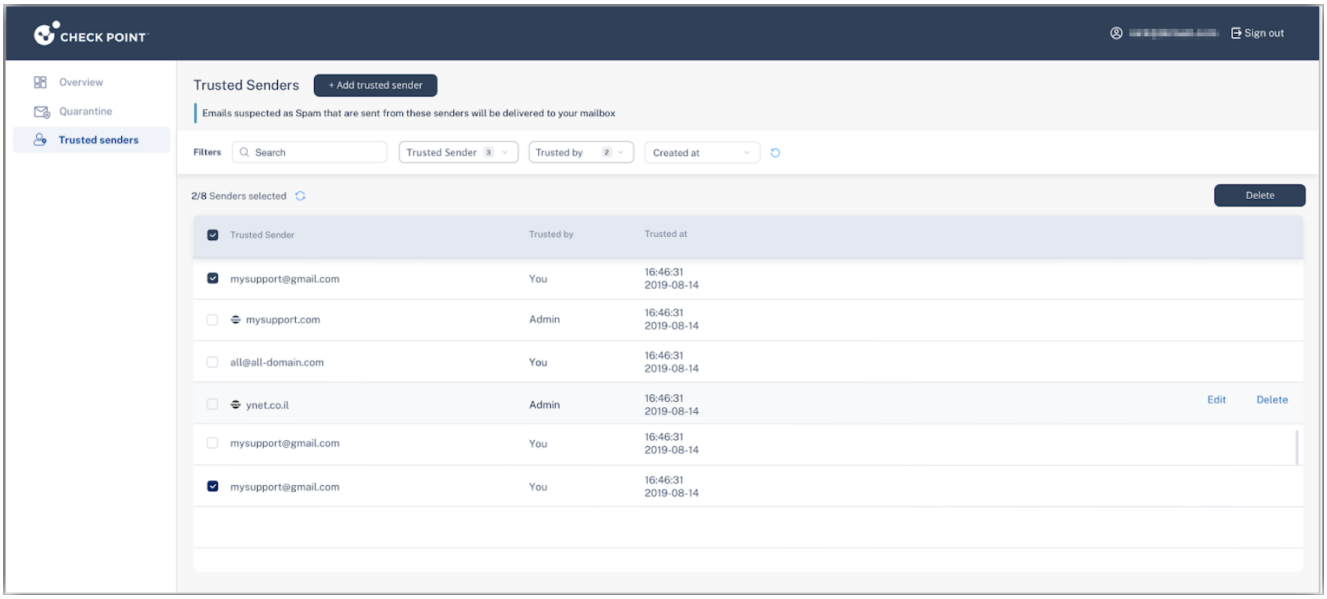

# Trusted Senders

Trusted Senders are legitimate senders whose emails are sent to the spam folder of a user. When you see such an email from a legitimate person being moved to the spam folder, you can add them to the **Trusted Senders** list.

When Avanan sees a sender in the **Trusted Senders** list, it automatically moves the email to the inbox instead of the spam folder.

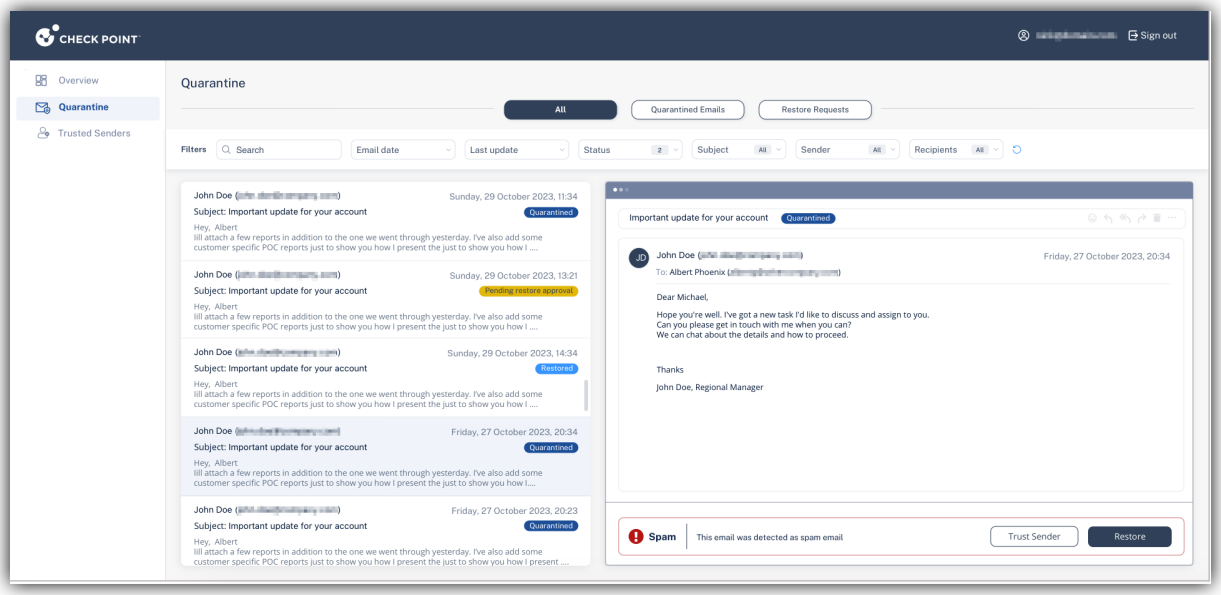
**Note** - Adding a sender to the **Trusted Senders** does not guarantee that the email will always be delivered to your mailbox. Avanan scans these emails for potential threats and can quarantine them.

To view the **Trusted Senders** page, from the left navigation panel, click **Trusted senders**.



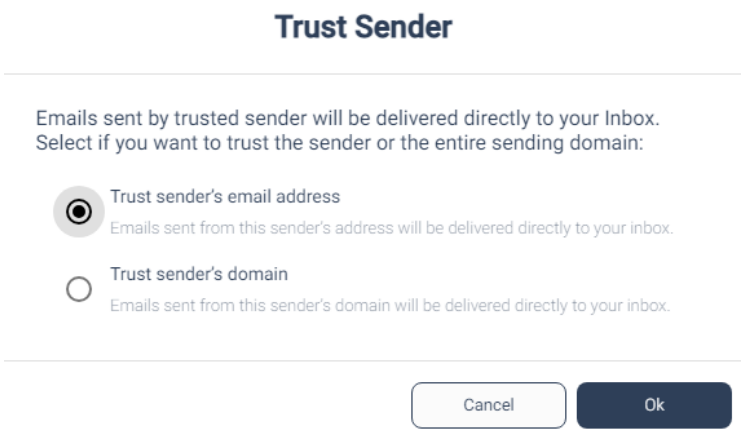

# Adding Trusted Senders

1. From the left navigation pane, click **Quarantine**.

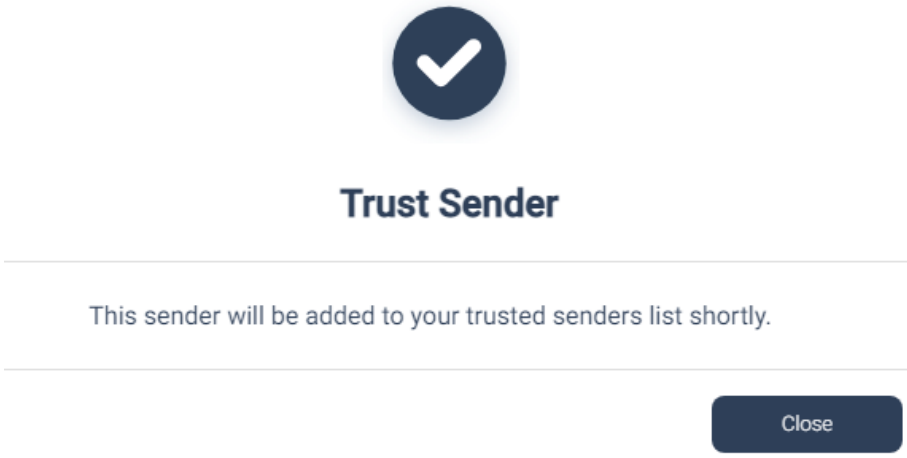



2. Select the spam email you want to add to the trusted senders.
3. Click **Trust Sender**.

   The **Trust Sender** window appears.




4. Select the required option:
   - **Trust sender's email address** - Emails sent from this sender's address are delivered directly to your mailbox.
   - **Trust sender's domain** - Emails sent from this sender's domain are delivered directly to your mailbox.
5. Click **OK**.

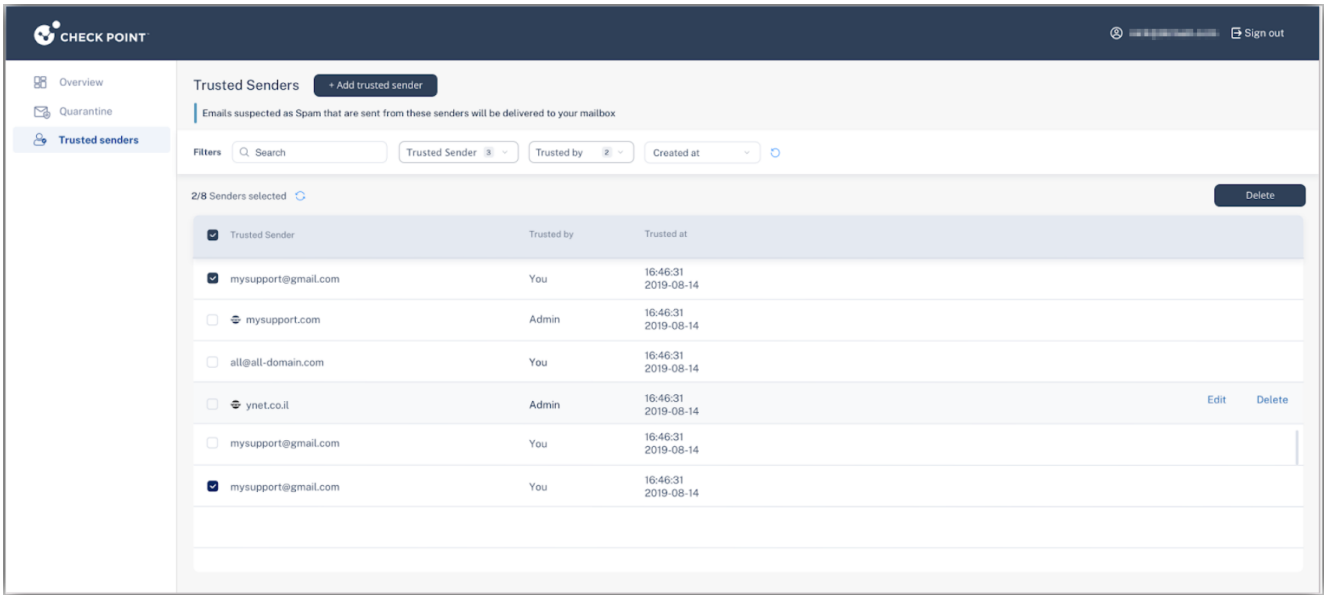



   The system adds this sender to the trusted senders list. To view the list of trusted domains or senders, see *"Viewing Trusted Senders" below*.
6. Click **Close**.

# Viewing Trusted Senders

The **Trusted senders** page shows the list of email address and domains that are added to the Trusted Senders.

To view the **Trusted senders** page, from the left navigation pane, click **Trusted senders**.




To delete a trusted sender, select the checkbox relevant to the sender and click **Delete**.

### To edit a trusted sender:

1. Select the checkbox relevant to the sender.
2. Click **Edit** from the last column.
3. Make the required changes and **Submit**.

# Acting on Quarantined Emails

To keep your inbox safe, your organization uses Avanan to quarantine emails, files, and messages based on its security policies and settings. This process ensures harmful content is contained before it reaches your inbox.

Additionally, Attachment Cleaning removes malicious content from email attachments while securely storing the original versions in quarantine for reference or restoration if needed.

Depending on your organization's policy, you can request the restoration of quarantined emails. Administrators review these requests and decide whether to approve them. This process helps maintain a secure and efficient communication environment for everyone.

- *"Requesting a Restore from Quarantine" below*
- *"Restore Requests for Emails Sent to Groups" on page 22*
- *"Restoring Emails Without Administrator Approval" on the next page*

## Requesting a Restore from Quarantine

If your organization has configured the policy to allow you to restore quarantined emails or attachments that were mistakenly flagged, you can use the link provided in the email to request their release.


**Note** - This procedure is applicable for emails sent only for individuals. For the procedure for emails sent to groups, see *"Restore Requests for Emails Sent to Groups" on page 22*

**To request a restore from quarantine:**

1. Click on the link in the email you received.
2. On the **User Verification** page that appears, do these:

a. Enter your email address and click **Submit**.

   Avanan sends a verification code to your email address.

b. Enter the verification code you received and click **Submit**.

   **Note** - Once authenticated, the user does not need to authenticate again in the same browser for the next 30 days.

3. Enter the reason for your request to release the email from quarantine and click **Submit**.

   You will receive a notification that the request is sent to the administrator.

4. If the request is approved by the administrator, the original message gets delivered to all the recipients of the restored email.

# Restoring Emails Without Administrator Approval

If your organization has configured the policy to allow you to restore quarantined emails or attachments that were mistakenly flagged without the administrator's approval, you can use the link provided in the email to release them.

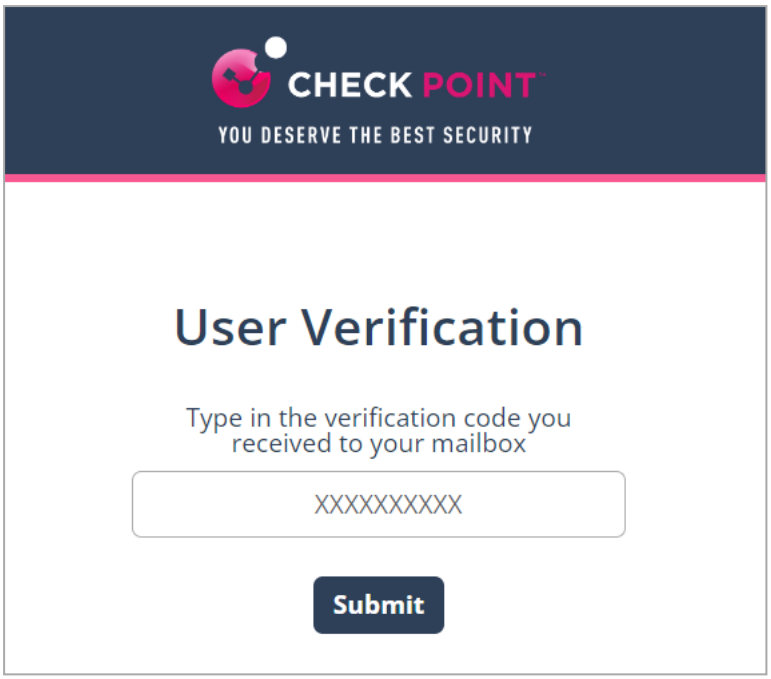
**o restore a quarantined email:**

1. Click on the link in the email notification you received for the quarantined email.
2. On the **User Verification** page that appears, do these:

   a. Enter your email address and click **Submit**.

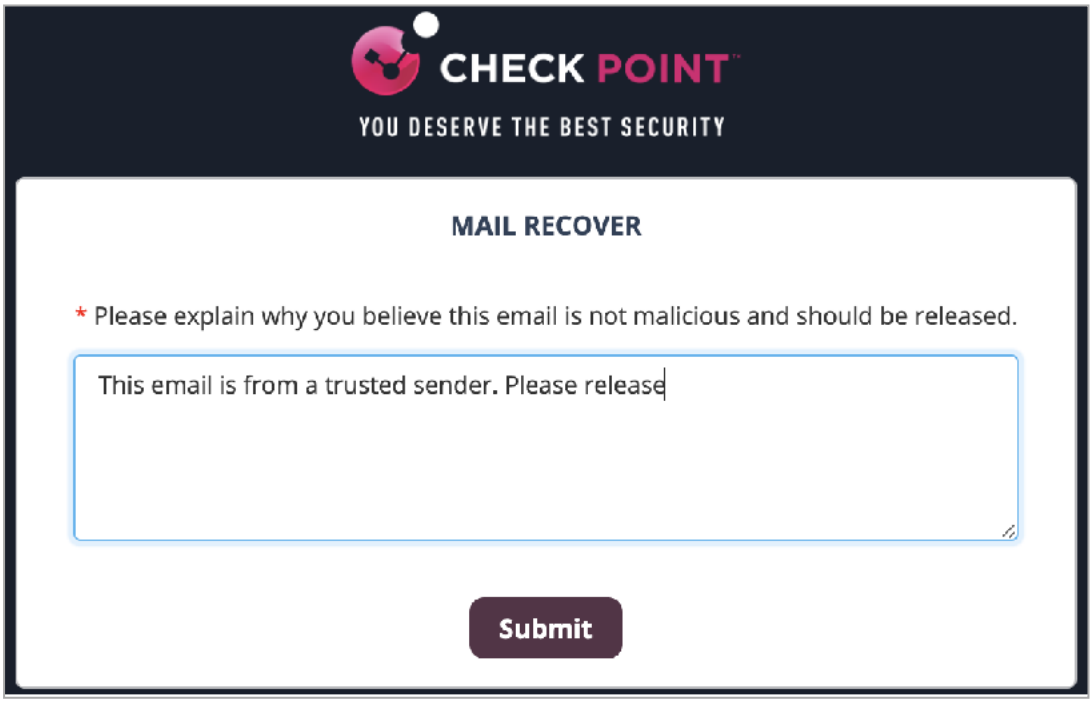
      Avanan sends a verification code to your email address.

b. Enter the verification code you received and click **Submit**.

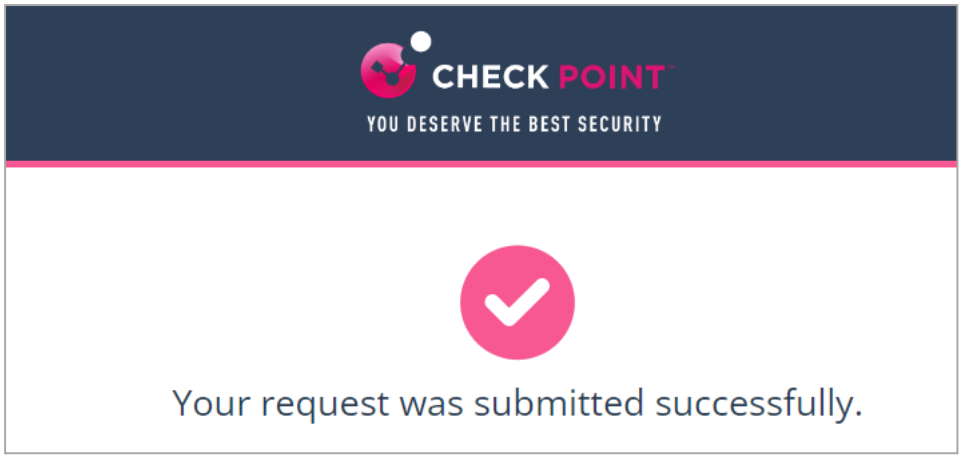



**Note** - Once authenticated, the user does not need to authenticate again in the same browser for the next 30 days or until the cookies are cleared, whichever is earlier.

3. Enter the reason for your request to restore the original email and click **Submit**.




The system shows the request status and the email gets delivered to the mailbox in a couple of minutes.




**Note** - The email received time is the restore time of the email, and not the original email sent time.

# Restore Requests for Emails Sent to Groups

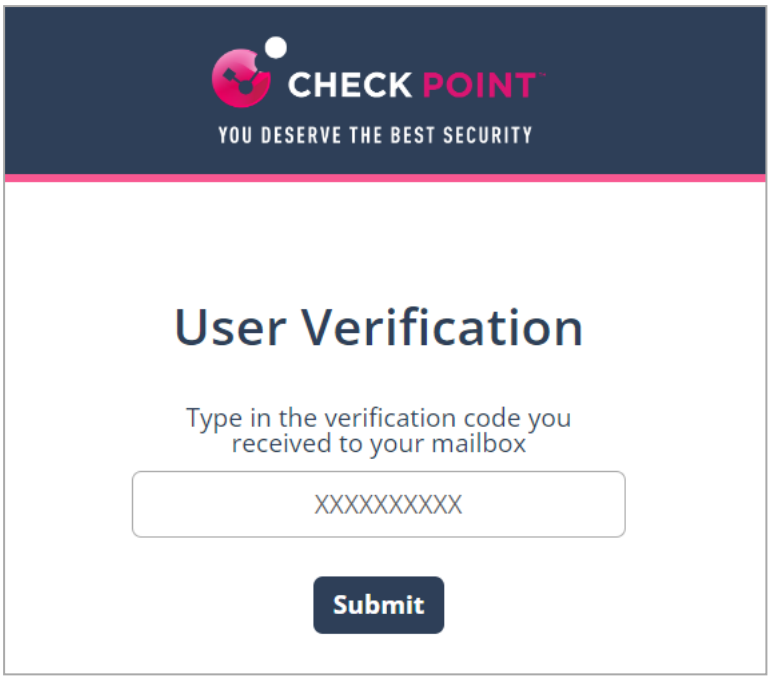
If your organization has configured the policy to allow you to restore quarantined emails or attachments sent to groups that were mistakenly flagged, you can use the link provided in the email to request their release.

**o request to restore a quarantined or cleaned email:**

1. Click on the link in the email notification you received for the quarantined or cleaned email.
2. On the **User Verification** page that appears, do these:
    a. Enter your email address and click **Submit**.

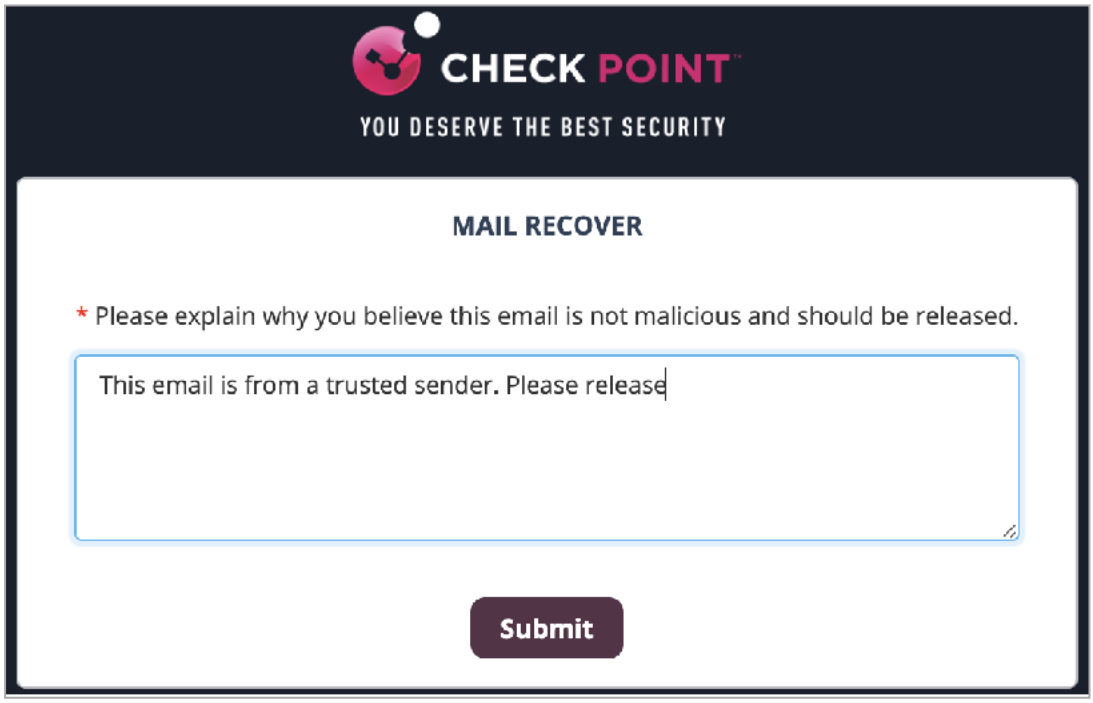
    Avanan sends a verification code to your email address.

b. Enter the verification code you received and click **Submit**.

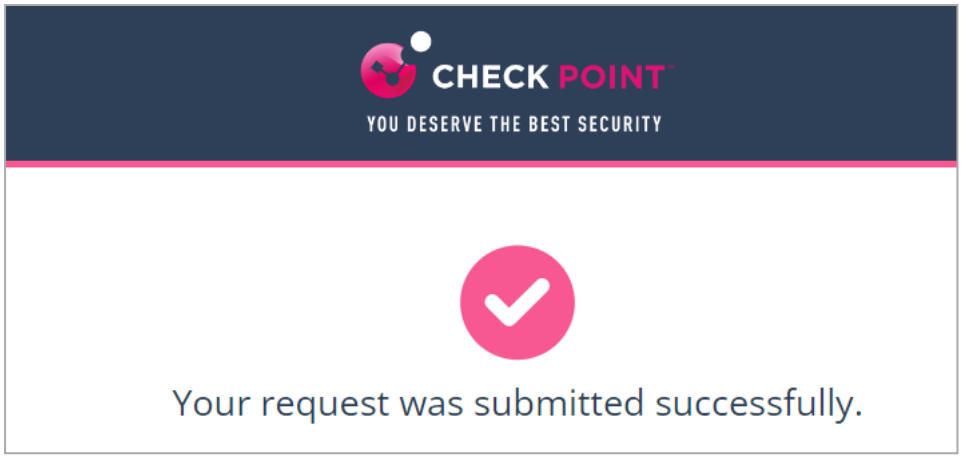



**Note** - Once authenticated, the user does not need to authenticate again in the same browser for the next 30 days.

3. Enter the reason for your request to restore the original email and click **Submit**.




The system shows the request status and the email is delivered to the mailbox in a couple of minutes.



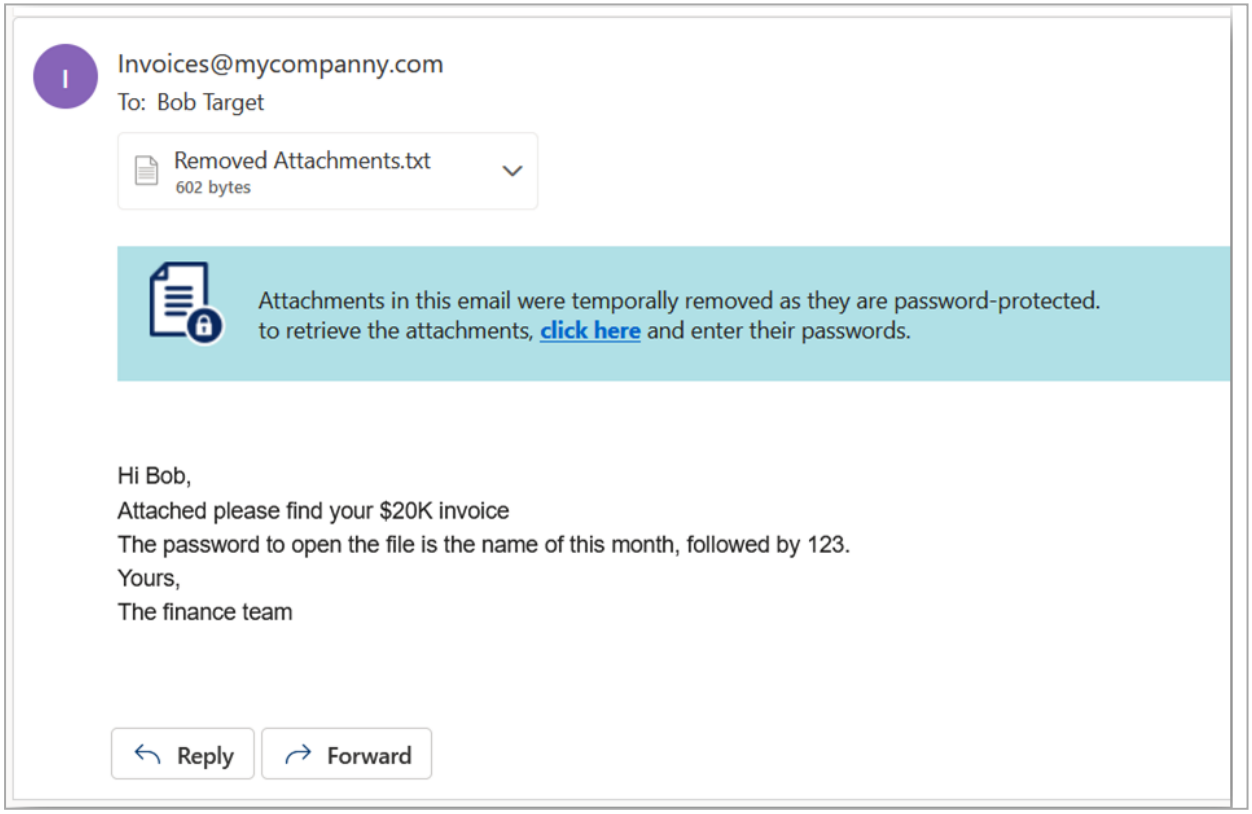

**Note** - The email received time is the restore time of the email, and not the original email sent time.

# Requesting Passwords from End Users

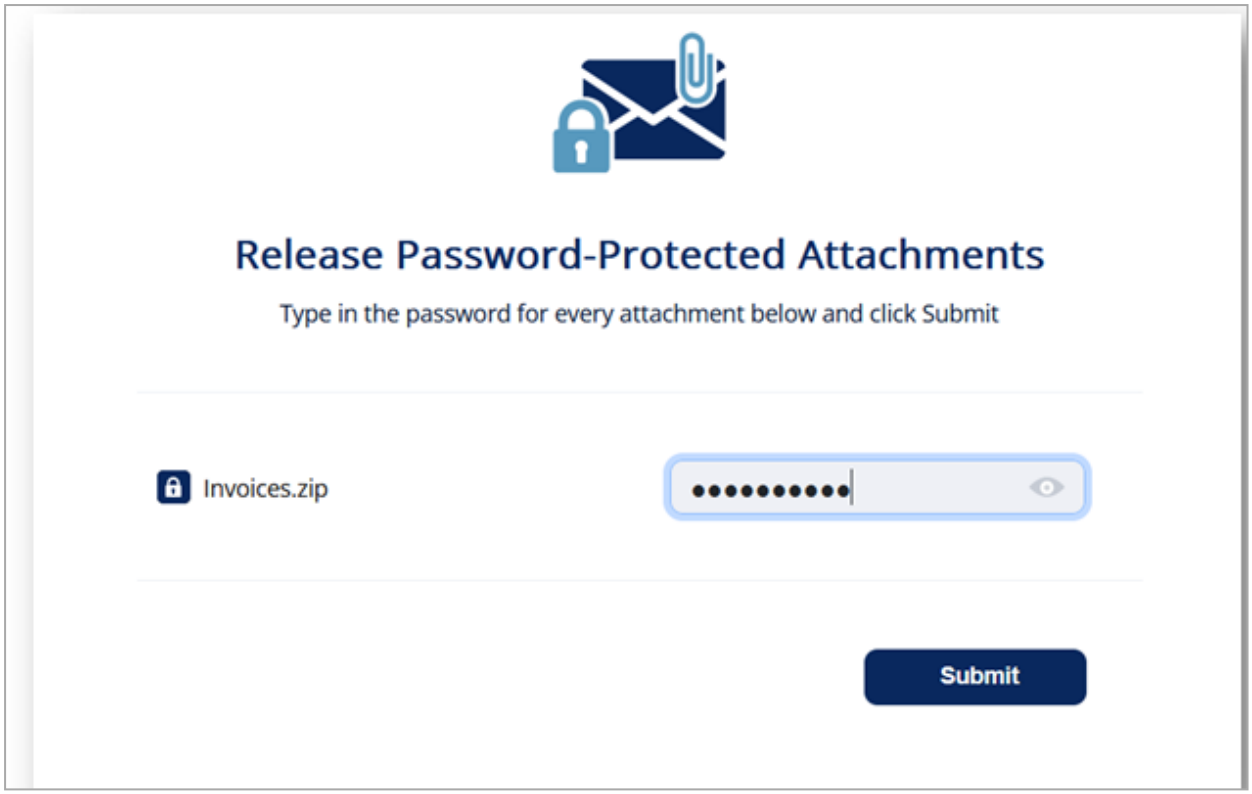
To secure sensitive data transmitted via email or other file-sharing methods, your organization uses Avanan with password-protected attachments, adding an extra layer of protection against unauthorized access and data breaches.


**To restore the password protected attachments :**

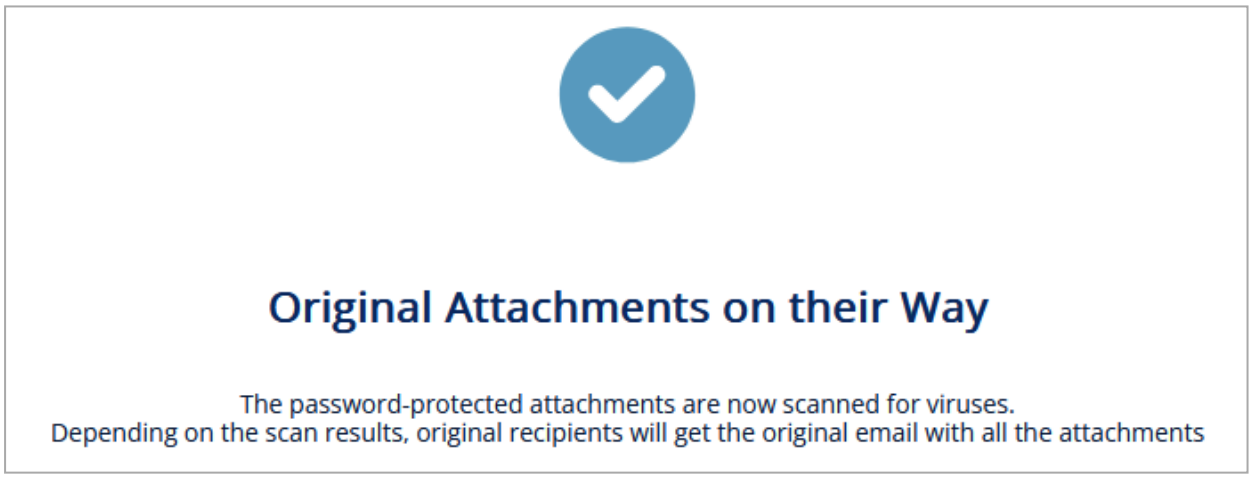
1. Click the link in the warning banner of the email.




2. Enter the password for the attachment and click **Submit**.

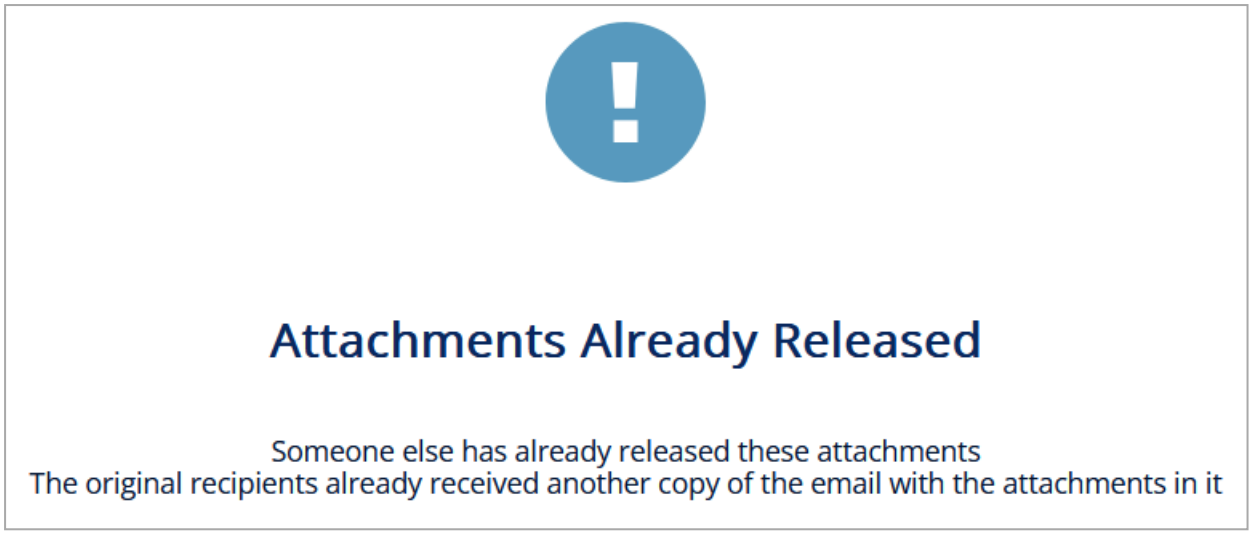



After you submit, the Anti-Malware engine scans the attachment for malicious content.



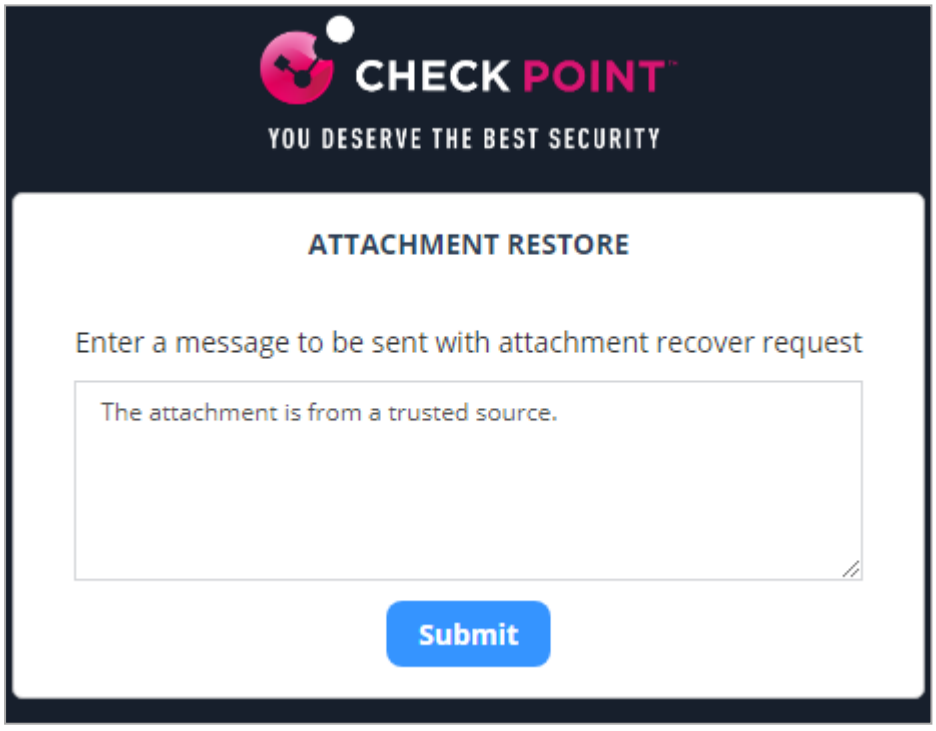

If the Anti-Malware engine finds the attachment as clean, the original email with password-protected attachment gets delivered to the original recipients of the email.

If the email was already released, this message appears:

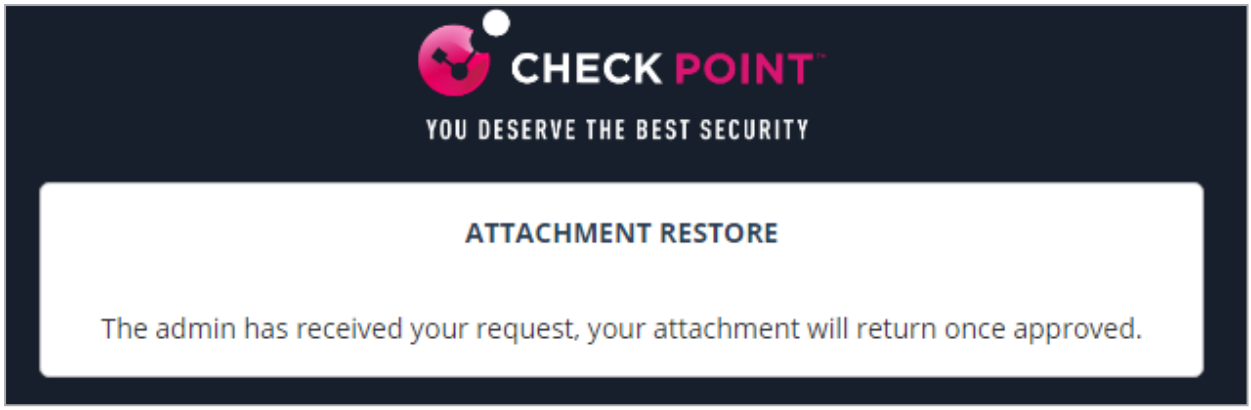



**To restore the email and its attachments :**

1. Click the link provided in the email.
2. If prompted, enter the reason for restoring the attachment, and click **Submit**.




After you submit, the admin receives the request.




After the admin approves, the user receives the original email.

# Attachment Cleaning

To help keep your inbox safe, your organization may apply an Attachment Cleaning policy to your email attachments. This process reduces security risks by removing harmful content before the files are delivered to you.

## Why Attachments Get Cleaned

Email attachments can sometimes include hidden threats, such as:

- **Macros**: Small programs that can execute harmful code.
- **Embedded Content**: Scripts or objects that may carry malware.
- **Links**: URLs that might lead to phishing sites or unsafe downloads of malicious files.

## What Happens to Your Files

Depending on your organization's security settings, files are processed in one of two ways:

- **Cleaned**:
  - Risky elements (like macros or scripts) are removed.
  - The file type remains unchanged (for example, a Word document stays a Word document).

  Example: A DOC file with macros is cleaned to a DOC file without any macros or embedded content.
- **Converted to PDF**:
  - The file is converted into a PDF and removes active content.
  - The PDF is safer to open but may lose certain features (like clickable links).

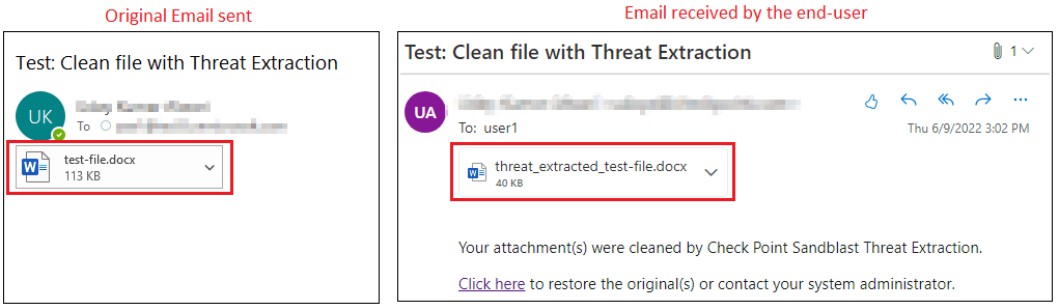
  Example: An Excel file with embedded links becomes a simple PDF without clickable content.

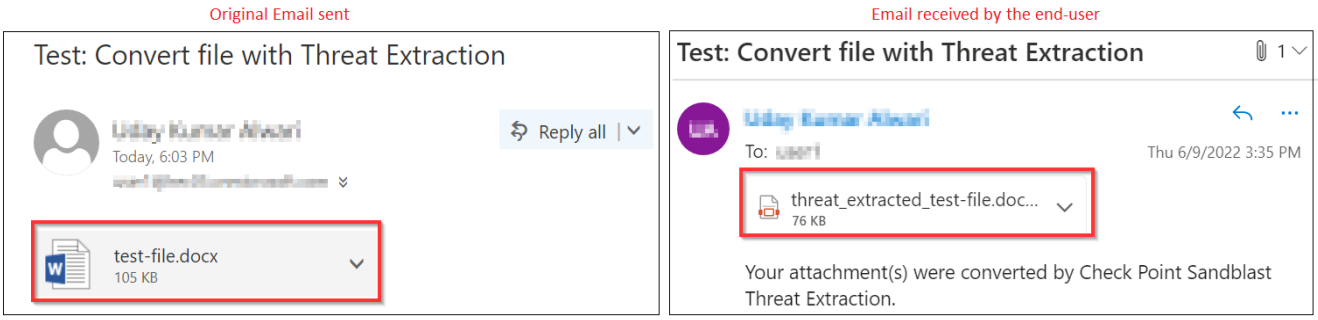
## What You Need to Do

Nothing—this happens automatically! If a file looks different (for example, missing links or buttons), it's due to the security process.

**Note** - Depending on your organization's policy, you may be able to request the original version of a cleaned file if necessary.

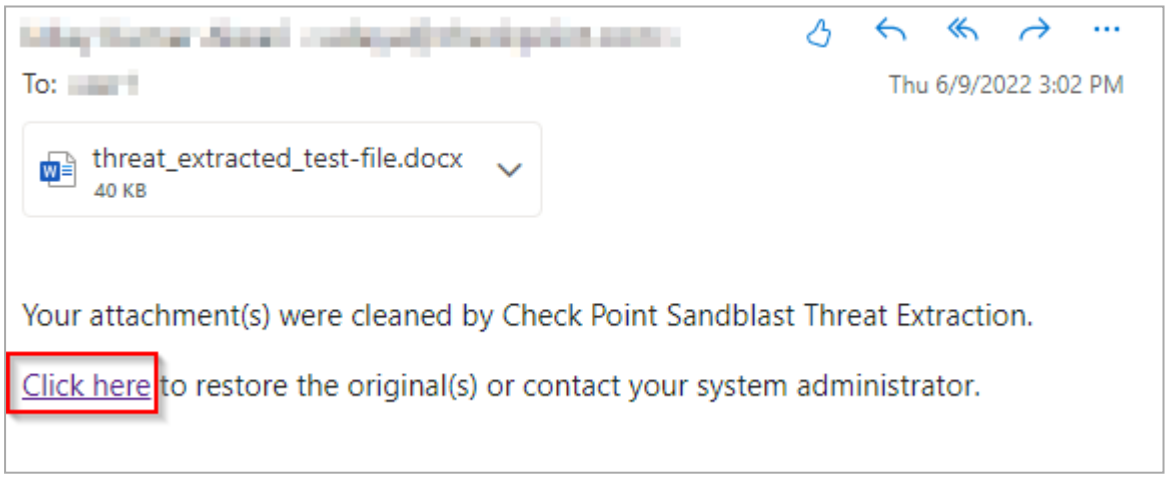
# User Experience for Attachment Cleaning




### To request to restore the original email:

1. Click the link below the attachment in the email.




2. If prompted, enter the reason for restoring the attachment, and click **Submit**.

   After you submit, the administrator receives the request.

   After the administrator approves the request, the system delivers the original email to mailbox.

3. If the is configured such that it does not require administrator's approval to restore the attachment, the original email is delivered to the user immediately.

# Click-Time Protection

Click-Time Protection is a proactive security measure that replaces links in email bodies and attachments with secure, inspected URLs. When you click a link, the destination website is dynamically inspected to ensure it is not a phishing site.

Avanan secures emails by replacing URLs in emails and their attachments with protected links, based on the organization's security policies.

## What Happens to URLs

- All URLs in emails and attachments are rewritten with a protected link.
- The rewritten URL displays a tool-tip with the original link, indicating the protection.
- Tool-tips are formatted for platforms like Microsoft Outlook for Mac and Outlook Web Access.
- On some clients, like Outlook for Windows, the raw rewritten URL may be shown instead of the tool-tip.

## Why Links Are Rewritten

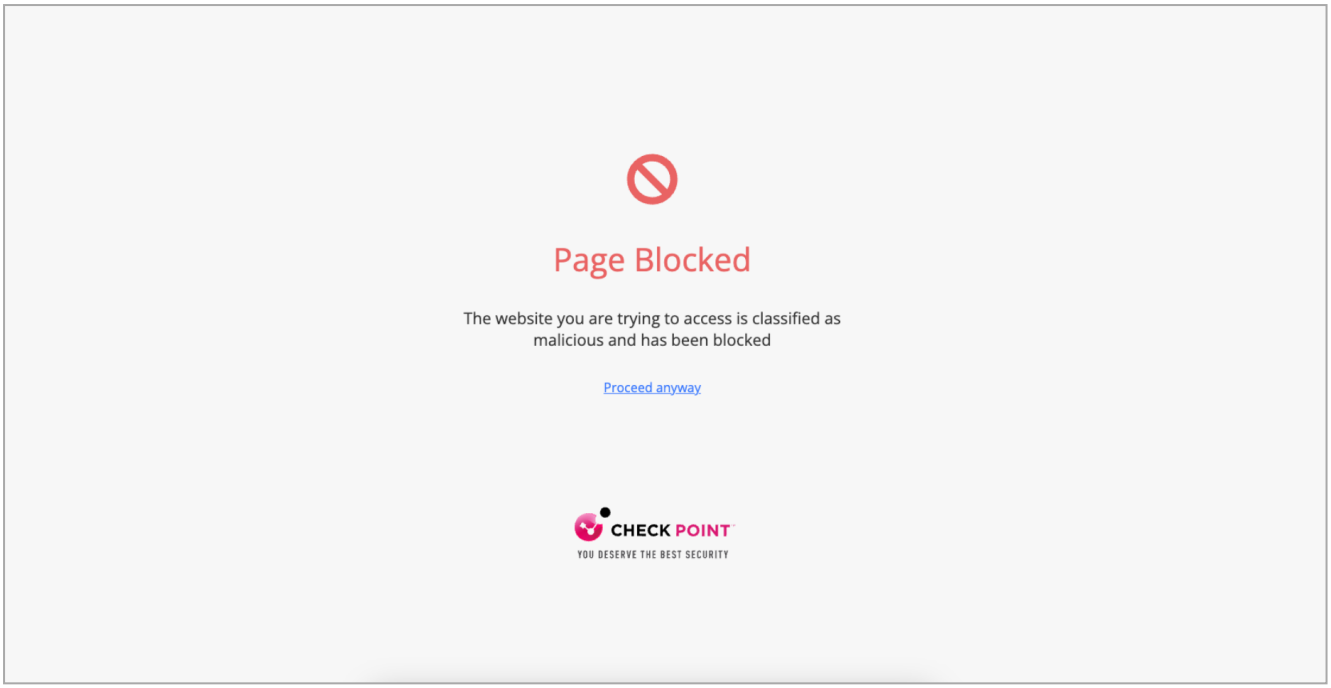
Rewriting links ensures that:

- Every click is checked for security in real time.
- Malicious links are intercepted before reaching the destination.
- Users are notified if a link or file poses a security risk.

### Clicks on Malicious Websites

When click on the URL of a website, Avanan checks the target URL.

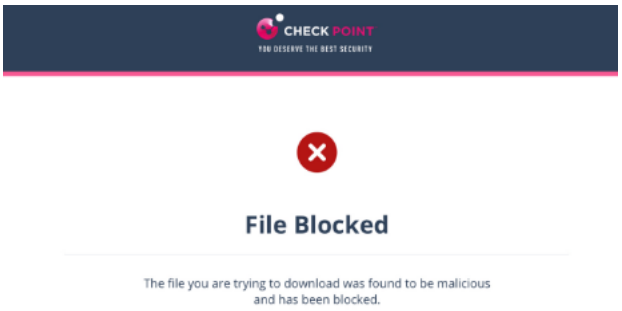
- If the URL is not found to be malicious, will be redirected to the original URL.
- If the URL is found to be malicious, will be forwarded to a warning page.
    - If the workflow for malicious URLs is to , an additional **Proceed anyway** link will be available in the warning page.



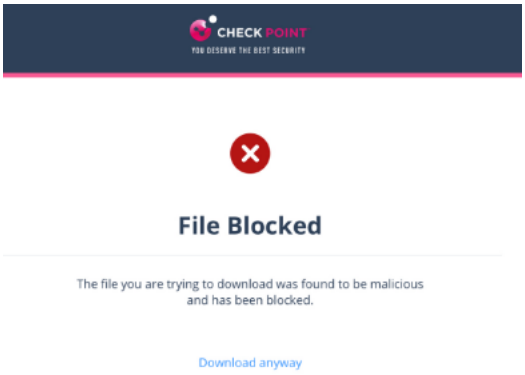

# Clicks on Direct Download Links - User Experience

When clicks a direct download link, the Anti-Malware security engine emulates the file.

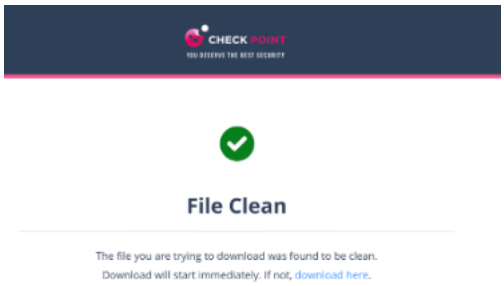
- If the file is detected as malicious:
  - If the configured workflow is , it blocks the file and shows the warning page.



- If the configured workflow is , it blocks the file and shows the warning page. However, the user can click **Download anyway** to download the file.

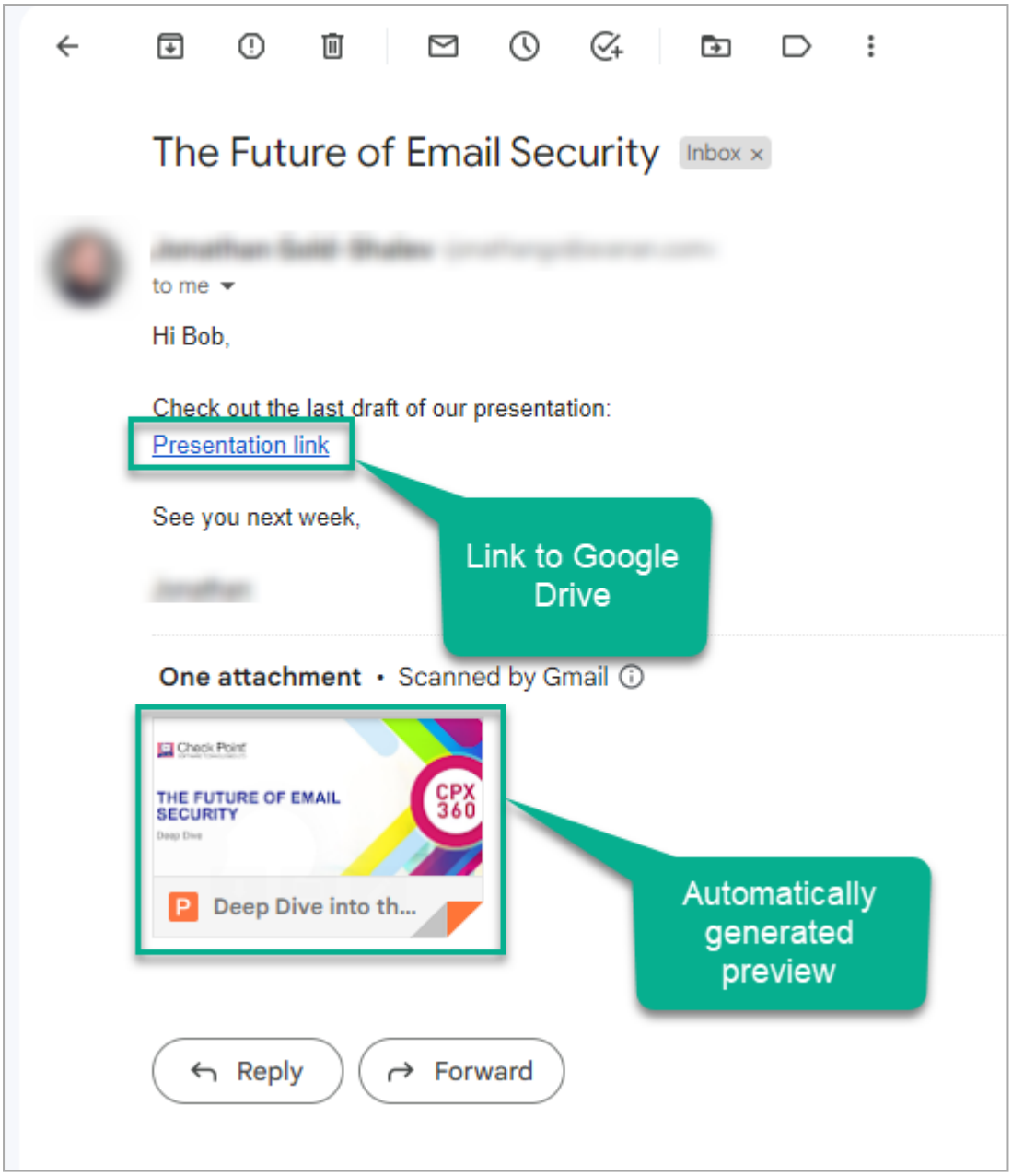



- If the file is detected as clean, it shows the notification and downloads the file.




# Google Drive Preview Links

By default, in the Gmail interface, when there is a link to a file in Google Drive, the email shows the file preview as if it was attached to the email.

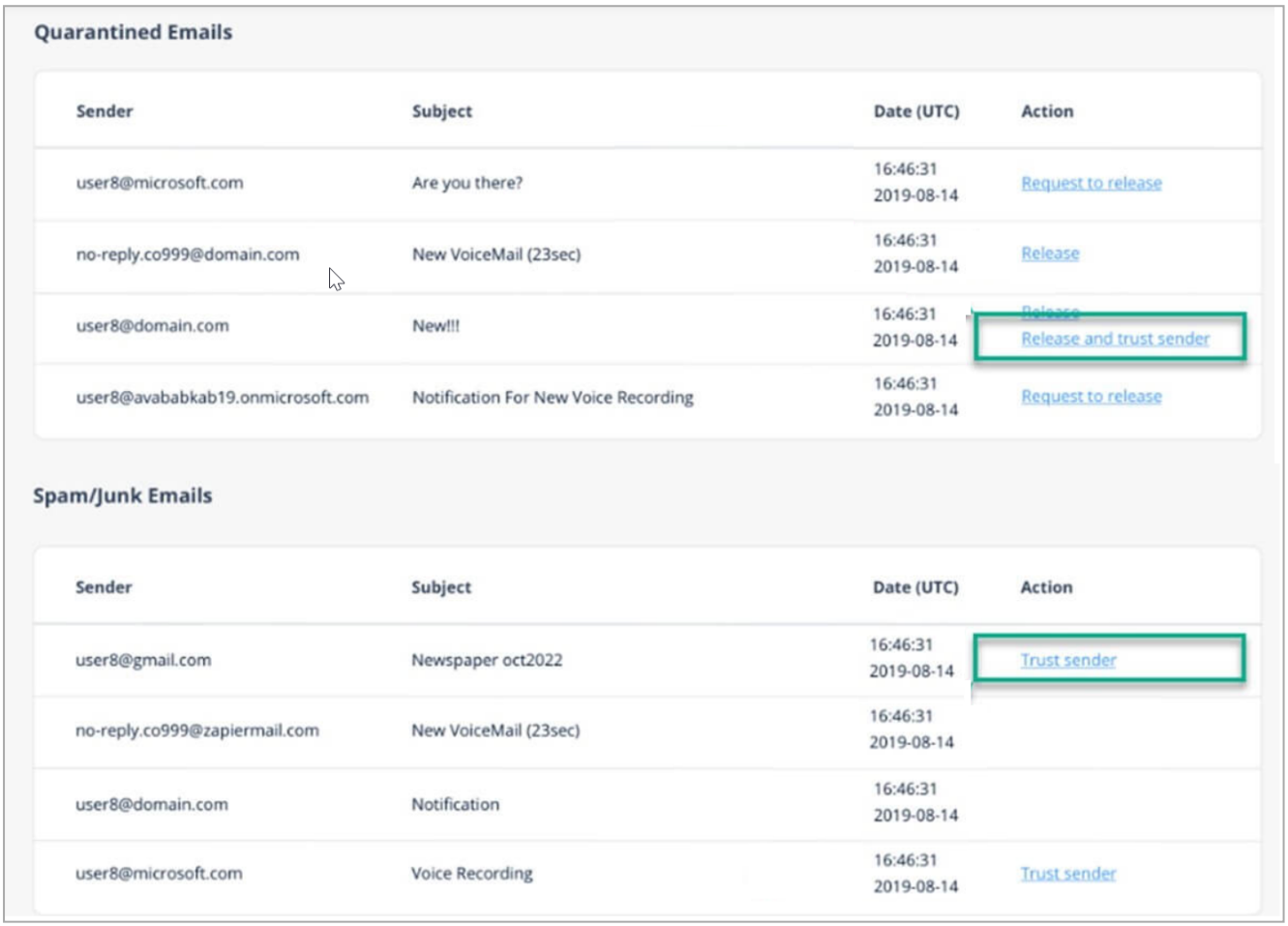



But, when Avanan rewrites the link, the system does not show the file preview.

# Trusting Senders

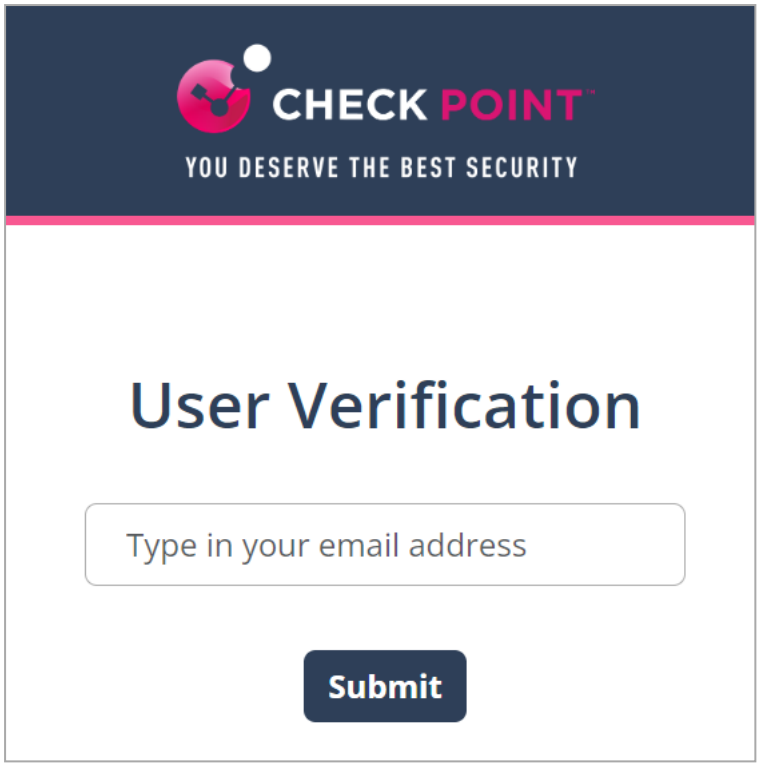
When spam is detected in emails and the Anti-Phishing engine marks an email as spam, it will be moved to the Spam or Junk Email folder by Office 365, based on the configured Mail Flow rules and actions.

## How to Trust a Sender

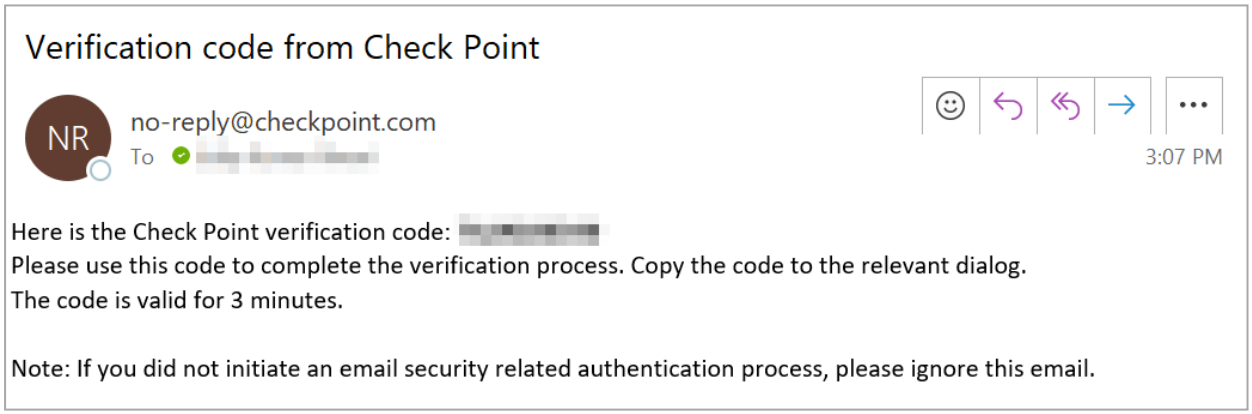



**To trust a sender or domain:**

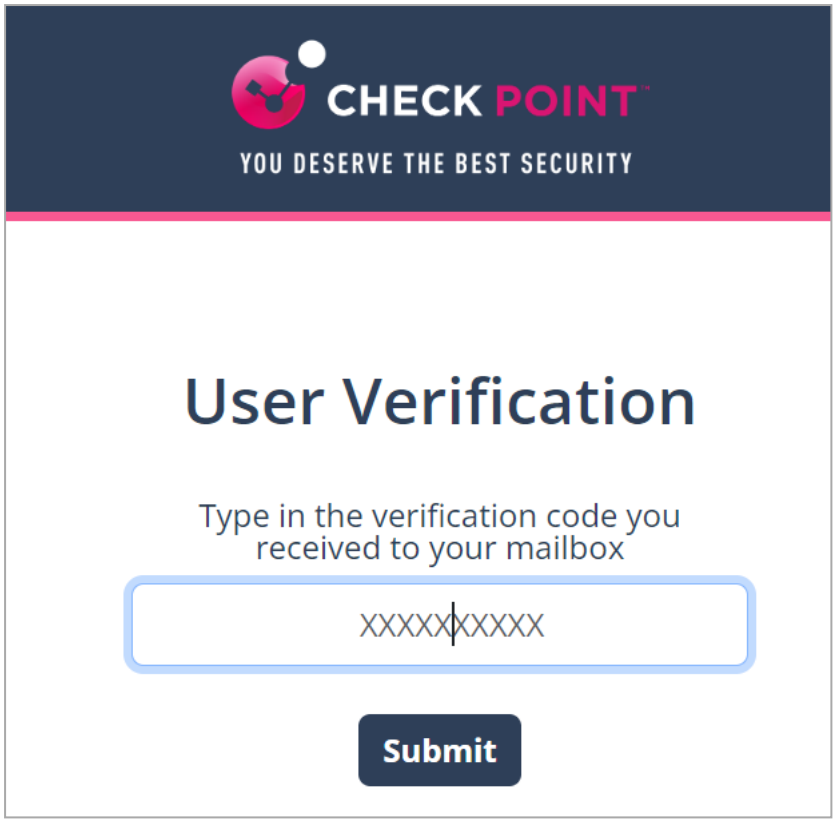
1. Click **Trust sender** in the .
2. Enter your email address and click **Submit**.



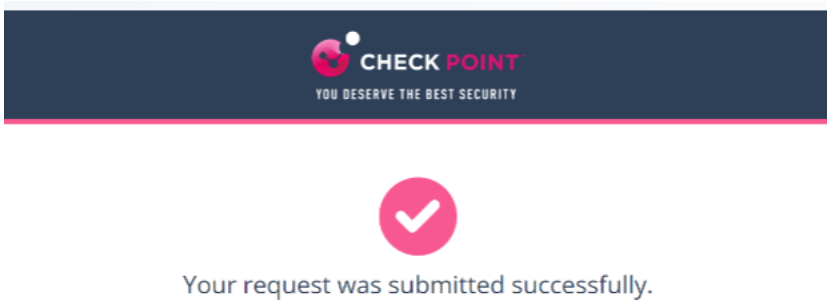

The system sends an email notification with a verification code.




Enter the verification code received from the email and click **Submit**.




After successful verification, the system shows the status.




Once an administrator approves the request, the system adds the sender to the trusted senders list.

# Graymail

Graymails are legitimate but often unwanted emails, such as newsletters and promotional emails, which many users find unnecessary, making it harder to find important messages.

The Graymail workflow moves these unwanted emails to a dedicated folder in the user's mailbox, ensuring a well-maintained inbox and enhancing productivity.

The system creates a **Deliver promotional emails to a dedicated folder** rule in the user's mailbox and delivers promotional emails to the dedicated folder. Graymails are then routed to this dedicated folder.

# Data Loss Prevention (DLP)

## Overview

Data Loss Prevention (DLP) helps prevent data breaches and unauthorized sharing by scanning content based on policies set by your administrator. DLP can scan emails, attachments, shared files, and text messages. It also uses Optical Character Recognition (OCR) to extract and analyze text from images.

The system detects potentially sensitive information such as:

- Credit card numbers
- Social Security Numbers (SSNs)
- Bank routing numbers
- Data protected under HIPAA

## Impact of DLP Policies on You

### Emails (Office 365 Mail and Google Gmail)

If your organization's policy is configured to detect sensitive information in emails:

- The system may block the email from being sent.
- You will receive a notification explaining why the email was blocked.

### File Sharing Applications (Office 365 OneDrive, SharePoint)

If your administrator has enabled DLP for file uploads:

- The system may block uploads that contain sensitive content.
- You will receive a notification explaining the reason for the block.

### Messaging (Microsoft Teams)

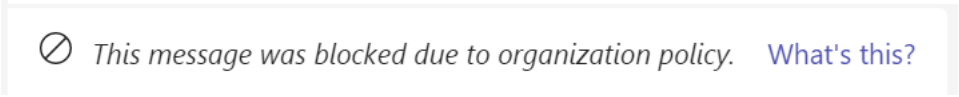
If your organization's policy includes scanning messages for sensitive content:

- The message will be blocked if sensitive data is detected.
- Both the sender and recipient will see a tombstoned message indicating the content was blocked due to the organization's policy.

# Example Scenario

Let's say your organization has a DLP policy that prohibits sharing credit card information.

- Sender's Experience:
  - You send a message in Microsoft Teams containing credit card details. The message is blocked, and you receive a tombstoned message stating the content was blocked due to policy.


- Recipient's Experience:
  - The recipient sees a tombstoned message with the same notification, ensuring sensitive content is not shared.
  - 

# Smart Banners

## Overview

**Smart Banners** are labels added to safe incoming emails to help you stay alert and follow security best practices. They serve the following purposes:

- **Identify suspicious emails** – Highlight external, unverified, or potentially fraudulent messages.
- **Make you cyber-aware** – Draw your attention to suspicious elements that, combined with your own judgment, may reveal a malicious email.
- **Remind you to follow company policy** – Prompt you to follow specific guidelines, such as handling invoices or billing change requests appropriately.

## Supported Smart Banners

Avanan supports these **Smart Banners**:

| Category | Smart Banner Name | Description |
|---|---|---|
| Business email compromise | Sender resembles a real contact | Email from a sender that resembles but is not identical to a contact the recipient is corresponding with. |
| | Request to update payment details [1] | Email that resembles a request from vendors to change their payment details. |
| | Invoice from a new vendor [1] | Email with an invoice from a vendor that never contacted before. |
| | Payroll information update request [1] | Emails from external senders requesting to update their payroll information. |
| Financial transaction requests | Emails with Invoices / POs [1] | Email that contains a request for payment in the form of invoice or purchase order. |
| | Payment request via payment service | Email that contains a payment request received via accounts in payment services. |

| Category | Smart Banner Name | Description |
|---|---|---|
| Avoiding inspection | Emails with links to restricted resources | Email with links to resources with restricted access, possibly in order to avoid inspection. |
| | Emails that appear to be from an e-sign service [6] | Emails that contains a link to an e-sign document, possibly in order to avoid inspection. |
| Fundamentals | Sender name different than address | Email from sender with a name that is significantly different from the email address which may indicate an impersonation attempt. |
| | Reply-to domain recently created and its address is different than the sender's | Email with reply-to address different from sender address and whose reply-to domain is created recently. |
| | Sender domain created recently [2] | Email whose sender domain was created recently. |
| | Sender SPF failed | Email that failed SPF checks. |
| | Incoming emails from external senders | Email from an external sender (outside the organization). |
| Impersonation | First-time sender to recipient [3,4,5] | Email from a sender that never sent an email to the recipient before. |
| | First-time sender to recipient domain [4,5] | Email from a sender that never exchanged an email with the recipient domain before. |
| | Sender resembles a person within the organization | Emails from a first-time sender whose display name is identical to a person within the organization. |

[1] These banners apply only to emails written in English.

[2] This banner will be applied to emails only if the sender's domain was created in the last 100 days.

[3] The First-time sender banner will not be applied to the recipient's emails after 24 hours from the sender's first email.

[4] If an email is sent to multiple recipients, the banner will be added only if the condition applies to all recipients.

[5] The banner will not be added if the sender domain regularly interacts in high volumes with other recipients from your domain. This exception does not apply to public domains. For example, *gmail.com*.

[6] If an email appears to reference an electronic signature and may contain links that cannot be inspected for phishing or viruses, ensure its authenticity before clicking any links or taking further action.

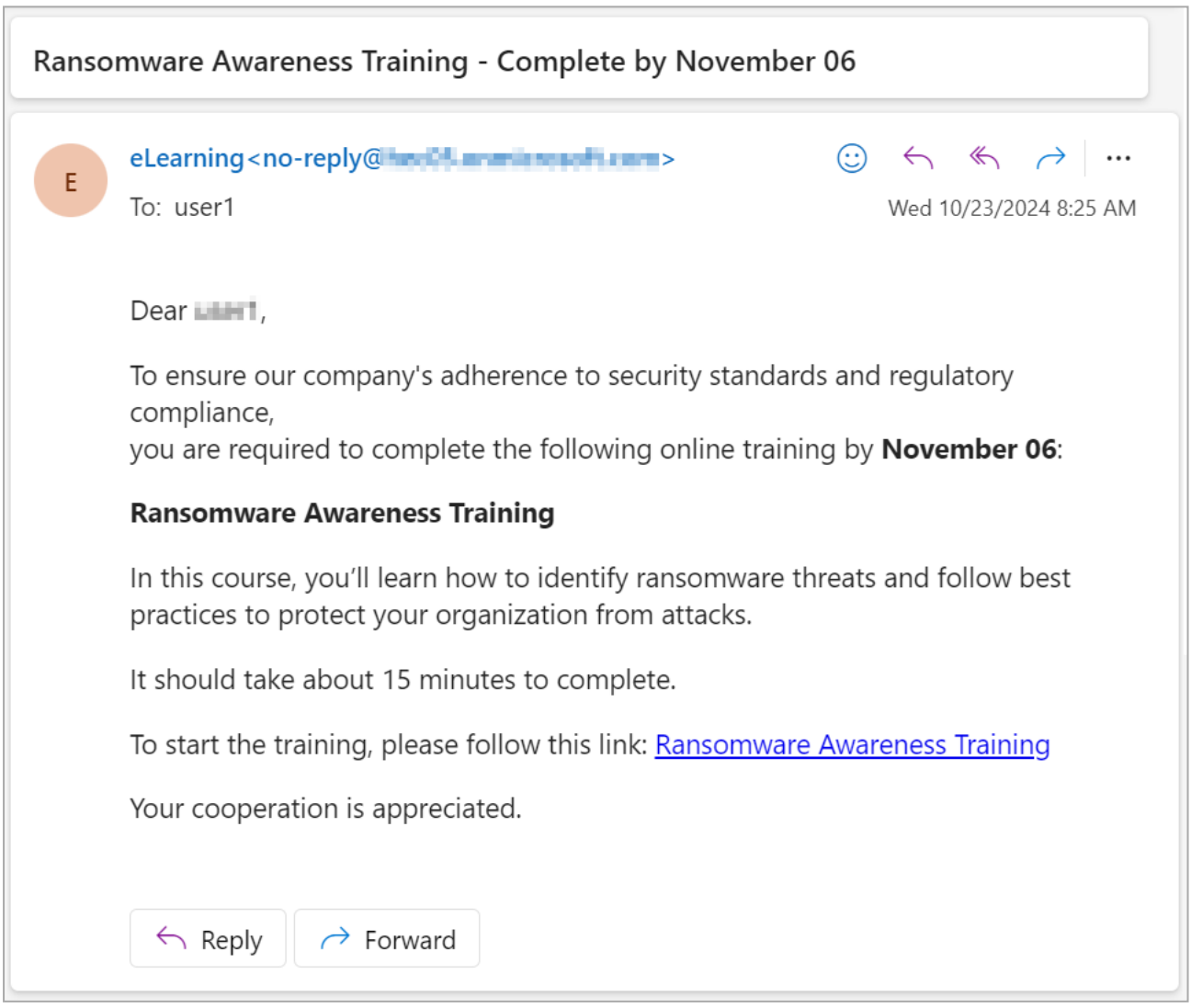
# Security Awareness Training

## Overview

The security awareness training is designed to help you understand key cybersecurity practices, recognize potential threats, and protect both your personal and organizational data. This training helps you learn how to stay safe online, spot suspicious emails or messages, and protect company and personal information. It also helps reduce the chances of mistakes that could lead to security issues.

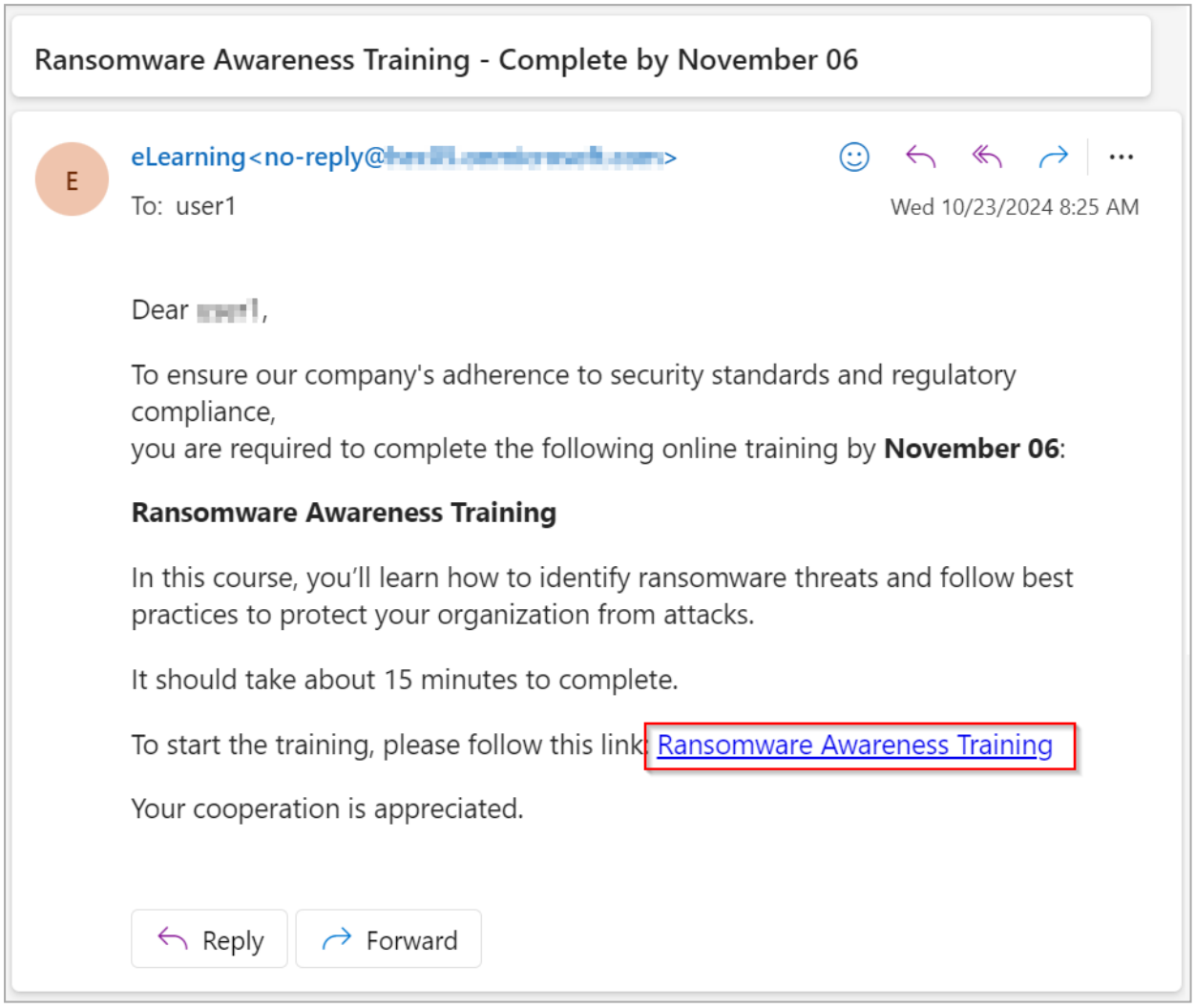
## Starting a Training Module

As per the security training policy configured by the administrator, emails with the necessary training details. The emails contain the training module name, duration, due date, and a link to access the training module.



**To start the training module:**

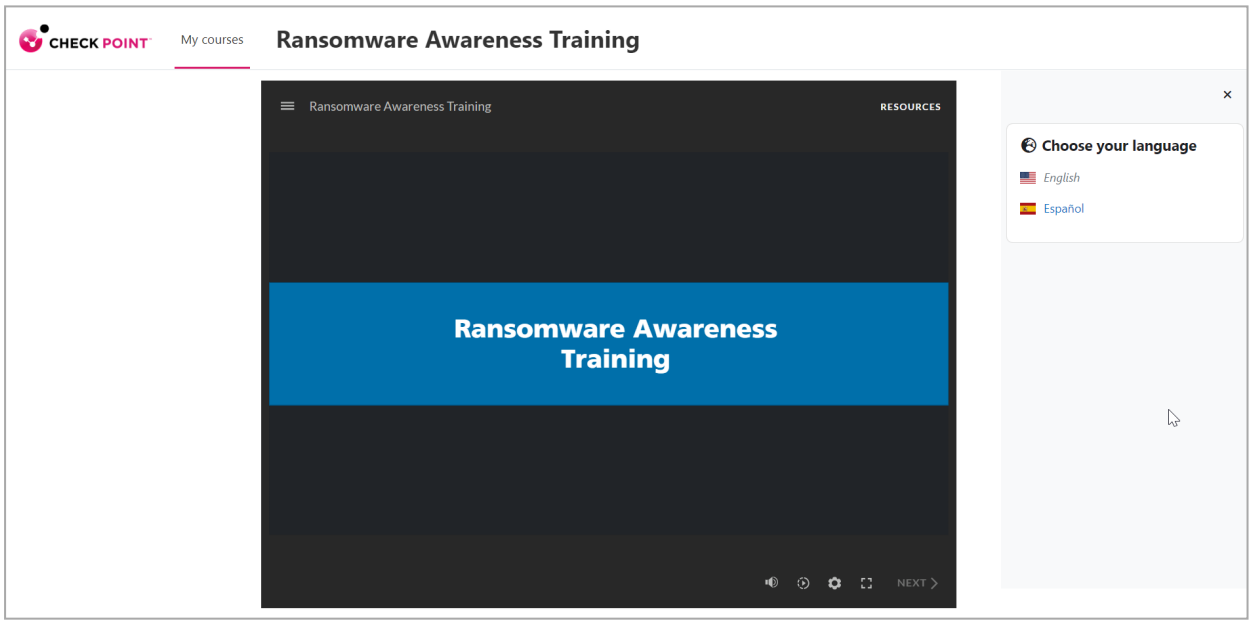
1. Click the link provided in the email.




The **Welcome to Security Awareness Training** page appears.


2. Click **Sign in with Microsoft**.
3. Enter your organization's Microsoft credentials and sign in.

   The training module page appears.




4. (Optional) If the training module is available in multiple languages, the **Choose your language** widget appears to the right of the screen. Select the required language.

**Note** - The system determines the user's language for phishing simulation emails and training modules based on Microsoft account attributes:

- **preferredLanguage**: If this attribute is set, the system uses it as the primary language (if supported).
- **usageLocation**: If **preferredLanguage** is not defined. By default, the system selects the primary language of the country specified in **usageLocation**.
  For more information about supported languages, see *Supported Languages for Phishing Simulations* and *Supported Languages for Training Modules*.

5. (Optional) To view the different sections in the training module, click the  icon.

   The **Menu** appears, displaying the different sections in the training module.

6. If required, click **Start** to begin the training.

The training includes a quiz with multiple questions to help understand the content. It also covers key use cases and provides strategies to protect against security threats.

# Check Point Copyright Notice