



imperiasti®

Líder es Cumplir

Cómo protegernos del correo Spoofing

El correo electrónico spoofing es una técnica utilizada por los ciberdelincuentes para falsificar la dirección de correo electrónico de un remitente, haciéndola parecer legítima con el objetivo de engañar a los destinatarios y llevar a cabo actividades maliciosas. Aquí hay algunas medidas que puedes tomar para protegerte del correo spoofing:

Verifica las direcciones de correo electrónico:

Siempre verifica cuidadosamente las direcciones de correo electrónico de los remitentes, especialmente si recibes mensajes inesperados o sospechosos. Presta atención a detalles sutiles, como caracteres mal escritos o cambios en el dominio que puedan pasar desapercibidos.

Usa autenticación de correo electrónico (SPF, DKIM, DMARC):

Estas son tecnologías de autenticación que permiten a los servidores de correo electrónico verificar la autenticidad del mensaje y del remitente. SPF (*Sender Policy Framework*) especifica qué servidores están autorizados para enviar correo en nombre de un dominio, DKIM (*DomainKeys Identified Mail*) utiliza firmas digitales para verificar la autenticidad del mensaje y DMARC (*Domain-based Message Authentication, Reporting, and Conformance*) combina SPF y DKIM para proporcionar políticas más claras sobre cómo se deben manejar los mensajes no autenticados.

Implementa políticas de DMARC más estrictas: DMARC te permite especificar qué hacer con los mensajes que no pasan las autenticaciones SPF y DKIM. Puedes configurar políticas más estrictas para rechazar o marcar como spam los mensajes no autenticados.

Usa una solución de seguridad confiable:

Utiliza un software antivirus y antimalware confiable en tus dispositivos para detectar y prevenir posibles amenazas. Estas soluciones pueden ayudarte a identificar correos electrónicos maliciosos y prevenir ataques.

Mantén el software actualizado:

Asegúrate de que tus programas de correo electrónico y sistemas operativos estén siempre actualizados con las últimas versiones y parches de seguridad. Los ciberdelincuentes a menudo aprovechan las vulnerabilidades conocidas en software desactualizado.

Educa a los usuarios:

Si estás en un entorno empresarial, es fundamental educar a los empleados sobre los riesgos del correo electrónico spoofing y proporcionar pautas claras sobre cómo identificar correos electrónicos sospechosos y cómo actuar ante ellos.

Ten presente en ser cauteloso con los enlaces y archivos adjuntos. No hagas clic en enlaces ni descargues archivos adjuntos de correos electrónicos sospechosos o no solicitados, especialmente si provienen de remitentes desconocidos. Estos enlaces pueden dirigirte a sitios web maliciosos o descargar malware en tu sistema.

Confirma solicitudes de transferencias de dinero o información sensible. Si recibes un correo electrónico solicitando una transferencia de dinero u otra información confidencial, verifica la solicitud directamente con el remitente a través de un canal



imperasti®

Líder es Cumplir

diferente, como una llamada telefónica.

Recuerda que ninguna medida es 100% infalible, pero al combinar varias de estas estrategias, puedes reducir significativamente el riesgo de caer en trampas de correo electrónico spoofing.

Héctor M. Amodeo

Socio

Gerente Comercial