

Using Microsoft 365 Defender with Security Awareness Training

<https://campus.barracuda.com/doc/96013389/>

Note:

This article applies to organizations that do NOT use Email Gateway Defense (part of Barracuda Email Protection) or other non-Microsoft email protection product.

If you point your MX records directly at Microsoft 365 or turn on Microsoft's Secure By Default feature, be sure to follow the instructions in this article.

Background

Microsoft 365 Defender now includes Microsoft ZAP (Zero-hour purge), which scans emails for phishing content to protect email systems from potential phishing attacks. This includes legitimate, *simulated* phishing attacks used for training from Security Awareness Training and other providers. In addition, Microsoft 365 Defender no longer honors overrides for the Outlook Safe Senders list or IP Allow List (connection filtering). This article describes how to use Microsoft's Advanced Delivery Policy so you can successfully use Security Awareness Training along with Microsoft 365 Defender.

Using Microsoft 365 Defender, or Secure By Default, can result in:

- On the front end – Intended campaign email recipients do not receive phishing campaign messages. Instead, campaign emails are sent to the recipients' Junk folders or to a system mailbox for administrators.
- On the back end – Microsoft interrogates external links in campaign emails, resulting in clicks in the campaign. These are clicks made by a machine, not by human interaction, but are attributed to the email recipient. This skews your campaign results.

Following the instructions in the next section to achieve the following results, enabling Security Awareness Training to operate without interference from Microsoft 365 Defender. Links in this section lead to Microsoft documentation.

- Filters in [Exchange Online Protection \(EOP\)](#) and Microsoft Defender for Microsoft 365 allows messages to pass through.*
- [Safe sender lists in Exchange Online Protection \(EOP\)](#)*
- [Zero-hour Purge \(ZAP\)](#) for spam and phishing allows messages to pass through.*
- [Default system alerts](#) are not triggered for these scenarios.
- [Automated investigation and response \(AIR\) and clustering in Defender for Microsoft 365](#) ignores these campaign messages.
- Specifically for third-party phishing simulations:
 - [Admin submissions](#) generates an automatic response saying that the message is part of a

- phishing simulation campaign and isn't a real threat. Alerts and AIR will not be triggered.
- [Safe Links in Defender for Microsoft 365](#) does not block or detonate the specifically identified URLs in these messages.
 - [Safe Attachments in Defender for Microsoft 365](#) does not detonate attachments in these messages.

*Note that you cannot bypass malware filtering or ZAP for malware.

Configuring the Advanced Delivery Policy in Microsoft 365 Defender

These instructions are based on Microsoft's instructions, with information specific to Security Awareness Training added.

To configure the Advanced Delivery Policy in Microsoft 365 Defender:

1. Log into the Microsoft 365 Defender **Advanced Delivery** page (<https://security.microsoft.com/advanceddelivery>).
Once here, if you are logged in to Microsoft 365, but don't see the **Phishing simulation** tab, click on **Policies and Rules** in the navigation at top-left. You should have access to the elements on this page. If you see the message *You cannot access controls on this page*, contact your Microsoft 365 administrator.
2. On the **Advanced delivery** page, select the **Phishing simulation** tab, and then do one of the following:
 - First configuration (if there are no configured phishing simulations): Click **Add**.
 - Subsequent configurations (if there are configured phishing simulations present): Click **Edit**.
3. On the **Edit third-party phishing simulation** window that opens, configure the following settings:
Required to ensure addressees receive incoming campaign email:
 - **Sending Domains (Required):** The MAIL FROM address (also known as the RFC5321.MailFrom address, P1 sender, or envelope sender) is the email address used in the SMTP transmission of the message.
 - Expand this setting and enter at least one email address domain (e.g., example.com). Click inside the text box, enter a domain name, then press **Enter** or select the value displayed below the box. You can repeat this step as many times as necessary, to add up to 10 entries.
To determine the domain(s) to enter, look for the MAIL FROM address, P1 sender, or envelope sender you use in the SMTP transmission of a campaign message. This email address is typically recorded in the Return-Path header field in the message header. When setting up your Security Awareness Training email campaign, you selected this domain for the **Email Account for Sending** setting in the **Content** section of the campaign, as described in [Creating and Generating an Email Campaign](#).
 - **Sending IP (Required):** Expand this setting and enter the IP address range listed

below. Click inside the text box, enter a domain name, then press **Enter** or select the value displayed below the box. You can repeat this step as many times as necessary, to add up to 10 entries.

- 3.145.232.16/28


Note: There must be a match between at least one Sending domain and one Sending IP, but no association between values is maintained.

Required to ensure URLs present in simulation messages are not blocked:

- **Simulation URLs to allow (Optional):** Expand this setting and enter specific domains that are part of your phishing simulation campaign and should not be blocked or detonated. Click inside the text box, enter a domain name, then press **Enter** or select the value displayed below the box. You can repeat this step as many times as necessary, to add up to 10 entries.

Sample entry: `neverclick.net/*`

Tips for entries:

- *Do not* enter `http://` or `https://` at the beginning of the domain.
- *Do* end each domain with `/*`.
- If you are using a custom subdomain, specify it as part of the domain. Sample entry: `subdomain.neverclick.net/*`
- To remove an existing value, locate the value, then click Remove .

4. To complete the process:

- First configuration: Click **Add**, then click **Close**.
Subsequent configuration: Click **Save**, then click **Close**.

For additional information, refer to the following Barracuda Campus articles:

- [Understanding Clicks](#) for information on machine clicks.
- [Email Allow List and Best Practices](#) for information on allowing emails and IPs when working with Security Awareness Training campaigns.

For more information on Microsoft 365 Defender, refer to the following Microsoft articles:

- [Configure the delivery of third-party phishing simulations to users and unfiltered messages to SecOps mailboxes](#)
- [Zero-hour auto purge \(ZAP\) in Exchange Online](#)
- [Microsoft 365 Defender](#)

Figures

1. MSremove.png

© 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.