

## **El problema de malware que fue un rompecabezas para Uber, según Doctormoviles.com**

**El uso inadecuado de cualquier dispositivo electrónico, ya sea móvil, tablet u ordenador, puede ocasionar problemas muy graves relacionados con virus, malware, etc**

Esto puede suponer que datos importantes como la ubicación, cuentas bancarias, contraseñas de redes sociales y otros elementos se encuentren en peligro de ser hackeados, lo cual desencadenaría una serie de desgracias para los usuarios que sería preferible evitar. Algo parecido le pasó a Uber, una de las empresas de transporte más conocidas mundialmente en la actualidad. Si se quiere conocer más información, click aquí.

El problema de los teléfonos inteligentes, es que estos pueden tener malware para smartphone que hacen que todos los datos personales que se encuentran en estos dispositivos sean un objetivo para aquellas personas que se dedican a estafar o robar por Internet. Lo peor es que con el tiempo cada vez consiguen crear más medios para poder hacerse con este tipo de información, comprometiendo así la seguridad de los usuarios.

El último malware que se ha detectado fue un desagradable código para Android, el denominado FakeApp. Esta aplicación se encargaba de robar datos y en este caso, suplantó a Uber provocando graves daños para la compañía. El troyano FakeApp fue descubierto por la firma Symantec a través de un monitoreo regular realizado en las aplicaciones de Android. Este virus se apoderaba de la pantalla del teléfono de los usuarios a intervalos regulares, de manera que interrumpía su actividad y recogía datos importantes y delicados.

Por lo general, este malware intenta pasar desapercibido, por lo que intentaba engañar de forma inteligente a las personas para que fueran revelando su información más relevante. FakeApp se hizo pasar por la aplicación Uber, insistiendo a los usuarios de que debían iniciar sesión en la aplicación con su número de teléfono, además de su contraseña y su registro. Sin embargo, lo que ello provocaba era dar estos datos a personas que no querían usarlos para buenos fines.

Este robo se encontraba cubierto por la aplicación que utiliza URI de enlace profundo de Uber, de forma que se activara la actividad de "solución de viaje" a continuación. De esta manera, todo parecía normal y legal, aunque esa información lo que estaba haciendo era ser transmitida a un servidor remoto. Por tanto, los números de móvil, así como las contraseñas o datos de tarjetas de crédito, cada cual más valioso que el anterior, ya que muchas personas no utilizan los inicios de sesión recomendados, y eso atrae a ladrones de cuentas.

Además, al combinarse un número de móvil con el secuestro de SIM, los estafadores pueden ingresar a cuentas protegidas con autenticación. La mejor manera de evitar esto, según Symantec, es asegurarse de no descargar nunca una aplicación que se encuentre fuera de plataformas oficiales

como Google Play Store o App Store, que están totalmente verificadas y además son verdaderamente seguras. De esta forma, se asegurarán de que sus datos se encontrarán protegidos de forma totalmente garantizada, y no expuestos a ningún ladrón o estafador que pueda quedarse con información muy relevante que pueda ocasionar problemas realmente graves.

**Datos de contacto:**

Eduardo Laserna Montoya  
629456410

Nota de prensa publicada en: [Madrid](#)

Categorías: [Viaje Automovilismo](#) [Turismo](#) [Ciberseguridad](#) [Industria](#) [Automotriz](#)

---

**NotasdePrensa**

<https://www.notasdeprensa.es>