How to Create a Content Policy to Prevent Employee Impersonation

https://campus.barracuda.com/doc/95264664/

These instructions apply to customers not currently using Office 365. If you are using Office 365, contact your sales representative to discuss Barracuda Sentinel.

Employee impersonation is one of many sophisticated email threats organizations encounter. Employee impersonation attacks occur in many different ways, one of the most common being display name spoofing. Display name spoofing attacks attempt to deceive recipients by changing the display name of their email to impersonate an employee. These emails typically come from legitimate email accounts, such as Gmail or Yahoo, and do not contain any links or attachments. They are designed using social engineering.

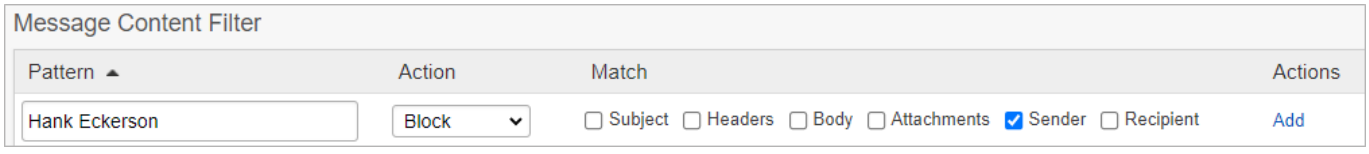
To protect against these attacks, you should use a combination of gateway defenses with an API based inbox defense, which uses AI to analyze historical email information to stop sophisticated email threats from reaching your users' inboxes, along with user awareness training. If you are unable to use inbox defense, you can create content policies at the gateway to block unwanted emails.

While content filtering is not foolproof, they do provide a greater level of control than that of unrestricted content.

To create a content policy:

1. Log into Barracuda Essentials and go to the **Inbound Settings > Content Policies** page.
2. Under **Message Content Filter** section, type in the name of the employee for the **Pattern**.
3. Select **Block** for the **Action**.
4. Select **Sender** for the **Match**.
5. Click **Add**.

For example, if you want to block display name spoofing attacks for your CEO "Hank Eckerson", your inbound content policy would be similar to this.



Note that these policies will block ALL inbound mail that contain that specific pattern. If an email is received from someone who has the same name, their mail will also be blocked. To allow an external email that has the same display name as a protected employee, you must

create an IP or sender based exemption.

Figures

© 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.