

Estos son los riesgos ocultos de subir tus fotos personales a ChatGPT

06/04/2025



OpenAI liberó al público su herramienta de creación de imágenes personalizadas en ChatGPT. La nueva función provocó la semana pasada un boom de virales, una tendencia de la que casi nadie quiso quedarse afuera.

Esta novedosa herramienta permite transformar fotos reales de personas en estilos artísticos específicos, como el popular estilo Studio Ghibli, y otros formatos inspirados en series como Los Simpson, South Park o Rick & Morty.

Sin embargo, detrás de esta moda aparentemente inofensiva se esconden importantes **riesgos relacionados con la privacidad y la seguridad de los datos personales**.



Los riesgos de seguridad y privacidad de subir fotos personales a ChatGPT. (Imagen: Grok).

Así funciona ChatGPT

El chatbot de IA usa **datos proporcionados por los usuarios para generar contenido personalizado**. Al subir una imagen a la plataforma, los usuarios otorgan su **consentimiento para que esa tecnología recopile información** necesaria para procesar y recrear la imagen.

Según la política de privacidad de OpenAI, los datos obtenidos pueden incluir no solo el contenido cargado, sino también información personal como **nombre, historial de operaciones y detalles de contacto**.

Si bien **OpenAI** asegura que esa información no se almacena indefinidamente y es utilizada para mejorar sus servicios o entrenar nuevos modelos de inteligencia artificial, esta recopilación **plantea preocupaciones sobre el uso comercial y la exposición involuntaria de información sensible**.

Las imágenes pueden **contener metadatos ocultos, como ubicación geográfica y fecha de captura**, que podrían ser explotados sin

el conocimiento del usuario.

Entonces, ¿cuáles son los riesgos?

Si subís una foto a ChatGPT, técnicamente **perdés el control sobre cómo se almacena o procesa** esa imagen. A pesar de que OpenAI dice que los datos se usan para mejorar el modelo, existe el **riesgo de que, en el futuro, la foto pueda ser utilizada de maneras no previstas** (por ejemplo, en entrenamiento de sistemas de **reconocimiento facial** sin tu consentimiento).

Además, a diferencia de herramientas como Google Fotos o iCloud, **ChatGPT no es un servicio de almacenamiento seguro**. Si le enviás una foto, **no hay opción de borrarla manualmente después**.

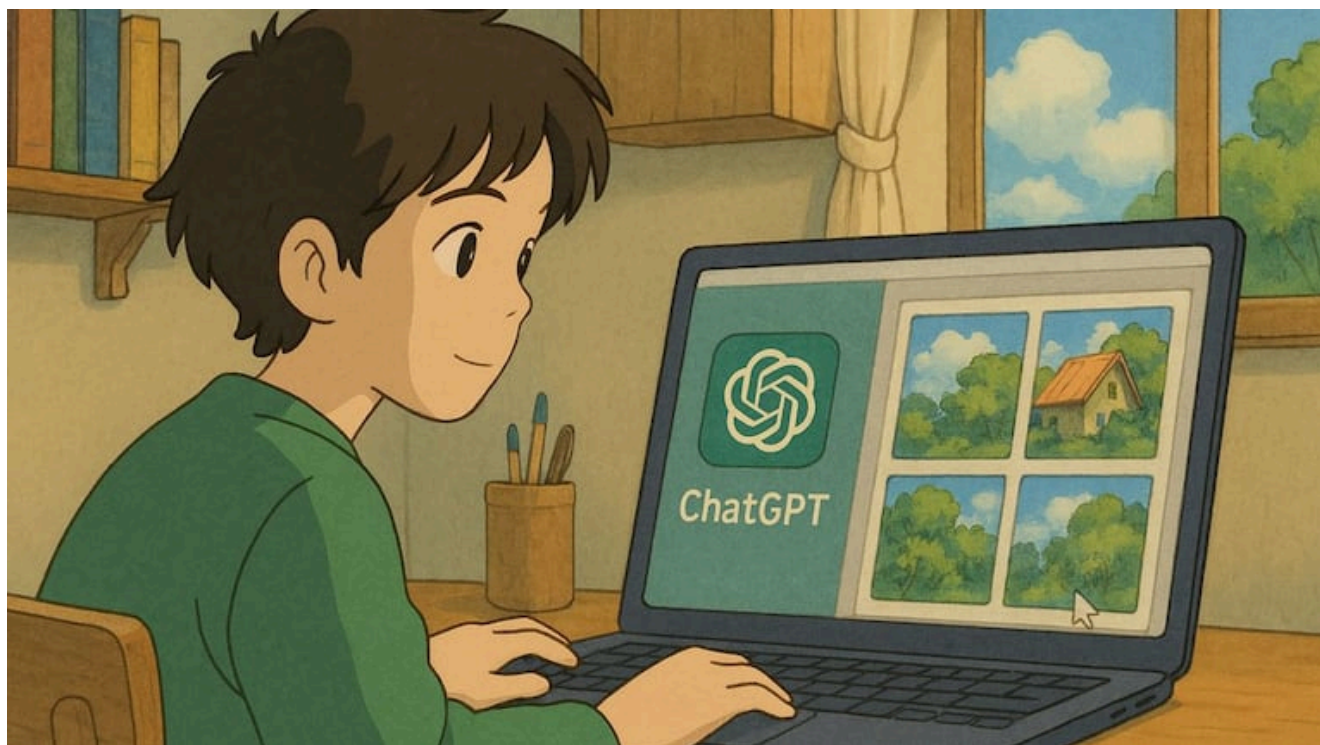
Uno de los peligros más alarmantes es la posibilidad de que menores de edad aparezcan en las imágenes compartidas con ChatGPT. Esto no solo representa un problema ético, sino también un **peligro potencial para la seguridad de los niños**.

Si bien OpenAI asegura que los chats y las fotos no son compartidas, **no hay garantía absoluta de que tus imágenes no puedan ser accedidas por terceros** en caso de una filtración de datos.

Es más, **si las credenciales de acceso a ChatGPT son comprometidas** (hackeadas), ciberdelincuentes podrían **acceder al historial** de conversaciones y utilizar la información obtenida para **ataques de ingeniería social o suplantación de identidad**.

OpenAI también advierte en sus preguntas frecuentes que no se debe compartir información sensible en la plataforma, ya que los datos proporcionados durante las sesiones activas podrían ser recordados por el sistema. A pesar de que emplea medidas avanzadas de seguridad, como cifrado de conversaciones, **estas**

garantías no eliminan completamente el riesgo.



Los trucos para usar el flamante generador de imágenes de OpenAI. (Foto: Creada con ChatGPT).

Recomendaciones para minimizar riesgos al subir fotos a ChatGPT

- **No subas fotos con información sensible** (caras de menores, documentos, ubicaciones, etc.).
- **Si necesitas analizar una foto**, usá servicios especializados con cifrado y políticas claras de privacidad.
- **Revisa los Términos de Servicio** de ChatGPT/OpenAI para entender cómo manejan los datos.

Por ese motivo, **evitá compartir imágenes personales en ChatGPT o cualquier IA a menos que sea estrictamente necesario y estés consciente de los riesgos.**

Fuente: TN