

[Home < https://easydmarc.com/>](https://easydmarc.com/)

[Knowledge Base <](#)

[https://easydmarc.com/blog/category/knowledge-base/>](https://easydmarc.com/blog/category/knowledge-base/)

[Source Configuration <](#)

[https://easydmarc.com/blog/category/knowledge-base/source-configuration/>](https://easydmarc.com/blog/category/knowledge-base/source-configuration/)

Exciting News! Microsoft Now Fully Respects DMARC Policy as Anticipated

Exciting News! Microsoft Now Fully Respects DMARC Policy as Anticipated

Published on: July 19, 2023

3 Min Read

Last Modified on: May 7, 2025



Microsoft and DMARC

SPF and DKIM Setup:

Step by Step



Recently, Microsoft made significant changes to their DMARC policy handling, which is of utmost importance.

For your information, DMARC is a standard designed to prevent spoofing by verifying the identity of email senders. If an email fails **DMARC validation** <<https://easydmarc.com/tools/dmarc-lookup>> , it raises suspicions that the sender may not be genuine, potentially indicating fraudulent content. The 'p=' value within a DMARC record indicates the sender's policy for their domain, dictating the receiver's actions when an email fails DMARC validation. The policy can have three values: none, quarantine, and reject. The DMARC "reject" policy (p=reject) is the strictest level of the policy, and it instructs the receiver to outright reject any emails that fail the DMARC check.

Previously, Microsoft was not adhering to DMARC policies as expected, allowing emails that failed DMARC checks to bypass rejections set in the DMARC policy 'p=reject.' Consequently, if users hadn't activated the rule to reject non-authenticated emails received from domains protected with a DMARC "reject" policy, they would still receive these non-authenticated emails instead of them being rejected.

Microsoft has recently made significant updates to their DMARC policy handling, impacting both consumer and enterprise customers. For their consumer services (live.com / outlook.com / hotmail.com), they have now aligned their DMARC policy handling with the sender's DMARC policy. This means that if an email fails DMARC validation and the sender's policy is set to p=reject, Microsoft will reject the email. This change aims to enhance email security and protect users from potentially fraudulent or spoofed emails.



For emails that fail DMARC validation with a reject policy and the corresponding action is taken on the message, the sender will receive a non-delivery report (NDR) containing the following message:

"550 5.7.509: Access denied, sending domain example.com does not pass DMARC verification and has a DMARC policy of reject".

Microsoft has introduced new flexibility for their Enterprise customers regarding the handling of emails that fail DMARC validation. Now, customers have the option to choose different actions based on the policy set by the domain owner, such as p=reject or p=quarantine.

To establish a new Anti-Phishing policy and ensure that you honor the DMARC policy as expected, kindly adhere to the following instructions:

Visit the Microsoft 365 Defender portal at https://security.microsoft.com <https://login.microsoftonline.com/common/oauth2/authorize?client_id=80ccca67-54bd-44ab-8625-4b79c4dc7775&response_type=code%20id_token&scope=openid%20profile&state=OpenIdConnect.AuthenticationProperties%3DobXbxlgLXS3lj qWtpvUhRhOZ5qwTQPg761fCZUMHyZ6Gm-7kSVibN4oZ3uqA--ivdm2HuWgJEeawCwRnsrYV2h-nu_GYkrGMAvFqVXKD8AhEfo6wzu_2wV5aNh1YTQhxLbIcQN3t-7Fe7II6pJfPEg&response_mode=form_post&nonce=638822416275284865.N2RiZDAwNDYtOGUxMC00ZDRiLTk2OWYtNTM4YTY4YjYwODMyMmE0Njl2NDktM2E2Ni00OTA0LWlONdctYWE3OTI5N2E0NTI5&client-request-id=8aeb6d40-a319-4e3d-b868-eea221c6a364&redirect_uri=https%3A%2F%2Fsecurity.microsoft.com%2F&claims=%7B%22id_token%22%3A%7B%22xms_cc%22%3A%7B%22values%22%3A%5B%22CP1%22%5D%7D%7D%7D&x-client-SKU=ID_NET472&x-client-ver=8.3.0.0> .

Navigate to "Email & Collaboration" > "Policies & Rules" > "Threat policies" > "Anti-phishing" within the "Policies" section.

If you prefer to access the Anti-phishing page directly, you can use the URL:

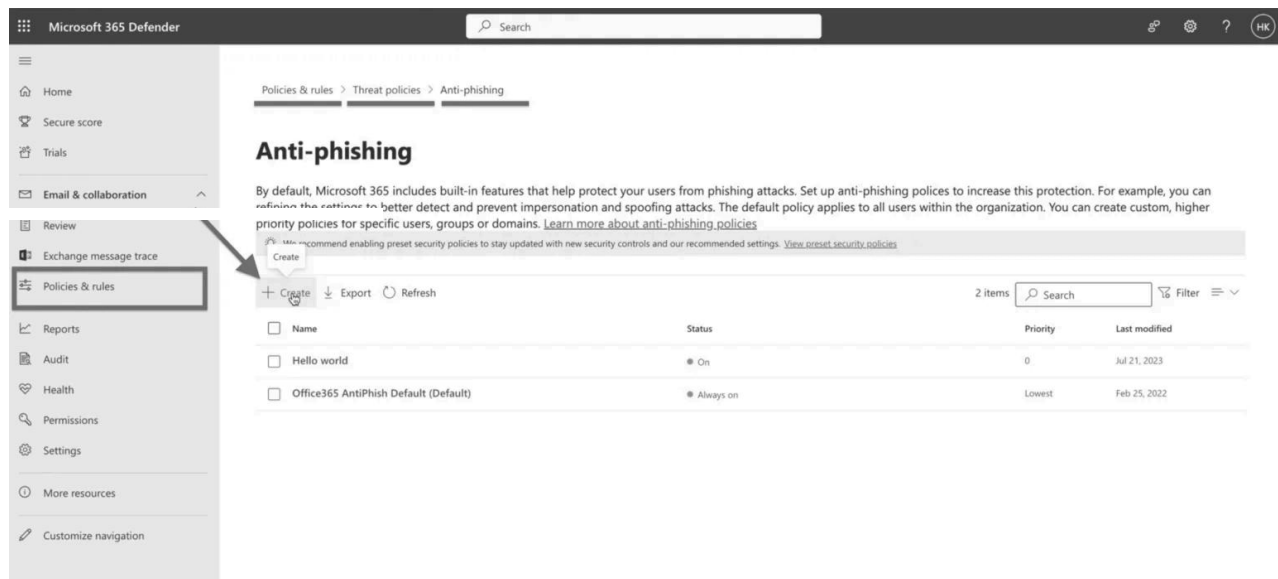
https://security.microsoft.com/antiphishing <
https://login.microsoftonline.com/common/oauth2/authorize?
client_id=80ccca67-54bd-44ab-8625-
4b79c4dc7775&response_type=code%20id_token&scope=openid%20pr
ofile&state=OpenIdConnect.AuthenticationProperties%3DLNdAXw1lQpH
-BOo0E53ba8TCICfvOvlh9G5v58PfgML8dTloMcwdSjmPH4--
fon7kuqML1d4yRFtM8fjA_HwgjbmOLl1phlawNu3h81t-UkYXUiJ_ONjSrg-
u_fJgsHtHi5ZQIALvNVhehhIYLn0FZO9P569WZfSQEbXz0XCiow&respons
e_mode=form_post&nonce=638822416702884373.N2lxNTUzZTgtNGU0
Zi00MWJhLWJkM2ltMWM1OGM0MTMxYjY5NzA5NjFiNGEtMWQyZC00
OTNiLTg2NmMtYjZiNmMwZjMyM2Nj&client-request-id=be0f53f4-1395-
4bbe-93e8-
3e2889679fff&redirect_uri=https%3A%2F%2Fsecurity.microsoft.com%
2F&claims=%7B%22id_token%22%3A%7B%22xms_cc%22%3A%7B%
22values%22%3A%5B%22CP1%22%5D%7D%7D%7D&x-client-
SKU=ID_NET472&x-client-ver=8.3.0.0> .

1. On the Anti-phishing page, select

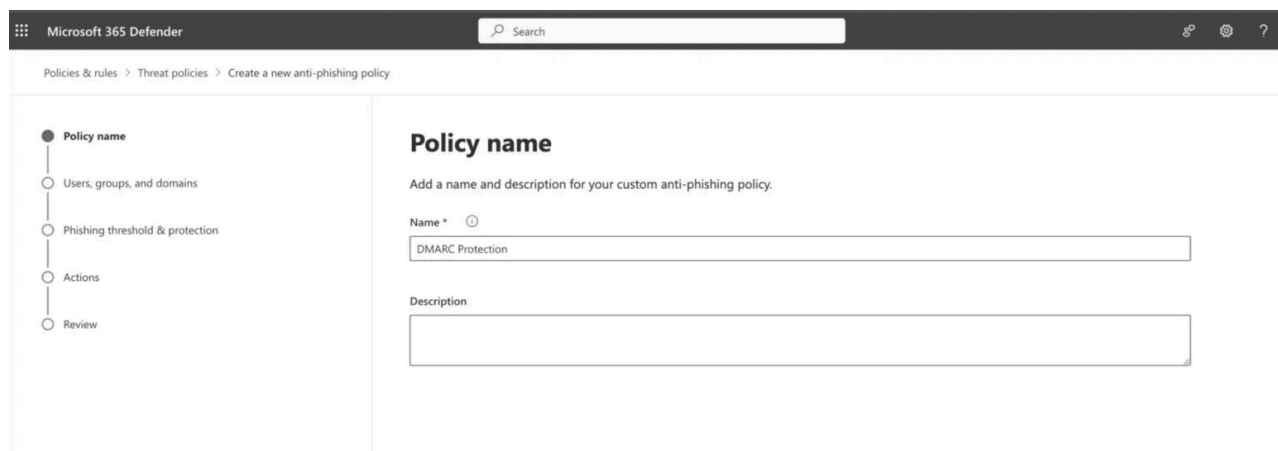


Create to open the new anti-phishing policy wizard.





2. On the "Policy name" page enter a unique, descriptive name for the policy and click "Next".



3. On the Users, groups, and domains page, mention the domain/s the policy applies to, and click on "Next."



Microsoft 365 Defender

Policies & rules > Threat policies > Create a new anti-phishing policy

Policy name

Users, groups, and domains

Phishing threshold & protection

Actions

Review

Users, groups, and domains

Add users, groups and domains to include or exclude in this policy.

Include these users, groups and domains *

Users

And

Groups

And

Domains

khatchoian.com

☐ Exclude these users, groups and domains

4. Ensure that "Enable Spoof Intelligence" is activated, then proceed by clicking "Next."

Microsoft 365 Defender

Policies & rules > Threat policies > Create a new anti-phishing policy

Policy name

Users, groups, and domains

Phishing threshold & protection

Actions

Review

Phishing threshold & protection

Set your phishing thresholds and desired impersonation and spoof protections for this policy. [Learn more](#)

Spoof

☒ **Enable spoof intelligence (Recommended)**

Choose how you want to filter email from senders who are spoofing domains. To control which senders are allowed to spoof your domains or external domains, use the [Tenant Allow/Block List Spoofing page](#). [Learn more about Spoof Intelligence](#)

5. Enable the option "Honor DMARC record policy when the message is identified as spoof."



The screenshot shows the 'Microsoft 365 Defender' interface. The breadcrumb trail is 'Policies & rules > Threat policies > Create a new anti-phishing policy'. On the left, a navigation pane lists steps: 'Policy name', 'Users, groups, and domains', 'Phishing threshold & protection', 'Actions' (highlighted), and 'Review'. The main content area is titled 'Actions' and contains the following text: 'Set what actions you'd like this policy to take on messages. You may need to turn on certain protections to access all available policy actions.' Below this, there are three conditional action settings, each with a dropdown menu highlighted by a red box: 1. 'If the message is detected as spoof and DMARC Policy is set as p=quarantine' with the action 'Quarantine the message'. 2. 'If the message is detected as spoof and DMARC Policy is set as p=reject' with the action 'Reject the message'. 3. 'If the message is detected as spoof by spoof intelligence' with the action 'Move the message to the recipients' Junk Email folders'. At the bottom, there is a section 'Safety tips & indicators' with three checkboxes: 'Show first contact safety tip (Recommended)' (unchecked), 'Show (?) for unauthenticated senders for spoof' (checked), and 'Show "via" tag' (checked).

- If the message is detected as spoof and DMARC Policy is set as p=quarantine, select **"Quarantine the message"**
- If the message is detected as spoof and DMARC Policy is set as p=reject, select **"Reject the message"**
- If the message is detected as spoof by spoof intelligence, select **"Move the message to the recipients' Junk Email folders"**

6. Finally, submit the policy.

