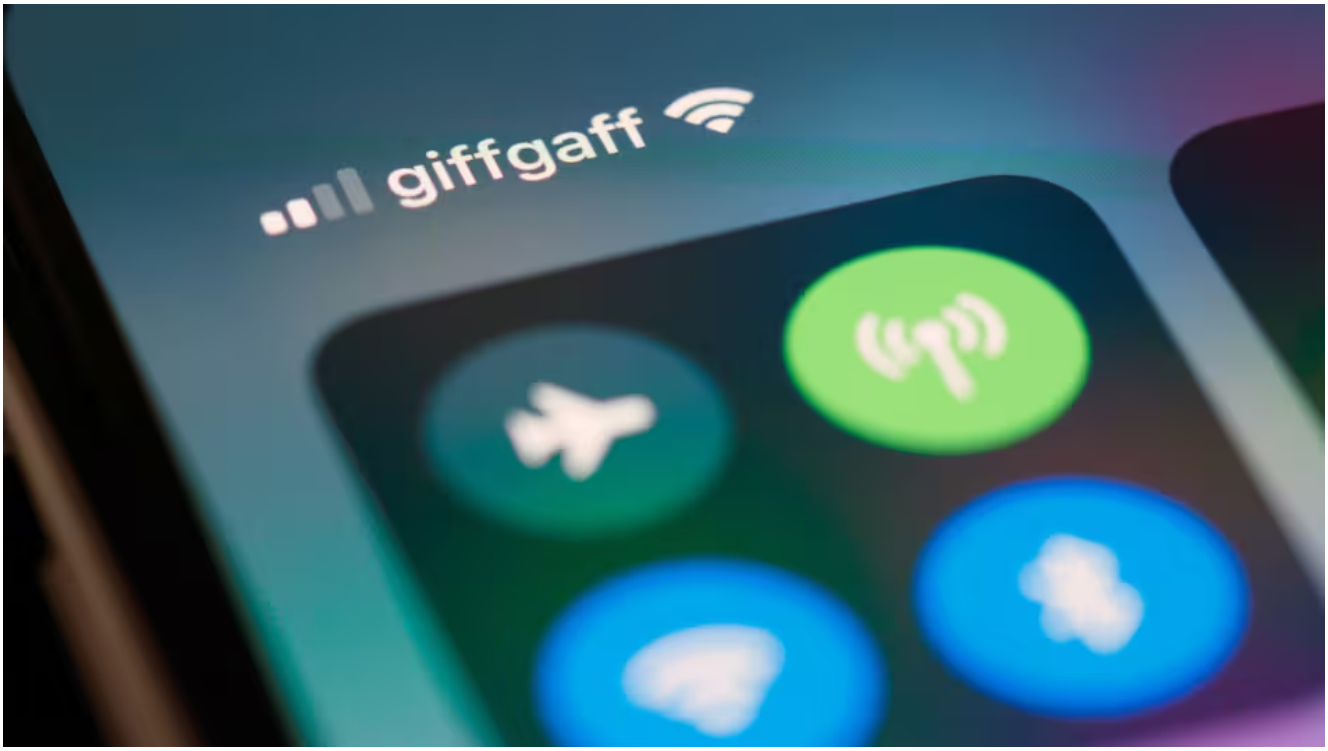
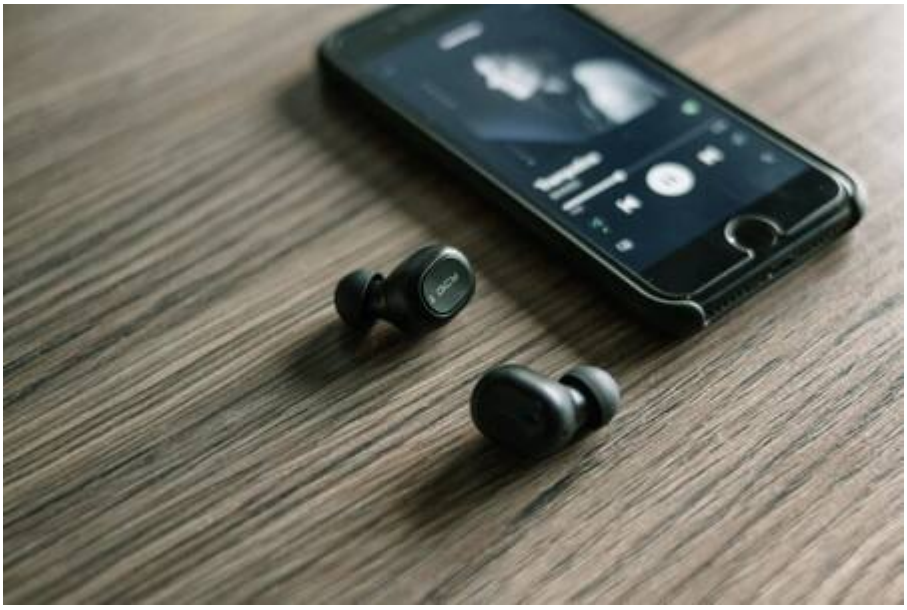
Seguridad para el celular: la función que debe estar apagada en todo momento para evitar ser rastreado

18/03/2026



El **Bluetooth** es una de las **funciones más utilizadas** en los **teléfonos móviles** para compartir archivos o conectar dispositivos. Sin embargo, **mantener esta herramienta activada durante mucho tiempo**, especialmente en lugares públicos, **puede aumentar el riesgo de sufrir ciberataques, robo de información o fraudes digitales**.

Aunque para muchos usuarios parece una función inofensiva, expertos en ciberseguridad advierten que **el Bluetooth puede ser aprovechado por delincuentes informáticos para acceder a datos privados sin que la víctima lo note**. Por eso recomiendan desactivarlo cuando no esté en uso y tomar algunas medidas básicas de seguridad.



Problemas con el uso del Bluetooth.

¿Qué es el Bluetooth y por qué puede ser un riesgo?

El **Bluetooth** permite transferir fotos, videos, documentos o aplicaciones mediante una **conexión inalámbrica de corto alcance**. También se utiliza para conectar auriculares, relojes inteligentes, parlantes y otros dispositivos.

Pero esta misma tecnología puede convertirse en una **puerta de entrada para los ciberdelincuentes**, que aprovechan fallas de seguridad o configuraciones abiertas para infiltrarse en los teléfonos.

Uno de los **ataques más conocidos es el Bluesnarfing**, una técnica que permite a los hackers **robar información confidencial del dispositivo**.

Según el Instituto Nacional de Ciberseguridad, el nombre surge de la combinación de “Bluetooth” y “snarf”, un término que significa copiar o extraer datos sin autorización.

En este tipo de ataque, **los ciberdelincuentes detectan dispositivos con Bluetooth encendido y visible**. Luego utilizan herramientas especializadas para **acceder a información**

sensible como:

- **Fotos y videos**,
- **Archivos personales**,
- **Conversaciones o chats**,
- **Contactos**,
- **Datos bancarios**.

Todo esto puede ocurrir sin que el usuario se dé cuenta.

Otros ciberataques que usan Bluetooth

El Bluesnarfing no es el único método utilizado por los delincuentes digitales. Existen otros ataques similares que también aprovechan esta conexión inalámbrica:

- **Bluejacking**: envío de mensajes no solicitados a dispositivos cercanos.
- **Bluebugging**: acceso remoto al teléfono para manipular funciones, instalar malware o espiar al usuario.

La mayoría de estos ataques funcionan a una distancia de hasta 10 o 15 metros, por lo que el responsable suele estar relativamente cerca de la víctima, por ejemplo, en un café, aeropuerto o transporte público.

¿Cómo evitar ataques por Bluetooth?

Los especialistas recomiendan aplicar algunas medidas simples para reducir los riesgos de seguridad en el celular.

Consejos clave para proteger tu

dispositivo:

Apagar el Bluetooth cuando no lo estés utilizando.

- **Evitar usar esta función en lugares públicos** con mucha gente.
- **No transferir información sensible mediante Bluetooth**.
- **Rechazar conexiones desconocidas** o automáticas.
- **Desactivar el modo visible** del dispositivo.
- **Aceptar solo conexiones de dispositivos confiables**.
- **Eliminar equipos vinculados** que ya no utilices.

Estas prácticas ayudan a reducir significativamente las posibilidades de sufrir ataques.

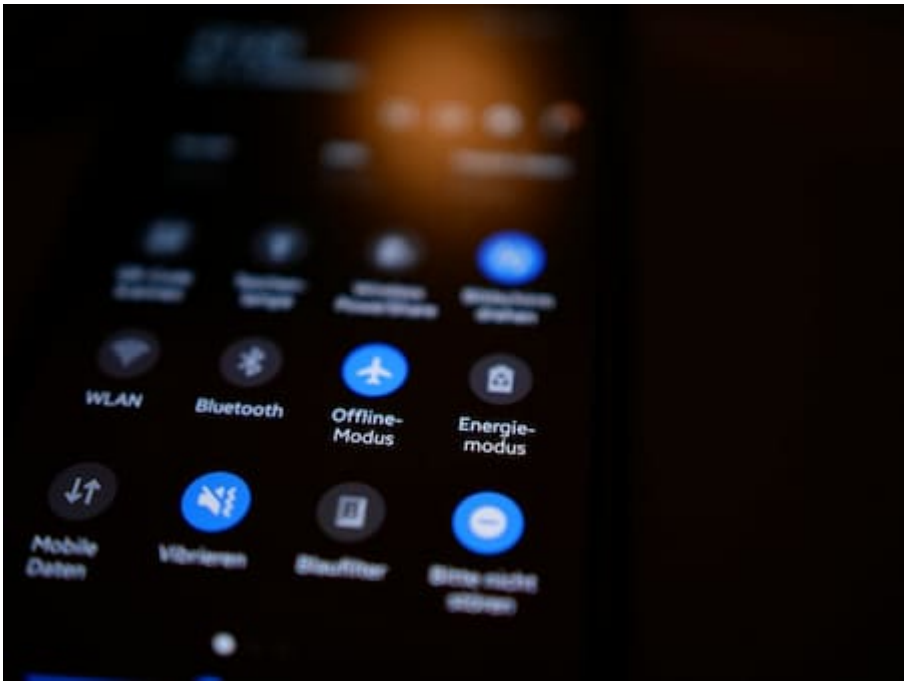
Señales de que tu celular pudo haber sido hackeado

Existen algunos indicios que podrían alertar sobre un posible acceso no autorizado al dispositivo.

Entre los síntomas más frecuentes se encuentran:

- **La batería se descarga más rápido** de lo normal.
- **Aparecen búsquedas en internet que no realizaste**.
- **Detectás aplicaciones instaladas que no descargaste**.
- **Hay movimientos sospechosos en cuentas o datos personales**.

Si notas alguna de estas señales, lo recomendable es desactivar el Bluetooth inmediatamente, revisar las conexiones activas y realizar un análisis de seguridad en el teléfono.



Las precauciones que hay que tener al usar el Bluetooth.

Un hábito simple que puede evitar muchos problemas

El **Bluetooth** sigue siendo una herramienta muy útil para el uso diario del celular. Sin embargo, **mantenerlo activado de forma permanente puede aumentar la exposición a riesgos digitales**.

Por eso, los expertos recomiendan adoptar un hábito sencillo pero efectivo: **encender el Bluetooth solo cuando sea necesario y apagarlo al terminar de usarlo**. Esta pequeña acción puede marcar la diferencia para mantener protegida tu información personal.

Fuente: Canal 26