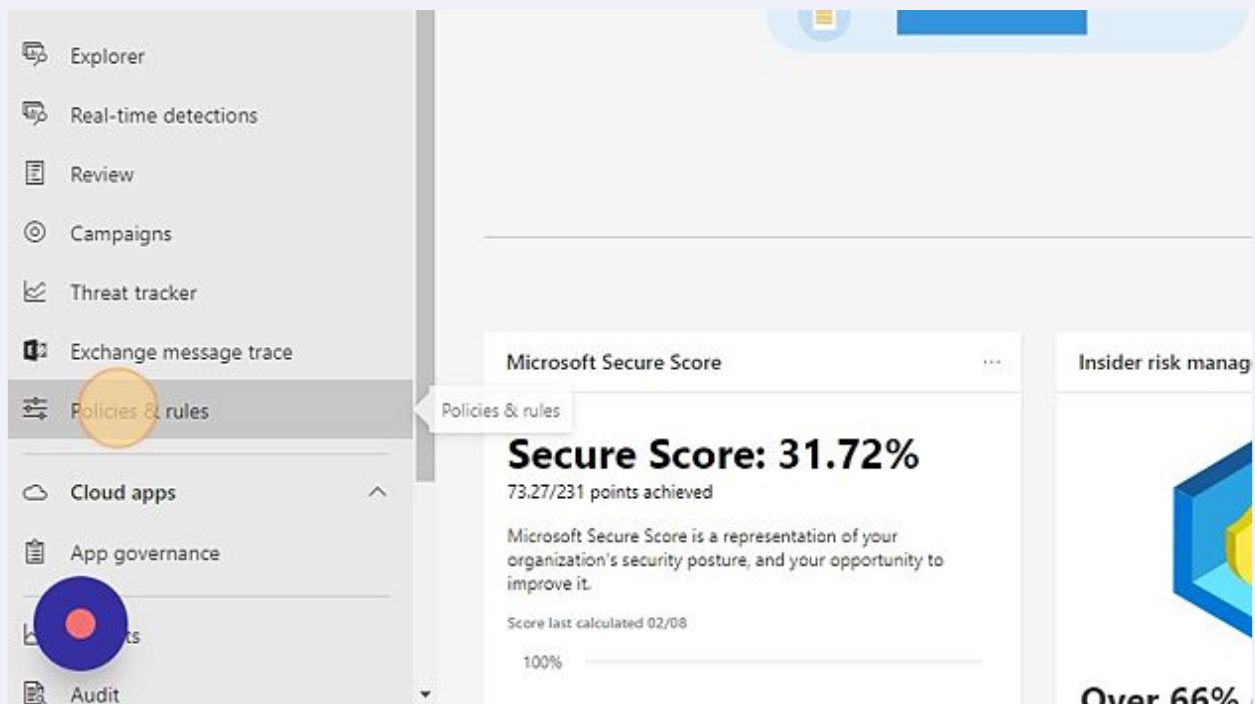


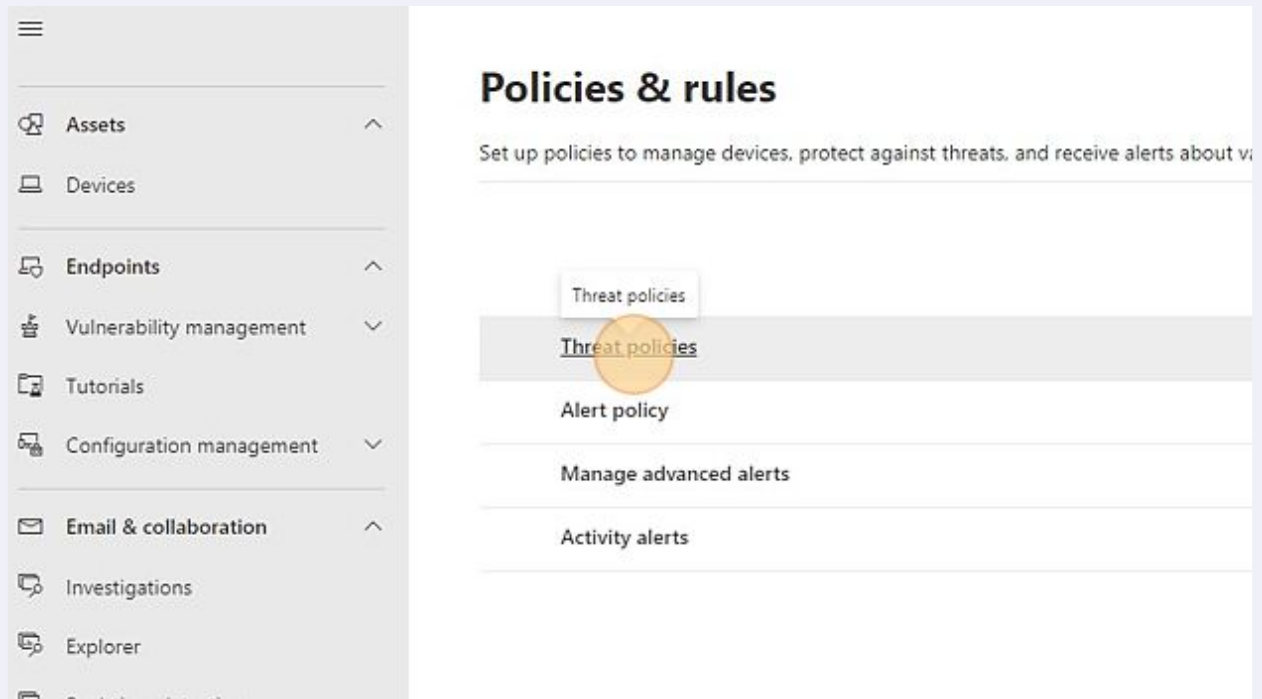
How to Configure an Anti-Phishing Policy in Microsoft 365

1 Navigate to security.microsoft.com

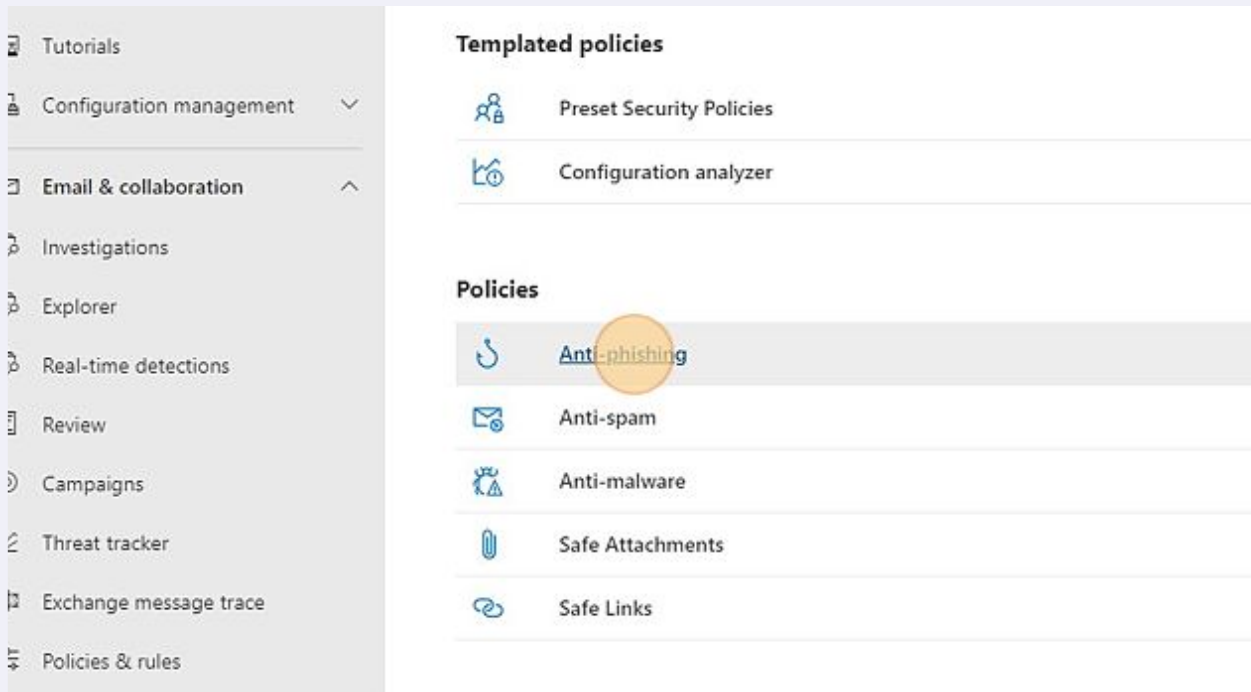
2 Click "Policies & rules"



3 Click "Threat policies"



4 Click "Anti-phishing"



5 Click "Create"

Assets ^

Devices

Endpoints ^

Vulnerability management v

Tutorials

Configuration management v

Email & collaboration ^

Investigations

Explorer

Real-time detections

Review

Anti-phishing

By default, Microsoft 365 includes built-in features that help protect your organization and prevent impersonation and spoofing attacks. The default policy applies [anti-phishing policies](#).

Recommend enabling preset security policies to stay updated with new security controls.

Create

+ Create Export Refresh

☐ Name

☒ Office365 AntiPhish Default (Default)

6 Name your policy "Default-Anti-Phishing-Policy" and click "Next"

Create new policy

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

Name * ⓘ

Default-Anti-Phishing-Policy

Description

Next

7 Add your domains to the selection

Threat policies > Create a new anti-phishing policy

Include these users, groups and domains

Users

And

Groups

And

Domains

☐ Exclude these users, groups and domains

8 Set the "Phishing email threshold" to 3

Threat policies > Create a new anti-phishing policy

Phishing threshold & protection

Set your phishing thresholds and desired impersonation and spoof protection

Phishing email threshold ⓘ

1 - Standard

This is the default value. The severity of the action that's taken on the high, or very high confidence).

Impersonation

☐ Enable users to protect (0/350) ⓘ

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

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

[Manage 0 sender\(s\)](#)

☐ Enable domains to protect (0)

9 Click "Enable User Impersonation Protection"

and domains

Phishing threshold & protection

Set your phishing thresholds and desired impersonation and spoof protection.

Phishing email threshold ⓘ

3 - More Aggressive

Messages that are identified as phishing with a medium or high degree of confidence are treated as if they were identified as phishing.

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](#)
[Manage 0 sender\(s\)](#)

☐ **Enable domains to protect (0)**
Enable impersonation protection for these internal and external domains.
[Manage 0 custom domain\(s\)](#)

Add trusted senders and domains (0)

10 Click "Add user" and select your VIP users.

Manage senders for impersonation protection

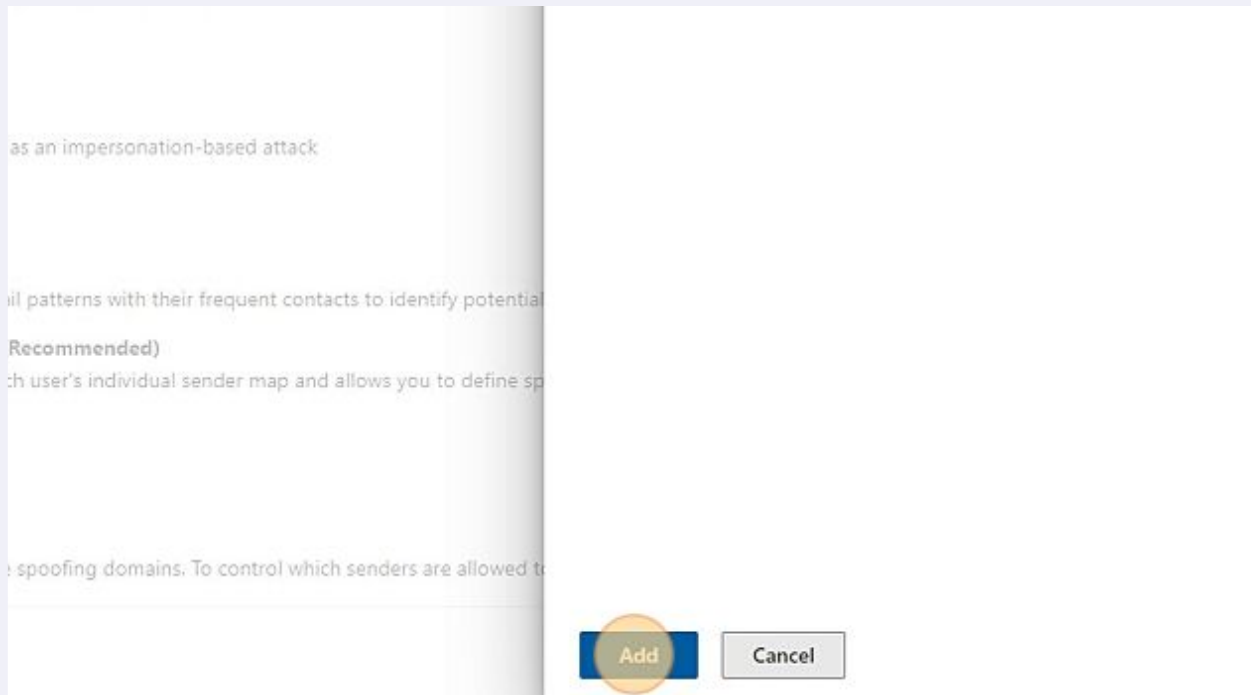
Add up to 350 internal and external senders to protect from being impersonated by attackers. We recommend adding people in key roles.
[Learn more about adding senders to protect](#)

Add user

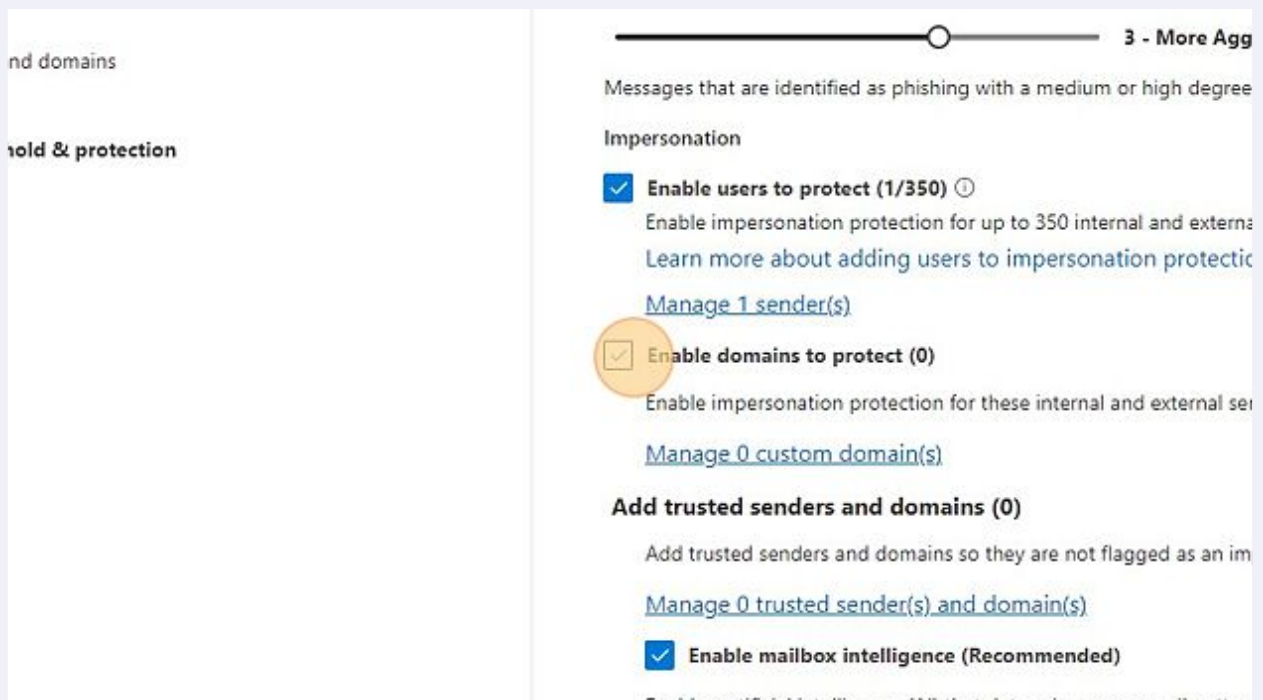
0 items

Display name	Sender email address
No data available	

11 Click "Add"



12 Click "Enable domains to protect"



13 Click "Include domains I own"

Impersonation

☒ **Enable users to protect (1/350)** ⓘ

Enable impersonation protection for up to 350 internal and external users.
[Learn more about adding users to impersonation protection](#)
[Manage 1 sender\(s\)](#)

☒ **Enable domains to protect (0)**

Enable impersonation protection for these internal and external senders.

☒ **Include domains I own** ⓘ
[View my domains](#)

☐ **Include custom domains** ⓘ
[Manage 0 custom domain\(s\)](#)

Add trusted senders and domains (0)

Add trusted senders and domains so they are not flagged as an impersonation source.
[Manage 0 trusted sender\(s\) and domain\(s\)](#)

☒ **Enable mailbox intelligence (Recommended)**



Alert!

If you have other custom domains that you would like to include, add them here.

14 Click "Enable mailbox intelligence"

The screenshot shows a configuration page with a left sidebar and a main content area. In the main content area, the 'Include domains I own' checkbox is checked, with a link 'View my domains' below it. The 'Include custom domains' checkbox is unchecked, with a link 'Manage 0 custom domain(s)' below it. A section titled 'Add trusted senders and domains (0)' contains a link 'Manage 0 trusted sender(s) and domain(s)'. Below this, the 'Enable mailbox intelligence (Recommended)' checkbox is checked and highlighted with an orange circle. Its description reads: 'Enables artificial intelligence (AI) that determines user email patterns'. Under the 'Spoof' section, the 'Enable spoof intelligence (Recommended)' checkbox is also checked. Its description reads: 'Choose how you want to filter email from senders who are spoofing domains, use the Tenant Allow/Block List Spoofing page. Learn more about Spoof Intelligence'. At the bottom, there are 'Back' and 'Next' buttons.

☒ Include domains I own [View my domains](#)

☐ Include custom domains [Manage 0 custom domain\(s\)](#)

Add trusted senders and domains (0)

Add trusted senders and domains so they are not flagged as an imper

[Manage 0 trusted sender\(s\) and domain\(s\)](#)

☒ **Enable mailbox intelligence (Recommended)**

Enables artificial intelligence (AI) that determines user email patterns v

Spoof

☒ **Enable spoof intelligence (Recommended)**

Choose how you want to filter email from senders who are spoofing d
domains, use the [Tenant Allow/Block List Spoofing page](#).
[Learn more about Spoof Intelligence](#)

[Back](#) [Next](#)

15 Click "Enable intelligence for impersonation protection"

This screenshot is similar to the previous one, showing the same configuration page. The 'Enable mailbox intelligence' checkbox remains checked. The 'Enable Intelligence for impersonation protection (Recommended)' checkbox is now checked and highlighted with an orange circle. Its description reads: 'Enables enhanced impersonation results based on each user's inc messages'. The 'Enable spoof intelligence' checkbox remains checked. The 'Back' and 'Next' buttons are still at the bottom.

☐ Include custom domains [Manage 0 custom domain\(s\)](#)

Add trusted senders and domains (0)

Add trusted senders and domains so they are not flagged as an impe

[Manage 0 trusted sender\(s\) and domain\(s\)](#)

☒ **Enable mailbox intelligence (Recommended)**

Enables artificial intelligence (AI) that determines user email patterns v

☒ **Enable Intelligence for impersonation protection (Recommen**

Enables enhanced impersonation results based on each user's inc
messages

Spoof

☒ **Enable spoof intelligence (Recommended)**

Choose how you want to filter email from senders who are spoofing c
domains, use the [Tenant Allow/Block List Spoofing page](#).
[Learn more about Spoof Intelligence](#)

[Back](#) [Next](#)

16 Click "Enable spoof intelligence (Recommended)"

[Manage 0 custom domain\(s\)](#)
Add trusted senders and domains (0)
Add trusted senders and domains so they are not flagged as an impersonation
[Manage 0 trusted sender\(s\) and domain\(s\)](#)
☒ **Enable mailbox intelligence (Recommended)**
Enables artificial intelligence (AI) that determines user email patterns with the
☒ **Enable Intelligence for impersonation protection (Recommended)**
Enables enhanced impersonation results based on each user's individual messages

Spoof
☒ **Enable spoof intelligence (Recommended)**
Choose how you want to filter email from senders who are spoofing domains, use the [Tenant Allow/Block List Spoofing page](#).
[Learn more about Spoof Intelligence](#)

Back

Next

17 Click "Next"

[Manage 0 custom domain\(s\)](#)
Add trusted senders and domains (0)
Add trusted senders and domains so they are not flagged as an impersonation-base
[Manage 0 trusted sender\(s\) and domain\(s\)](#)
☒ **Enable mailbox intelligence (Recommended)**
Enables artificial intelligence (AI) that determines user email patterns with their frequ
☒ **Enable Intelligence for impersonation protection (Recommended)**
Enables enhanced impersonation results based on each user's individual sender messages

Spoof
☒ **Enable spoof intelligence (Recommended)**
Choose how you want to filter email from senders who are spoofing domains. To cor
domains, use the [Tenant Allow/Block List Spoofing page](#).
[Learn more about Spoof Intelligence](#)

Back

Next

18 Set all available options to "Quarantine the message"

Set what actions you'd like this policy to take on messages. You may need to turn on

Message actions

If a message is detected as user impersonation

Don't apply any action

Redirect the message to other email addresses

Move the 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

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

If the message is detected as spoof by spoof intelligence

Move the message to the recipients' Junk Email folders

19 Click "Default Quarantine Policy" for all selections.

Message actions

If a message is detected as user impersonation

Quarantine the message

We'll quarantine the message for you to review and decide whether it should

Apply quarantine policy

Select an option

Default Quarantine Policy

DefaultFullAccessPolicy

AdminOnlyAccessPolicy

DefaultFullAccessWithNotificationPolicy

Don't apply any action

We'll deliver the message to the intended recipients without any other action

If the message is detected as spoof by spoof intelligence

20 Click "Show user impersonation safety tip"

If the message is detected as spoof by spoof intelligence

Quarantine the message

We'll quarantine the message for you to review and decide when to release it

Apply quarantine policy

Default Quarantine Policy

Safety tips & indicators

- ☒ Show first contact safety tip (Recommended)
- ☒ Show user impersonation safety tip
- ☐ Show domain impersonation safety tip
- ☐ Show user impersonation unusual characters safety tip
- ☒ Show (?) for unauthenticated senders for spoof
- ☒ Show "via" tag

Back Next

21 Click "Show domain impersonation safety tip"

If the message is detected as spoof by spoof intelligence

Quarantine the message

We'll quarantine the message for you to review and decide when to release it

Apply quarantine policy

Default Quarantine Policy

Safety tips & indicators

- ☒ Show first contact safety tip (Recommended)
- ☒ Show user impersonation safety tip
- ☒ Show domain impersonation safety tip
- ☐ Show user impersonation unusual characters safety tip
- ☒ Show (?) for unauthenticated senders for spoof
- ☒ Show "via" tag

Back Next

22 Click "Show user impersonation unusual characters safety tip"

If the message is detected as spoof by spoof intelligence

Quarantine the message

We'll quarantine the message for you to review and decide when to release it.

Apply quarantine policy

Default Quarantine Policy

Safety tips & indicators

- ☒ Show first contact safety tip (Recommended)
- ☒ Show user impersonation safety tip
- ☒ Show domain impersonation safety tip
- ☒ Show user impersonation unusual characters safety tip
- ☒ Show (?) for unauthenticated senders for spoof
- ☒ Show "via" tag

Back Next

23 Click "Show (?) for unauthenticated senders for spoof"

If the message is detected as spoof by spoof intelligence

Quarantine the message

We'll quarantine the message for you to review and decide when to release it.

Apply quarantine policy

Default Quarantine Policy

Safety tips & indicators

- ☒ Show first contact safety tip (Recommended)
- ☒ Show user impersonation safety tip
- ☒ Show domain impersonation safety tip
- ☒ Show user impersonation unusual characters safety tip
- ☒ Show (?) for unauthenticated senders for spoof
- ☒ Show "via" tag

Back Next

24 Click "Show 'via' tag"

If the message is detected as spoof by spoof intelligence

Quarantine the message

We'll quarantine the message for you to review and decide whether it should be delivered.

Apply quarantine policy

Default Quarantine Policy

Safety tips & indicators

- ☒ Show first contact safety tip (Recommended)
- ☒ Show user impersonation safety tip
- ☒ Show domain impersonation safety tip
- ☒ Show user impersonation unusual characters safety tip
- ☒ Show (?) for unauthenticated senders for spoof
- ☒ Show "via" tag

Back Next

25 Click "Next"

If the message is detected as spoof by spoof intelligence

Quarantine the message

We'll quarantine the message for you to review and decide whether it should be delivered.

Apply quarantine policy

Default Quarantine Policy

Safety tips & indicators

- ☒ Show first contact safety tip (Recommended)
- ☒ Show user impersonation safety tip
- ☒ Show domain impersonation safety tip
- ☒ Show user impersonation unusual characters safety tip
- ☒ Show (?) for unauthenticated senders for spoof
- ☒ Show "via" tag

Back Next

26 Review your settings and click "Submit"

	<p>User impersonation protection</p> <ul style="list-style-type: none">● On for 1 user(s) <p>Domain impersonation protection</p> <ul style="list-style-type: none">● On for owned domains● Off - 0 domain(s) specified <p>Trusted impersonated senders and domains</p> <ul style="list-style-type: none">● Off <p>Mailbox intelligence</p> <ul style="list-style-type: none">● On <p>Mailbox intelligence for impersonations</p> <ul style="list-style-type: none">● On <p>Spoof intelligence</p> <ul style="list-style-type: none">● On <p>Edit protection settings</p>
<div>Back Submit</div>	