Ghibli y las fotos virales, ¿qué riesgos hay detrás de la herramienta de IA?

Usuarios dan acceso no sólo a fotografías sino a mucha de la información almacenada en sus dispositivos, lo que puede ser aprovechado por ciberdelincuentes y estafadores

La tendencia por tener una fotografía al estilo Ghibli pone en riesgo los **datos biométricos,** advirtieron expertos a los internautas; es decir, subirte al furor por estas imágenes podría ponerte en riesgo de una estafa.
Debido a que la Inteligencia Artificial como Grock, la IA de "X", recopila muchos datos, como la ubicación y el contenido que sube una persona a redes sociales, las imágenes ingresadas a este sistema pueden ser usadas y almacenadas por la plataforma.
Al respecto, Laura Enríquez, comisionada del InfoCDMX, alertó que este tipo de datos son compartidos con proveedores, empresas afiliadas y terceros con los que internautas interactúan.
"Ningún servicio es totalmente gratuito. Hoy nuestros datos personales son una moneda de cambio, y antes de subir una imagen, conoce qué implicaciones puede tener para tu privacidad", escribió en redes sociales.
Para colmo, la creación de estas imágenes pone en riesgo el medio ambiente, pues se realiza por medio de la Inteligencia Artificial que opera a partir de un gran número de servidores, y debido a la cantidad de consumidores que la usan, es necesario el uso de agua para enfriarlos.
Entonces, en al menos cinco días, 216 millones de litros de agua fueron consumidos por la IA, y con esta cantidad un millón 350 personas hubieran podido tomar un baño en la regadera.

¿Cómo se crean?

Las personas pueden generar una imagen al estilo Ghibli mediante el ChatGPT y Grock, y la intención de la tendencia es reimaginar momentos de la vida cotidiana con un estilo caricaturesco.
Para obtener una foto con dicho estilo, una persona deberá acceder a https://x.com/i/grok?, ahí deberá subir una imagen clara y escribir lo siguiente: transforma esta foto al studio Ghibli", y de inmediato la Inteligencia Artificial de "X" generar la foto.
Mientras, en https://chatgpt.com/ las personas podrán llegar al mismo resultado escribiendo lo siguiente: transforma esta foto al estilo Ghibli, manteniendo el mismo fondo y expresión del rostro".

¿A quiénes estafan?

Las personas que pueden ser víctimas de estafas son aquellas que desconocen la existencia y el uso de la Inteligencia Artificial, por ello en redes sociales, usuarios están ofreciendo sus servicios para generar este tipo de imágenes.
Los precios van desde los 10 pesos por foto y hasta los 150 pesos para más de diez fotos a generar, sin embargo, estas se generan de manera gratuita y usan la Inteligencia Artificial de ChatGPT o Grock.

Principales riesgos en ciberseguridad

* Riesgo de privacidad y uso indebido de datos: Las aplicaciones de edición de imágenes requieren acceso a la galería del dispositivo y a información personal. Algunas reservan el derecho de almacenar y utilizar las fotos con fines comerciales o de entretenimiento.
* Robo de identidad y deepfakes: Al compartir imágenes propias en plataformas de terceros, se corre el riesgo de que sean utilizadas para la creación de deepfake o suplantaciones de identidad y esto puede derivar en fraudes digitales.
* Vulnerabilidad en la seguridad del dispositivo: Algunas aplicaciones maliciosas pueden solicitar permisos excesivos que comprometen la seguridad del dispositivo, esto incluye acceso a la cámara, micrófono o incluso datos sensibles.
* Phishing y malware: La popularidad de estas herramientas ha generado el surgimiento de aplicaciones falsas que pueden contener malware o servir como anzuelo para ataques de phishing.

Recomendaciones:

* Leer los términos y condiciones: Antes de utilizar una aplicación, revisa cómo maneja tus datos y si los almacenará o compartirá con terceros.
* Evitar subir fotos sensibles: No compartas imágenes que podrían comprometer tu privacidad o la de otras personas.
* Usar plataformas seguras: Opta por aplicaciones de desarrolladores confiables y descargarlas desde tiendas oficiales como Google Play o App Store.
* Revisar los permisos que solicita la aplicación: Si una app pide acceso innecesario a tu dispositivo, es mejor evitar su uso.
* Actualizar el software de tu dispositivo: Mantener actualizados el sistema operativo y las aplicaciones reduce la posibilidad de vulnerabilidades.