User-Reported Emails

https://campus.barracuda.com/doc/84313664/

> Some of the functionality described in this article – Creating an Incident from User-Reported Emails – is available only with Barracuda Email Protection Premium and Premium Plus plans. To upgrade to one of these plans, contact your Barracuda Networks Sales Representative.

You can view and create incidents based on emails that users report as suspicious. Be sure to read to the end of the article to learn about the ways that users can report the emails.

Viewing the User-Reported Emails Page

To view the **User-Reported Emails** page:

1. Open **Incident Response**, either from with Barracuda Control Center or by logging into https://forensics.barracudanetworks.com/.
2. From the menu, select **User-Reported Emails**.

Chart: Top 5 Reporters

This chart shows the five users in your organization who report the most emails as suspicious. You can use this chart to see their reporting records. At a glance, you can review whether the emails they are reporting actually require remediation. If there are fewer than five users in your organization who have reported emails, the chart shows all users who have reported suspicious emails.

Each bar of the chart can contain multiple segments. Hover over each segment to see the exact number of emails it contains.

- **Blue: Remediated** – These emails were potential threats that became the basis of new incidents.
- **Green: Dismissed** – The administrator determined these emails did not pose a threat and dismissed them.
- **Orange: Pending Review** – The administrator has not yet reviewed these items. The administrator will determine whether these emails must be remediated or if they can be dismissed.

Interpreting the Results

- Users with large blue sections on their bar chart are more accurate in their reporting of

suspicious emails. They are assets to your organization, helping to keep others safe.
- Users with large orange sections are reporting a lot of emails as suspicious, but many of these emails did not require remediation. You might choose to have these users learn more about common traits of suspicious emails, perhaps by reviewing videos included in Security Awareness Training.

Viewing an Incident from User-Reported Emails

To view an Incident from User-Reported Emails:

1. Open the **User-Reported Emails** page, as described above.
2. The table on the **User-Reported Emails** page displays information about suspicious emails that were reported by users, including:
   - **Last Reported Date** – The date the email was reported. If the same email was reported more than once, the most recent date it was reported.
   - **Users Reported** – How many unique users reported this email. Hover over this value to see the corresponding email address(es).
   - **Sender Email** – Email address for the sender of the suspicious email.
   - **Subject** – Subject of the suspicious email.
   - **Affected Mailboxes** – How many mailboxes in your organization also received this suspicious email.
3. Optionally, dismiss an incident because it appears to be innocuous. Click the **X** icon for that row of the table. That email item is removed from the table. To see user-reported email you have dismissed, click **Show Dismissed** above the table. To view **User-Reported Emails** again, click **Show Submitted**.

Creating an Incident from User-Reported Emails

This functionality is available only with Barracuda Email Protection Premium and Premium Plus plans. To upgrade to one of these plans, contact your Barracuda Networks Sales Representative.

When viewing incidents from User-Reported Emails, as described above, in Step 3, you can also choose to create an incident based on a user-reported email.

Click **Create Incident** for that email. Follow the incident creation wizard steps as described in Creating an Incident. The relevant information from the email you selected is automatically entered into the search screen of the wizard.

Barracuda Networks recommends:

- First remediating emails with a warning symbol ⚠, indicating a known threat.

- Prioritizing remediating emails that affect multiple mailboxes.

Sending Alerts for User-Reported Emails

You can configure the system to automatically send alerts to the security team when a user reports a suspicious email.

To create automatic alerts when a user reports a suspicious email:

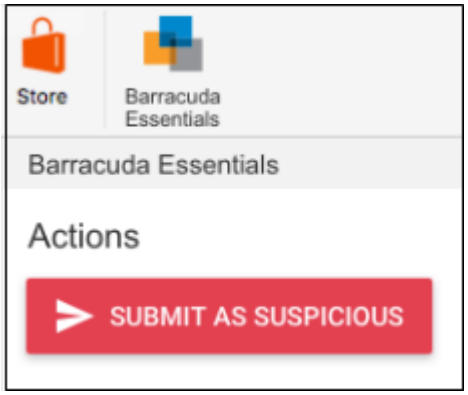
1. In the Menu, select **Settings**.
2. Specify that you want to send alerts to the security team.
3. Specify whether you want to use the same email address for the security team members that you alert for other messages.
   If you choose to use the same email address, it will autofill for you. Otherwise, an email address to receive these alerts.

How Users Report Suspicious Emails

Users reporting email as suspicious must have the Microsoft REST API enabled. Without the Microsoft REST API enabled, any emails that user might report will not appear in the **User-Reported Emails** page of Barracuda Forensics and Incident Response.

From the Barracuda Outlook Add-In

Within the Barracuda Outlook Add-In, users can report suspicious emails, as shown below. This allows end users to be active participants in reporting phishing and spear-phishing emails. These reports go to Barracuda Central and Incident Response. Administrators of Incident Response can investigate these end-user reported emails, create incidents, and take corrective action.



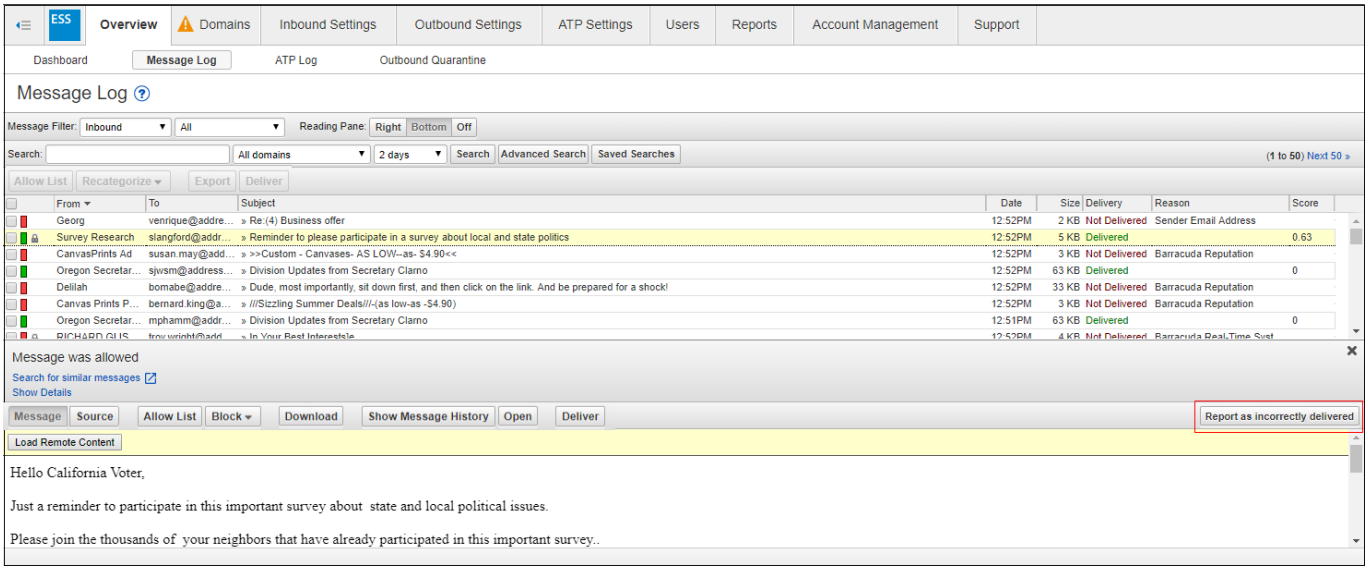
For more information, refer to Barracuda Essentials for Email Security Outlook Add-In.

From the Email Gateway Defense Message Log

> Note that you must activate Email Gateway Defense to use this functionality.

Administrators reviewing message logs within Email Gateway Defense might notice that there is suspicious email. Messages marked as Incorrectly Delivered are reported both to Barracuda Central and to Incident Response where they can be investigated.

To report email as incorrectly delivered, select a message in the Message Log and click **Report as Incorrectly Delivered** above the message preview.



For more information, refer to Understanding the Message Log in the Email Gateway Defense documentation.

Figures