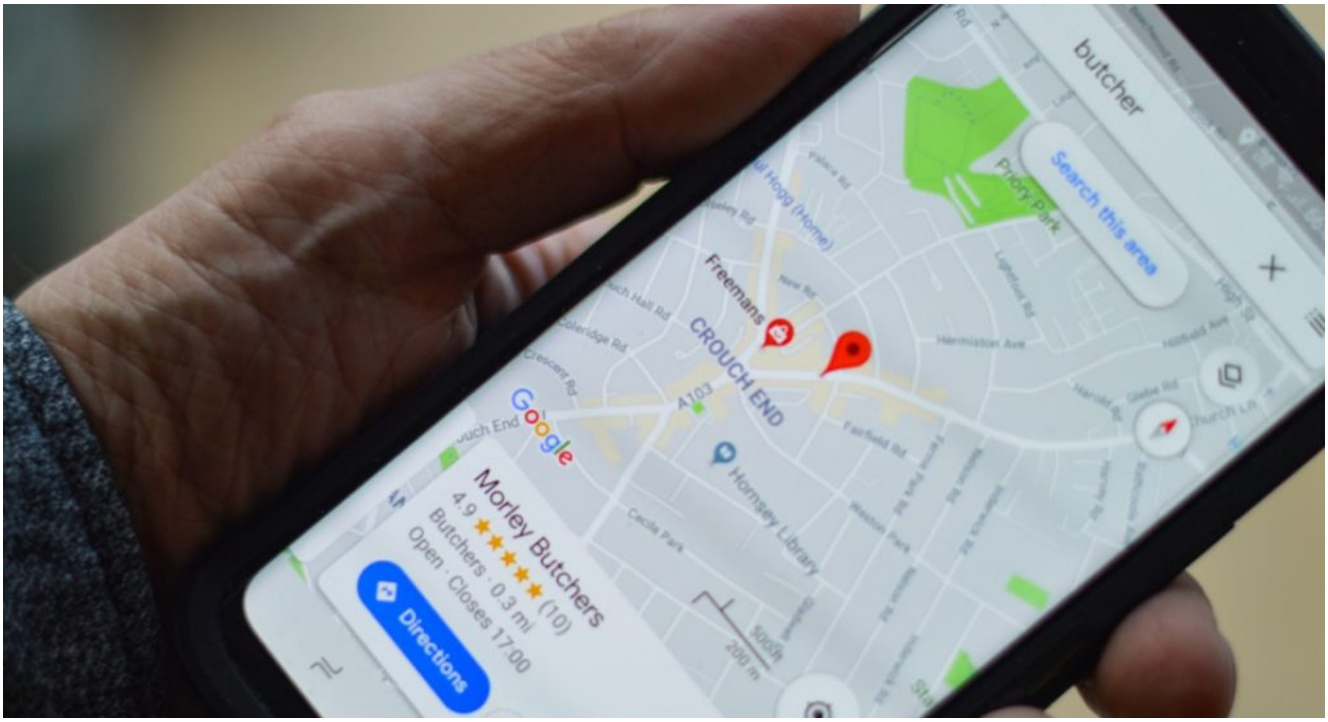
# Alerta por GPS falsos: cómo funciona el hackeo mediante geolocalización en los celulares

20/02/2024




A medida que las aplicaciones se vuelven cada vez más esenciales en la vida diaria, la seguridad y la integridad de estas se vuelven sumamente importantes. En este sentido, uno de los desafíos en la seguridad de los teléfonos celulares es la manipulación de la **geolocalización**, un método que los hackers utilizan para acceder a datos sensibles.

Según el informe de **Seguridad de Consumo de Appdome**, el 56% de los usuarios considera que las marcas y desarrolladores de aplicaciones para celular deben asumir la responsabilidad de garantizar una experiencia segura para el consumidor.

Los **hackeos a través de geolocalización** se producen luego de que los usuarios compartan su ubicación o accedan a servicios específicos fuera de una región geográfica. Principalmente, se

activa en aplicaciones de juegos, páginas de apuestas o plataformas de streaming.

**Tom Tovar**, cocreador y CEO de **Appdome**, explicó: "Ahora que las aplicaciones móviles son el canal dominante para juegos y apuestas, utilizar una solución de seguridad unificada para la protección de los usuarios. **Las marcas deben fortalecer sus controles** frente a las amenazas de seguridad, permitiendo a los bancos online, la tecnología financiera, los juegos, los servicios de streaming y otros clientes garantizar el uso autorizado de la aplicación y protegerse contra el fraude móvil y la apropiación de cuentas".

## Fraudes a través del GPS: una amenaza vigente

La **geolocalización** es un componente sensible en las aplicaciones móviles, afectando diversas funciones esenciales de la experiencia del usuario. **La precisión y autenticidad de la información de ubicación son fundamentales para el funcionamiento general de la aplicación**.

Sin embargo, la manipulación de esta información se convirtió en una preocupación debido a las diversas tácticas utilizadas por los delincuentes, desde proxys maliciosos hasta **falsificación de información GPS**, suplantación de identidad y el cambio de tarjetas **SIM**, entre otros.

La geolocalización ayuda a dirigir a los usuarios hacia flujos específicos y proporciona datos precisos según su ubicación. No obstante, cuando se falsifica **la ubicación GPS** en una aplicación móvil **Android**, los datos de localización transmitidos por el **Sistema de Posicionamiento Global (GPS)** se modifican, dando la impresión de que el dispositivo se encuentra en un lugar diferente al real.

Esta alteración no solo genera flujos no deseados en la

aplicación, sino que también abre la puerta a **actividades maliciosas**, especialmente para impulsar actividades fraudulentas como robo de información sensible, hackeo de cuentas bancarias, entre otros.

# Cómo detectar aplicaciones con GPS falso

Las aplicaciones de GPS falso manipulan los datos de ubicación de un dispositivo móvil para proporcionar coordenadas GPS falsas, **anulando la información auténtica** proporcionada por los sensores GPS del sistema operativo del dispositivo.

Los atacantes suelen descargar estas aplicaciones junto con la aplicación auténtica que desean engañar, interactuando para que acepte datos de ubicación falsos como si provinieran directamente del sistema operativo. Este proceso desencadena **actividades perjudiciales**, como suplantación de ubicación, elusión de restricciones de licencia y problemas de seguridad y privacidad.

Para combatir esta amenaza, se requieren **algoritmos** sofisticados que identifiquen y bloqueen las señales GPS falsas. Estos algoritmos no solo detectan patrones de falsificación, sino que también pueden identificar y **mitigar el uso de aplicaciones de terceros** diseñadas para manipular datos de ubicación. Además, la herramienta puede detectar e impedir intentos de eludir restricciones geográficas mediante el uso de **redes privadas virtuales** (VPN).

Fuente: Canal 26