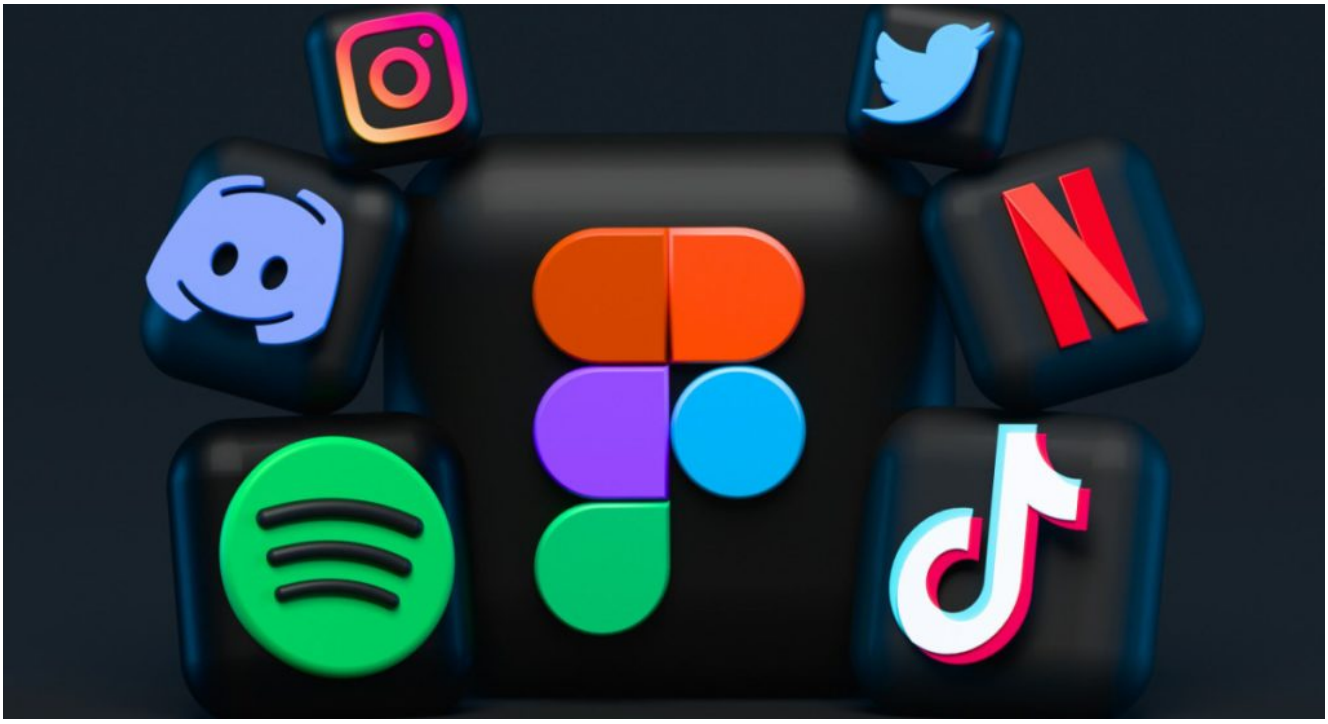
Eliminalas de tu celular: las aplicaciones que podrían robarte información personal y poner en riesgo tu seguridad

13/01/2025



Hay algunas aplicaciones de **Google Play Store** en las que detectaron la presencia de **malware**. Estos programa malignos suelen ocultarse detrás de apps «**seguras**» y ponen en riesgo la seguridad de las personas.

Uno de los malware más peligrosos es **Anatsa**, también conocido como **TeaBot**. Este virus extrae credenciales bancarias e información financiera.

¿Cuáles son las aplicaciones que

podrían contener un virus?

Según Zscaler, una empresa de seguridad digital, entre las aplicaciones que ya infectaron al menos **70.000 teléfonos Android**, se encuentran **PDF Reader & File Manager y QR Reader & File Manager**, entre otras similares.

La compañía **Threat Fabric** informó que este troyano causó aproximadamente **150.000 infecciones en Google Play**, principalmente en las aplicaciones vinculadas con la productividad.

Aunque estas aplicaciones ya fueron eliminadas de las tiendas oficiales, **los usuarios deben estar en estado de alerta.**

Se deben descargar aplicaciones de páginas oficiales. Foto: Unsplash

¿Cómo proteger nuestros celular? Desconfiando de aquellas aplicaciones que solicitan **permisos innecesarios** para su funcionalidad y descargándolas solo en tiendas oficiales.

¿Cómo saber si mi celular tiene virus?

1. **Funcionamiento lento**: los procesadores hacen que el celular responda rápido a cualquier acción. Si se nota cierta ralentización, es probable que tengas un huésped indeseado.
2. **Aplicaciones desconocidas**: puede pasar que veamos una app que no recordemos haber descargado. Uno de los escenarios probables ante ello es que se instaló por medio de un malware.
3. **Poca duración de los datos**: si se acabaron tus datos de un momento a otro, es posible que sea un archivo maligno enviando tu información.

4. **Temperatura del celular**: los calentamientos de la batería o del equipo mismo es otro aviso de malware o virus en tu dispositivo, ya que ejecuta procesos que no estás usando.
5. **Duración de la batería**: si la batería no dura es porque está dañada o porque hay un malware ejecutando procesos sin tu conocimiento.

Cómo descubrir si hay otras personas conectadas a mi WiFi

A continuación, los tres pasos para chequear si hay infiltrados conectados a tu WiFi, según ‘Fing’.

- 1- Acceder a Google Play o App Store y descargar la aplicación, según el sistema operativo de tu dispositivo móvil o computadora.
- 2- Una vez instalada, se debe realizar un escaneo de la red. Esto generará un listado de todos los dispositivos conectados, con detalles como la dirección IP, la MAC y, en ocasiones, el nombre del dispositivo.
- 3- Revisar el listado para identificar cualquier dispositivo desconocido. Hay que tener en cuenta que no solo aparecerán celulares o computadoras, sino también otros dispositivos como routers, impresoras o Chromecast.

Fuente: Canal 26