El FBI alertó sobre los peligros ocultos en las aplicaciones que usamos en el celular

08/04/2026

El FBI emitió una advertencia pública sobre aplicaciones móviles que, aun pareciendo inofensivas, pueden **recopilar datos más allá de lo necesario** y trasladarlos **fuera del control del usuario.** La agencia señala que otorgar **permisos de aplicaciones** sin revisar facilita que nombres, números y correos circulen **sin el consentimiento explícito** del propietario del dispositivo.

Los especialistas recuerdan que **muchas apps solicitan accesos a la agenda** o al almacenamiento y el usuario suele aceptar por comodidad. Eso permite a desarrolladores o terceros **cruzar información** y, en algunos casos, continuar **registrando actividad en segundo plano.** Es clave cuestionar cada permiso y preguntarse si la función justifica el acceso solicitado.

Otro punto que alarma a la FBI es el **destino de esos datos:** no

siempre quedan en servidores locales y, cuando migran a infraestructuras en otros países, las normas pueden permitir que **autoridades accedan a ellos**. Por eso la trazabilidad y la política de privacidad de la app deben ser revisadas antes de confiar información sensible.

Señales de que algo anda mal

Si el teléfono empieza a **consumir batería más rápido** de lo habitual, **registra un uso de datos inusual** o aparecen **movimientos extraños** en cuentas vinculadas, conviene sospechar. También hay indicios menos evidentes, como **procesos que se ejecutan sin abrir la app.** Ante dudas, cortar permisos y revisar actividad es prudente.

Cómo reducir el riesgo

Antes de instalar, conviene **revisar punto por punto los permisos solicitados** y evitar ofrecer accesos que no aporten valor real. **No sincronices la agenda** si no es imprescindible y bajá aplicaciones solo desde tiendas oficiales. Además, **revisar periódicamente la configuración de privacidad** ayuda a limitar la exposición provocada por los **permisos de aplicaciones**.

Los expertos suman prácticas complementarias: **comprobar reseñas y permisos antes de instalar,** mantener el sistema operativo y las apps actualizadas, y **desconfiar de programas que pidan accesos extraños.** En casos de duda, eliminar la aplicación y cambiar contraseñas vinculadas es un buen arranque. También es recomendable **usar herramientas de privacidad** y controlar los respaldos en la nube.

El aviso del FBI persigue que la gente **no dé por segura una app solo por su reputación.** Pequeñas rutinas —leer permisos, limitar sincronizaciones y revisar políticas— disminuyen el riesgo de filtraciones. En un entorno donde los datos viajan a

gran velocidad, la **prevención y controles periódicos** funcionan como la primera línea de defensa.

Fuente: La 100