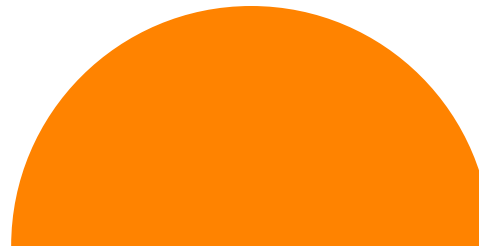




Configuración de la Directiva Contra Phishing

Dago Ramírez
Líder Técnico



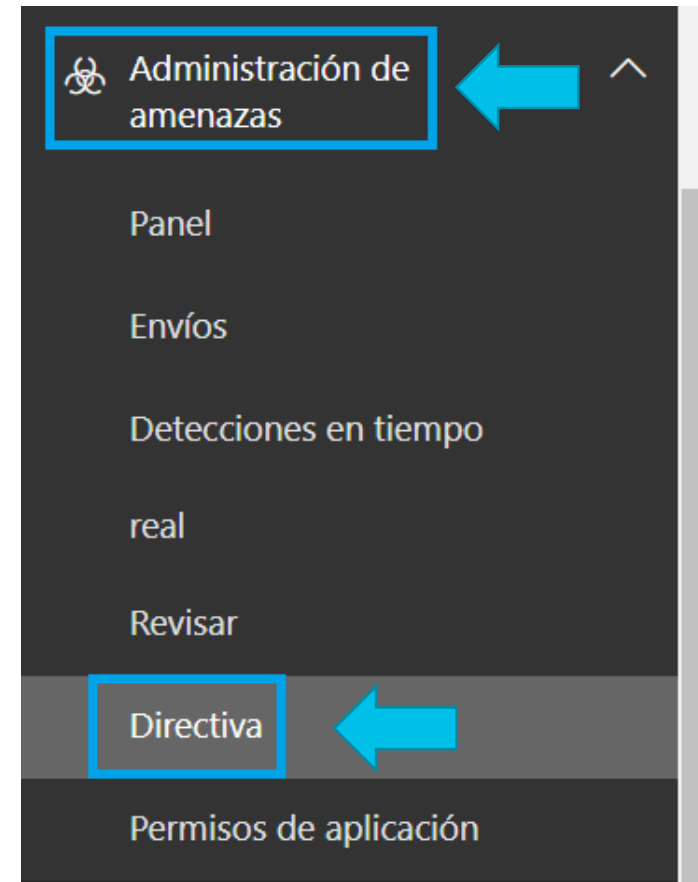
Directiva Antiphishing



Directiva Antiphishing

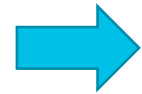
A continuación se describe el proceso de configuración de la directiva contra suplantación de identidad. Realice los siguientes pasos:

1. Vaya a <https://protection.office.com> e inicie sesión con las credenciales de su cuenta de administrador.
2. En el panel de navegación izquierdo, en **Administración de amenazas**, elija > **Directiva**



Directiva Antiphishing

1. En el página de **Directivas** seleccione **Protección contra phishing**



Directivas



Protección contra phishing



Contra spam



Protección antimalware



Datos adjuntos seguros



Vínculos seguros

Directiva Antiphishing

1. Clic en **Directiva predeterminada** para personalizar la directiva

Inicio > Directiva > Protección contra phishing

Protección contra phishing

De forma predeterminada, Office 365 incluye características integradas que ayudan a proteger a los usuarios de ataques de phishing. Configure directivas con protección contra phishing para aumentar esta protección, por ejemplo, restringiendo la configuración para detectar y prevenir mejor los ataques de suplantación de identidad y suplantación electrónica. La directiva predeterminada se aplica a todos los usuarios dentro de la organización y es una vista única donde se puede ajustar la protección contra el phishing. Las directivas personalizadas pueden crearse y configurarse para determinados usuarios, grupos o dominios dentro de la organización y tendrán prioridad sobre la directiva predeterminada para los usuarios con ámbito. [Obtener más información acerca de las directivas de protección contra phishing](#)

[+ Crear](#) [Actualizar](#) [Directiva predeterminada](#) [Filtrar](#)

Nombre  [Prioridad](#) ^ Estado Última modificación

Directiva Antiphishing

1. Clic en **Editar** para cambiar los valores predeterminados

Editar la directiva Office365 AntiPhish Default

Eliminar directiva ↑ Aumentar prioridad ↓ Disminuir prioridad

Estado	Activado	
Última modificación	30 de marzo de 2021	
Configuración de directiva	Nombre de la directiva	Office365 AntiPhish Default
	Descripción	
Suplantación	Usuarios que se protegerán	Desactivado
	Proteger todos los dominios que me pertenecen	Desactivado
	Proteger dominios concretos	Desactivado
	Acción > Suplantación de usuario	No aplicar ninguna acción
	Acción > Suplantación de dominio	No aplicar ninguna acción
	Consejos de seguridad > Suplantación de usuario	Desactivado
	Consejos de seguridad > Suplantación de dominio	Desactivado
	Consejos de seguridad > Caracteres extraños	Desactivado
	Inteligencia de buzones	Activado
	Inteligencia de buzones > Protección	Desactivado



Directiva Antiphishing

1. Clic en **Agregar dominios que deban protegerse**
2. Active la opción **Incluir automáticamente los dominios que me pertenecen**
3. Active la opción **Incluir dominios personalizados** para agregar sus propios dominios o dominios de proveedores o socios con los que colabora
4. Escriba los dominios

Office365 AntiPhish Default

Editando Agregar dominios que deben protegerse

Agregar dominios que deben protegerse

Incluir automáticamente los dominios que me pertenecen ¹ Desactivado

[Ver dominios que me pertenecen](#)

Incluir dominios personalizados ¹ Desactivado

Agregar dominios ¹

Escriba los nombres de dominio (por ejemplo, "contoso.com") y pulse Entrar. No debe preceder los nombres con un signo de arroba (@).

Guardar Cancelar

Directiva Antiphishing

1. Clic en **Acciones**
2. Seleccione la acción a realizar **Si el correo electrónico lo envía un usuario suplantado** dando clic en el menú desplegable
3. Seleccione la acción a realizar **Si el correo electrónico lo envía un dominio suplantado** dando clic en el menú desplegable
4. Clic en **Activar sugerencias de seguridad de suplantación** para activar los mensajes de advertencia

Editar directiva de suplantación

Office365 AntiPhish Default

Editando Acciones

Si un atacante suplanta a los usuarios o dominios que especificó, aplicaremos las acciones que elija aquí.

Si el correo electrónico lo envía un usuario suplantado:

No aplicar ninguna acción

Entregaremos el mensaje a los destinatarios previstos sin aplicar acciones adicionales.

Si el correo electrónico lo envía un dominio suplantado:

No aplicar ninguna acción

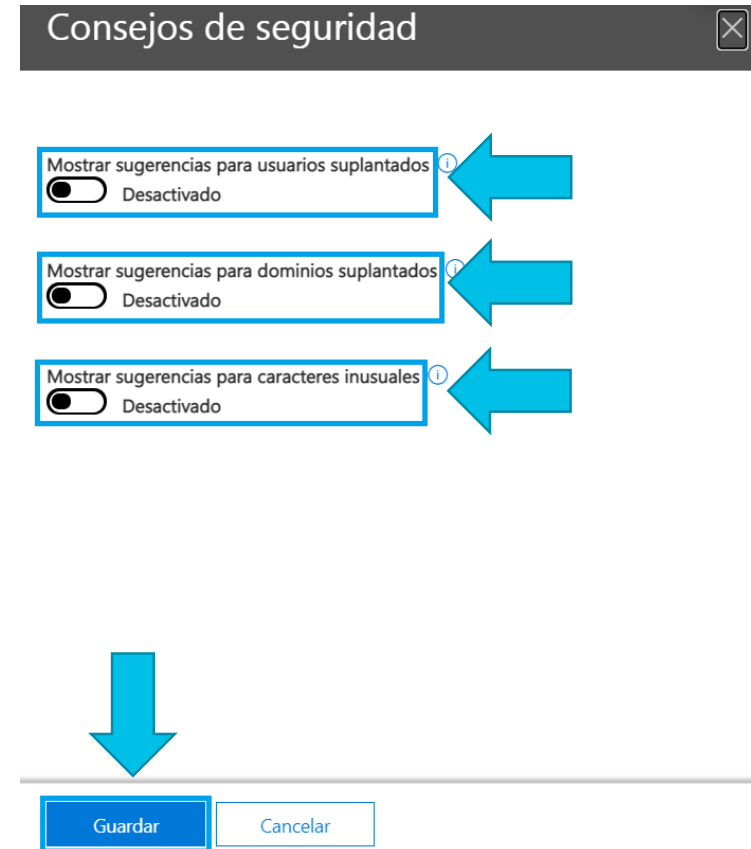
Entregaremos el mensaje a los destinatarios previstos sin aplicar acciones adicionales.

Activar sugerencias de seguridad de suplantación para mostrar una advertencia de correo electrónico al destinatario, si se detecta que el mensaje es un ataque de suplantación.

Guardar Cancelar

Directiva Antiphishing

1. Active **Mostrar sugerencias para usuarios suplantados**
2. Active **Mostrar sugerencias para dominios suplantados**
3. Active **Mostrar sugerencias para caracteres inusuales**
4. Clic en **Guardar**



Directiva Antiphishing

1. Clic en **Inteligencia de buzones**
2. Si está desactivado, active **¿Quiere habilitar la inteligencia de buzones?**
3. Active la opción **¿Habilitar la protección de suplantación basada en la inteligencia de buzones?**
4. Seleccione la acción a realizar **Si el correo electrónico lo envía un usuario suplantado** dando clic en el menú desplegable

Editar directiva de suplantación

Office365 AntiPhish Default

Editando Inteligencia de buzones

La inteligencia de buzones analiza los patrones de flujo de correo de los usuarios basados en la nube para determinar con qué contactos se comunican con mayor frecuencia. Esto nos ayuda a identificar con más facilidad los casos en los que un mensaje de correo electrónico podría ser de un atacante que esté suplantando a uno de esos contactos.

[Más información sobre la inteligencia de buzones](#)

¿Quiere habilitar la inteligencia de buzones?

Activado

¿Habilitar la protección de suplantación basada en la inteligencia de buzones?

Desactivado

Si un atacante suplanta a un usuario protegido por la inteligencia de buzones, aplicaremos la acción que elija aquí.

Si el correo electrónico lo envía un usuario suplantado:

No aplicar ninguna acción

Entregaremos el mensaje a los destinatarios previstos sin aplicar acciones adicionales.

Directiva Antiphishing

Puede agregar dominios o remitentes de confianza. Si lo hace, estos dominios o remitentes nunca se clasificarán como atacantes de suplantación, por lo tanto, la directiva no se aplicará en este caso.

Clic en **Guardar** para salvar los cambios realizados.

Office365 AntiPhish Default

Editando Agregar dominios y remitentes de confianza

Los mensajes de las direcciones de correo electrónico de los remitentes y los dominios que agregue aquí nunca se clasificarán como ataques de suplantación. Así pues, las acciones y la configuración de esta directiva no se aplicarán a los mensajes de estos remitentes y dominios.

Remitentes de confianza
Escribir dirección de correo electrónico

Dominios de confianza
Escriba los nombres de dominio (por ejemplo, "contoso.com") y pulse Entrar. No debe preceder los nombres con un signo de arroba (@).

Guardar Cancelar



¡Gracias!



Dago Ramírez
dramirez@techsoup.org

