PRIVACIDAD Y APLICACIONES DE DISPOSITIVOS MÓVILES

Las aplicaciones móviles pueden recopilar información de su dispositivo móvil con fines legítimos, pero estas herramientas también pueden poner en riesgo su privacidad. Proteja su privacidad de datos siendo inteligente con las aplicaciones que instala y revisando los permisos que tiene cada aplicación.

¿Cuáles son los riesgos asociados con las aplicaciones de dispositivos móviles?

Las aplicaciones (Apps) en su teléfono inteligente u otros dispositivos móviles pueden ser herramientas convenientes para acceder a las noticias, obtener direcciones, compartir viajes o jugar juegos. Pero estas herramientas también pueden poner en riesgo su privacidad. Cuando *descarga una aplicación*, es posible que *solicite permiso* para acceder a información personal, como **contactos de correo electrónico, almacenamiento, registros de llamadas y datos de ubicación**, desde su dispositivo. Las aplicaciones *pueden recopilar esta información con fines legítimos*; por ejemplo, una aplicación de viaje compartido necesitará sus datos de ubicación para poder recogerlo. Sin embargo, debe tener en cuenta que los desarrolladores de aplicaciones **tendrán acceso a esta información** y **pueden compartirla con terceros**, como las empresas que desarrollan anuncios dirigidos en función de su ubicación e intereses.

¿Cómo puede evitar las aplicaciones maliciosas y limitar la información que las aplicaciones recopilan sobre ti?

1. Antes de instalar una aplicación

- **Evite aplicaciones potencialmente dañinas (PHA – Potentially Harmful Applications)**: *reduzca* el riesgo de descargar PHA al limitar descargas **a las tiendas de aplicaciones oficiales**, como el fabricante de su dispositivo o la tienda de aplicaciones del sistema operativo. **NO** descargue de **fuentes desconocidas**, tampoco **instale** certificados de Empresas que **no sean de confianza**. Además, debido a que se sabe que las aplicaciones maliciosas se deslizan a través de la

seguridad de tiendas de aplicaciones de buena reputación, **siempre lea** las revisiones e investigue al desarrollador antes de descargar e instalar una aplicación.

- **Sea inteligente con sus Aplicaciones**: antes de descargar una aplicación, **asegúrese** de entender **a qué información accederá** la Aplicación. *Lea los permisos* que solicita la aplicación *y determine* si los datos a los que solicita acceder *están relacionados* con el propósito de la aplicación. Lea la política de privacidad de la Aplicación para ver **si**, o **cómo se compartirán sus datos**. Considere **no instalar** la Aplicación si la política es vaga con respecto a con quién comparte sus datos o si la solicitud de permisos parece excesiva.

2. En aplicaciones ya instaladas

- **Revise los permisos de la Aplicación**: **revise** los permisos que tiene cada aplicación. Asegúrese de que las aplicaciones instaladas solo tengan acceso a la información que necesitan y **elimine** los permisos innecesarios de cada aplicación**.** Considere **eliminar** aplicaciones con permisos excesivos. Preste especial atención a las aplicaciones que tienen acceso a su *lista de contactos, cámara, almacenamiento, ubicación y micrófono*.
- **Limite los permisos de Ubicación**: algunas aplicaciones tienen acceso a los servicios de ubicación del dispositivo móvil y, por lo tanto, tienen acceso a la **ubicación física** aproximada del usuario. Para las aplicaciones que requieren acceso a los datos de ubicación para funcionar, considere la posibilidad de **limitar** este acceso solo cuando la aplicación está en uso.
- **Mantenga el software de la Aplicación actualizado**: las aplicaciones con software **desactualizado** pueden correr el riesgo de explotar **vulnerabilidades** conocidas. **Proteja** su dispositivo móvil de malware **instalando** actualizaciones de la aplicación a medida que se lanzan.
- **Elimine las Aplicaciones que no necesita**: para evitar la recolección innecesaria de datos, **desinstale** las aplicaciones que ya no utiliza.
- **Tenga cuidado al iniciar sesión en aplicaciones con cuentas de redes sociales**: algunas aplicaciones están integradas con sitios de redes sociales; en

estos casos, *la aplicación puede recopilar información de su cuenta de redes sociales y viceversa*. Asegúrese de sentirse cómodo con este tipo de intercambio de información antes de iniciar sesión en una aplicación a través de su cuenta de red social. Alternativamente, use su dirección de correo electrónico y una contraseña única para iniciar sesión.

¿Qué pasos adicionales puede tomar para proteger los datos en sus dispositivos móviles?

- **Limite las actividades en las redes públicas de Wifi:** las redes públicas de Wi-Fi en lugares como aeropuertos y cafeterías ofrecen a los atacantes la oportunidad de **interceptar información confidencial**. Cuando utilice una conexión inalámbrica pública o no segura, *evite* usar aplicaciones y sitios web que *requieran información personal,* por ejemplo, un **nombre de usuario** y una **contraseña**. Además, *desactive* la configuración de **Bluetooth** en sus dispositivos cuando no esté en uso.
- **Tenga cuidado al cargar**: **evite** conectar su teléfono inteligente a **cualquier computadora** o **estación de carga** que no controle, como una estación de carga en una terminal de aeropuerto o una computadora compartida en una biblioteca. La conexión de un dispositivo móvil a una computadora mediante un cable USB puede permitir que el *software* que se ejecuta en esa computadora *interactúe con el teléfono* de una manera que no puede anticipar. Por ejemplo, una computadora maliciosa podría **obtener acceso a sus datos confidenciales** o instalar un nuevo software.
- **Proteja su dispositivo contra el robo**: tener acceso físico a un dispositivo hace que sea más fácil para un atacante **extraer** o **corromper** información**. No deje** su dispositivo desatendido en público o en áreas de fácil acceso.
- **Proteja sus datos si su dispositivo es robado**: asegúrese de que su dispositivo **requiera una contraseña** o un **identificador biométrico** para acceder a él, de modo que, si es robado, los ladrones tendrán *acceso limitado a sus datos*. Si le roban su dispositivo, comuníquese **de inmediato** con su proveedor de servicios para proteger sus datos.