07/01/2025

Las 8 cosas que nunca deberías publicar en redes sociales, según expertos en ciberseguridad

Compartir momentos en redes sociales es entretenido, pero también puede ser riesgoso.

Las redes sociales son parte de nuestra vida cotidiana, pero compartir demasiada información puede ponernos en riesgo. Desde la suplantación de identidad hasta robos físicos, los ciberdelincuentes aprovechan las publicaciones descuidadas para llevar a cabo sus ataques. Aprende cuáles son las ocho cosas que nunca deberías publicar y cómo proteger tu privacidad en línea.

1. Información personal identificable

Datos como tu número de teléfono, dirección o cualquier otra información que permita identificarte pueden ser utilizados por ciberdelincuentes para cometer fraudes o robar tu identidad. Evita compartir detalles que puedan comprometer tu seguridad o la de tu familia.

2. Planes de viaje

Anunciar tus vacaciones antes de tiempo es una invitación para que posibles ladrones aprovechen tu ausencia. En lugar de publicar tus planes, espera a regresar para compartir fotos y experiencias de tu viaje.

3. Tu ubicación en tiempo real

Publicar fotos o check-ins que revelen tu ubicación puede ser peligroso, ya que expone tus rutinas y hábitos diarios. Esta información podría ser usada por delincuentes para planificar ataques físicos o robos.

4. Compras costosas

Mostrar objetos de alto valor, como joyas, dispositivos electrónicos o vehículos, puede convertirte en un blanco para robos. Además, este tipo de publicaciones puede generar comentarios negativos o envidias innecesarias en tus redes.

5. Fotos de menores

Compartir imágenes de niños, especialmente sin su consentimiento, puede ser riesgoso. Estas fotos pueden ser mal utilizadas, incluso en contenidos inapropiados como deepfakes. Piensa dos veces antes de publicar imágenes que comprometan la privacidad de los menores.

6. Conversaciones privadas o detalles íntimos

Publicar discusiones personales o detalles sensibles en redes sociales puede generar malentendidos y conflictos. Mantén esos temas en un ámbito privado para evitar problemas innecesarios.

7. Información financiera

Nunca publiques detalles relacionados con tus finanzas personales, como recibos de sueldo, inversiones o números de cuenta. Este

tipo de información puede ser utilizada por estafadores para vulnerar tu seguridad económica.

8. Problemas laborales o comentarios negativos sobre el trabajo

Criticar a tu jefe, compañeros o lugar de trabajo en redes sociales puede tener consecuencias graves, desde conflictos con colegas hasta despidos. Las empresas suelen monitorear la actividad online de sus empleados, y un comentario inapropiado puede afectar tu reputación profesional.

Consejos para mantenerte seguro en redes sociales

- Sé consciente de lo que compartes: Antes de publicar algo, piensa si te sentirías cómodo compartiéndolo con desconocidos.
- Revisa tu lista de contactos: Elimina personas que no reconozcas o que no necesiten acceso a tus publicaciones.
- Ajusta la configuración de privacidad: Restringe quién puede ver tu lista de amigos, fotos y publicaciones.
- Activa la autenticación de doble factor (2FA): Refuerza la seguridad de tus cuentas para evitar accesos no autorizados.
- Haz privada tu cuenta: Si compartes contenido sensible, como fotos de menores o de tu casa, configura tu perfil para que solo tus seguidores aprobados puedan verlo.

Mantenerse seguro en redes sociales requiere un equilibrio entre compartir momentos y proteger tu privacidad. Al evitar publicar información sensible y ajustar tus configuraciones de seguridad, puedes disfrutar de estas plataformas sin comprometer tu bienestar personal. Recuerda que la prevención siempre es la mejor defensa.

Fuente: https://es.gizmodo.com/

LINK DE LA NOTICIA