






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
	Anti-malware	Protect your organization's email from malware, including what actions to take and who to notify if malware is detected
	Safe Attachments	Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams
	Safe Links	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.
---	--------------------------	--




By default, Microsoft 365 includes built-in features that help protect your users from phishing attacks. Set up anti-phishing policies 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](#)


 **0 impersonated domain(s) and user(s)** over the past 7 days. [View impersonations](#)


 Create



 Export


 Refresh

1 item

 Search

 Filter

Name	Status	Priority	Last modified
Office365 AntiPhish Default (Default)	 Always on	Lowest	Dec 14, 2021



Office365 AntiPhish Default (Default)

● Always on | Priority Lowest | Tue Dec 14 2021

Description

-

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

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

By default, Microsoft 365 includes built-in features that help protect your users from phishing attacks. Set up anti-phishing policies 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](#)

 **0 impersonated domain(s) and user(s)** over the past 7 days. [View impersonations](#)

 Create  Export  Refresh  More actions 

1 of 1 selected

 Search

 Filter



 Name	Status	Priority	Last modified
 Office365 AntiPhish Default (Default)	 Always on	Lowest	Dec 14, 2021

Policy name

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

Name ^{*} ⓘ

anto-phishing policy1

Description

Next

Cancel

Users, groups, and domains

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

Include these users, groups and domains

Users

DS Diego Siciliani X

Groups

Domains

Back

Next

This threshold controls the sensitivity for applying machine learning models to messages for determining a phishing verdict.

- ✓ Policy name
- ✓ Users, groups, and domains
- Phishing threshold & protection**
- Actions
- Review

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

Phishing email threshold ⓘ

☐ 1 - Standard

This is the default value. The severity of the action that's taken on the message depends on the degree of confidence that the message is phishing (low, medium, high, or very high confidence).

Impersonation

☐ Enable users to protect (0/350) ⓘ

Enable impersonation protection for up to 350 internal and external users.

[Learn more about adding users to impersonation protection](#)

We recommend adding users in key roles. Internally, these might be your CEO, CFO, and other senior leaders. Externally, these could include council members or your board of directors.

Back

Next

Cancel

- ☐ 1 - Standard
- ☒ 2 - Aggressive
- ☐ 3 - More Aggressive
- ☐ 4 - Most Aggressive



- ✓ Policy name
- ✓ Users, groups, and domains
- ✓ Phishing threshold & protection
- Actions**
- Review

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.

Message actions

If message is detected as an impersonated user

Don't apply any action

We'll deliver the message to the intended recipients without any other actions applied.

If message is detected as an impersonated domain

Don't apply any action

Back

Next

Redirect message to other email addresses

Move message to the recipients' Junk Email folders

Quarantine the message

Deliver the message and add other addresses to the Bcc line

Delete the message before it's delivered

Don't apply any action

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



If message is detected as an impersonated domain


Don't apply any action



Back

Next

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) ⓘ

☐ Show user impersonation safety tip ⓘ

☐ Show user impersonation unusual characters safety tip ⓘ

☒ Show (?) for unauthenticated senders for spoof ⓘ

☒ Show "via" tag ⓘ

Back

Next

Review

Review your policy before creating it.

Policy name

Antio-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

Impersonated user protection

● On for 0 user(s)

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

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](#)