Listas blancas de phishing y mitigación de falsos positivos

Guía de referencia rápida

Versión: 2.3

Revisado: Diciembre 2024

Contenidos

venza®

Introducción

Esta guía proporciona instrucciones para la lista blanca y la mitigación de falsos positivos en el servidor de correo electrónico, cortafuegos, filtros de spam, y varias otras herramientas para asegurar:

- **Las campañas de phishing de VENZA** se entregan a los destinatarios para que las prueben.
- **Los informes de cumplimiento de phishing de VENZA** proporcionan resultados procesables para su corrección.

Las instrucciones están organizadas por herramienta o recurso.

Para garantizar el éxito de la campaña, siga las instrucciones tanto del servidor de correo electrónico como de las herramientas o recursos adicionales que utilice su organización.

Lista blanca

Las listas blancas son una práctica de seguridad que consiste en crear una lista de direcciones de correo electrónico, dominios o direcciones IP autorizadas para enviar correos electrónicos al sistema de correo electrónico de una organización sin ser bloqueadas o marcadas como spam.

Mitigar los falsos positivos

Un falso positivo es un error que se produce cuando un sistema informa de un evento, como que un objetivo ha hecho clic en un correo electrónico de phishing, cuando el usuario final no lo ha hecho físicamente. No se limitan a ningún proveedor o herramienta específica y se producen en todas las plataformas de simulación de phishing.

Los falsos positivos suelen estar causados por el filtro de seguridad de los proveedores de correo electrónico. Los filtros inspeccionan el contenido de los correos electrónicos antes de enviarlos a la bandeja de entrada del destinatario. Para la herramienta de simulación de phishing, esto se registra como una acción y se notifica como tal.

Una vez creadas las listas blancas, se pueden promulgar reglas y configuraciones adicionales en la administración del correo electrónico para mitigar esta incidencia, entre las que se incluyen:

- Configuración del gateway de correo electrónico
- Reglas del servidor
- Actualización de directivas en la administración del correo electrónico

VENZA Información sobre listas blancas

Dirección IP de la campaña

108.163.193.74

Dominios

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	

URL de la página de destino

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	

Proveedores de correo electrónico en lista blanca

Google

Listas blancas por dirección IP

1. Accede a la plataforma Google Workspace Admin.
2. Ve a *Aplicaciones* y, a continuación, a Google Workspace.
3. Selecciona *Gmail* en la parte izquierda.
4. Seleccione su dominio en la sección *Unidad organizativa* de la página.
5. Desplácese hasta la pestaña *Spam, phishing y malware* en la parte derecha de la página.
6. En la pestaña *Spam, phishing y malware*, desplácese hasta la configuración Lista permitida de correo electrónico. O, en el campo de búsqueda, introduce "email allowlist".
7. En el campo *Email Allowlist*, introduzca VENZA IP Address (**108.163.193.74**).
8. Haga clic en *Guardar* en la parte inferior de la página.

Añadir filtro antispam personalizado

1. Accede a la plataforma Google Workspace Admin.
2. Ve a *Aplicaciones* y, a continuación, a Google Workspace.
3. Selecciona *Gmail* en la parte izquierda.
4. En la página *Configuración de Gmail*, selecciona *Spam, phishing y malware*.
5. Seleccione su dominio en la sección *Unidad organizativa* de la página.
6. Desplácese hasta *Spam* y haga clic en *Configurar* o en *Añadir otra regla.*
7. En el cuadro *Añadir configuración*, introduzca un nombre único (por ejemplo, VENZA Phishing.)
8. En el *encabezado Opciones para omitir filtros y banners de advertencia*, desplácese hasta *Omitir filtros de spam y ocultar advertencias para mensajes de remitentes o dominios de las listas seleccionadas*.
9. En esas opciones, *seleccione Crear o Editar* lista.
10. En la ventana *Gestionar lista de direcciones*, seleccione *Añadir lista de direcciones*.

11. Seleccione *Direcciones de carga masiva*.
    a. Introduzca los dominios de la campaña de phishing de VENZA, cada uno separado por una coma, o copie el texto que se proporciona a continuación:
    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. Haga clic en *Guardar.*
12. En la página *Agregar configuración* original, activa la función *Navegar para omitir filtros de spam y ocultar advertencias de mensajes de remitentes o dominios de listas seleccionadas* marcando la casilla que aparece junto a ella.
13. Seleccione debajo la función *Utilizar lista existente* y seleccione la lista que acaba de crear.
14. Asegúrese de que la casilla está marcada.

Añadir direcciones IP como pasarelas de entrada

1. Accede a la plataforma Google Workspace Admin.
2. Ve a *Aplicaciones* y, a continuación, a Google Workspace.
3. Selecciona *Gmail* en la parte izquierda.
4. En la página *Configuración de Gmail*, selecciona *Spam, phishing y malware*.
5. A la izquierda, seleccione su organización de nivel superior.
6. Desplácese hasta la *opción Pasarela de entrada* y haga clic en *Editar*.
7. Rellene los siguientes datos:
    a. En *Gateway IPs*, haz clic en add e introduce VENZA IP Address (**108.163.193.74**).
    b. Asegúrese de que la casilla junto a *Rechazar todo el correo que no proceda de* IPs de *pasarela* ***no*** esté marcada.
    c. Marque la casilla junto *a Requerir TLS para conexiones desde las pasarelas de correo electrónico anteriores.*
    d. Marque la casilla junto a *El mensaje se considera spam si coincide la siguiente regexp de encabezado*.
        I. En el cuadro de expresión de texto que aparece a continuación, escriba una etiqueta que no sea probable encontrar en un correo electrónico de prueba de phishing.
        II. Puede ser una combinación aleatoria de letras, por ejemplo: *sduenvgdopajwdkasd*.

e. Marque la casilla junto a *Desactivar la evaluación de spam de Gmail en el correo de esta puerta de enlace; utilizar valor de encabezado.*
f. Haga clic en *Guardar.*

Listas blancas Harmony Email & Collaboration (Avanan) en Google

1. Accede a la plataforma Google Workspace Admin.
2. Ve a *Aplicaciones* y, a continuación, a *Google Workspace*.
3. Selecciona *Gmail* en la parte izquierda.
4. A la izquierda, seleccione su organización de nivel superior.
5. En la página *Configuración de Gmail*, selecciona *Cumplimiento*.
6. Pase el cursor por encima de la opción *Cumplimiento de contenidos*.
7. Pulse el botón *Configurar* o *Añadir otro*.
8. En la ventana emergente *Añadir configuración*, desplácese hasta la sección *Cumplimiento de* contenido e introduzca la descripción de la regla (es decir, VENZA Phishing.)
9. En la sección número uno, *Mensajes de correo electrónico a afectar*, marque la casilla junto a *Entrada*.
10. En la sección número dos, *Expresiones*, haga clic en *Añadir*.
11. Aparecerá una ventana emergente. En el primer menú desplegable, seleccione *Coincidencia de metadatos*.
12. En el menú desplegable *Atributo*, seleccione *IP de origen*.
13. En el menú desplegable *Match type*, seleccione *Source IP is within the following range*.
14. Introduzca la dirección IP de VENZA (108.163.193.74) en el campo *Tipo de coincidencia*.
15. Haga clic en *Guardar* para volver a la sección *Expresiones*.
16. Vuelva a hacer clic en *Añadir*.
17. Aparecerá una ventana emergente. En el primer menú desplegable, seleccione *Coincidencia de metadatos*.
18. En el menú desplegable *Atributo*, seleccione *IP de origen*.
19. En el menú desplegable *Match type*, seleccione *Source IP is not within the following range.*
20. Introduzca la dirección IP de VENZA (108.163.193.74) en el campo *Tipo de coincidencia*.
21. Haga clic en *Guardar.*

22. En la sección *Encabezados*, marque la casilla situada junto a *Añadir encabezados personalizados*.
23. Debajo del campo *Encabezados personalizados*, haga clic en *Añadir*.
24. Escriba o copie y pegue "X-CLOUD-SEC-AV-Info" (sin comillas) en el campo *Clave de encabezado*.
25. En el campo *Valor del encabezado*, escriba "[nombredelportal],google_mail,inline " (sin comillas), pero sustituya [nombredelportal] por el nombre del portal de su organización.
    - Haga clic aquí para obtener instrucciones sobre cómo encontrar el nombre del portal Harmony Email & Collaboration de su organización.
26. Haga clic en *Guardar*.
27. Revise y, a continuación, finalice la configuración haciendo clic en *Guardar*.

Microsoft 365

Nota: estas instrucciones no se aplican a servidores de correo que sean Exchange 2010 o anteriores.

Política de entrega avanzada de listas blancas

1. Inicie sesión en el centro de administración de Microsoft 365 a través de la cuenta de usuario.
2. Vaya *al Centro de administración*.
3. Navegue hasta *Seguridad*.
4. En *Seguridad*, vaya a la sección *Correo electrónico y colaboración* y seleccione *Políticas y reglas*.
5. Navegue hasta *Políticas de amenazas*.
6. Navegue hasta Entrega *avanzada*
7. Seleccione la pestaña *Simulación de phishing* en la página *Entrega avanzada*.
8. Haga clic en *Editar*.
9. Introduzca la siguiente información en la sección *Editar simulación de phishing de* terceros.
    a. En *Dominio*, introduzca VENZA Phishing Campaign Domains.
    b. En *IP de envío*, introduzca la dirección IP de VENZA (**108.163.193.74**).
    c. En *Simulaciones URL a permitir*, introduzca las URL de la campaña de phishing de VENZA.

Políticas adicionales sobre amenazas Exención

1. Inicie sesión en el centro de administración de Microsoft 365 a través de la cuenta de usuario.
2. Vaya *al Centro de administración*.
3. Ir a *Seguridad*
4. Haga clic en *Políticas y reglas* y seleccione *Antispam* en las opciones de *Políticas*.
5. Haga clic en *Política de filtro de conexión* y seleccione *Editar filtro de conexión*.
6. Añade la dirección IP de VENZA (**108.163.193.74**) en la sección titulada *Permitir siempre mensajes de las siguientes direcciones IP o rango de direcciones*.

7. Active la opción *Activar* lista *segura*.
8. Haga clic en *Guardar*.

Filtro antispam Bypass

1. Inicie sesión en el centro de administración de Microsoft 365 a través de la cuenta de usuario.
2. Vaya a *Exchange* y, a continuación, a *Flujo de correo*.
3. Desde *Flujo de correo*, vaya a *Reglas*.
4. Haga clic en el botón + *Añadir una regla*.
5. Seleccione la opción *Bypass Spam* Filter, creando un nombre para la regla cuando se le solicite.
6. Introduzca las siguientes opciones:
   a. En la sección *Aplicar esta regla si...*, seleccione *El remitente*. A continuación, seleccione *Dirección IP La dirección IP se encuentra en alguno de estos rangos o coincide exactamente*.
      I. A la derecha, junto a *Introducir texto*, haga clic en *Introducir* palabras, lo que abrirá la ventana *Especificar intervalos de direcciones IP*.
      II. Introduzca la dirección IP de VENZA (**108.163.193.74**).
      III. Haga clic en *Guardar*.
   b. En el campo *Hacer lo siguiente...*, haga clic en el botón + (más) para crear una nueva regla.
      I. Haga clic en la opción *Modificar las propiedades del mensaje*.
      II. Seleccione la opción *Establecer el nivel de confianza de spam (SCL)*.
      III. Haga clic en la opción *Establecer el nivel de confianza de spam (SCL)* en ***"-1"***.
      IV. Haga clic en *Bypass Spam Filtering*.
      V. Haga clic en *Guardar*.
   c. Permaneciendo en el campo *Hacer lo siguiente...*, haga clic en el botón + (más) para crear otra regla.
      I. Haga clic en la opción *Modificar las propiedades del mensaje*.
      II. Seleccione la opción *Establecer un encabezado de mensaje*.
      III. Haz clic en *Introducir palabras*.
      IV. En el campo, escriba "X-MS-Exchange-Organization-BypassClutter".
      V. Haga clic en *Guardar*.

VI. Haga clic en "*Introducir palabras*" y en el *valor de la cabecera y* escriba manualmente "True".

VII. Haga clic en *Guardar.*

7. Asegúrese de que el estado de la nueva regla está activado.
   a. Si está desactivada, haga clic en la regla recién creada.
   b. Haz clic en *Activar*.
   c. Haga clic en el botón *Editar configuración de reglas* de la ventana para guardarla como activada.

Lista blanca de Harmony Email & Collaboration (Avanan) en Microsoft 365

1. Inicie sesión en el centro de administración de Microsoft 365.
2. Vaya *al Centro de administración*.
3. Navegue hasta *Exchange*.
4. En el *Panel de navegación*, haga clic en *Flujo de correo*.
5. Haga clic en *Reglas*.
6. Haga clic en el *signo más (+)* en la parte superior de la página.
7. En el menú desplegable, haga clic en *Crear una nueva regla*.
8. En la ventana emergente *Nueva regla*, introduzca un nombre personalizado en el campo *Nombre*, (por ejemplo, VENZA Phishing.)
9. En el menú desplegable *Aplicar esta regla si...*, haga clic en la opción *El remitente*. A continuación, seleccione *Dirección IP está en cualquiera de estos rangos o coincide exactamente con* la selección.
10. Introduzca la IP de VENZA (**108.163.193.74**) en la ventana emergente.
11. Haga clic en *Guardar*.
12. En el menú desplegable *Hacer lo siguiente...*, seleccione *Modificar las propiedades del mensaje*.
13. Seleccione *Establecer una cabecera de mensaje*.
14. Haga clic en la opción *Introducir texto* debajo del menú *Haga lo siguiente...*.
15. Escribe o copia y pega "X-CLOUD-SEC-AV-Info" (sin comillas) en el campo de la ventana emergente.
16. Haga clic en *Guardar*.

17. Haga clic en la segunda opción *Introducir texto*
18. En la ventana emergente, escriba o copie y pegue "[nombredelportal],office365_emails,inline" (sin comillas), pero sustituya [nombredelportal] por el nombre del portal de su organización.
    - Haga clic aquí para obtener instrucciones sobre cómo encontrar el nombre del portal Harmony Email & Collaboration de su organización.
19. Haga clic en *Guardar*.
20. Haga clic en *Siguiente*.
21. En la página *Establecer configuración de reglas*, desplácese al *modo Regla* y seleccione *Aplicar*.
22. Marque la casilla *Detener el procesamiento de más reglas* en la parte inferior de la página.
23. Haga clic en *Siguiente*.
24. Revise la configuración y finalice haciendo clic en *Finalizar*.
25. Mueva la prioridad de esta regla por encima de la regla de *flujo de correo Avanan Harmony Email - Protect*.

Protección avanzada contra amenazas Exenciones de enlace

1. Inicie sesión en el centro de administración de Microsoft 365 a través de la cuenta de usuario.
2. Vaya a *Exchange* y, a continuación, a *Flujo de correo*.
3. Desde *Flujo de correo*, vaya a *Reglas*.
4. Haga clic en el botón + *Añadir una regla*.
5. Crear nombre para la regla.
6. Introduzca las siguientes opciones:
    a. En la sección *Aplicar esta regla si...*, seleccione *El remitente*. A continuación, seleccione *La dirección IP está en cualquiera de estos rangos o coincide exactamente*.
        I. A la derecha, junto a *Introducir texto*, haga clic en *Introducir* palabras, lo que abrirá la ventana *Especificar intervalos de direcciones IP*.
        II. Introduzca la dirección IP de VENZA (**108.163.193.74**).
        III. Haga clic en *Guardar*.
    b. En la sección *Haga lo siguiente*, seleccione la opción *Modificar las propiedades del mensaje*.
        I. Seleccione la opción *Establecer un encabezado de mensaje*.

II. Establezca el encabezado del mensaje como *X-MS-Exchange-Organization-SkipSafeLinksProcessing.*
III. Establezca el valor en "1".

c. Haga clic en *Guardar.*

8. Asegúrese de que el estado de la nueva regla está activado.
   a. Si está desactivada, haga clic en la regla recién creada.
   b. Haz clic en *Activar.*
   c. Haga clic en el botón *Editar configuración de reglas* de la ventana para guardarla como activada.

Microsoft Exchange (2016, 2019)

Listas blancas por dirección IP

1. Inicie sesión en su cuenta del Centro de administración de Exchange y vaya a *Flujo de correo.*
2. En *Flujo de correo*, seleccione *Reglas*.
3. Haga clic en + *Añadir regla* y seleccione *Crear una nueva regla* en el menú desplegable.
4. En el campo de texto superior, proporcione a la regla un nombre personalizado (por ejemplo, VENZA Phishing.)
5. En la sección *Aplicar esta regla si...*, seleccione *El remitente* en el cuadro de la izquierda y *La dirección IP está en cualquiera de estos rangos o coincide exactamente* en el cuadro de la derecha.
6. En la ventana emergente *Especificar rangos de direcciones IP*, introduce VENZA IP (**108.163.193.74**).
7. Haga clic en *Guardar.*
8. En la sección *Haga lo siguiente*, seleccione *Modificar las propiedades del mensaje* en el cuadro de la izquierda y *establezca una cabecera de* mensaje en el cuadro de la derecha.
9. Debajo de los campos de la sección *Haga lo siguiente* que acaba de editar, haga clic en la opción de la izquierda/primera *Introducir texto*.
10. Escriba "X-MS-Exchange-Organization-BypassClutter" (sin comillas) en el campo.
11. Haga clic en Guardar.
12. Debajo de los campos de la sección *Haz lo siguiente* que acabamos de editar, haz clic en la opción de la derecha/segunda *Introducir texto*.

13. Escriba "true" (sin comillas, distingue mayúsculas de minúsculas)
14. Haga clic en *Guardar.*
15. Haga clic en el símbolo + *(signo más)* situado a la derecha de la *sección Haga lo siguiente…*
16. En los dos nuevos menús desplegables que han aparecido bajo *Y;* seleccione la opción *Modificar las propiedades del mensaje* en la parte izquierda.
17. En el menú desplegable de la derecha, debajo de *Y*, seleccione la opción *Establecer el nivel de confianza de spam (SCL).*
18. Seleccione la opción *Bypass spam filtering* en la ventana emergente *Especificar SCL*.
19. Haga clic en *Guardar.*
20. Haga clic en *Siguiente* para pasar a la página *Establecer configuración de reglas*.
21. Deje igual todas las opciones/configuraciones de la página *Establecer configuración de reglas*.
22. Haga clic en *Siguiente.*
23. En la página *Revisar y finalizar*, haga clic en *Finalizar.*

Filtros antispam y cortafuegos de listas blancas

AppRiver

Filtro antispam de listas blancas

1. Inicie sesión en el Centro de administración de AppRiver.
2. Vaya a *Filtros,* una pestaña seleccionable en la parte superior de la página.
3. En la parte izquierda de la página *Filtros*, seleccione *Direcciones IP.*
4. Haga clic en el botón *Añadir* situado bajo el encabezado *Direcciones IP permitidas*.
5. Añade la IP de VENZA (**108.163.193.74**).
6. Haga clic en *Guardar*.

Barracuda Essentials

Servicio de seguridad del correo electrónico en la nube

1. Inicie sesión en la plataforma Barracuda Cloud Control.
2. Vaya a *Seguridad del correo electrónico*.
3. En *Seguridad de correo electrónico*, vaya a *Configuración de entrada*.
4. Desde *Configuración de Entrada*, navegue a *Políticas de Dirección IP*.
5. Selecciona la sección *Bloqueo/Exención de IP* y, en la línea superior, introduce la dirección IP de VENZA (**108.163.193.74**).
6. En el campo *Máscara de red*, introduzca **255.255.255.255**
7. En el campo *Política*, seleccione *Exento*.
8. Haga clic en *Añadir* para finalizar el proceso.

Listas blancas de Email Security Gateway

1. Inicie sesión en el portal web de Barracuda Email Security Gateway.
2. Desde el panel de control, vaya a la página *BLOQUEAR/ACCEDER*.
3. Desde la página *BLOCK/ACCEPT*, vaya a *Filtros IP*. .
4. Selecciona la sección *IP/Rango permitido* y en la línea superior, introduce la dirección IP de VENZA (**108.163.193.74**).
5. En el campo *Máscara de red*, introduzca **255.255.255.255**

6. En el campo *Política*, seleccione *Exento*.
7. Haga clic en *Añadir* para finalizar el proceso.

Exención de Barracuda Advanced Threat Protection

1. Inicie sesión en el portal web de Barracuda Email Security Gateway.
2. En el panel de control, vaya a la página *Configuración de ATP*.
3. Introduzca la dirección IP de VENZA (**108.163.193.74**).
4. En el campo *Máscara de red*, introduzca **255.255.255.255**
5. Haga clic en *añadir* para completar.

Permitir lista de remitentes

1. Inicie sesión en la consola Barracuda Admin.
2. Vaya *al panel de control*.
3. *Vaya a Ajustes.*
4. Navegue hasta *Remitentes permitidos*.
5. Introduzca los nombres de dominio de la campaña de phishing VENZA.
6. Haga clic en *Guardar*.

Seguridad del correo electrónico en la nube de Cisco

Listas blancas por dirección IP

1. En la consola de administración de Cisco IronPort, vaya a la pestaña *Políticas de correo*.
2. Seleccione *HAT Overview* y asegúrese *de que InboundMail* lister está seleccionado.
3. Haga clic en *LISTA BLANCA*. Si no ves *WHITELIST*, crea un grupo con este título.
4. Haga clic en *Añadir remitente* y, a continuación, añada la IP de VENZA (**108.163.193.74**).
5. Haga clic en *Enviar* y, a continuación, en *Confirmar cambios*.

Lista blanca Filtro de brotes Escaneo

1. En la consola de administración de Cisco IronPort, vaya a la pestaña *Políticas de correo*.
2. En la sección *Modificación de mensajes*, introduzca la IP de VENZA (**108.163.193.74**) en la tabla *Bypass Domain Scanning*.

3. Haga clic en *Enviar* y, a continuación, en *Confirmar cambios*.

Fortinet FortiGate

URL de campaña en lista blanca

1. Inicie sesión en su cuenta administrativa de Fortinet.
2. Vaya a *Perfiles de seguridad* y, a continuación, a *Filtro web*.
3. Cree un nuevo filtro y, a continuación, expanda *Filtro URL de estado*, actívelo y seleccione *Crear*.
4. Introduzca las URL de la campaña de phishing de VENZA
   a. Todas las URL de las campañas deben introducirse individualmente, sin https://.
5. En Tipo, seleccione *Simple*.
6. Asegúrese de que *Estado* está activado.

Mimecast

Añadir una política de remitentes permitidos

NOTA: No edite la política predeterminada Remitente permitido. Cree una nueva política para cada dirección de listas blancas y minimización de falsos positivos.

1. Inicie sesión en la consola de administración de Mimecast.
2. En el botón de la barra de herramientas *Administración*, seleccione la opción de menú *Pasarela / Políticas*.
3. En la lista de políticas, seleccione *Remitentes permitidos*.
4. Haga clic en el botón *Nueva política*.
5. Rellene los campos de la política como se indica a continuación:
   a. **Opciones**
      I. Narrativa política: Phishing VENZA
      II. Política de remitentes permitidos: Permitir remitente
   b. **Correos electrónicos de**
      I. Direcciones basadas en: Ambos
      II. Se aplica a: Todos
      III. Específicamente: Se aplica a todos los remitentes
   c. **Emails a**

I. Se aplica a: Todos
II. Específicamente: Se aplica a todos los destinatarios

d. Validez

I. Activar/Desactivar: Activar
II. Establecer la política como Perpetua: Siempre activada
III. Intervalo de fechas: Todo el tiempo
IV. Política de anulación: Marcada.
V. Bidireccional: Desmarcado.

e. Rangos IP de origen

I. Introduzca la dirección IP de VENZA y añada */32* (por ejemplo, **108.163.193.74/32**).

6. *Guardar* y *salir*.

Listas grises

1. Inicie sesión en la consola de administración de Mimecast.
2. En el botón de la barra de herramientas *Administración*, seleccione la opción de menú *Pasarela / Políticas*.
3. En la lista de políticas, seleccione *Greylisting*.
4. Haga clic en el botón *Nueva política*.
5. Rellene los campos de la política como se indica a continuación:
   a. **Opciones**
      I. Narrativa política: GreyList Bypass VENZA Phishing
      II. Política de remitentes permitidos: No tomar medidas
   b. Correos electrónicos de
      I. Direcciones basadas en: La dirección del remitente
      II. Se aplica a: Todos
      III. Específicamente: Se aplica a todos los remitentes
   c. Emails a
      I. Se aplica a: Todos
      II. Específicamente: Se aplica a todos los destinatarios
   d. Validez
      I. Activar/Desactivar: Activar
      II. Establecer la política como Perpetua: Siempre activada

III. Intervalo de fechas: Todo el tiempo
IV. Política de anulación: Marcada.
V. Bidireccional: Desmarcado.

e. **Rangos IP de origen**
   I. Introduzca la dirección IP de VENZA y añada */32* (por ejemplo, **108.163.193.74/32**).

6. *Guardar* y *salir*.

Autenticación de entrada DNS

1. Inicie sesión en la consola de administración de Mimecast.
2. En el botón de la barra de herramientas *Administración*, seleccione la opción de menú *Pasarela / Políticas*.
3. En el menú desplegable *Definiciones*, vaya a la opción *Autenticación DNS-Entrada*.
4. Seleccione Nueva autenticación DNS - Comprobaciones de entrada.
5. Crear un nombre para la *Nueva Autenticación DNS*
6. Deje todas las opciones sin marcar.
7. Haga clic en *Guardar* y *salir.*
8. Navegue hasta el botón de la barra de herramientas *Administración* y seleccione la opción de menú *Pasarela / Políticas*.
9. En la lista de políticas, seleccione *Autenticación DNS* - Política de *entrada*.
10. Haga clic en el botón *Nueva política*.
11. Rellene los campos de la política como se indica a continuación:
    a. **Opciones**
       I. Narrativa política: VENZA DNS Auth
       II. Política de remitentes permitidos: Sin autenticación
    b. **Correos electrónicos de**
       IV. Direcciones basadas en: Ambos
       I. Se aplica a: Todos
       II. Específicamente: Se aplica a todos los remitentes
    c. **Emails a**
       I. Se aplica a: Grupos de direcciones
       II. Específicamente: Administradores de seguridad del correo electrónico

d. **Validez**
    VI. Activar/Desactivar: Activar
        I. Establecer la política como Perpetua: Siempre activada
        II. Intervalo de fechas: Todo el tiempo
        III. Política de anulación: Marcada.
        IV. Bidireccional: Desmarcado.
e. **Rangos IP de origen**
    I. Introduzca la dirección IP de VENZA y añada */32* (por ejemplo, **108.163.193.74/32**).

12. *Guardar* y *salir*.

Política de elusión de URL

1. Inicie sesión en la consola de administración de Mimecast.
2. En el botón de la barra de herramientas *Administración*, seleccione la opción de menú *Pasarela / Políticas*.
3. En la lista de políticas, seleccione *URL Protection Bypass.*
4. Haga clic en el botón *Nueva política*.
5. Rellene los campos de la política como se indica a continuación:
    a. **Opciones**
        I. Narrativa política: Evasión de URL de phishing de VENZA
        II. Seleccione una opción: No tomar ninguna medida
    b. **Correos electrónicos de**
        I. Direcciones basadas en: Ambos
        II. Se aplica a: Todos
        III. Específicamente: Se aplica a todos los remitentes
    c. **Emails a**
        I. Se aplica a: Direcciones internas
        II. Específicamente: Se aplica a todos los destinatarios internos
    d. **Validez**
        I. Activar/Desactivar: Activar
        II. Establecer la política como Perpetua: Siempre activada
        III. Intervalo de fechas: Todo el tiempo
        IV. Política de anulación: Marcada.

V. Bidireccional: Desmarcado.

e. **Rangos IP de origen**

I. Introduzca la dirección IP de VENZA y añada */32* (por ejemplo, **108.163.193.74/32**).

6. *Guardar* y *salir*.

Proofpoint

IP de listas seguras Proofpoint Essentials

1. Inicie sesión en Proofpoint Essentials y vaya a *Configuración de seguridad.*
2. Vaya a *Correo electrónico* y luego a *Listas de remitentes.*
3. Seleccione Lista de remitentes seguros.
4. Introduzca la dirección IP de VENZA (**108.163.193.74**) en el campo correspondiente.
5. Haga clic en *Guardar.*

Lista segura de dominios en Proofpoint Essentials

1. Inicie sesión en Proofpoint Essentials y vaya a *Configuración de seguridad.*
2. Vaya a *Correo electrónico* y, a continuación, a *Políticas de filtrado.*
3. En la pestaña *Entrada*, haga clic en *Nuevo filtro.*
4. Cree un nombre personalizado para el filtro (por ejemplo, VENZA Phishing.)
5. Asegúrese de que *la Dirección* está configurada como *Entrante* y, a continuación, haga clic en Continuar.
6. En la sección *Lógica del filtro*, asegúrese de que el filtro *Ámbito* está establecido en <Empresa>.
7. Seleccione los siguientes campos en los cuadros desplegables situados debajo de la sección *Si*:
   a. Primer cuadro desplegable: Dirección del remitente.
   b. Segundo cuadro desplegable: IS
   c. Tercer cuadro desplegable: Introduzca uno de los dominios de la campaña de phishing de VENZA.
8. En la sección *Hacer*, seleccione *Permitir* en el menú desplegable *Acciones.*
9. En el cuadro *Detalles del filtro*, situado a la derecha, describa el filtro si es necesario.
10. Haga clic en *Guardar.*

11. Siga los pasos del 3 al 10 para cada uno de los dominios de la campaña de phishing de VENZA.

Listas blancas en Proofpoint Enterprise

1. Inicie sesión en el portal Proofpoint Enterprise Admin.
2. *Vaya a Protección del correo electrónico.*
3. En *Protección contra spam*, seleccione la opción *Lista segura de la organización.*
4. Haz clic en *Añadir.*
5. En la ventana emergente *Proofpoint -Global Safe*, rellene los campos como se indica a continuación:
   a. Tipo de filtro: Nombre de host del remitente
   b. Operador: Igual a
   c. Valor: Introduzca los dominios de la campaña de phishing de VENZA.
6. Haga clic en *Guardar cambios.*

Listas blancas en Proofpoint URL Defense

1. Inicie sesión en el portal Proofpoint Enterprise Admin.
2. *Vaya a Protección del correo electrónico.*
3. En el menú desplegable *Protección frente a ataques selectivos*, seleccione *Defensa frente a URL.*
4. Haga clic en *Políticas de reescritura de URL.*
5. Vaya a la sección *Excepciones* e introduzca VENZA Phishing Campaign Domains.
6. Haga clic en *Guardar cambios.*

Lista blanca de Proofpoint Email Firewall

1. Inicie sesión en el portal Proofpoint Enterprise Admin.
2. Vaya a *Email Firewall* y seleccione *Reglas.*
3. En *Configuración de reglas*, seleccione la opción *Activar.*
4. Introduzca un nombre personalizado para la regla (por ejemplo, VENZA Phishing.)
5. En la sección *Condiciones*, seleccione *Añadir.*
6. Introduzca cada uno de los dominios de la campaña de phishing de VENZA.
7. En la sección *Disposición*, seleccione *Entregar ahora* como *Método de entrega.*
8. Haga clic en *Guardar.*

Sophos

Modificar lista de permitidos/bloqueados en Sophos Email

1. Inicie sesión en Sophos Email Appliance (SEA.)
2. Vaya a *Configuración* y luego a *Política*.
3. Desde *Política*, vaya a *Listas de permitidos*.
4. Haga clic en la lista correspondiente en función de la información que aparece a continuación para abrir la ventana *Editor de listas* y continuar:
   a. Filtro de spam fuera de SEA: **pestaña Remitentes.**
      I. Introduzca cada elemento requerido en el campo de texto *Añadir* entradas.
      II. Haz clic en *Añadir.*
      III. Introduzca individualmente cada uno de los dominios de la campaña de phishing de VENZA.
   b. No hay filtro de spam fuera de SEA: **pestaña Hosts**.
      I. Introduzca cada elemento requerido en el campo de texto *Añadir* entradas.
      II. Haz clic en *Añadir.*
      III. Introduzca la dirección IP de VENZA (**108.163.193.74**).

Listas blancas en Sophos XG Firewall

1. Inicie sesión en el portal de Sophos XG Firewall.
2. Haz clic en *Web.*
3. *Vaya a Excepciones.*
4. Haga clic en *Añadir excepción*.
5. Crea un nombre (VENZA Phishing) y una descripción.
6. En *Omitir las comprobaciones o acciones seleccionadas*, marque cada casilla para los productos de Sophos aplicables.
7. En el cuadro *Buscar/Agregar*, introduzca VENZA Phishing Campaign Domains en el formato que se indica a continuación:
   a. ^([A-Za-z0-9.-]*\.)?ABC\.com\.?/
      I. En "ABC", introduzca el nombre de dominio de la campaña de phishing VENZA antes del dominio de nivel superior.
      II. En ".com", introduzca el dominio de nivel superior del dominio de la campaña de phishing de VENZA.

8. Haga clic en *Guardar.*

SonicWall

Listas blancas de IP en el dispositivo de seguridad de correo electrónico

1. Inicie sesión en el dispositivo SonicWall de administración.
2. Haz clic en *Gestionar*.
3. En la sección *Servicios de seguridad*, vaya a *Antispam*.
4. En *Antispam*, vaya a *Libreta de direcciones* y, a continuación, a *Permitidos*.
5. Haz clic en *Añadir.*
6. Seleccione *IPs* en el menú desplegable *Seleccionar tipo de lista*.
7. En el cuadro de texto, introduzca la dirección IP de VENZA (**108.163.193.74)**
8. Haz clic en *Añadir*.

Listas blancas de IP en la política CFS de SonicWall

1. Inicie sesión en la página de gestión de SonicWall.
2. Haga clic en *Políticas* y seleccione *Objetos*.
3. En *Opciones de dirección*, haga clic en *Añadir*.
4. En el cuadro de texto, introduzca la dirección IP de VENZA (**108.163.193.74)**
5. Vuelva a *Políticas* y seleccione *Objetos*.
6. En *Grupos de direcciones*, seleccione Añadir.
7. Introduzca un nombre personalizado para el *grupo de exclusión* (por ejemplo, VENZA Phishing).
8. Resalta la dirección IP de VENZA añadida anteriormente (**108.163.193.74)** y haz clic en la flecha adyacente para mover el grupo a la casilla de la derecha.
9. Haga clic en *Aceptar.*
9. Ahora, inicie sesión en el dispositivo SonicWall admin.
10. Haga clic en *Gestionar* y vaya a *Servicios de seguridad*.
11. En *Servicios de seguridad*, vaya a *Filtro de contenidos.*
12. Haga clic en la opción *Dirección excluida*
13. Seleccione el *Grupo de exclusión* creado anteriormente (es decir, VENZA Phishing) en el menú desplegable.

14. Haga clic en *Aceptar*.

SpamTitan

Añadir direcciones IP permitidas

1. Inicie sesión en el portal SpamTitan Email Security.
2. Vaya a *Configuración del sistema* y, a continuación, a *Retransmisión de correo*.
3. Seleccione *Controles IP* y haga clic en *Añadir*.
4. En la ventana emergente *Añadir IP permitida*, rellene los siguientes campos siguiendo los pasos que se indican a continuación:
   a. IP/Red: Introduzca la dirección IP de VENZA (**108.163.193.74**)
   b. Máscara de red: Introduzca 255.255.255.255
   c. Tipo de dirección: Seleccione IPv4
5. Haga clic en *Guardar*.

Ayuda

Estamos aquí para ayudarle en cada paso del proceso de creación de listas blancas y mitigación de falsos positivos de phishing. Si tiene algún problema o pregunta, póngase en contacto con nosotros.

Contacte con nosotros

Correo electrónico

Teléfono

Chat en directo

Billete

Póngase en contacto con su proveedor de servicios de correo electrónico

Si tiene dificultades técnicas específicas de su sistema de correo electrónico o de las herramientas mencionadas, póngase en contacto directamente con su proveedor de servicios de correo electrónico. Ellos pueden proporcionarle asistencia y solución de problemas adicionales adaptados a su plataforma de correo electrónico.

Acerca de VENZA

VENZA es un proveedor líder de soluciones de protección de datos que ayudan al sector hotelero a mitigar las vulnerabilidades y garantizar el cumplimiento de la normativa. VENZA presta asistencia a más de 2.000 hoteles en todo el mundo, manteniendo a los huéspedes y sus datos a salvo de infracciones con una visibilidad de 360 grados para una gestión proactiva de los riesgos. Esto permite a los gestores de los establecimientos centrarse en el servicio a los huéspedes y en fomentar la confianza en su marca.

Visite www.VENZAGroup.com para obtener más información.

Póngase en contacto con nosotros

Ventas: sales@venzagroup.com

Éxito de clientes: success@venzagroup.com