

## Investigating Inbox Rules

<https://campus.barracuda.com/doc/79466439/>

A hacker taking over accounts might create inbox rules to cover their tracks. Rules that might signify an account takeover include rules that:

- delete emails that the hacker has sent
- delete reply emails sent to a hacker account
- automatically forward emails to external addresses

Inbox rules are only monitored for accounts with paid licenses. Free or student account mailbox rules are not monitored.

You can investigate inbox rules recently changed in your Microsoft 365 accounts to see if there is anything unusual.

### For a Specific Email or Account

To investigate inbox rules for a specific email or Microsoft 365 account:

1. Log into Impersonation Protection at <https://sentinel.barracudanetworks.com/signin>.
2. Click the menu button in the top left corner and select **Account Takeover Protection**. Then select the **Inbox Rules** tab.
3. In the **Investigate Mailbox** section, click the **Name or email of account** field and select the desired name.
4. Click **View Inbox Rules** to see the inbox rules associated with that user or account. There, you can determine if anything looks suspicious and take appropriate actions.

### For Recently Changed Rules

The Inbox Rules Change Feed provides visibility across all of your accounts in your Microsoft 365 tenant, enabling you to identify suspicious rules across your entire environment in one place.

To investigate inbox rules that have recently changed:

1. Log into Impersonation Protection at <https://sentinel.barracudanetworks.com/signin>.
2. Click the menu button in the top left corner and select **Account Takeover Protection**. Then select the **Inbox Rules** tab.
3. Under **Inbox Rules Change Feed**, examine the list of rule changes. For details on a specific action, click **Investigate**. Determine if anything looks suspicious and take appropriate actions.



© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.