Set up Office 365 ATP anti-phishing and anti-phishing policies

- 08/29/2019
- *Contributors(Maratmussabekov;J Caparas;Johan Freelancer9;Chris Davis;Ross Adams;Jose Gabriel Ortega Castrp;SriRaman;Peter BaumGartner*)

ATP anti-phishing protection, part of Office 365 Advanced Threat Protection, can help protect your organization from malicious impersonation-based phishing attacks and other phishing attacks. If you're an Office 365 Enterprise global or security administrator, you can set up ATP anti-phishing policies.

Phishing attacks come in a variety of forms from commodity-based attacks to targeted spear phishing or whaling. With the growing complexity, it's difficult for even a trained eye to identify some of these sophisticated attacks. Fortunately, Office 365 Advanced Threat Protection can help. You can set up an ATP anti-phishing policy to help ensure that your organization is protected against such attacks.

Note

ATP anti-phishing is only available in Advanced Threat Protection (ATP). ATP is included in subscriptions, such as Microsoft 365 Enterprise, Microsoft 365 Business, Office 365 Enterprise E5, Office 365 Education A5, etc. If your organization has an Office 365 subscription that does not include Office 365 ATP, you can potentially purchase ATP as an add-on. For more information, see Office 365 Advanced Threat Protection plans and pricing and the Office 365 Advanced Threat Protection Service Description. Make sure your organization is using the latest version of Office 365 ProPlus on Windows to take full advantage of ATP anti-phishing protection.

An anti-phishing policy is also available for Office 365 Exchange Online Protection, with a limited set of anti-spoofing protection that is intended to protect against authentication-based and deception-based attacks.

What to do:

1. Review the prerequisites.
2. Learn about your anti-phishing and ATP anti-phishing policy options.
3. Set up an anti-phishing policy or an ATP anti-phishing policy.

Important

To learn how multiple technologies are applied, see What policy applies when multiple protection methods and detection scans run on your email.

Review the prerequisites

- To define (or edit) ATP policies, you must be assigned an appropriate role. Some examples are described in the following table:

Table 1

Role	Where/how assigned
Office 365 Global Administrator	The person who signs up to buy Office 365 is a global admin by default. (See About Office 365 admin roles to learn more.)
Security Administrator	Azure Active Directory admin center (https://aad.portal.azure.com)
Exchange Online Organization Management	Exchange admin center (https://outlook.office365.com/ecp) or PowerShell cmdlets (See Exchange Online PowerShell)

- To learn more about roles and permissions, see Permissions in the Office 365 Security & Compliance Center.
- You will probably set up multiple anti-phishing policies for your organization. Office 365 enforces these policies in the order they're listed on the **Anti-phishing page** and **ATP anti-phishing** pages in the Security & Compliance Center. Once you've reviewed your policy options, take some time to determine how many policies you'll need and the priority for each.
- Plan to spend about 5-15 minutes to set up your first anti-phishing policy.
- Allow up to 30 minutes for your new or updated policy to spread to all Office 365 datacenters.

Set up an anti-phishing or ATP anti-phishing policy

Each organization in Office 365 has a default anti-phishing policy that applies to all users. You can create multiple custom anti-phishing policies that you can scope to specific users, groups, or domains within your organization. The custom policies you create take precedence over the default policy. You add, edit, and delete anti-phishing policies in the Office 365 Security & Compliance Center.

1. Go to https://protection.office.com and sign in with your work or school account.
2. In the Office 365 Security & Compliance Center, in the left navigation pane, under **Threat management**, choose **Policy**.
3. On the **Policy** page, choose **Anti-phishing** or **ATP anti-phishing**.
4. On the **Anti-phishing** or **ATP anti-phishing** page, do one of the following:
    - To add a new policy select **+ Create**.
    - To edit an existing policy, select the policy name from the list displayed on the **Anti-phishing** page. (Alternately, you can or choose **Default Policy** above the list.) On the page that appears, choose **Edit policy**.

5. Specify the name, description, and settings for your policy. See Learn about ATP anti-phishing policy options for more details.
6. Once you have reviewed your settings, choose **Create this policy** (or **Save**).

Learn about ATP anti-phishing policy options

As you set up or edit your ATP anti-phishing policies, you can choose from several options that provide the most sophisticated and comprehensive protection, as described in the following table:

Table 2

This setting	Does this	Use when you want to:
Add users to protect	Defines which email addresses will be protected by the policy. You can add up to 60 internal and external addresses that you want to protect from impersonation.	When you want to ensure that mail from outside your organization isn't an impersonation of one of the users on the list of users you are protecting. Examples of users you might want to protect are high-level executives, business owners, external board members, and so on. This list of protected users is different from the list of people to which the policy applies, or rather, for which the policy is enforced. You define the applies to list in the **Applied to** section of the policy options. For example, if you add `Mary Smith <marys@contoso.com>` as a user to protect, then apply the policy to the group "All Users". This would ensure that a mail that appeared to impersonate "Mary Smith" sent to a user in the "All Users" group would be acted on by the policy.
Add domains to protect	Allows you to choose which domains you want to protect from impersonation. You can specify that the policy includes all of your custom domains, a comma-separated list of domains, or a combination of the two. If you choose **Automatically include domains that I own**, and you later add a domain to your Office 365 organization, this anti-phishing policy will be in place for the new domain.	Whenever you want to ensure that mail from outside your organization isn't an impersonation of one of the domains defined in your list of verified domains or that of a partner domain.

Table 2

This setting	Does this	Use when you want to:
Choose actions	Choose the action to take when Office 365 detects an impersonation attempt against the users and domains you added to the policy. You can choose different actions for users and domains in the same anti-phishing policy. These actions apply to any incoming email that has been identified by Office 365 as impersonating a user account or domain that is under the protection of this anti-phishing policy. **Quarantine message** Email will be sent to Office 365 quarantine. When you choose this option, the email is not sent to the original recipient. **Redirect message to another email address** Email will be sent to the email address you specify. You can specify multiple email addresses. When you choose this option, the email is not sent to the original recipient. **Move message to the recipients' Junk email folder** Email will be sent to the recipients' Junk email folder. When you choose this option, the email is still sent to the original recipient but is not placed in the recipient's inbox. **Deliver the message and add other addresses to the Bcc line** Email will be delivered to the original recipient. In addition, the users you identify will be added to the bcc line of the message before it's delivered. When you choose this option, the email is still sent to the original recipient's inbox. **Don't apply any action** Email will be delivered to the original	When you want to take an action on messages that Office 365 has determined to be an impersonation of a user or domain as defined in the policy.

Table 2

This setting	Does this	Use when you want to:
	recipient's inbox. No other action will be taken on the email message. **Turn on phishing protection tips** Enables anti-phishing safety tips in email.	
Enable mailbox intelligence	Enables or disables mailbox intelligence for this policy. You can only enable mailbox intelligence for cloud-based accounts, that is, accounts whose mailbox is hosted entirely in Office 365.	This feature uses machine learning to determine a user's email patterns with their contacts. With this information, the AI can better distinguish between genuine and phishing emails.
Enable mailbox intelligence based impersonation protection	Enables or disables mailbox intelligence for impersonation protection for this policy. The important aspect here is the control of the impersonation for a given mailbox.	When you want to enhance impersonation results for users based on each user's individual sender map. This intelligence allows Office 365 to customize user impersonation detection and better handle false positives. When user impersonation is detected, based on mailbox intelligence, you can define what action to take on the message.
Add trusted senders and domains	Defines email addresses and domains that will not be considered impersonation by this policy. Messages from the sender email addresses and domains you add as trusted senders and domains won't ever be classified as an impersonation-based attack. As a result, the actions and settings in this policy won't be applied to messages from these senders and domains. The maximum limit for these lists is approximately 1000 entries.	When users interact with domains or users that trigger impersonation but are considered to be safe. For example, if a partner has the same/similar display name or domain name as a user defined on the list.
Applied to	Defines the recipients whose incoming email messages will be subject to the rules of the policy. You can create conditions and exceptions for the recipients associated with the policy.	Each policy must be associated with a set of users, for example, users in a particular group or domain.

Table 2

This setting	Does this	Use when you want to:
	For example, you can create a global policy for your organization by applying the rule to all recipients in your domain. You can also create exception rules, such as a rule that does not scan email messages for a specific group of recipients.	
Advanced phishing thresholds	Defines the level of settings for how phishing messages are handled. **Standard**: Email suspected to be phish is handled in the standard way. **Aggressive**: The system handles emails suspected to be phish with a high degree of confidence, the same way as those suspected with a very high degree of confidence. **More aggressive**: The system handles emails suspected to be phish with a medium or high degree of confidence, the same way as those suspected with a very high degree of confidence. **Most aggressive**: The system handles emails suspected to be phish with a low, medium, or high degree of confidence, the same way as those suspected with a very high degree of confidence.	When you want to be more aggressive in the treatment of potentially phishing messages within Office 365. For example, messages with a very high probability of being phish will have the most aggressive actions taken on them while messages with a low probability have less aggressive actions taken on them. This setting also impacts other parts of the filtering system that combine signals. This doesn't necessarily mean different actions are implemented. Essentially you set the probability of mail being phish, to determine the (same) designated action. The chance of moving good messages increases as the level of settings increases.

Learn about anti-phishing policy options

As you set up or edit your anti-phishing, you can choose from several options, as described in the following table:

Table 3

This setting	Does this	Use when you want to:
Applied to	Defines the recipients whose incoming email messages will be subject to the rules of the policy.	Each policy must be associated with a set of users, for example,

Table 3

This setting	Does this	Use when you want to:
	You can create conditions and exceptions for the recipients associated with the policy. For example, you can create a global policy for your organization by applying the rule to all recipients in your domain. You can also create exception rules, such as a rule that does not scan email messages for a specific group of recipients.	users in a particular group or domain.
Choose actions	Choose the action to take when Office 365 detects an intra-org or external-org spoofing attempt against your users. These actions apply to any incoming email that has been identified by Office 365 as a spoofing attempt for users that are under the protection of this anti-phishing policy. **Quarantine message** Email will be sent to Office 365 quarantine. When you choose this option, the email is not sent to the original recipient. **Move message to the recipients' Junk email folder** Email will be sent to the recipients' Junk email folder. When you choose this option, the email is still sent to the original recipient but is not placed in the recipient's inbox. **Don't apply any action** Email will be delivered to the original recipient's inbox. No other action will be taken on the email message.	When you want to take an action on messages that Office 365 has determined to be a spoofing attempt of internal or external domains as defined in the policy.

After your organization has set up anti-phishing policies or ATP anti-phishing policies, you can see how the service is working by viewing reports for Advanced Threat Protection.

Example: Anti-phishing policy to protect a user and a domain

This example sets up a policy called "Domain and CEO" that provides both user and domain protection from impersonation and then applies the policy to all email received by users within the domain `contoso.com`. The security administrator has determined that the policy must meet these business requirements:

- The policy needs to provide protection for the CEO's email account and the entire domain.
- Messages that are determined to be impersonation attempts against the CEO's user account need to be redirected to the security administrator's email address.

- Messages that are determined to be impersonation attempts against the domain are less urgent and should be quarantined for later review.

The security administrator at Contoso might use values like the following in order to create an anti-phishing policy that meets these needs.

Table 4

Setting or option	Example
Name	Domain and CEO
Description	Ensure that the CEO and our domain are not being impersonated.
Add users to protect	The CEO's email address at a minimum.
Add domains to protect	The organizational domain that includes the office of the CEO.
Choose actions	If email is sent by an impersonated user: Choose **Redirect message to another email address** and then type the email address of the security administrator, for example, `securityadmin@contoso.com`. If email is sent by an impersonated domain: Choose **Quarantine message**.
Mailbox intelligence	By default, mailbox intelligence is selected when you create a new anti-phishing policy. Leave this setting **On** for best results.
Add trusted senders and domains	For this example, don't define any overrides.
Applied to	Select **The recipient domain is**. Under **Any of these**, select **Choose**. Select **+ Add**. Select the checkbox next to the name of the domain, for example, `contoso.com`, in the list and then select **Add**. Select **Done**.

Delete an anti-phishing or ATP anti-phishing policy

You can delete custom policies that you created by using the Security & Compliance Center. You can't delete the default policy for your organization. We recommend using the Security & Compliance Center to review or edit any of your ATP policies.

1. Go to https://protection.office.com and sign in with your work or school account.
2. In the left navigation, under **Threat management**, choose **Policy**.
3. On the **Policy** page, choose **Anti-phishing** or **ATP anti-phishing**.
4. On the **Anti-phishing** or **ATP anti-phishing** page, select the policy name from the list.
5. On the page that appears, choose **Delete policy**. Allow up to 30 minutes for your changes to spread to all Office 365 datacenters.