Google confirma que 2.500 millones de cuentas de Gmail fueron hackeadas: cómo protegerse

Google confirmó que un grupo de ciberdelincuentes accedió a una de sus bases de datos y obtuvo la información de 2.500 millones de cuentas de Gmail, comprometiendo la seguridad de millones de usuarios en todo el mundo.

La compañía informó sobre el ataque en su blog oficial y brindó detalles sobre cómo ocurrió, quiénes resultaron afectados y qué medidas de seguridad deben tomar tanto usuarios particulares como empresas.

El 5 de agosto de 2025, el Google Threat Intelligence Group (GTIG) confirmó que hackers lograron penetrar una de sus bases de datos corporativas alojadas en Salesforce, una plataforma utilizada para la gestión de relaciones con clientes.

El grupo detrás de este ataque, identificado como ShinyHunters (o UNC6040 en los informes técnicos), logró capturar información durante un breve periodo antes de que los equipos de Google detectaran el acceso y bloquearan la intrusión.

De acuerdo con la compañía, los atacantes accedieron a información empresarial considerada básica y en su mayoría pública. Entre los datos expuestos se incluyen nombres comerciales y detalles de contacto, tanto de cuentas de Gmail como de usuarios de servicios como Google Cloud.

Aunque la clave o las contraseñas no formaban parte de los datos comprometidos, el ataque implica riesgos reales para quienes usan estos servicios.

La operación de los atacantes no aprovechó una vulnerabilidad técnica en Salesforce, sino que se sirvió principalmente de ingeniería social. El modus operandi fue el siguiente: los hackers, haciéndose pasar por soporte técnico, realizaron llamadas telefónicas a empleados de organizaciones, simulando asistir en tareas habituales.

Durante estas conversaciones, guiaron a sus víctimas para que autorizasen conexiones sospechosas desde aplicaciones modificadas, en particular versiones falsas del Data Loader (una aplicación legítima de Salesforce). Esta autorización permitió a los agresores copiar datos desde el sistema atacado.

Quiénes fueron los afectados por el hackeo en Gmail

El ataque se centró principalmente en pequeñas y medianas empresas que usaban los servicios de Google a través de Salesforce, aunque el número real de personas y empresas potencialmente implicadas es difícil de dimensionar. Cerca de

2.500 millones de cuentas de Gmail estuvieron expuestas, lo que representa una filtración de dimensiones nunca vistas.
Google ha enviado notificaciones por correo electrónico a los usuarios y organizaciones cuyos datos se vieron comprometidos. A la vez, aclaró que la brecha no incluyó datos sensibles como contraseñas, credenciales de acceso u otra información financiera directa.

Sin embargo, al tener en su poder nombres y direcciones de correo asociadas a cuentas empresariales, los delincuentes pueden intentar otros ataques como phishing o suplantación de identidad, utilizando la información robada para engañar y solicitar datos confidenciales adicionales.

Además, la actividad de extorsión asociada a este tipo de intrusiones estuvo presente. Los responsables del ataque se comunicaron con organizaciones víctimas a través de correos electrónicos y realizar llamadas telefónicas exigiendo pagos en bitcoin dentro de plazos de 72 horas, amenazando con hacer pública la información sustraída.

Cómo protegerse de este tipo de hackeos en Gmail

La experiencia reciente obliga a extremar precauciones, especialmente ante correos electrónicos o llamadas apócrifas provenientes de entidades reconocidas. Aquí se detallan las acciones más importantes para minimizar riesgos:
Para usuarios particulares:

- No responder correos sospechosos: ante mensajes que parezcan proceder de bancos, redes sociales o Google solicitando información adicional, nunca brindes datos personales o claves.
- Verificar la procedencia de las comunicaciones: los correos de Google genuinos provienen de direcciones oficiales y no piden que se envíen contraseñas.
- Activar la verificación en dos pasos (MFA): aumenta la seguridad de la cuenta requiriendo una segunda prueba de identidad antes de acceder
- Actualizar y fortalecer contraseñas: usa claves robustas que combinen letras, números y símbolos, y evita repetirlas en diferentes servicios.
- Supervisar movimientos inusuales: controla periódicamente la actividad de tu cuenta y revisa si existen accesos desconocidos.
- Mantener actualizados sistemas y aplicaciones: instala las actualizaciones aconsejadas por Google, que corrigen posibles vulnerabilidades.

Para empresas y administradores:

- Limitar los permisos según el principio de menor

privilegio: da a cada usuario solo el acceso estrictamente necesario para su tarea, especialmente a herramientas como Data Loader.

- Gestión rigurosa de aplicaciones conectadas: supervisa qué aplicaciones tienen acceso a tus plataformas y quién puede autorizarlas.
- Restringir el acceso según dirección IP: establece controles para que solo puedan ingresar aquellos que utilicen redes y ubicaciones predefinidas.
- Capacitación continua a empleados: realiza entrenamientos periódicos sobre riesgos de ingeniería social, phishing y prácticas de seguridad digital.
- Auditorías y monitoreo permanente: revisa perfiles, permisos asignados y actividad inusual de manera regular. Utiliza plataformas de monitoreo ofrecidas por Salesforce y otras herramientas especializadas.
- Implementar alertas automáticas: usa sistemas que detecten grandes descargas de datos o comportamientos anómalos en la nube, con el fin de reaccionar a tiempo ante posibles intrusiones.
- Prestar atención a extorsiones: descarta mensajes o llamadas que te exijan pagos rápidos en monedas digitales, reporta inmediatamente estos incidentes a los canales oficiales.

Con información de Infobae