HORNETSECURITY

DMARC MANAGER

LA SOLUCIÓN CONTRA EL SPOOFING EN EL CORREO ELECTRÓNICO

La confianza es fundamental en las comunicaciones por correo electrónico entre empresas. Sin embargo, los ciberdelincuentes se aprovechan de ella mediante técnicas de "spoofing", haciéndose pasar por dominios o personas de confianza para cometer fraudes, lo que a menudo termina en ataques de Business Email Compromise (BEC).

CONSECUENCIAS DEL SPOOFING EN EL CORREO ELECTRÓNICO:

- **Pérdidas económicas** debido a correos fraudulentos, como facturas falsas.
- **Daño a la reputación** de la empresa por suplantación de identidad, generando desconfianza entre clientes y socios.
- **Mayor riesgo de ataques de phishing,** que exponen datos sensibles de la empresa.

DMARC: TU DEFENSA CONTRA LA SUPLANTACIÓN DE CORREOS ELECTRÓNICOS

DMARC (Autenticación de Mensajes, Informes y Conformidad Basada en el Dominio) es un protocolo de seguridad para el correo electrónico que ayuda a las empresas a prevenir el fraude y la suplantación de identidad. Trabaja junto con **SPF** y **DKIM** para asegurar que solo los correos autorizados se envíen desde tu dominio, protegiendo así tu marca y tus comunicaciones.

CÓMO FUNCIONA:

SPF revisa el registro del servidor remitente para confirmar que el correo electrónico se envió desde una dirección IP autorizada. Si la IP está en el registro SPF, la verificación pasa; si no, falla.	**DKIM** verifica que el correo esté firmado de forma criptográfica con la clave privada del dominio remitente y comprueba la firma con la clave pública correspondiente. Si coinciden, la verificación pasa; si no, falla.	**DMARC** asegura que la dirección en el campo "Desde" del correo esté alineada con el mismo dominio que SPF y DKIM validaron.	Por último, la **policy tag** ("p") en el registro DMARC del dominio remitente le indica al servidor receptor cómo debe tratar el correo según los resultados de estas verificaciones.

HORNETSECURITY

Configurar y mantener las políticas de DMARC, DKIM y SPF puede ser un auténtico quebradero de cabeza, sobre todo cuando estás trabajando para organizaciones grandes y complejas, con numerosos dominios, configuraciones diversas y, posiblemente, distintos requisitos para cada dominio.

POR SUERTE, EXISTE UNA SOLUCIÓN. **EVITA COMPLICACIONES AL CONFIGURAR DMARC CON DMARC MANAGER**

CON DMARC MANAGER PODRÁS:

» Ver quién envía correos desde un dominio y devolver el control total al propietario, reforzando y protegiendo la reputación de tu marca.

» Configurar y gestionar de forma sencilla las políticas de **DMARC, DKIM** y **SPF** para múltiples dominios, siguiendo siempre las mejores prácticas.

» Recibir informes claros sobre el estado de entrega y autenticación de tus correos, ayudando a identificar campañas legítimas y detectar posibles intentos de suplantación.

» Optimizar las campañas de marketing por correo electrónico, asegurando que los correos masivos lleguen a su destino al cumplir con los estándares de autenticación de proveedores como Yahoo y Gmail.

» Cumplir con normativas globales e industriales, como PCI DSS, NIST, GDPR, HIPAA, entre otras.

DESCUBRE MÁS

EMAIL: info@hornetsecurity.com | www.hornetsecurity.com