MINIMIZING PHISHING FALSE POSITIVES

QUICK REFERENCE GUIDE

CONTENTS

OVERVIEW

What's a False Positive?

A false positive is an error that occurs when a system reports an event, such as a target clicking on a phishing email, that did not actually occur. False positives happen on all types of phishing simulation systems and are not limited to any specific vendor or tool.

What's a Click?

To understand how false positives occur, it is necessary how the system measures responses. A "click" is defined as any interaction with a link, such as a user clicking with their mouse. However, this may also include a system, such as email security software, that inspects an email prior to it reaching the inbox.

Common Causes

False positives are typically caused by the security filter of email providers. Filters inspect the contents of emails before releasing them to the recipient's inbox. To the phishing tool, this registers as a click and is reported as such.

SOLUTIONS

VENZA understands the importance of accurate data and takes active steps to mitigate false positives. Important steps include:

1. **IP Whitelisting**

Whitelisting is a cybersecurity and information technology (IT) term that refers to allowing certain email domains (e.g., example@domain.com) and internet protocols (IPs) through a company's defenses.

Add VENZA's incoming campaign IPs to your network's whitelist can prevent your email security systems from triggering false positives.

2. **Internal IP Filtering**

Provide your Customer Success Coach with a list of internal IP addresses that can be used in an internal filtering process.

WHITELISTING CISCO

Objective: Using Cisco Ironport security software, you can safelist (whitelist) VENZA to allow your users to receive our simulated phishing and system emails.

If you run into problems while safelisting in Cisco Ironport, we suggest you first reach out directly to Cisco for assistance.

- ## USING WHITELISTING

Steps:

1. From the Cisco Ironport admin console, navigate to the **Mail Policies** tab.
2. Select **HAT Overview** and ensure that **InboundMail lister** is selected.
3. Click **WHITELIST**. If you do not see **WHITELIST**, you can create your group titled as such.
4. Click **Add Sender** and add the VENZA IP (108.163.193.74).
5. Click **Submit** and then **Commit Changes**.

- ## SKIPPING OUTBREAK FILTER SCANNING

Steps:

1. From the Cisco Ironport admin console, navigate to the **Mail Policies** tab.
2. Under the **Message Modification** section, enter the VENZA IP (108.163.193.74) in the **Bypass Domain Scanning** table.
3. Click **Submit** and then **Commit Changes**.

WHITELISTING FORTINET

Objective: Using Fortinet security software, you can safelist (whitelist) VENZA to allow your users to receive our simulated phishing and system emails.

If you run into problems while safelisting in Fortinet, we suggest you first reach out directly to Fortinet for assistance.

- ### USING STATIC URL FILTER

Steps:

1. Log in to your Fortinet account.
2. Navigate to **Security Profiles** > **Web Filter**.
3. Create a new web filter or select one to edit.
4. Expand **Static URL Filter**, enable **URL Filter**, and select **Create**.
5. Enter URLs without "https.". A list of URLs is included at the end of this Quick Reference Guide.
6. Select Type: **Simple**.
7. Select the Action to take against matching URLs: **Allow**.
8. Confirm that **Status** is Enabled.

WHITELISTING GMAIL

Objective: These instructions will help you configure the delivery of third-party phishing simulations to Google Gmail.

Note: You must have an administrator account to perform this process, and changes may take up to 24 hours to take effect.

- ### ADD AN IP ADDRESS TO YOUR ALLOWLIST

Steps:

1. Sign in to your Google Admin console.
2. In the Admin Console, go to **Menu** > **Apps** > **Google Workspace** > **Gmail** > **Spam, Phishing and Malware**.
3. On the left, select the top-level organization. This is usually your domain.
4. On the **Spam, phishing, and malware** tab, scroll to the **Email allowlist** setting. Or, in the search field, enter **email allowlist**.
5. Enter the IP address for VENZA Phishing™: 108.163.193.74
6. At the bottom of the page, click **Save**.

- ### CREATE AN APPROVED SENDERS LIST TO BYPASS SPAM FILTERS

Steps:

1. Sign in to your Google Admin console.
2. In the Admin Console, go to **Menu** > **Apps** > **Google Workspace** > **Gmail** > **Spam, Phishing and Malware**.
3. On the left, select an organizational unit.
4. Point to **Spam** and click **Configure**.
5. For a new setting, enter a unique name or description.
6. Check the **Bypass spam filters for messages received from addresses or domains within these approved senders lists** box.
7. Click **Create or edit** to create a list of approved senders.
8. Scroll to the bottom of **Manage address lists**, and click **Add address** list.
9. Enter a name for the new list.
10. Click **Add address**.
11. Enter email addresses or domain names. Use a space or comma between each entry.
12. Click **Save** to save the new address list.

WHITELISTING MICROSOFT 365

Objective: These instructions will help you configure the delivery of third-party phishing simulations to Microsoft 365 Defender.

Note: You must be assigned permissions (Organization Management or Security Administrator) in Exchange Online before you can perform these procedures.

Note: Users may receive a false positive if they report an email using the Report Message add-in.

- ### USING ADVANCED DELIVERY

Steps:

1. Open the Microsoft 365 Defender portal.
2. Go to **Email & Collaboration** > **Policies & Rules** > **Threat policies** page > **Rules** section > **Advanced delivery**.

3. On the **Advanced delivery** page, select the **Phishing simulation** tab, and then do one of the following steps:
    a. Click **Edit**, or
    b. If there are no configured phishing simulations, click **Add**.
4. In the **Edit third-party phishing simulation** flyout that opens, configure the following settings:
    a. **Domain**: Expand this setting and enter at least one email address domain by clicking in the box, entering a value, and then pressing **Enter**. A list of domains necessary for VENZA Phishing™ is included at the end of this Quick Reference Guide.
    b. **Sending IP**: Expand this setting and enter a valid IPv4 address by clicking in the box, entering **108.163.193.74**, and then pressing **Enter**.
    c. **Simulation URLs to allow**: Expand this setting and enter URLs provided by your VENZA Customer Success Coach. Note: this field is not required for all phishing campaigns.
5. Once you're finished, click **Add** and then **Close**.

• USING THE IP ALLOW LIST

Caution: Without additional verification like mail flow rules, email from sources in the IP Allow List skips spam filtering and sender authentication (SPF, DKIM, DMARC) checks. This creates a high risk of attackers successfully delivering email to the Inbox that would otherwise be filtered.

Steps:

1. Open the Microsoft 365 Defender portal.
2. Go to **Email & Collaboration** > **Policies & Rules** > **Threat Policies** > **Anti-spam**
3. Click **Connection filter policy** and then **Edit connection filter policy**.
4. Add the IP address below to the **Always allow messages from the following IP addresses or address range** field:
    a. 108.163.193.74
5. Press **enter** and click **save** to enable the new settings.

- ## USING THE ALLOWED SENDER OR ALLOWED DOMAIN LISTS

Caution: This method creates a high risk of attackers successfully delivering email to the Inbox that would otherwise be filtered; however, the allowed senders or allowed domains lists don't prevent malware or high confidence phishing messages from being filtered.

Steps:

1. Open the Microsoft 365 Defender portal
2. Go to **Email & Collaboration** > **Policies & Rules** > **Threat Policies** > **Anti-spam**
3. Click **+** to create a policy and select **Inbound** from the drop-down list.
4. The policy wizard opens. On the **Name your policy** page, configure these settings:
    a. **Name**: enter a unique, descriptive name for the policy.
    b. **Description**: Enter an optional description for the policy.

    When you're finished, click **Next**.

5. On the **Users, groups, and domains** page, identify the internal recipients that the policy applies to (recipient conditions):
    a. **Users**: The specified mailboxes, mail users, or mail contacts.
    b. **Groups**: Members of the specified distribution groups or mail-enabled security groups.
    c. **Domains**: All recipients in the specified accepted domains in your organization.

    When you're finished, click **Next**.

6. On the **Bulk email threshold & spam properties** page that appears, configure settings as needed. When you're finished, click **Next**.
7. On the **Actions** page that appears configure settings as needed.
8. On the **Allow & block list** flyout that appears, click **Allowed** > **Domains** > **Allow domains**.
9. Click **+** to **Add domains**.
10. Enter the domains listed at the end of this QRG in the **Domain** box.
11. Click **Add domains**, then **Next** when you're ready to continue.
12. On the **Review** page that appears, review your settings. You can select **Edit** in each section to modify the settings within the section. Or you can click **Back** or select the specific page in the wizard.

    When you're finished, click **Create**.

WHITELISTING MIMECAST

Objective: Using Mimecast security software, you can safelist (whitelist) VENZA to allow your users to receive our simulated phishing and system emails.

If you run into problems while safelisting in Mimecast, we suggest you first reach out directly to Mimecast for assistance.

• CREATING A PERMITTED SENDERS POLICY

We advise creating a new Permitted Sender Policy within your Mimecast console to safelist the VENZA.

Note: Do not edit your default Permitted Sender Policy. Instead, create a new one.

Steps:

1. From the Mimecast Administration Console, open the **Administration Toolbar**.
    a. Select **Gateway | Policies**.
    b. Select **Permitted Senders**.
    c. Select **New Policy**.
2. Select the below settings under the **Options**, **Emails From**, **Emails To**, and **Validity** sections.
3. For more information, see Mimecast's Configuring a Permitted Senders Policy.

Option	Settings
Options	
Policy Narrative	Phishing Permitted Senders
Select Option	Permit Sender
Emails From	
Applies To	Internal Addresses
Specifically	Applies to all Internal Recipients
Validity	
Enable/Disable	Enable
Set policy as perpetual	Always On
Date Range	All Time

Policy Override	Checked
Bi-directional	Unchecked
Source IP Ranges (n.n.n.n/x)	108.163.193.74

Adding VENZA to the permitted sender's list (see above) should bypass Greylisting. However, we recommend following the below Greylisting steps to improve email deliverability.

Steps:

1. From the Mimecast Administration Console, open the **Administration Toolbar**.
    a. Select **Gateway | Policies**.
    b. Select **Permitted Senders**.
    c. Select **New Policy**.
2. Select the below settings under the **Options**, **Emails From**, **Emails To**, and **Validity** sections.

Option	Settings
Options	
Policy Narrative	VENZA Greylist
Select Option	Take No Action
Emails From	
Addresses Based On	The Return Address
Applies From	Email Addresses
Specifically	Applies to all External Senders
Emails To	
Applies To	Internal Addresses
Specifically	Applies to all Internal Recipients
Validity	
Enable/Disable	Enable
Set policy as perpetual	Always On
Date Range	All Time

Policy Override	Checked
Bi-directional	Unchecked
Source IP Ranges (n.n.n.n/x)	108.163.193.74

- ## CREATING A URL PROTECTION BYPASS POLICY

Steps:

1. From the Mimecast Administration Console, open the **Administration Toolbar**.
    a. Select **Gateway | Policies**.
    b. Select **Permitted Senders**.
    c. Select **New Policy**.
2. Select the below settings under the **Options**, **Emails From**, **Emails To**, and **Validity** sections.

Option	Settings
Options	
Policy Narrative	Phishing URL Protection Bypass
Select Option	Disable URL Protection
Emails From	
Addresses Based On	Both
Applies From	Everyone
Specifically	Applies to all Senders
Emails To	
Applies To	Internal Addresses
Specifically	Applies to all Internal Recipients
Validity	
Enable/Disable	Enable
Set policy as perpetual	Always On
Date Range	All Time
Policy Override	Checked

Bi-directional	Unchecked
Source IP Ranges (n.n.n.n/x)	108.163.193.74
Hostname(s)	Leave blank

WHITELISTING SOPHOS

Objective: Using Sophos security software, you can safelist (whitelist) VENZA to allow your users to receive our simulated phishing and system emails.

If you run into problems while safelisting in Sophos, we suggest you first reach out directly to Sophos for assistance.

- ## MODIFYING ADD/BLOCK LISTS IN SOPHOS EMAIL APPLIANCE

Steps:

1. In your SEA manager, navigate to **Configuration** > **Policy** > **Allow Lists**.
2. Click the appropriate list to display the **List Editor** dialog box.
3. Select the **Senders** tab if you have an additional spam filter in front of SEA. Select the **Hosts** tab if you do not have an additional spam filter in front of SEA.
4. In the **Add entries** text box, enter each required item and click **Add**.
5. If in the Senders tab, enter VENZA domain names, one by one. These domains are listed at the end of this Quick Reference Guide.
6. If in the Hosts tab, enter the VENZA IP address. The VENZA IP address is listed at the end of this Quick Reference Guide.

- ## WHITELISTING IN SOPHOS XG FIREWALLS

Steps:

1. Log in to the portal for the firewall.
2. Click on **Web**, located on the left.
3. Click on **Exceptions**, located on the top.
4. If you don't have an exceptions list, click **Add Exception**.
5. Provide a name (**VENZA**) and an optional description for the list.

6. Check the boxes to the right under **Skip the selected checks or actions** for your purchased services.
7. Check **URL pattern matches**.
8. Enter the phishing domains one line at a time in the **Search/Add** box. These are located at the end of this Quick Reference Guide.
9. Click **Save** at the bottom of the page.

IP ADDRESS TO WHITELIST

108.163.193.74

PHISHING CAMPAIGN DOMAINS

account-profile.com	hotelreview.today
collectionsagency.co	humanresource.center
corporateoffice.biz	legalactions.org
discriminationweb.com	shipmentnotice.com
documentsservice.com	use-fedex.com
employeerewards.site	yelprating.com
expedia-us.com	your-account-login.com

CONTACT

Help Desk: noreply@venzagroup.com

Sales: sales@venzagroup.com

Customer Success: success@venzagroup.com