LITORALPRESS

Fecha: 01-08-2025
Medio: Publimetro
Supl. : Publimetro
Tipo: Noticia general
Título: Cómo cuidar tu privacidad en redes sociales sin dejar de compartir

Pág. : 10
Cm2: 627,5

Tiraje: 84.334
Lectoría: 382.227
Favorabilidad: No Definida

fayerwayer **FW**

Reto. Con el auge de la Inteligencia Artificial y los deepfakes, distinguir entre humanos y bots es cada vez más difícil. Conoce cómo algunas soluciones ofrecen una prueba de humanidad anónima para proteger tu identidad sin sacrificar tu experiencia digital

Cómo cuidar tu privacidad en redes sociales sin dejar de compartir

FOTOS: FREEPIK

Erika Padrón
Metro World News

Las redes sociales como Instagram, TikTok o Facebook se han convertido en una extensión de nuestra vida diaria. Compartimos viajes, momentos felices, logros personales y hasta lo que comemos o compramos.

Esta costumbre de mostrarlo todo, conocida como oversharing, ha transformado la manera en que nos relacionamos, pero también ha abierto la puerta a riesgos como fraudes, suplantación de identidad, extorsiones, acoso y hasta secuestros.

Sin embargo, proteger tu privacidad no significa que tengas que dejar de usar redes sociales o mantener un perfil bajo. Al contrario: si adoptas estrategias de seguridad adecuadas, puedes seguir muy activo, compartir lo que deseas de forma más consciente y hasta hacer crecer tu comunidad digital de manera responsable y segura.

LO QUE HOY DEBES HACER

De acuerdo con Raúl Fernández, ingeniero QA y especialista en ciberseguridad en Klibu —una plataforma que ayuda a verificar la identidad de personas o empresas antes de hacer negocios con ellas—, los hábitos que antes parecían exagerados, como usar "modo fantasma" o limitar la información personal, hoy son herramientas fundamentales para cuidar nuestra integridad.

Incluso, cada vez más personas optan por ocultar rostros de menores, eliminar seguidores desconocidos o restringir quién ve sus publicaciones, entendiendo que estas decisiones no son un lujo, sino una necesidad frente a los riesgos digitales.

De hecho, según datos de la Secretaría de Seguridad Ciudadana (SSC), en México se reciben cerca de tres mil reportes mensuales relacionados con incidentes cibernéticos, de los cuales 38% están ligados a fraudes y suplantación de identidad.

Sigue estas 7 PRACTICAS CLAVES

Kíblu nos comparte estas acciones que puedes implementar para tener mayor control sobre tu información personal en redes:

La clave está en el equilibrio

- Puedes seguir disfrutando de redes sociales, compartiendo contenido y construyendo tu marca personal, siempre que lo hagas con conciencia y tomando decisiones inteligentes para protegerte.
- **Cuidar tu privacidad** no es una moda, es una herramienta de autoprotección digital indispensable.

"Lo que se comparte en redes sociales puede parecer inofensivo, pero los delincuentes digitales no necesitan mucho para armar un perfil completo. Desde una simple historia con ubicación hasta una imagen familiar, todo puede convertirse en una pieza clave para un fraude o una suplantación de identidad. El control sobre la vida digital no es exageración, es un acto de responsabilidad".

RAÚL FERNÁNDEZ,
ingeniero QA y especialista en ciberseguridad en Klibu.

1. **Desactiva la ubicación automática en publicaciones**
Compartir tu ubicación en tiempo real puede parecer inofensivo, pero en realidad permite a terceros identificar tus rutinas, saber si estás fuera de casa o anticipar tus movimientos.

2. **Oculta el rostro de menores**
Usar emojis o stickers para cubrir el rostro de niños y niñas es una medida eficaz contra el robo de imágenes, la creación de perfiles falsos o la exposición de menores en contextos inapropiados.

3. **Limita quién ve tus historias y publicaciones**
Todas las redes sociales ofrecen herramientas de privacidad: úsalas. Puedes restringir tus publicaciones solo a personas de confianza o crear listas específicas para ciertos contenidos.

4. **Elimina seguidores que no conoces o no generan confianza**
Hacer limpieza periódica de tus contactos es clave. Aunque tengas miles de seguidores, asegúrate de que no haya perfiles sospechosos, sin foto o sin actividad real.

5. **Piensa dos veces antes de presumir logros o posesiones materiales**
Mostrar compras, autos nuevos o viajes costosos puede parecer inofensivo, pero también puede atraer estafadores o personas malintencionadas. Evita compartir datos sensibles como montos, ubicaciones o recibos.

6. **Activa la verificación en dos pasos**
Esta función añade una capa extra de protección a tus cuentas, solicitando un código adicional cuando alguien intenta ingresar desde un dispositivo nuevo.

7. **Evita vincular redes personales con datos financieros o profesionales sensibles**
Es recomendable separar tus perfiles personales de aquellos en los que manejas temas laborales o bancarios. Así, si una cuenta se ve comprometida, el impacto será menor y más controlado.