CÓMO PROTEGERSE DEL SPOOFING EN EL CORREO ELECTRÓNICO

El spoofing es cuando un atacante falsifica la dirección de remitente para suplantar tu dominio y engañar a los usuarios.

¿CÓMO PROTEGERSE?

1 Implementa DMARC, SPF y DKIM

Son los 3 estándares fundamentales para verificar que los correos provienen realmente de tu dominio.

2 Configura correctamente tus registros DNS

Publica y mantén actualizados los registros SPF, DKIM y DMARC de tu dominio.

3 Usa TLS para cifrar el correo

El cifrado protege el contenido del correo durante su tránsito (no reemplaza a la autenticación).

4 Capacita a tus usuarios

Enséñales a identificar correos sospechosos, no hacer clic en enlaces ni compartir información sensible.

5 Utiliza filtros y soluciones antiphishing

Complementa con filtros en la puerta de enlace de correo para bloquear amenazas conocidas.

6 Monitorea y revisa informes

Revisa periódicamente los reportes DMARC para detectar intentos de suplantación y mejorar tu postura.

DMARC, SPF Y DKIM: ¿QUÉ SON Y CÓMO TE PROTEGEN?

SPF
(Sender Policy Framework)

Especifica qué servidores de correo están autorizados a enviar correos en nombre de tu dominio.

Evita que atacantes usen servidores no autorizados para suplantar tu dominio.

Ejemplo de registro SPF:

```
v=spf1 ip4:203.0.113.10 include:_spf.google.com -all
```

DKIM
(DomainKeys Identified Mail)

Firma digitalmente tus correos para demostrar que el mensaje no fue alterado y realmente fue enviado por tu dominio.

Asegura la integridad del correo y valida la autenticidad del remitente.

Ejemplo de registro DKIM:

```
default._domainkey.tudominio.com. IN TXT v=DKIM1; k=rsa; p=MIIB...AB
```

DMARC
(Domain-based Message Authentication, Reporting & Conformance)

Indica a los servidores qué hacer con los correos que fallen SPF o DKIM (ninguno, cuarentena o rechazar) y recibe reportes de actividad.

Te da visibilidad, control y protección contra el uso indebido de tu dominio.

Ejemplo de registro DMARC:

```
v=DMARC1; p=quarantine; rua=mailto:dmarc@tudominio.com; puf=mailto:dmarc@tudominio.com; pct=100
```

VENTAJAS DE IMPLEMENTAR DMARC, SPF Y DKIM

Protege tu marca y reputación
Impide que atacantes suplanten tu dominio para enviar spam, phishing o malware.

Mejora la entregabilidad
Aumenta la confianza de los proveedores de correo y reduce la probabilidad de ir a spam.

Visibilidad y control
Los reportes DMARC te permiten detectar usos no autorizados y tomar acciones oportunas.

Cumplimiento y confianza
Demuestra buenas prácticas de seguridad y cumple con requisitos de estándares y regulaciones.

Reducción de fraudes y pérdidas
Disminuye el riesgo de ataques de ingeniería social, fraudes financieros y robo de información.

Tranquilidad y escalabilidad
Fortalece tu postura de seguridad y te prepara para el crecimiento de tu organización.

En resumen:
DMARC, SPF y DKIM trabajan juntos para garantizar que tus correos sean auténticos, confiables y lleguen a la **bandeja de entrada**.

AUTENTICA TU DOMINIO.
PROTEGE TU NEGOCIO.