# Configuring Anti-phishing

Microsoft 365 Admin center – Security –Policies and rules – Threat Policies – Anti-phishing

## Policies

Anti-phishing

Protect users from phishing attacks, and configure safety tips on suspicious messages.

Anti-spam

Protect your organization's email from spam, including what actions to take if spam is detected



Protect your organization's email from malware, including what actions to take and who to notify if malware is deter-



Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams



Protect your users from opening and sharing malicious links in email messages and Office apps

#### Rules

Tenant Allow/Block Lists

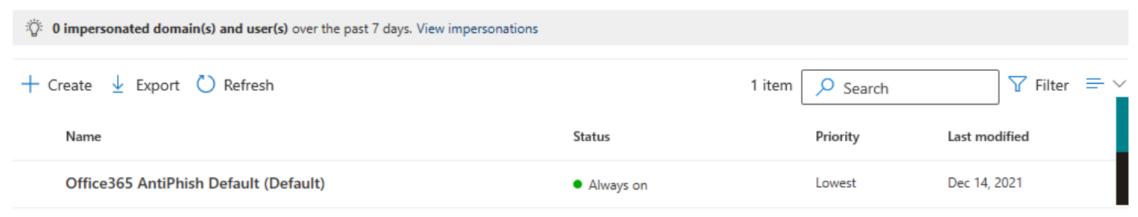
Manage allow or block entries for your organization.





Policies & rules > Threat policies > Anti-phishing

By default, Microsoft 365 includes built-in features that help protect your users from phishing attacks. Set up anti-phishing polices to increase this protection. For example, you can refining the settings to better detect and prevent impersonation and spoofing attacks. The default policy applies to all users within the organization. You can create custom, higher priority policies for specific users, groups or domains. Learn more about anti-phishing policies



#### Office365 AntiPhish Default (Default)

Always on | Priority Lowest | Tue Dec 14 2021

D	esc	rın	TI6	on
				•

\_

#### Phishing threshold & protection

#### Phishing threshold

1 - Standard

#### Impersonated user protection

Off - 0 sender(s) specified

#### Impersonated domain protection

- Off for owned domains
- Off 0 domain(s) specified

#### Trusted impersonated senders and domains

Off

#### Mailbox intelligence

On

#### Mailbox intelligence for impersonations

Off (Mailbox intelligence must be turned on to access this)

#### Spoof intelligence

On

# Edit protection settings Actions

If message is detected as an impersonated user

Don't apply any action

If message is detected as an impersonated domain

Don't apply any action

If Mailbox Intelligence detects an impersonated user

Don't apply any action

If message is detected as spoof

Move message to the recipients' Junk Email folders

First contact safety tip

Off

User impersonation safety tip

Off

Domain impersonation safety tip

Off

Unusual characters safety tip

Off

Unauthenticated senders symbol (?) for spoof

On

Show "via" tag

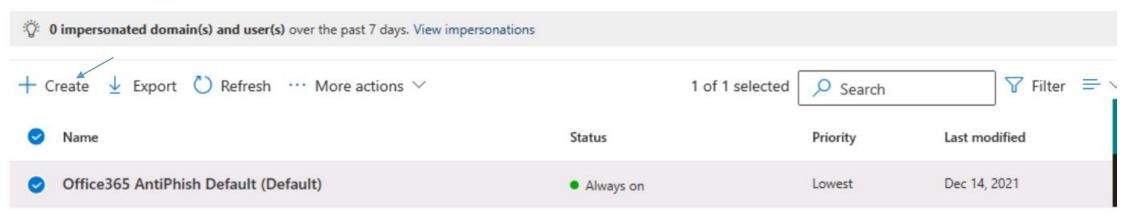
On

Edit actions

Close

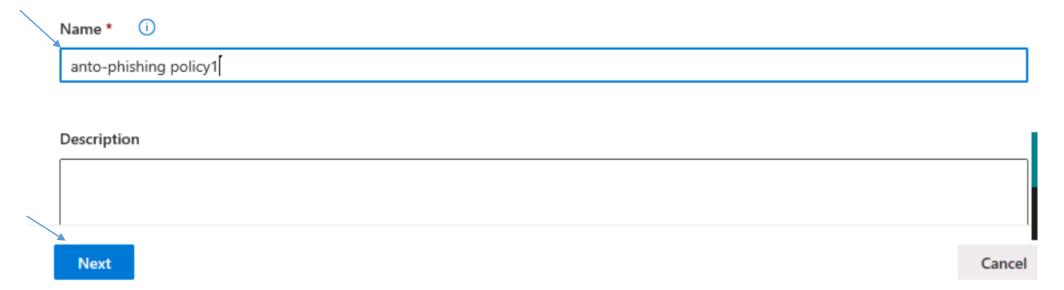
Home Policies & rules > Threat policies > Anti-phishing

By default, Microsoft 365 includes built-in features that help protect your users from phishing attacks. Set up anti-phishing polices to increase this protection. For example, you can refining the settings to better detect and prevent impersonation and spoofing attacks. The default policy applies to all users within the organization. You can create custom, higher priority policies for specific users, groups or domains. Learn more about anti-phishing policies



# **Policy name**

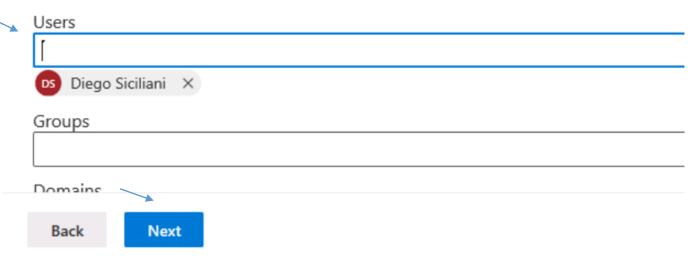
Add a name and description for your custom anti-phishing policy.

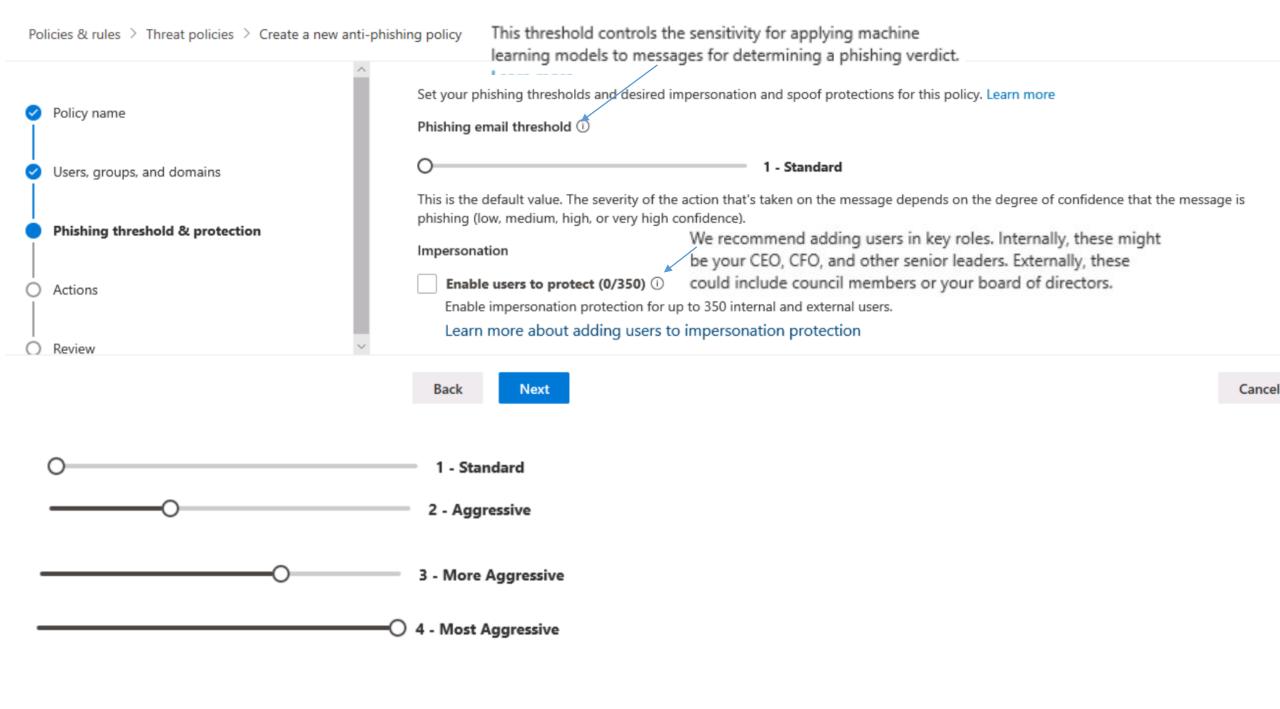


# Users, groups, and domains

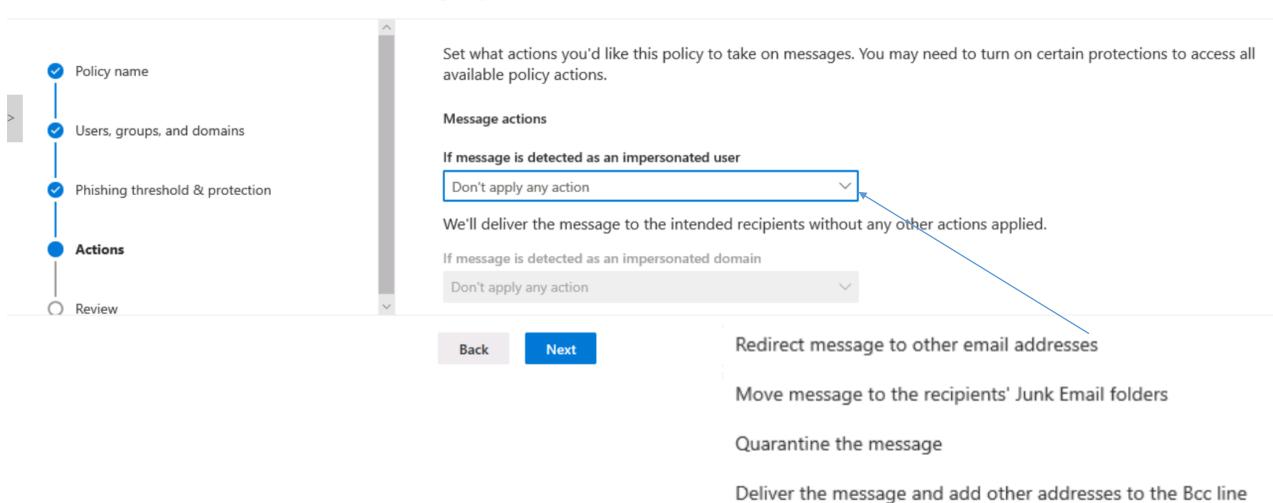
Add users, groups and domains to include or exclude in this policy.

#### Include these users, groups and domains





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



Don't apply any action

Delete the message before it's delivered

### Message actions If message is detected as an impersonated user Quarantine the message We'll quarantine the message for you to review and decide whether it should be released. Learn how to manage quarantined messages Apply quarantine policy DefaultFullAccessPolicy $\vee$ If message is detected as an impersonated domain Don't apply any action Next Back Cancel

If Mailbox Intelligence detects an impersonated user Don't apply any action If message is detected as spoof Move message to the recipients' Junk Email folders Move message to the recipients' Junk Email folders Quarantine the message Show first contact safety tip (Recommended) ① Show user impersonation safety tip ① Show user impersonation unusual characters safety tip ① Show (?) for unauthenticated senders for spoof ① Show "via" tag ① Next Back



### Review

Review your policy before creating it.

Policy name

anto-phishing policy1

Edit policy name

Users, groups, and domains

Included users

DiegoS@M365x29238024.OnMicrosoft.com

Edit users, groups, and domains

Phishing threshold and protections

Phishing threshold

4 - Most Aggressive

mpersonated user protection

On for 0 user(s)

mpersonated domain protection

- Off for owned domains
- Off 0 domain(s) specified

Trusted impersonated senders and domains

Off

Mailbox intelligence

On

Mailbox intelligence for impersonations

Off (Mailbox intelligence must be turned on to access this)

Spoof intelligence

On

Edit protection settings

Actions

If message is detected as an impersonated user

Quarantine the message DefaultFullAccessPolicy

If message is detected as an impersonated domain

Don't apply any action

If Mailbox Intelligence detects an impersonated user

Don't apply any action

If message is detected as spoof

Move message to the recipients' Junk Email folders

First contact safety tip

Off

User impersonation safety tip

Off

Domain impersonation safety tip

Off

Unusual characters safety tip

Unauthenticated senders symbol (?) for spoof

On

Show "via" tag

On

Edit actions

Back

Submit