Whitelist Microsoft Office 365

Why Whitelist in Office 365?

Whitelisting ensures the **CyTech - AQUILA Phishing Simulation(PS) Module** functions without issue and prevents PS emails from being automatically moved to the spam folder or notifying users about potential phishing emails. The Connection Filter Policy and Spam Filtering both required to be whitelisted.

Key Configurations:

1. **Microsoft Defender**
   - Whitelist the Connection Filter Policy
   - Whitelist Using Advanced Delivery Policies
2. **Exchange Admin Center**
   - Whitelist Spam Filtering
   - Whitelist Advanced Threat Protection (ATP)

Whitelist Connection Filter Policy

The Office 365 Exchange Connection Filter identifies good or bad source email servers by their IP addresses. The actions below will allow all emails from CyTech IP addresses to be received.

Whitelist the Connection Filter Policy

1. Login to Microsoft Defender, click here - **Microsoft Defender.**

2. Navigate through **Email & Collaboration>Policies & Rules>Threat Policies>Anti-spam.**

3. Click on "**Connection filter policy**". Then click on "**Edit connection filter policy**".

4. Add the **IP's** to the "Always allow messages from the following IP addresses or address range:". Then click the "**Save**" button.

Allow IP's: 35.153.237.243(Mail Server), **107.22.65.180**(Landing Page)

Whitelist Using Advanced Delivery Policies in Microsoft Defender for Office 365

Phishing simulations are attacks orchestrated by your security team and used for training and learning. Simulations can help identify vulnerable users and lessen the impact of malicious attacks on your organization.

Third-party phishing simulations require at least one Sending domain entry [source domain or DKIM] AND at least one Sending IP entry. Simulations URLs to allow entries are optional, and prevent the simulated phishing URLs from being blocked at time of click.

1. Go to **Email & Collaboration > Policies & Rules > Threat policies > Advanced delivery in the Rules section**.

2. In the Advanced delivery menu, navigate to the Phishing simulation tab and press Edit to either add new or configure existing values. After editing all the needed Domain, Sending IP and Simulation URLs to allow**.** Click **"Save".**

3. On the Edit third-party phishing simulation menu that opens, configure the following settings:

- **Domain:** Expand this setting and enter at least one sending domain specific for campaign by clicking in the box, entering a value, and then pressing Enter or selecting the domains displayed below. Repeat this step as many times as necessary. You can add up to 20 entries.
  - slackj.com
  - ttrelli.com
  - airbnd.cc
  - attlassians.com
  - eebbey.com
  - lastpasss.net
  - my1psswords.com
  - zooms.cc
  - 0365.click
  - micros0ft.click
  - offlce.click

- **Sending IP:** Expand this setting and enter at least one valid IPv4 address by clicking in the box, entering a value, and then pressing Enter or selecting the value that's displayed below the box. Repeat this step as many times as necessary. You can add up to 10 entries.
  - **35.153.237.243**(Mail Server)
  - **107.22.65.180**(Landing Page)

-

Simulation URLs to allow: Expand this setting and optionally enter specific URLs that are part of your phishing simulation campaign that should not be blocked or detonated by clicking in the box, entering a value, and then pressing Enter or selecting the value that's displayed below the box.

- For the URL syntax format, see URL syntax for the Tenant Allow/Block List (opens in a new tab). These URLs are wrapped at the time of the click, but they aren't blocked.
- When you're finished, you can click Add, and click close afterward if this was a first-time addition, or if you were editing existing values click Save and then click Close.

- Manage allows and blocks in the Tenant Allow/Block List
- Refer to these simulation URLs to allow in your campaign:
    - slackj.com/*
    - ttrelli.com/*
    - airbnd.cc/*
    - attlassians.com/*
    - eebbey.com/*
    - lastpasss.net/*
    - my1psswords.com/*
    - zooms.cc/*
    - 0365.click/*
    - micros0ft.click/*
    - offlce.click/*

Whitelist Spam Filtering

All mail systems have spam filtering. As the CyTech PS emails are "phishing: by definition, the Microsoft spam filter must be whitelisted. The steps below outline how to disable all spam checks for CyTech PS emails, so you won't experience issues with 100% clicked and 100% opened emails, even if the users don't click on them.

Steps to Whitelist the Spam Filtering

1. Login to Exchange Admin Center, click here - **Exchange Admin Center.**
2. Navigate through **Mail flow>Rules>+Add a rule>"Create a new rule"**.
3. Give the rule a name, such as "**CyTech Spam Filtering**". Click on "**Apply this rule if → " The sender"** → "**IP address is in any of these ranges or exactly matches".**
4. Specify the IP addresses in the field IP's: **35.153.237.243**(Mail Server), **107.22.65.180** (Landing Page). Please do not forget to click on "**Save**".
5. Click the add button **"+"** to add another rule condition for the The sender.
6. Click on "**The sender....**" → "**domains is**". Specify the domain in your case. Then click " **Save**".

    - slackj.com
    - ttrelli.com
    - airbnd.cc
    - attlassians.com

- eebbey.com
- lastpasss.net
- my1psswords.com
- zooms.cc
- 0365.click
- micros0ft.click
- offlce.click

1. Click on "**Do the following → Modify the message properties → Set a Message Header**"
2. Click the "**Enter text**" buttons by the right side of the "**Do the following**" field and enter these values: "**MS-Exchange-Organization-BypassClutter**" and "**true**".
3. Click on the add button "**+**" sign, to add another rule condition.
4. Choose "**Modify the message properties → Set the spam confidence level (SCL)** " and select "**Bypass Spam Filtering**", this will set the value of SCL to **-1**. Then click " **Save**" button.
5. Click the "**Next**" button.
6. Leave the Set Rule settings as is and proceed to the Review and finish window and save the rule.
7. Please make sure the rule is **Enabled**, and priority is **set to "0"**.

Whitelist ATP by Email Header for Mail Filtering

1. Add another rule >**Add a rule>"Create a new rule"**.
2. Give the rule a name, such as "**Bypass ATP Links**". Click on "**Apply this rule if → "The message headers...." → "includes any of these words".**
3. Click → **Enter text**.
4. Specify header name → **X-PHISHTEST** and specify words or phrases → **CYTECH**.
5. In the "**Do the following**" condition select "**Modify the message properties**" and "**set a message header**".
6. Insert below into the "**Enter text**" fields:
   - Click the first *Enter text... link and set the message header to **X-MS-Exchange-Organization-SkipSafeLinksProcessing**.
   - Click the second *Enter text... link and set the value to **1**.
7. Click the "**Next**" button.
8. Leave the Set Rule settings as is and proceed to the Review and finish window and save the rule.
9. Please make sure the rule is **Enabled**, and priority is **set to "1"**.

*If you need further assistance, kindly contact our support at **support@cytechint.com** for prompt assistance and guidance.*

Revision #4
Created 29 May 2025 09:38:25 by Richmond Abella
Updated 11 July 2025 06:36:34 by Richmond Abella