Después de un largo período de pruebas beta, Google lanzó la semana pasada Android 11, la última versión del sistema operativo móvil de la compañía, con funciones que ofrecen mejor control sobre la seguridad y privacidad de los datos.

Google informó en su último anuncio que el sistema operativo Android 11 incluye algunas nuevas medidas integradas, diseñadas para mantener los datos de los usuarios seguros de forma predeterminada, aumentar la transparencia y ofrecer un mejor control.

Entre las nuevas características de seguridad y privacidad destacan:

1.- Permisos únicos

Al igual que la función ya existente en iOS, la función de *«permiso de una sola vez»* permite a los usuarios otorgar a las aplicaciones acceso de un solo uso a los permisos más sensibles del dispositivo, como ubicación, micrófono y cámara.

Por lo tanto, las aplicaciones deben volver a obtener los permisos antes de volver a evaluar los sensores. Esta función no es nueva en Android, pero anteriormente, solo estaba disponible para usar al descargar una nueva aplicación de Google Play Store.

Algunas aplicaciones pueden activar el mismo mensaje de permiso después de la instalación y otras al acceder a los sensores por primera vez, lo que aumenta una capa de privacidad.

2.- Restablecimiento automático de permisos para aplicaciones no utilizadas

Esta nueva función podría ser útil en un escenario en el que no se haya interactuado con una aplicación instalada durante meses o que se haya olvidado por completo después de descargar y otorgar los permisos requeridos.

Además de ser una amenaza para la privacidad, estas aplicaciones podrían seguir

consumiendo los recursos de hardware del dispositivo o seguir accediendo a los datos en segundo plano.

Para solucionar esto, la nueva función de restablecimiento automático de permisos de Android 11, permite al sistema restablecer de forma automática los permisos de tiempo de ejecución confidenciales para una aplicación que el usuario no ha utilizado durante meses.

Cabe mencionar que siempre se puede volver a otorgar permisos a dichas aplicaciones cada vez que se vuelvan a utilizar.

3.- Parches de seguridad rápidos a través de los módulos de Play Store

Aunque Google ahora requiere que los fabricantes de teléfonos inteligentes implementen actualizaciones de seguridad periódicas para los usuarios, todavía no ayuda a los usuarios finales a corregir vulnerabilidades críticas antes de que los hackers las exploten.

Con Android 11, la empresa aumentó la integración de la aplicación Google Play Store en el dispositivo, lo que permite descargar e instalar parches de seguridad críticos del sistema operativo como módulos al instante, desde los servidores de Google.

Esto significa que los usuarios de Android 11 recibirán parches de seguridad y errores tan pronto como estén disponibles en lugar de depender de los fabricantes de dispositivos para lanzar actualizaciones a nivel de SO.

4.- Aplicación de almacenamiento con alcance para proteger los datos

Introducido en la versión de Android Q el año pasado, la aplicación de almacenamiento de alcance también está disponible en la última versión con cambios menores.

Debido a que está habilitado para todas las aplicaciones de forma predeterminada, las aplicaciones no requieren ningún permiso especial para guardar y acceder a sus propios archivos de espacio aislado en el almacenamiento externo.

Sin embargo, al suponer que una aplicación solicita permisos relacionados con el almacenamiento en tiempo de ejecución, significa que la aplicación solicita un acceso amplio al almacenamiento externo.

5.- Restringir el acceso innecesario a la ubicación en segundo plano

Uno de los cambios de privacidad más importantes en Android 11 involucra la restricción mayoritaria del acceso de las aplicaciones a la ubicación del fondo del dispositivo.

Cuando una aplicación solicita permiso para acceder a su ubicación, Android 11 garantiza primero otorgar solo la ubicación en primer plano, y si también requiere acceso a la ubicación desde el fondo, la aplicación debe realizar una solicitud de permiso por separado.

Esta segunda solicitud requiere que los usuarios sigan pasos adicionales, en lugar de presionar ciegamente *«ok, ok, permitir»*, desde el indicador. Por lo tanto, las aplicaciones no tienen acceso a más datos de los que necesitan.

Para habilitar el acceso a la ubicación en segundo plano, los usuarios deben configurar la opción *«permitir todo el tiempo»* para el permiso de ubicación de la aplicación en una página de configuración.

Además, Google también requiere que los desarrolladores de aplicaciones de Android expliquen por qué su aplicación necesita acceso a la ubicación en segundo plano en primer lugar.