Phishing Whitelisting and Mitigating False Positives

Quick Reference Guide

Version: 2.3

Revised: December 2024

Contents

venza®

Introduction

This guide provides instructions for whitelisting and mitigating false positives in email server, firewalls, spam filters, and various other tools to ensure:

- **VENZA Phishing Campaigns** are delivered to recipients for testing.
- **VENZA Phishing Compliance Reports** provide actionable results for remediation.

Instructions are organized by the tool or resource.

To ensure a successful campaign, follow the directions for both the email server and any additional tools or resources your organisation uses.

Whitelisting

Whitelisting is a security practice that involves creating a list of approved email addresses, domains, or IP addresses that are allowed to send emails to an organisation's email system without being blocked or flagged as spam.

Mitigating False Positives

A false positive is an error that occurs when a system reports an event, such as a target clicking on a phishing email, when the end-user did not physically do so. They are not limited to any specific vendor or tool and occur in all phishing simulation platforms.

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 simulation tool, this registers as an action and is reported as such.

After whitelisting has occurred, additional rules and configurations may be enacted in email administration to mitigate this occurrence, including:

- Email Gateway Configuration
- Server-Side Rules
- Updating Policies in Email Administration

VENZA Whitelisting Information

Campaign IP Address

108.163.193.74

Domains

account-profile.com	expedia-us.com	usa-fedex.com
collectionsagency.com	noreply@venzagrc.com	yelprating.com
corporateoffice.biz	hotelreview.today	your-account-login.com
discriminationweb.com	humanresources.center	noreply@venzapeak.com
documentsservice.com	legalactions.org	root@internal.venzapeak.com
employeerewards.site	shipmentnotice.com	

Landing Page URLs

accounts.your-account-login.com	giftcard.your-account-login.com	reviewdocs.your-account-login.com
bdaycard.your-account-login.com	guestpromo.your-account-login.com	rewards.your-account-login.com
benefits.your-account-login.com	invoices.your-account-login.com	services.your-account-login.com
benifits.your-account-login.com	legalactions.your-account-login.com	shipmentnotice.your-account-login.com
collectionsagency.your-account-login.com	linkdin.your-account-login.com	subscription.your-account-login.com
debtcollections.your-account-login.com	newjobs.your-account-login.com	survey.your-account-login.com
directdeposit.your-account-login.com	payroll.your-account-login.com	trynet.your-account-login.com
documentshare.your-account-login.com	phishing.venzagroup.com	verify.your-account-login.com
documents.your-account-login.com	phonebill.your-account-login.com	wiretransfers.your-account-login.com
docusigning.your-account-login.com	promo.your-account-login.com	yelprating.your-account-login.com
email.your-account-login.com	publicadvise.your-account-login.com	

Whitelisting Email Providers

Google

Whitelisting by IP Address

1. Log into Google Workspace Admin platform.
2. Navigate to *Apps* then navigate to Google Workspace.
3. Select *Gmail* from the left-hand side.
4. Select your domain from the *Organizational Unit* section of the page.
5. Scroll to the *Spam, Phishing, and Malware* tab on the right-hand side of the page.
6. On the *Spam, Phishing, and Malware* tab, scroll to the *Email Allowlist* setting. Or, in the search field, enter "email allowlist."
7. In the *Email Allowlist* field, input VENZA IP Address (**108.163.193.74**).
8. Click *Save* at the bottom of the page.

Add Custom Spam Filter

1. Log into Google Workspace Admin platform.
2. Navigate to *Apps* then navigate to Google Workspace.
3. Select *Gmail* from the left-hand side.
4. On *Settings for Gmail* page, select *Spam, Phishing and Malware*.
5. Select your domain from the *Organizational Unit* section of the page.
6. Scroll to *Spam* and click *Configure* or *Add another rule.*
7. In the *Add setting* box, enter a unique name (i.e VENZA Phishing.)
8. Under the *Options to bypass filters and warning banners header*, scroll down to *Bypass spam filters and hide warnings for messages from senders or domains in selected lists*.
9. From those options, *Select Create or Edit* list.
10. *Manage Address List* window, select *Add Address List*.
11. Select *Bulk Upload Addresses*.
    a. Input the VENZA Phishing Campaign Domains, each separated by a comma, or copy the text provided below:

    humanresources.center,documentsservice.com,legalactions.org,employeerewards.site,your-account-login.com,corporateoffice.biz,employeerewards.site,collectionsagency.co,corporateoffice.biz,employeerewards.site,account-profile.com,shipmentnotice.com,yelprating.com

b. Click *Save.*

12. In the original *Add Setting* page, enable the *Navigate to Bypass spam filters and hide warnings for messages from senders or domains in selected lists* feature by checking the box beside it.
13. Select *Use Existing List* function beneath it and select the list just created.
14. Ensure the box is checked.

Add IP Addresses as Inbound Gateways

1. Log into Google Workspace Admin platform.
2. Navigate to *Apps* then navigate to Google Workspace.
3. Select *Gmail* from the left-hand side.
4. On *Settings for Gmail* page, select *Spam, Phishing and Malware*.
5. On the left, select your top-level organization.
6. Scroll to the *Inbound gateway setting*, then click *Edit*.
7. Fill out the information as follows:
   a. Under *Gateway IPs*, click add and input VENZA IP Address (**108.163.193.74**).
   b. Ensure the box next to *Reject all mail not from gateway* IPs is ***not*** checked.
   c. Check the box next *to Require TLS for connections from the email gateways above.*
   d. Check the box next to *Message is considered spam if the following header regexp matches.*
      I. In the text expression box below, type out a tag that is not likely to be found in a phishing test email.
      II. This could be a random assortment of letters, for instance: *sduenvgdopajwdkasd*.
   e. Check the box next to *Disable Gmail spam evaluation on mail from this gateway; use header value.*
   f. Click *Save.*

Whitelisting Harmony Email & Collaboration (Avanan) in Google

1. Log into Google Workspace Admin platform.
2. Navigate to *Apps* then navigate to *Google Workspace*.
3. Select *Gmail* from the left-hand side.
4. On the left, select your top-level organization.

5. On *Settings for Gmail* page, select *Compliance*.
6. Hover cursor over *Content Compliance* setting.
7. Click *Configure* or *Add Another* button.
8. In the *Add Setting* pop-up window, scroll to the content *Compliance* section and enter description of rule (i.e. VENZA Phishing.)
9. Under section number one, *Email messages to affect*, check the box next to *Inbound.*
10. Under section number two, *Expressions*, click *Add*.
11. A pop-up window will appear. From the first drop-down menu, select *Metadata match*.
12. From the *Attribute* drop-down menu, Select *source IP*.
13. From the *Match type* drop down menu, select *Source IP is within the following range.*
14. Enter the VENZA IP Address (108.163.193.74) into *Match type* field.
15. Click *Save* to return to *Expressions* section.
16. Click *Add* again.
17. A pop-up window will appear. From the first drop-down menu, select *Metadata match*.
18. From the *Attribute* drop-down menu, Select *source IP*.
19. From the *Match type* drop down menu, select *Source IP is not within the following range.*
20. Enter the VENZA IP Address (108.163.193.74) into *Match type* field.
21. Click *Save.*
22. In the *Headers* section, check the box next to *Add custom headers*.
23. Beneath the *Custom headers* field, click *Add*.
24. Type or copy and paste "X-CLOUD-SEC-AV-Info" (no quotes) into the *Header key* field.
25. In the *Header value* field, type "[portalname],google_mail,inline " (no quotes), but replace [portalname] with the name of your organisation's portal.
    - Click here for instructions on how to find your organisation's Harmony Email & Collaboration portal name
26. Click *Save*.
27. Review, then finalize settings by clicking *Save*.

Microsoft 365

Note: these instructions do not apply to mail servers that are Exchange 2010 or earlier.

Whitelisting Advanced Delivery Policy

1. Log into Microsoft 365 admin center via user account.
2. Navigate to *Admin Center*.
3. Navigate to *Security.*
4. In *Security*, navigate to *Email & Collaboration* section and select *Policies & Rules.*
5. Navigate to *Threat Policies*.
6. Navigate to *Advanced delivery*
7. Select the *Phishing Simulation* tab on *Advanced Delivery* page.
8. Click *Edit*.
9. Input the following information into the *Edit Third party Phishing Simulation* section.
   a. In *Domain*, input VENZA Phishing Campaign Domains.
   b. In *Sending IP*, input VENZA IP Address (**108.163.193.74**).
   c. In *Simulations URLs to Allow*, enter VENZA Phishing Campaign URLs.

Additional Threat Polices Exemption

1. Log into Microsoft 365 admin center via user account.
2. Navigate to *Admin Center*.
3. Navigate to *Security*
4. Click on *Policies & Rules* and select *Anti-Spam* under *Policies* options.
5. Click *Connection Filter Policy* and select the *Edit Connection Filter*.
6. Add VENZA IP Address (**108.163.193.74**) into the section titled *Always allow messages from the following IP addresses or address range*.
7. Enable *Turn on Safe* list option.
8. Click *Save*.

Spam Filter Bypass

1. Log into Microsoft 365 admin center via user account.
2. Navigate to *Exchange* and then *Mail Flow.*

3. From *Mail Flow*, navigate to *Rules.*
4. Click the + *Add a Rule* button.
5. Select the *Bypass Spam Filter* option, creating a name for the rule when prompted.
6. Input the following options:
    a. In the *Apply this rule if…* section, select *The Sender*. Then, select *IP address IP address is in any of these ranges or exactly matches*.
        I. On the right-hand side next to *Enter Text* click *Enter Words* which will bring up the *Specify IP Address Ranges* window.
        II. Input VENZA IP Address (**108.163.193.74**).
        III. Click *Save*.
    b. In the *Do the Following…* field, click the + (plus) button to create a new rule.
        I. Click *Modify the message properties* option.
        II. Select the *Set the spam confidence level (SCL)* option.
        III. Click the *Set the Spam Confidence level (SCL)* to ***"-1"*** option.
        IV. Click *Bypass Spam Filtering*.
        V. Click *Save.*
    c. Remaining on the *Do the Following…* field, click the + (plus) button to create another rule.
        I. Click *Modify the message properties* option.
        II. Select the *Set a Message Header* option.
        III. Click *Enter Words*.
        IV. In the field, type "X-MS-Exchange-Organization-BypassClutter".
        V. Click *Save*.
        VI. Click "*Enter Words*" and under the *Header Value and* manually type "True".
        VII. Click *Save.*
7. Ensure the new rule's status is set to enabled.
    a. If it is set to disabled, click on the newly set up rule.
    b. Click *Enable.*
    c. Click the *Edit Rule Settings* button on the window to save it as enabled.

Whitelisting Harmony Email & Collaboration (Avanan) in Microsoft 365

1. Log into Microsoft 365 admin center.
2. Navigate to *Admin Center*.
3. Navigate to *Exchange.*
4. On the *Navigation Panel*, click *Mail Flow*.
5. Click on *Rules.*
6. Click the *plus sign symbol (+)* at the top of the page.
7. From the drop-down menu, click *Create a new rule*.
8. In the *New Rule* pop-up window, enter a custom name in the *Name* field, (i.e. VENZA Phishing.)
9. In the *Apply this Rule If…* drop-down menu, click *The Sender* option. Then, select *IP Address is in any of these ranges or exactly matches* selection.
10. Enter VENZA IP (**108.163.193.74**) into the pop-up window.
11. Click *Save*.
12. From the *Do the following…* drop-down menu, select *Modify the message properties*.
13. Select *Set a message header.*
14. Click the *Enter Text* option beneath the *Do the following…*menu.
15. Type or copy and paste "X-CLOUD-SEC-AV-Info" (no quotes) into the pop-up's field.
16. Click *Save*.
17. Click the second *Enter Text* option
18. In the pop-up window, type or copy and paste "[portalname],office365_emails,inline" (no quotes), but replace [portalname] with the name of your organisation's portal
    - Click here for instructions on how to find your organisation's Harmony Email & Collaboration portal name.
19. Click *Save.*
20. Click *Next.*
21. In the *Set rule settings* page, navigate to *Rule mode* and select *Enforce*.
22. Check the *Stop processing more rules* box at the bottom of the page.
23. Click *Next.*
24. Review settings and finalize by clicking *Finish*.
25. Move this rule's priority above *Avanan Harmony Email - Protect mail flow* rule.

Advanced Threat Protection Link Exemptions

1. Log into Microsoft 365 admin center via user account.
2. Navigate to *Exchange* and then *Mail Flow.*
3. From *Mail Flow*, navigate to *Rules.*
4. Click the + *Add a Rule* button.
5. Create name for rule.
6. Input the following options:
    a. In the *Apply this rule if…* section, select *The Sender.* Then, select *IP address is in any of these ranges or exactly matches.*
        I. On the right-hand side next to *Enter Text* click *Enter Words* which will bring up the *Specify IP Address Ranges* window.
        II. Input VENZA IP Address (**108.163.193.74**).
        III. Click *Save.*
    b. In the *Do the following* section, select *Modify the message properties* option.
        I. Select the *Set a message header* option.
        II. Set the message header to *X-MS-Exchange-Organization-SkipSafeLinksProcessing.*
        III. Set the Value to "1".
    c. Click *Save.*
8. Ensure the new rule's status is set to enabled.
    a. If it is set to disabled, click on the newly set up rule.
    b. Click *Enable.*
    c. Click the *Edit Rule Settings* button on the window to save it as enabled.

Microsoft Exchange (2016, 2019)

Whitelisting by IP Address

1. Log in to your Exchange Admin Center account and navigate to *Mail Flow.*
2. From *Mail Flow*, select *Rules.*
3. Click the + *Add Rule* then select *Create a New Rule* from the drop-down.
4. In the top text field, provide the rule with a custom name (i.e. VENZA Phishing.)
5. In the *Apply this rule if…* section, select *The Sender* in the left-hand box and *IP address is in any of these ranges or exactly matches* in the right-hand box.

6. In the *Specify IP address ranges* pop-up window, enter VENZA IP (**108.163.193.74**).
7. Click *Save.*
8. In the *Do the following* section, select *Modify the message properties* in the left-hand box and *set a message header* in the right-hand box.
9. Beneath the fields in the *Do the Following* section just edited, click on the left-hand/first *Enter Text* option.
10. Type "X-MS-Exchange-Organization-BypassClutter" (no quotes) into the field.
11. Click Save.
12. Beneath the fields in the *Do the Following* section just edited, click on the right-hand side/second *Enter Text* option.
13. Type "true"(no quotes, case sensitive)
14. Click *Save.*
15. Click the + *(plus sign)* symbol on the right-hand side of the *Do the Following section*…
16. In the two new drop-down menus that have appeared under *And;* select *Modify the message properties* option on the left-hand side.
17. From the right-hand drop-down menu under *And*, select *set the spam confidence level (SCL)* option.
18. Select *Bypass spam filtering* option in the *Specify SCL* pop-up window.
19. Click *Save.*
20. Click *Next* to proceed to the *Set Rule Settings* page.
21. Leave all options/settings on the *Set Rule Settings* page the same.
22. Click *Next.*
23. On the *Review and finish* page, click *Finish.*

Whitelisting Spam Filters & Firewalls

AppRiver

Whitelisting Spam Filter

1. Log into AppRiver Admin Center.
2. Navigate to *Filters,* a selectable tab at the top of the page.
3. On the left-hand side of the *Filters* page, select *IP Addresses.*
4. Click the *Add* button beneath the *Allowed IP Addresses* header.
5. Add the VENZA IP (**108.163.193.74**).
6. Click *Save.*

Barracuda Essentials

Whitelisting Email Security Service on Cloud

1. Log into the Barracuda Cloud Control platform.
2. Navigate to *Email Security.*
3. From *Email Security*, navigate to *Inbound Settings.*
4. From *Inbound Settings*, navigate to *IP Address Policies.*
5. Select *IP Blocking/Exemption* section and in the topmost line, enter the VENZA IP Address (**108.163.193.74**).
6. In the *Netmask* field, input **255.255.255.255**
7. In the *Policy* field, select *Exempt.*
8. Click *Add* to finalize the process.

Whitelisting Email Security Gateway

1. Log into the Barracuda Email Security Gateway web portal.
2. From the dashboard, navigate to *BLOCK/ACCEPT* page.
3. From *BLOCK/ACCEPT* page, navigate to *IP Filters. .*
4. Select *Allowed IP/Range* section and in the topmost line, enter the VENZA IP Address (**108.163.193.74**).
5. In the *Netmask* field, input **255.255.255.255**

6. In the *Policy* field, select *Exempt.*
7. Click *Add* to finalize the process.

Barracuda Advanced Threat Protection Exemption

1. Log into the Barracuda Email Security Gateway web portal.
2. From the dashboard, navigate to *ATP Settings* page.
3. Enter the VENZA IP Address (**108.163.193.74**).
4. In the *Netmask* field, input **255.255.255.255**
5. Click *add* to complete.

Allow Senders list

1. Log into the Barracuda Admin console.
2. Navigate to *Dashboard.*
3. Navigate to *Settings.*
4. Navigate to *Allowed Senders.*
5. Enter VENZA Phishing Campaign Domain Names.
6. Click *Save.*

Cisco Cloud Email Security

Whitelisting by IP Address

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*, create a group with this title.
4. Click *Add Sender* and then add the VENZA IP (**108.163.193.74**).
5. Click *Submit* and then *Commit Changes.*

Whitelisting Outbreak Filter Scanning

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.*

Fortinet FortiGate

Whitelisting Campaign URLs

1. Log into your Fortinet administrative account.
2. Navigate to *Security Profiles*, then *Web Filter*.
3. Create a new filter, then expand *Status URL Filter*, enable it and select *Create.*
4. Input the VENZA Phishing Campaign URLs
   a. All campaign URLs must be input individually, without https://.
5. Under type, select *Simple.*
6. Ensure *Status* is enabled.

Mimecast

Add a Permitted Sender's Policy

NOTE: Do not edit the default Permitted Sender policy. Create a new policy for each Whitelisting and Minimizing False Positive direction.

1. Log into Mimecast Administration Console.
2. From the *Administration* toolbar button, select the *Gateway / Policies* menu item.
3. From the list of policies, select *Permitted Senders*.
4. Click the *New Policy* button.
5. Fill out the policy fields as outlined below:
   a. **Options**
      I. Policy Narrative: VENZA Phishing
      II. Permitted Sender Policy: Permit Sender
   b. **Emails From**
      I. Addresses Based on: Both
      II. Applies From: Everyone
      III. Specifically: Applies to all Senders
   c. **Emails To**
      I. Applies To: Everyone
      II. Specifically: Applies to all Recipients

d. **Validity**
    I. Enable/Disable: Enable
    II. Set Policy as Perpetual: Always On
    III. Date Range: All Time
    IV. Policy Override: Checked.
    V. Bi-Directional: Unchecked.
e. **Source IP Ranges**
    I. Enter the VENZA IP Address and add */32* (e.g. **108.163.193.74/32**).

6. *Save* and *Exit.*

Greylisting

1. Log into Mimecast Administration Console.
2. From the *Administration* toolbar button, select the *Gateway / Policies* menu item.
3. From the list of policies, select *Greylisting.*
4. Click the *New Policy* button.
5. Fill out the policy fields as outlined below:
    a. **Options**
        I. Policy Narrative: GreyList Bypass VENZA Phishing
        II. Permitted Sender Policy: Take no action
    b. **Emails From**
        I. Addresses Based on: The Return Address
        II. Applies From: Everyone
        III. Specifically: Applies to all Senders
    c. **Emails To**
        I. Applies To: Everyone
        II. Specifically: Applies to all Recipients
    d. **Validity**
        I. Enable/Disable: Enable
        II. Set Policy as Perpetual: Always On
        III. Date Range: All Time
        IV. Policy Override: Checked.
        V. Bi-Directional: Unchecked.

e. **Source IP Ranges**
    I. Enter the VENZA IP Address and add */32* (e.g. **108.163.193.74/32**).
6. *Save* and *Exit.*

DNS Inbound Authentication

1. Log into Mimecast Administration Console.
2. From the *Administration* toolbar button, select the *Gateway / Policies* menu item.
3. From the *Definitions* drop-town menu, navigate to *DNS Authentication-Inbound* option.
4. Select New DNS Authentication – Inbound Checks.
5. Create a name for the *New DNS Authentication*
6. Leave all options unchecked.
7. Click *Save* and *Exit.*
8. Navigate to the *Administration* toolbar button and select the *Gateway / Policies* menu item.
9. From the list of policies, select *DNS Authentication – Inbound* policy.
10. Click the *New Policy* button.
11. Fill out the policy fields as outlined below:
    a. **Options**
        I. Policy Narrative: VENZA DNS Auth
        II. Permitted Sender Policy: No Authentication
    b. **Emails From**
        IV. Addresses Based on: Both
        I. Applies From: Everyone
        II. Specifically: Applies to all Senders
    c. **Emails To**
        I. Applies To: Address Groups
        II. Specifically: Email Security Admins
    d. **Validity**
        VI. Enable/Disable: Enable
        I. Set Policy as Perpetual: Always On
        II. Date Range: All Time
        III. Policy Override: Checked.
        IV. Bi-Directional: Unchecked.

e. **Source IP Ranges**
    I. Enter the VENZA IP Address and add */32* (e.g. **108.163.193.74/32**).

12. *Save* and *Exit.*

URL Bypass Policy

1. Log into Mimecast Administration Console.
2. From the *Administration* toolbar button, select the *Gateway / Policies* menu item.
3. From the list of policies, select *URL Protection Bypass.*
4. Click the *New Policy* button.
5. Fill out the policy fields as outlined below:
    a. **Options**
        I. Policy Narrative: VENZA Phishing URL Bypass
        II. Select Option: Take No Action
    b. **Emails From**
        I. Addresses Based on: Both
        II. Applies From: Everyone
        III. Specifically: Applies to all Senders
    c. **Emails To**
        I. Applies To: Internal Addresses
        II. Specifically: Applies to all Internal Recipients
    d. **Validity**
        I. Enable/Disable: Enable
        II. Set Policy as Perpetual: Always On
        III. Date Range: All Time
        IV. Policy Override: Checked.
        V. Bi-Directional: Unchecked.
    e. **Source IP Ranges**
        I. Enter the VENZA IP Address and add */32* (e.g. **108.163.193.74/32**).
6. *Save* and *Exit.*

Proofpoint

Safelisting IPs Proofpoint Essentials

1. Log into Proofpoint Essentials then navigate to *Security Settings*
2. Navigate to *Email* then *Senders Lists.*
3. Select Safe Senders List.
4. Enter the VENZA IP Address (**108.163.193.74**) to the applicable field.
5. Click *Save.*

Safelisting Domains in Proofpoint Essentials

1. Log into Proofpoint Essentials then navigate to *Security Settings*
2. Navigate to *Email* then *Filter Policies.*
3. On the *Inbound* tab, click *New Filter.*
4. Create a custom name for the filter (i.e VENZA Phishing.)
5. Ensure the *Direction* is set to *Inbound,* then click Continue.
6. Under *Filter Logic* section, ensure the *Scope* filter is set to <Company>.
7. Select the following fields from the drown-down boxes below the *If* section:
   a. First drop-down box: Sender Address.
   b. Second drop-down box: IS
   c. Third drop-down box: Enter one of the VENZA Phishing Campaign Domains.
8. In *Do* section, select *Allow* from *Actions* drop-down menu.
9. In the *Filter Details* box on the right-hand side, describe the filter if need be.
10. Click *Save.*
11. Follow Steps 3-10 for each of the VENZA Phishing Campaign Domains.

Whitelisting in Proofpoint Enterprise

1. Log into Proofpoint Enterprise Admin portal.
2. Navigate to *Email Protection.*
3. Under *Spam Protection*, select *Organizational Safe List* option.
4. Click *Add.*
5. In the *Proofpoint -Global Safe* pop-up window, fill out the fields as outlined below:
   a. Filter Type: Sender Hostname

b. Operator: Equals
c. Value: Enter VENZA Phishing Campaign Domains.

6. Click *Save Changes.*

Whitelisting in Proofpoint URL Defense

1. Log into Proofpoint Enterprise Admin portal.
2. Navigate to *Email Protection.*
3. Under *Targeted Attack Protection* drop-down menu, select *URL Defense.*
4. Click *URL Rewrite Policies.*
5. Navigate to *Exceptions* section and enter VENZA Phishing Campaign Domains.
6. Click *Save Changes.*

Whitelisting Proofpoint Email Firewall

1. Log into Proofpoint Enterprise Admin portal.
2. Navigate to *Email Firewall* and then select *Rules.*
3. Under *Rule Settings*, select the *On* radio button for *Enable.*
4. Enter a custom name for the rule (i.e. VENZA Phishing.)
5. Under the *Conditions* section, select *Add.*
6. Enter each of the VENZA Phishing Campaign Domains.
7. Under the *Disposition* section, select *Deliver Now* as the *Delivery Method.*
8. Click *Save.*

Sophos

Modify Allow/Block List in Sophos Email

1. Log into Sophos Email Appliance (SEA.)
2. Navigate to *Configuration* then *Policy.*
3. From *Policy*, navigate to *Allow Lists.*
4. Click the applicable list based on the information below to open *List Editor* window and continue:
   a. Spam Filter Outside of SEA: **Senders tab.**
      I. Enter each required item in the *Add* entries text field.
      II. Click *Add.*

III. Individually enter each of the VENZA Phishing Campaign Domains.

b. No Spam Filter Outside of SEA: **Hosts tab.**

I. Enter each required item in the *Add* entries text field.

II. Click *Add.*

III. Input VENZA IP Address (**108.163.193.74**).

Whitelisting in Sophos XG Firewall

1. Log into Sophos XG Firewall portal.
2. Click on *Web.*
3. Navigate to *Exceptions.*
4. Click on *Add Exception.*
5. Create a name (VENZA Phishing) and a description.
6. Under *Skip the selected checks or actions*, check each box for applicable Sophos products.
7. In the *Search/Add* box, enter VENZA Phishing Campaign Domains in the format below:
   a. ^([A-Za-z0-9.-]*\.)?ABC\.com\.?/
      I. In "ABC", input VENZA Phishing Campaign Domain name before top-level domain.
      II. In ".com", input the top-level domain of the VENZA Phishing Campaign Domain.
8. Click *Save.*

SonicWall

Whitelisting IPs in Email Security Device

1. Log in to the admin SonicWall appliance.
2. Click *Manage.*
3. In the *Security Services* section, navigate to *Anti-Spam.*
4. From *Anti-Spam*, navigate to *Address book* then *Allowed.*
5. Click *Add.*
6. Select *IPs* from the *Select List Type* drop-down menu.
7. In the text box, enter the VENZA IP Address (**108.163.193.74)**

8. Click *Add.*

Whitelisting IPs in SonicWall's CFS Policy

1. Log in to SonicWall management page.
2. Click *Policies* then select *Objects*.
3. Under *Address Options*, click *Add.*
4. In the text box, enter the VENZA IP Address (**108.163.193.74)**
5. Navigate back to *Policies* then select *Objects.*
6. Under *Address Groups*, select Add.
7. Provide a custom name for the *Exclusion Group* (i.e VENZA Phishing.)
8. Highlight the previously added VENZA IP Address **(108.163.193.74)** and click the adjacent arrow to move the group to the box on the right.
9. Click *OK.*
9. Now, log in to the admin SonicWall appliance.
10. Click *Manage* and navigate to *Security Services*.
11. From *Security Services*, navigate to *Content Filter.*
12. Click the *Excluded Address* option
13. Select the previously created *Exclusion Group* (I.e. VENZA Phishing) from the drop-down menu.
14. Click *Accept.*

SpamTitan

Adding Allowed IP Addresses

1. Log into SpamTitan Email Security portal.
2. Navigate to *System Setup* then *Mail Relay*.
3. Select *IP Controls* then click *Add*.
4. In the *Add Allowed IP* pop-up window, complete the following fields following the steps below:
   a. IP/Network: Enter VENZA IP Address **(108.163.193.74)**
   b. Netmask: Enter 255.255.255.255
   c. Address Type: Select IPv4
5. Click *Save*.

Support

We are here to support you through every step of the whitelisting and mitigating phishing false positive process. If you encounter any issues or have questions, please reach out for support.

Contact Us

Email

Phone

Live Chat

Ticket

Contact Your Email Service Provider

If you are experiencing technical difficulties specific to your email system and/or the related tools above, please contact your email service provider directly. They can provide additional support and troubleshooting tailored to your email platform.

About VENZA

VENZA is a leading provider of security awareness data protection solutions that empower the hospitality industry to mitigate vulnerabilities and ensure compliance. VENZA supports over 2000 hotels globally, keeping guests and their data safe from breaches with 360-degree visibility for proactive management of risks. This allows property managers to focus on guest service and building trust in their brand.

Visit www.VENZAGroup.com for additional details.

Contact Us

Sales: sales@venzagroup.com

Customer Success: success@venzagroup.com