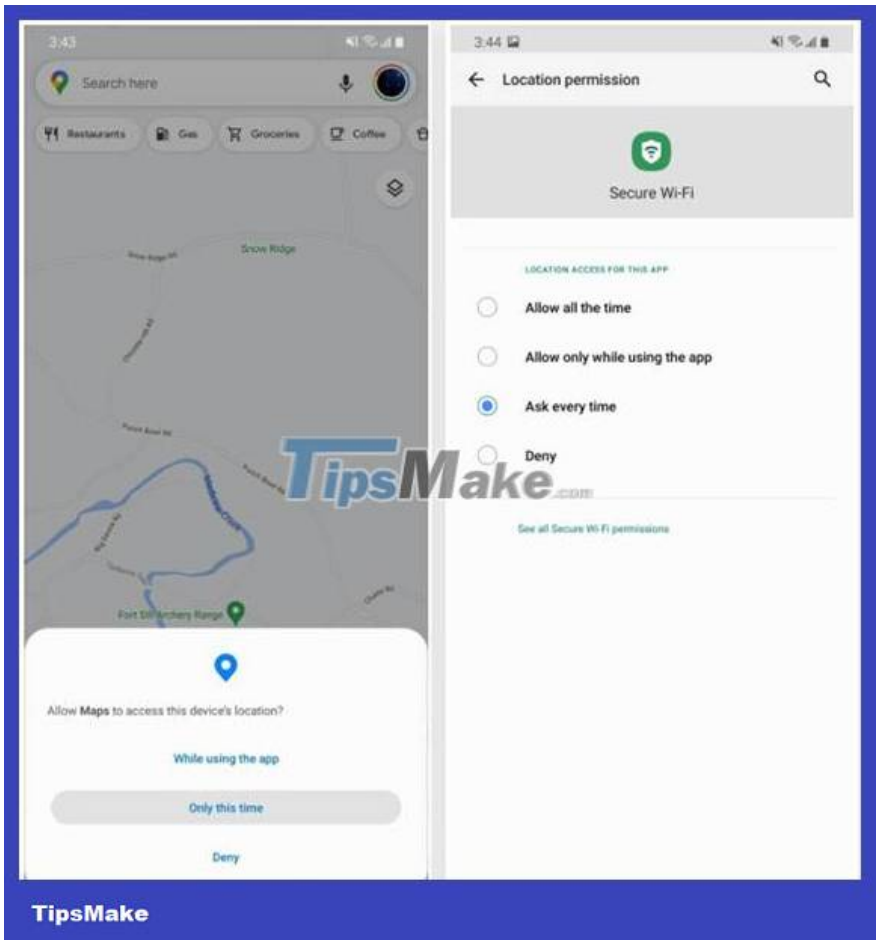
# How to secure your Galaxy phone with One UI

Google has gradually improved security and privacy on Android devices, but Samsung is one step ahead in this area. Therefore, Samsung's One UI 3.0 based on Android 11 is currently the most secure version of the operating system thanks to a few important changes and new features.

Google has gradually improved security and privacy on Android devices, but Samsung is one step ahead in this area. Therefore, Samsung's One UI 3.0 based on Android 11 is currently the most secure version of the operating system thanks to a few important changes and new features.

## Temporary permission

You can grant temporary app access. Camera, microphone and location will have a new option when the app 'asks for permission' which is 'Only this time'. When this option is selected, the application will only be accessed once. Next time if you want to access the above features, you will have to ask again.



## Background location access must be done manually

In One UI 3.0, the 'Allow all the time' option no longer appears when an app asks for access to your location. In previous versions, this option was to access your location while the app was running in the background.


Apps can still be allowed, but it's not as simple as a tap anymore. You must go to **Settings > Permission managers** to perform manual permission operations, or the application may add an option that takes you to the Settings menu.

## Access rights automatically reset

In One UI 3.0, when an app has not been used for several months, its permissions are automatically reset. Using the new 'Remove permissions if app isn't used' option in Settings (device must be running Android 11 to see this option), all access permissions are changed to 'Deny'.


## Protection against application queries

On previous versions of One UI, any app installed on your device could ask the system to access a list of all apps on the device. It will allow apps to check if there is a second app or an app they don't want to interact with.

However, this information can be used by other applications to track users and collect data, so One UI 3.0 has changed its policy. The list of applications on the device will be filtered by default when an app requests it. If there is information not provided in this list, applications can ad hoc queries.

## Automatically block repeated permission requests

Instead of receiving an access request that you previously denied, you can choose the 'don't ask again' option if the request happens a second time on One UI 3.0. You will no longer receive this access request, but you can still activate it manually in the system Settings.

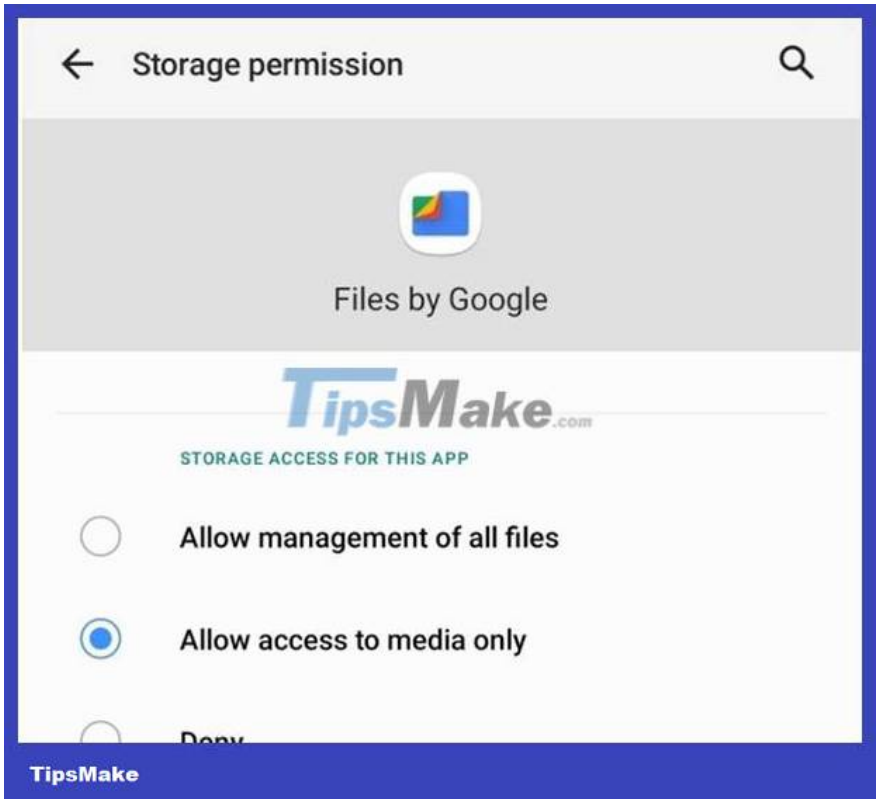
## Block spam

The FCC has an authentication tool called STIR/SHAKEN to verify phone numbers. They have asked all US carriers to implement this system into their networks to help combat robocalls and spam.

In One UI 3.0, call screening applications can access verification status from STIR/SHAKEN and use this information to improve blocking of unwanted calls.

## Scooped Storage operates at maximum efficiency

First introduced in One UI 2.0, Scooped Storage changed the way apps interact with your device's file system. It limits application access to only a few folders in internal memory, so applications cannot view other files. However, Scoped Storage caused many applications to stop working, forcing Google to stop this feature to upgrade and improve.




In One UI 3.0, apps must now use Scooped Storage. For file management apps, One UI 3.0 has a new 'All Files Access' permission, allowing them to function like previous versions. However, the application must meet certain requirements to receive access. All other applications are restricted to 'Media Only Access'.

## There is no default camera

One UI 3.0 also no longer has default camera settings. Although you can use third-party camera applications, applications that require the use of the camera must still use the device's pre-installed application. This will prevent apps from stealing location information by reading address tags in your photos.

## Turn off automatic USB audio routing

In Developer Options there is a new section called 'Disable USB audio routing'. When you connect an audio device to your phone via USB, it will deactivate automatic USB audio routing to that device.


## Protected location tracking

When an app needs to access antenna characteristics to improve tracking accuracy, One UI 3.0 has some limitations to protect your privacy. First, the API that allows apps to access this information is specific to the device model. Second, users must grant location permissions to the app to collect this information.