MINIMIZAR LOS FALSOS POSITIVOS DE PHISHING

GUÍA DE REFERENCIA RÁPIDA

CONTENIDO

VISIÓN GENERAL

¿Qué es un falso positivo?

Un falso positivo es un error que se produce cuando un sistema notifica un evento, como que un objetivo ha hecho clic en un correo electrónico de phishing, que en realidad no se ha producido. Los falsos positivos se producen en todos los tipos de sistemas de simulación de phishing y no se limitan a ningún proveedor o herramienta específicos.

¿Qué es un clic?

Para entender cómo se producen los falsos positivos, es necesario saber cómo mide el sistema las respuestas. Un "clic" se define como cualquier interacción con un enlace, como un usuario que hace clic con el ratón. Sin embargo, esto también puede incluir un sistema, como un software de seguridad de correo electrónico, que inspecciona un correo electrónico antes de que llegue a la bandeja de entrada.

Causas comunes

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 phishing, esto se registra como un clic y se notifica como tal.

SOLUCIONES

VENZA es consciente de la importancia de la exactitud de los datos y toma medidas activas para mitigar los falsos positivos. Entre las medidas importantes se incluyen:

1. **Listas blancas de IP**

Lista blanca es un término de ciberseguridad y tecnología de la información (TI) que se refiere a permitir ciertos dominios de correo electrónico (por ejemplo, example@domain.com) y protocolos de Internet (IP) a través de las defensas de una empresa.

Añadir las IP de las campañas entrantes de VENZA a la lista blanca de su red puede evitar que sus sistemas de seguridad de correo electrónico activen falsos positivos.

2. **Filtrado IP interno**

Proporcione a su Customer Success Coach una lista de direcciones IP internas que puedan utilizarse en un proceso de filtrado interno.

LISTAS BLANCAS CISCO

Objetivo: Utilizando el software de seguridad Ironport de Cisco, puede crear una lista segura (lista blanca) de VENZA para permitir que sus usuarios reciban nuestros correos electrónicos simulados de phishing y del sistema.

Si tiene problemas al crear una lista segura en Cisco Ironport, le sugerimos que primero se ponga en contacto directamente con Cisco para obtener ayuda.

- ### USO DE LISTAS BLANCAS

Pasos:

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**, puedes crear tu grupo titulado como tal.
4. Haz clic en **Añadir remitente** y añade la IP de VENZA (108.163.193.74).
5. Haga clic en **Enviar** y, a continuación, en **Confirmar cambios**.

- ### OMISIÓN DE LA EXPLORACIÓN DEL FILTRO DE BROTES

Pasos:

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**.

LISTAS BLANCAS FORTINET

Objetivo: Utilizando el software de seguridad de Fortinet, puede crear una lista segura (lista blanca) de VENZA para permitir que sus usuarios reciban nuestros correos electrónicos simulados de phishing y del sistema.

Si tiene problemas al crear una lista segura en Fortinet, le sugerimos que primero se ponga en contacto directamente con Fortinet para obtener ayuda.

- ### USO DEL FILTRO DE URL ESTÁTICAS

Pasos:

1. Inicie sesión en su cuenta de Fortinet.
2. Vaya a **Perfiles de seguridad** > **Filtro web**.
3. Crea un nuevo filtro web o selecciona uno para editarlo.
4. Expanda **Filtro estático de URL**, active **Filtro de URL** y seleccione **Crear**.
5. Introduzca las URL sin "https". Al final de esta Guía rápida se incluye una lista de URL.
6. Seleccione Tipo: **Simple**.
7. Seleccione la Acción a tomar contra las URLs coincidentes: **Permitir**.
8. Confirme que el **estado** es Activado.

LISTA BLANCA DE GMAIL

Objetivo: Estas instrucciones te ayudarán a configurar la entrega de simulaciones de phishing de terceros a Google Gmail.

Nota: Debe tener una cuenta de administrador para realizar este proceso, y los cambios pueden tardar hasta 24 horas en surtir efecto.

- ### AÑADE UNA DIRECCIÓN IP A TU LISTA DE PERMITIDAS

Pasos:

1. Accede a tu consola de administración de Google.
2. En la Admin Console, ve a **Menú** > **Aplicaciones** > **Espacio de trabajo de Google** > **Gmail** > **Spam, suplantación de identidad y software malintencionado**.
3. A la izquierda, seleccione la organización de nivel superior. Este suele ser su dominio.
4. En la pestaña **Spam, phishing y malware**, desplácese hasta la opción Lista permitida de correo **electrónico**. O, en el campo de búsqueda, introduzca lista de **correo permitido**.
5. Introduzca la dirección IP de VENZA Phishing™: 108.163.193.74

6. En la parte inferior de la página, haga clic en **Guardar**.

- ### CREAR UNA LISTA DE REMITENTES APROBADOS PARA ELUDIR LOS FILTROS DE SPAM

Pasos:

1. Accede a tu consola de administración de Google.
2. En la Admin Console, ve a **Menú** > **Aplicaciones** > **Espacio de trabajo de Google** > **Gmail** > **Spam, suplantación de identidad y software malintencionado**.
3. A la izquierda, seleccione una unidad organizativa.
4. Señale **Spam** y haga clic en **Configurar**.
5. Para una nueva configuración, introduzca un nombre o descripción únicos.
6. Marque la casilla **Anular filtros de spam para mensajes recibidos de direcciones o dominios incluidos en estas listas de remitentes aprobados**.
7. Haga clic en **Crear o editar** para crear una lista de remitentes aprobados.
8. Desplácese hasta la parte inferior de **Administrar listas de direcciones** y haga clic en **Añadir** lista de direcciones.
9. Introduzca un nombre para la nueva lista.
10. Haz clic en **Añadir dirección**.
11. Introduzca direcciones de correo electrónico o nombres de dominio. Utilice un espacio o una coma entre cada entrada.
12. Haga clic en **Guardar** para guardar la nueva lista de direcciones.

LISTAS BLANCAS DE MICROSOFT 365

Objetivo: Estas instrucciones le ayudarán a configurar la entrega de simulaciones de phishing de terceros a Microsoft 365 Defender.

Nota: Debe tener asignados permisos (Administrador de organización o Administrador de seguridad) en Exchange Online para poder realizar estos procedimientos.

Nota: Los usuarios pueden recibir un falso positivo si informan de un correo electrónico utilizando el complemento Informar de mensaje.

• UTILIZACIÓN DE LA ENTREGA AVANZADA

Pasos:

1. Abra el portal de Microsoft 365 Defender.
2. Vaya a **Correo electrónico y colaboración** > **Políticas y reglas** > Página **Políticas de amenazas** > Sección **Reglas** > **Entrega avanzada**.
3. En la página **Entrega avanzada**, seleccione la pestaña **Simulación de phishing** y, a continuación, realice uno de los siguientes pasos:
    a. Haga clic en **Editar** o
    b. Si no hay simulaciones de phishing configuradas, haga clic en **Añadir**.
4. En el menú desplegable **Editar simulación de phishing de terceros** que se abre, configure los siguientes ajustes:
    a. **Dominio**: Expanda esta configuración e introduzca al menos un dominio de dirección de correo electrónico haciendo clic en el cuadro, introduciendo un valor y pulsando **Intro**. Al final de esta Guía de referencia rápida se incluye una lista de los dominios necesarios para VENZA Phishing™.
    b. **IP de envío**: Amplíe esta opción e introduzca una dirección IPv4 válida haciendo clic en la casilla, introduciendo **108.163.193.74** y pulsando **Intro**.
    c. **URL de simulación a permitir**: Expanda esta configuración e introduzca las URL proporcionadas por su Asesor de éxito del cliente de VENZA. Nota: este campo no es necesario para todas las campañas de phishing.
5. Cuando hayas terminado, haz clic en **Añadir** y luego en **Cerrar**.

• USO DE LA LISTA DE IP PERMITIDAS

Precaución: Sin una verificación adicional como las reglas de flujo de correo, el correo electrónico procedente de fuentes de la lista de IP permitidas omite las comprobaciones de filtrado de spam y autenticación de remitentes (SPF, DKIM, DMARC). Esto crea un alto riesgo de que los atacantes envíen con éxito correo electrónico a la bandeja de entrada que, de otro modo, se filtraría.

Pasos:

1. Abra el portal de Microsoft 365 Defender.
2. Vaya a **Correo electrónico y colaboración** > **Políticas y normas** > **Políticas de amenazas** > **Antispam**

3. Haga clic en **Política de filtro de conexión** y, a continuación, en **Editar política de filtro de conexión**.
4. Añada la siguiente dirección IP al campo **Permitir siempre mensajes de las siguientes direcciones IP o rango de direcciones**:
    a. 108.163.193.74
5. Pulse **Intro** y haga clic en **Guardar** para activar la nueva configuración.

• USO DE LAS LISTAS DE REMITENTES PERMITIDOS O DOMINIOS PERMITIDOS

Precaución: Este método crea un alto riesgo de que los atacantes envíen con éxito correo electrónico a la Bandeja de entrada que, de otro modo, se filtraría; sin embargo, las listas de remitentes permitidos o de dominios permitidos no evitan que se filtren los mensajes de malware o de phishing de alta confianza.

Pasos:

1. Abra el portal de Microsoft 365 Defender
2. Vaya a **Correo electrónico y colaboración** > **Políticas y normas** > **Políticas de amenazas** > **Antispam**
3. Haga clic en **+** para crear una política y seleccione **Entrante** en la lista desplegable.
4. Se abre el asistente de políticas. En la página **Nombre de su política**, configure estos parámetros:
    a. **Nombre**: introduzca un nombre único y descriptivo para la política.
    b. **Descripción**: Introduzca una descripción opcional para la política.

    Cuando haya terminado, haga clic en **Siguiente**.

5. En la página **Usuarios, grupos y dominios**, identifique los destinatarios internos a los que se aplica la política (condiciones del destinatario):
    a. **Usuarios**: Los buzones, usuarios de correo o contactos de correo especificados.
    b. **Grupos**: Miembros de los grupos de distribución o grupos de seguridad habilitados para correo especificados.
    c. **Dominios**: Todos los destinatarios de los dominios aceptados especificados en su organización.

    Cuando haya terminado, haga clic en **Siguiente**.

6. En la página **Propiedades de umbral de correo masivo y spam** que aparece, configure los ajustes según sea necesario. Cuando haya terminado, haga clic en **Siguiente**.

7. En la página **Acciones** que aparece, configure los ajustes necesarios.
8. En la **lista** desplegable **Permitir y bloquear** que aparece, haga clic en **Permitido** > **Dominios** > **Permitir** dominios.
9. Haga clic en **+** para **Añadir dominios**.
10. Introduzca los dominios enumerados al final de esta QRG en la casilla **Dominio**.
11. Haz clic en **Añadir dominios** y, a continuación, en **Siguiente** cuando estés listo para continuar.
12. En la página **Revisar** que aparece, revise su configuración. Puede seleccionar **Editar** en cada sección para modificar la configuración dentro de la sección. También puede hacer clic en **Atrás** o seleccionar la página específica en el asistente.

    Cuando haya terminado, haga clic en **Crear**.

MIMECAST EN LISTA BLANCA

Objetivo: Utilizando el software de seguridad Mimecast, puede crear una lista segura (lista blanca) de VENZA para permitir que sus usuarios reciban nuestros correos electrónicos simulados de phishing y del sistema.

Si tiene problemas al crear una lista segura en Mimecast, le sugerimos que primero se ponga en contacto directamente con Mimecast para obtener ayuda.

- ### CREACIÓN DE UNA POLÍTICA DE REMITENTES PERMITIDOS

Te aconsejamos que crees una nueva política de remitentes permitidos en tu consola de Mimecast para incluir VENZA en una lista segura.

Nota: No edite su Política de Remitentes Permitidos predeterminada. En su lugar, cree una nueva.

Pasos:

1. En la consola de administración de Mimecast, abra la **barra de herramientas de administración**.
    a. Seleccione **Pasarela | Políticas**.
    b. Seleccione **Remitentes permitidos**.
    c. Seleccione **Nueva política**.
2. Seleccione los siguientes ajustes en las secciones **Opciones**, **Correos electrónicos de**, **Correos electrónicos a** y **Validez**.

3. Para obtener más información, consulte Configuración de una política de remitentes permitidos de Mimecast.

Opción	Ajustes
Opciones	
Narrativa política	Phishing Remitentes permitidos
Seleccionar opción	Permitir remitente
Correos electrónicos de	
Se aplica a	Direcciones internas
En concreto	Se aplica a todos los destinatarios internos
Validez	
Activar/Desactivar	Activar
Fijar la política como perpetua	Siempre encendido
Intervalo de fechas	Todos los tiempos
Política de anulación	Comprobado
Bidireccional	Sin marcar
Rangos IP de origen (n.n.n.n/x)	108.163.193.74

Si se añade VENZA a la lista de remitentes permitidos (véase más arriba), se evitará la inclusión en la lista gris. Sin embargo, recomendamos seguir los siguientes pasos para mejorar la entregabilidad del correo electrónico.

Pasos:

1. En la consola de administración de Mimecast, abra la **barra de herramientas de administración**.
    a. Seleccione **Pasarela | Políticas**.
    b. Seleccione **Remitentes permitidos**.
    c. Seleccione **Nueva política**.
2. Seleccione los siguientes ajustes en las secciones **Opciones**, **Correos electrónicos de**, **Correos electrónicos a** y **Validez**.

Opción	Ajustes

Opciones	
Narrativa política	VENZA Greylist
Seleccionar opción	No actuar
Correos electrónicos de	
Direcciones basadas en	Dirección del remitente
Se aplica a partir de	Direcciones de correo electrónico
En concreto	Se aplica a todos los remitentes externos
Emails a	
Se aplica a	Direcciones internas
En concreto	Se aplica a todos los destinatarios internos
Validez	
Activar/Desactivar	Activar
Fijar la política como perpetua	Siempre encendido
Intervalo de fechas	Todos los tiempos
Política de anulación	Comprobado
Bidireccional	Sin marcar
Rangos IP de origen (n.n.n.n/x)	108.163.193.74/24

- ## CREACIÓN DE UNA POLÍTICA DE ELUSIÓN DE PROTECCIÓN DE URL

Pasos:

1. En la consola de administración de Mimecast, abra la **barra de herramientas de administración**.
    a. Seleccione **Pasarela | Políticas**.
    b. Seleccione **Remitentes permitidos**.
    c. Seleccione **Nueva política**.
2. Seleccione los siguientes ajustes en las secciones **Opciones**, **Correos electrónicos de**, **Correos electrónicos a** y **Validez**.

Opción	Ajustes

Opciones	
Narrativa política	Evasión de la protección contra URL de phishing
Seleccionar opción	Desactivar la protección de URL
Correos electrónicos de	
Direcciones basadas en	Ambos
Se aplica a partir de	Todo el mundo
En concreto	Se aplica a todos los remitentes
Emails a	
Se aplica a	Direcciones internas
En concreto	Se aplica a todos los destinatarios internos
Validez	
Activar/Desactivar	Activar
Fijar la política como perpetua	Siempre encendido
Intervalo de fechas	Todos los tiempos
Política de anulación	Comprobado
Bidireccional	Sin marcar
Rangos IP de origen (n.n.n.n/x)	108.163.193.74/24
Nombre(s) de host	Dejar en blanco

SOPHOS EN LISTA BLANCA

Objetivo: Utilizando el software de seguridad de Sophos, puede crear una lista segura (lista blanca) de VENZA para permitir que sus usuarios reciban nuestros correos electrónicos simulados de phishing y del sistema.

Si tiene problemas con las listas seguras en Sophos, le sugerimos que primero se ponga en contacto directamente con Sophos para obtener ayuda.

- ### MODIFICACIÓN DE LISTAS DE ADICIÓN/BLOQUEO EN SOPHOS EMAIL APPLIANCE

Pasos:

1. En su gestor de SEA, vaya a **Configuración** > **Política** > **Listas de permitidos**.
2. Haga clic en la lista correspondiente para mostrar el cuadro de diálogo **Editor de listas**.
3. Seleccione la pestaña **Remitentes si tiene un filtro de spam adicional delante de SEA**. Seleccione la pestaña **Hosts si** no tiene un filtro de spam adicional delante de SEA.
4. En el cuadro de texto **Añadir entradas**, introduzca cada elemento necesario y haga clic en **Añadir**.
5. En la pestaña Remitentes, introduzca los nombres de dominio de VENZA, uno por uno. Estos dominios se enumeran al final de esta Guía de consulta rápida.
6. En la pestaña Hosts, introduzca la dirección IP de VENZA. La dirección IP de VENZA se indica al final de esta Guía de consulta rápida.

- ### LISTAS BLANCAS EN SOPHOS XG FIREWALLS

Pasos:

1. Inicie sesión en el portal del cortafuegos.
2. Haga clic en **Web**, situado a la izquierda.
3. Haga clic en **Excepciones**, situado en la parte superior.
4. Si no tiene una lista de excepciones, haga clic en **Añadir excepción**.
5. Introduzca un nombre (**VENZA)** y una descripción opcional para la lista.
6. Marque las casillas situadas a la derecha de **Omitir las comprobaciones o acciones seleccionadas** para los servicios adquiridos.
7. Comprobar **coincidencias de patrones de URL**.
8. Introduzca los dominios de phishing línea por línea en el cuadro **Buscar/Agregar**. Éstos se encuentran al final de esta Guía de consulta rápida.
9. Haga clic en **Guardar** en la parte inferior de la página.

DIRECCIÓN IP EN LA LISTA BLANCA

108.163.193.74

DOMINIOS DE CAMPAÑAS DE PHISHING

perfil-de-cuenta.com	hotelreview.today
agencia de cobros.co	centro.recursos.humanos
corporateoffice.biz	legalactions.org

discriminaciónweb.com	shippingnotice.com
documentsservice.com	use-fedex.com
employeerewards.site	yelprating.com
expedia-us.com	tu-cuenta-login.com

DOMINIOS DEL SISTEMA

venzagrc.com	venzapeak.com

PÓNGASE EN CONTACTO CON

Servicio de asistencia: noreply@venzagroup.com

Ventas: sales@venzagroup.com

Éxito de clientes: success@venzagroup.com