¿Estás al tanto de que tus correos electrónicos a Gmail y Yahoo! podrían ser rechazados a partir del 1 de febrero de 2024 si no configuras la autenticación de correo electrónico DMARC, SPF y DKIM para tu dominio de envío?

Estimado remitente de correo electrónico, Google y Yahoo! han implementado nuevas reglas estrictas obligatorias en cuanto a seguridad electrónica.

El 3 de octubre de 2023, Google y Yahoo anunciaron requisitos mandatorios que los remitentes masivos deben tener DMARC implementado a partir de febrero de 2024.

¿Qué sucede si ignoras los requisitos mandatorios de autenticación DMARC de Google y Yahoo?

Ignorar DMARC (Autenticación de Mensajes Basada en Dominio, Informes y Conformidad) en tu estrategia de seguridad de correo electrónico puede plantear varios riesgos y vulnerabilidades. DMARC está diseñado para combatir el phishing y el fraude por correo electrónico al proporcionar una forma para que los remitentes autentiquen sus correos electrónicos y protejan a los destinatarios de actividades maliciosas. Aquí hay algunos peligros asociados con ignorar DMARC:

Aumento de Ataques de Phishing:

Sin DMARC, los ciberdelincuentes pueden aprovechar la falta de autenticación y enviar correos electrónicos de phishing que parecen provenir de fuentes legítimas. Esto aumenta el riesgo de que los destinatarios sean víctimas de ataques de phishing, lo que puede resultar en el robo de credenciales, infecciones de malware u otras actividades maliciosas.

Suplantación de Marca:

DMARC ayuda a prevenir el suplantación de dominio y la suplantación de marca. Ignorar DMARC deja tu dominio vulnerable al abuso por parte de atacantes que pueden suplantar tu marca en campañas de phishing, lo que podría dañar la reputación de tu organización.

Fraude por Correo Electrónico y Compromiso Empresarial de Correo Electrónico (BEC):

DMARC desempeña un papel crucial en la prevención del fraude por correo electrónico y los ataques BEC. Sin DMARC, los atacantes pueden llevar a cabo estafas que involucran fraude financiero, acceso no autorizado a información sensible o actividades fraudulentas en nombre de una organización.

Falta de Visibilidad e Informes:

DMARC proporciona mecanismos de informes que permiten a los propietarios de dominios obtener información sobre quién está enviando correos electrónicos en su nombre y cómo esos correos electrónicos son gestionados por los proveedores de correo electrónico. Ignorar DMARC significa perder capacidades valiosas de visibilidad e informes, lo que dificulta la monitorización y análisis de las actividades de correo electrónico.

Impacto en la Entregabilidad de Correos Electrónicos:

Los proveedores de correo electrónico utilizan cada vez más políticas DMARC para determinar si entregar o rechazar correos electrónicos. Si tu dominio carece de una política DMARC o tiene una política débil, los correos electrónicos legítimos pueden estar en riesgo de ser marcados como spam o rechazados por los filtros de correo electrónico, afectando tu entregabilidad general de correos electrónicos.

Problemas de Cumplimiento Normativo:

En algunas industrias, el cumplimiento normativo requiere que las organizaciones implementen mecanismos de autenticación de correo electrónico como DMARC. Ignorar DMARC puede resultar en incumplimiento de las regulaciones de la industria, lo que lleva a posibles consecuencias legales y multas.

Pérdida de Confianza entre los Usuarios:

Si tu dominio de correo electrónico se utiliza con frecuencia en ataques de phishing, puede erosionar la confianza entre tus usuarios y clientes. Los usuarios pueden volverse escépticos respecto a los correos electrónicos de tu dominio, afectando la comunicación y causando posiblemente interrupciones en las operaciones comerciales legítimas.

Para mitigar estos riesgos, es importante implementar **DMARC y configurarlo adecuadamente.** Monitoriza regularmente los informes de DMARC, ajusta las políticas y toma medidas basadas en la información recibida.

Trabajar hacia la aplicación de **DMARC** ayuda a garantizar que solo los remitentes autorizados puedan utilizar tu dominio, reduciendo la probabilidad de actividades de phishing y fraudes.

¿Cuáles son los beneficios de implementar la autenticación DMARC?

Autenticación de Correo Electrónico:

DMARC autentica correos electrónicos al permitir a los remitentes publicar políticas para su dominio. Esto ayuda a garantizar que solo los remitentes autorizados puedan utilizar el dominio, reduciendo el riesgo de suplantación de dominio e impersonación.

Prevención de Phishing:

DMARC ayuda a prevenir ataques de phishing al dificultar que los atacantes se hagan pasar por dominios de confianza. Verifica la autenticidad del dominio del remitente, disminuyendo la probabilidad de que los destinatarios sean víctimas de estafas de phishing.

Protección de Marca:

Al prevenir la suplantación de dominio e impersonación de marca, DMARC protege la reputación de tu organización y contribuye a construir confianza entre los destinatarios. Asegura que los correos electrónicos enviados en nombre de tu dominio sean legítimos y no maliciosos.

Mejora de la Entregabilidad de Correos Electrónicos:

Muchos proveedores de correo electrónico utilizan políticas DMARC para determinar si entregar, marcar como spam o rechazar correos electrónicos entrantes. Implementar DMARC con una política de aplicación puede impactar positivamente en la entregabilidad de correos electrónicos al reducir las posibilidades de que los correos electrónicos legítimos sean marcados como spam.

Visibilidad e Informes:

DMARC proporciona mecanismos de informes que permiten a los propietarios de dominios obtener información sobre cómo se utiliza su dominio para la comunicación por correo electrónico. Estos informes incluyen información sobre el estado de autenticación del correo electrónico, fuentes de tráfico de correo electrónico y posibles abusos.

Aplicación Gradual de Políticas:

DMARC permite una implementación gradual, lo que permite a las organizaciones comenzar con una política de solo monitoreo (p=none). Esto les permite analizar informes y avanzar gradualmente hacia la aplicación (p=quarantine o p=reject) una vez que estén seguros del estado de autenticación de sus correos electrónicos.

Cumplimiento con Normas de la Industria:

En ciertas industrias, el cumplimiento normativo requiere la implementación de mecanismos de autenticación de correo electrónico. DMARC es reconocido como un estándar de la industria para la autenticación de correo electrónico y a menudo es un requisito para el cumplimiento con regulaciones.

Reducción del Riesgo de Compromiso Empresarial de Correo Electrónico (BEC):

DMARC ayuda a proteger contra ataques de Compromiso Empresarial de Correo Electrónico (BEC), donde los atacantes intentan suplantar a personas de confianza dentro de una organización para llevar a cabo fraudes financieros o actividades no autorizadas.

Notificación de Fallos de Autenticación:

DMARC permite a los propietarios de dominios recibir notificaciones cuando se producen fallos de autenticación, brindándoles la oportunidad de investigar y tomar medidas correctivas. Este enfoque proactivo ayuda a que las organizaciones estén informadas sobre posibles abusos de su dominio.

Estándar Global de Seguridad de Correo Electrónico:

DMARC es un estándar de seguridad de correo electrónico ampliamente adoptado y reconocido. Implementar DMARC alinea a tu organización con las mejores prácticas en autenticación de correo electrónico y contribuye a la mejora general de la seguridad de correo electrónico a nivel mundial.

Al implementar DMARC, las organizaciones pueden mejorar significativamente su postura de seguridad de correo electrónico, proteger su marca y contribuir a un entorno de correo electrónico más seguro tanto para remitentes como para destinatarios.

Así que a partir del 1 de febrero de 2024, los remitentes que envíen más de 5,000 mensajes al día a cuentas de Gmail o Yahoo deben cumplir con los requisitos de esta sección:

1. **Configuración de SPF y DKIM:**
   - Implementar autenticación de correo electrónico SPF y DKIM para tu dominio.

2. **Validación de Registros DNS:**
   - Asegurarse de que los dominios o IPs emisores tengan registros DNS válidos tanto hacia adelante como hacia atrás (registros PTR).

3. **Conexión TLS:**
– Utilizar una conexión TLS para transmitir correos electrónicos. Encuentra los pasos para configurar TLS en Google Workspace aquí (https://support.google.com/a/answer/2520500).

4. **Gestión de Tasa de Spam:**
   - Mantener tasas de spam por debajo del 0.10% en Postmaster Tools y evitar superar una tasa de spam del 0.30% o más.

5. **Formato de Mensajes:**
   - Formatear mensajes de acuerdo con el estándar de Formato de Mensaje de Internet (RFC 5322).

6. **Configuración de DMARC:**
   - Configurar la autenticación de correo electrónico DMARC para tu dominio emisor. Establecer la política de aplicación de DMARC en none.

7. **Soporte para Darse de Baja:**
– Los mensajes de marketing y suscripción deben facilitar la baja con un clic, con un enlace de darse de baja claramente visible en el cuerpo del mensaje.

8. **Verificación del Proveedor de Servicios de Correo Electrónico:**
   - Si utilizas un proveedor de servicios de correo electrónico (aweber, mailchimp, etc.), verifica que autentiquen el correo electrónico de tu dominio con SPF y DKIM. Siempre utiliza el correo electrónico de TU DOMINIO para marketing y respuestas automáticas.

9. **Uso Consistente del Dominio:**
– Recomendamos utilizar el mismo dominio para la autenticación de correo electrónico y alojar tu sitio web público.

Toma Acción Ahora:

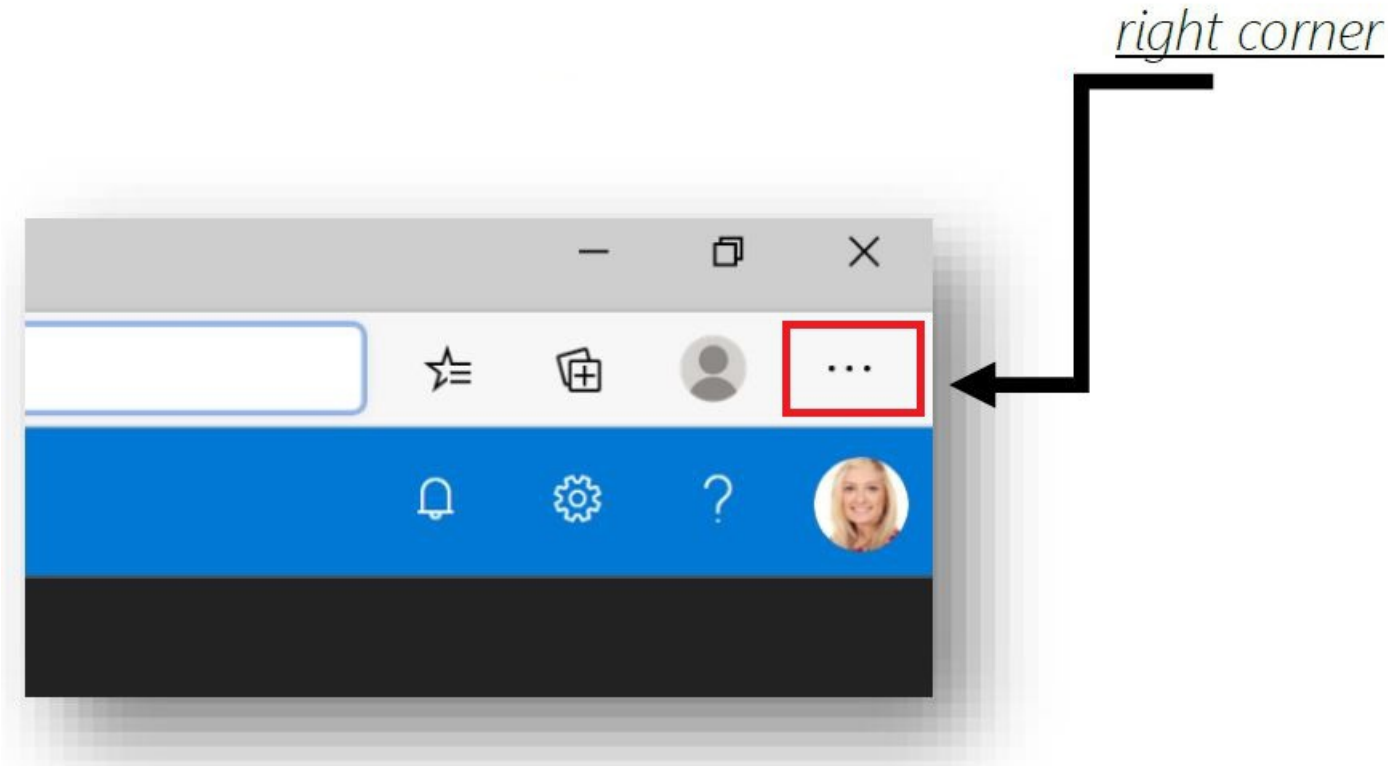
No cumplir con estos requisitos puede llevar a problemas de entrega de correo electrónico, clasificación como spam y susceptibilidad a suplantación y phishing. Actúa rápidamente para abordar el incumplimiento antes de la fecha límite especificada.

¿Cómo sabes si ya cumples con la autenticación DMARC obligatoria de Gmail? Así es cómo.

Envía un correo electrónico desde tu cuenta de interfaz web de "TU DOMINIO" a tu cuenta de Gmail.
Ejemplo: Si tu cuenta comercial es "soporte@networkmarketing.com", envíalo desde allí, NO desde ninguna otra cuenta de correo electrónico.

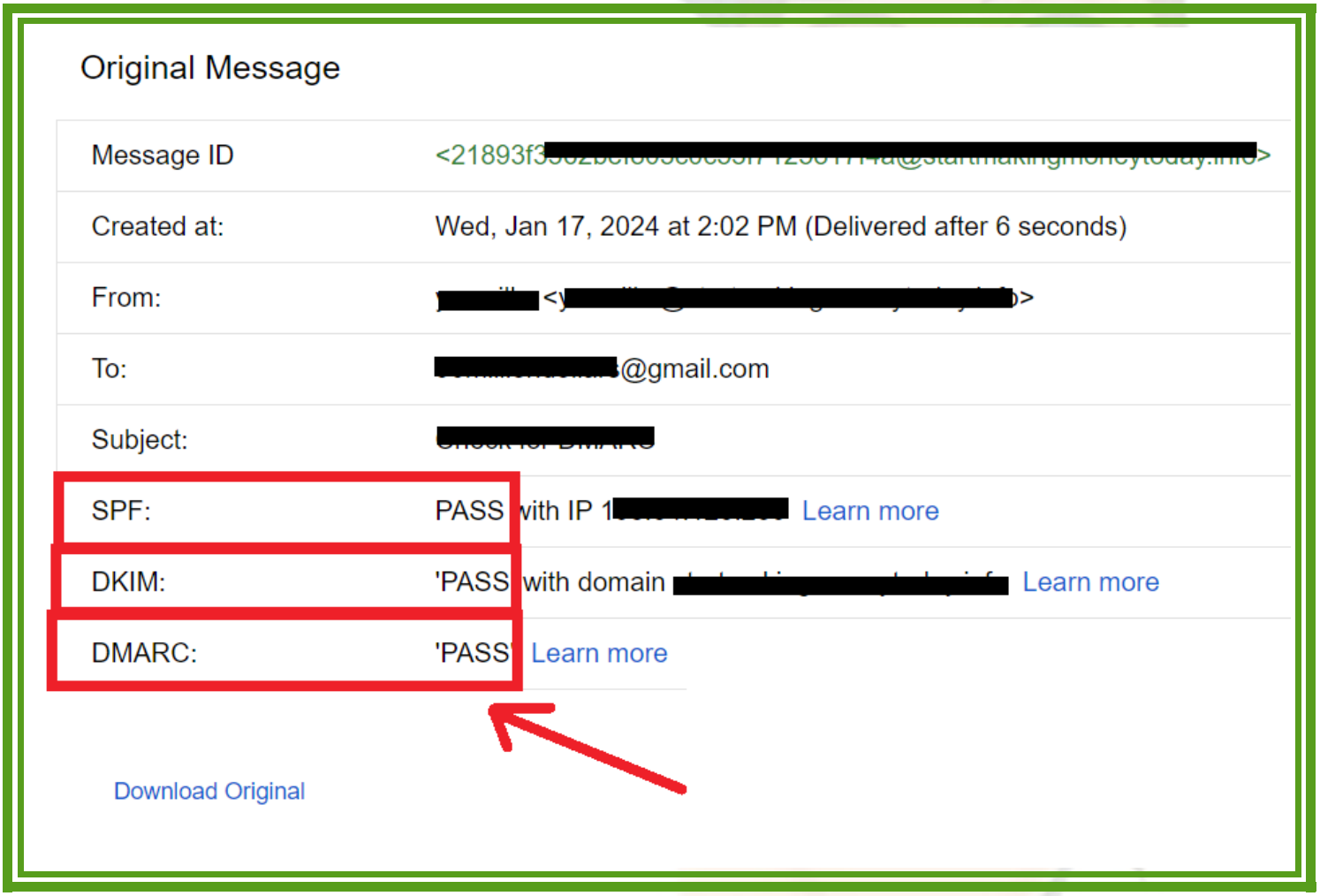
FROM: soporte@networkating.com
TO: tu@gmail.com

Una vez que recibas el correo electrónico de tu cuenta comercial en tu cuenta de gmail.com, ábrelo y haz clic en los **3 puntos en la esquina superior derecha**, y selecciona (“show original”)"Mostrar original".



Una vez que hagas eso, se abrirá en una nueva ventana. En esa ventana, deberías poder ver lo siguiente (imagen a continuación):

SPF: PASS
DKIM: PASS
DMARC: PASS



Si no tienes un DOMINIO, necesitas obtener uno lo antes posible.

¡**SI NO** ves lo que muestra la imagen de arriba, entonces necesitas realizar los cambios de inmediato!

¿Cómo Realizar los Cambios?

Puedes realizar los cambios desde tu **DNS/Cpanel** y editar **DMARC, SPF y DKIM**.

ADVERTENCIA: Si no tienes experiencia en la edición de información en tu Cpanel o DNS, no te recomendamos que lo intentes, ya que esto podría causar problemas en tu host o sitios web. Evita a toda costa.

Si estás familiarizado con la edición de tu Cpanel/DNS y sabes exactamente qué hacer, hazlo **INMEDIATAMENTE** antes de que sea demasiado tarde.

De lo contrario, si prefieres que alguien más experimentado lo haga por ti para protegerte, prevenir el spam, la suplantación y el phishing con la autenticación de Gmail, configurando la autenticación de correo electrónico DMARC, SPF y DKIM, avísanos y contáctanos. Te ayudaremos a hacerlo todo antes de que cause más daño.

Si necesitas asistencia, contáctanos por mensaje de texto al: (209) 730-6530

Guardar Nuestro Sitio Web: HAZ CLIC AQUÍ PARA IR A NUESTRO SITIO WEB

Esperamos que esta información sea útil.