# 5 types of mobile applications should not be installed on smartphones

With millions of apps available on smartphones today, it's no surprise that not all apps are reliable. Indeed, many mobile applications are designed to attack users' devices or steal personal information.

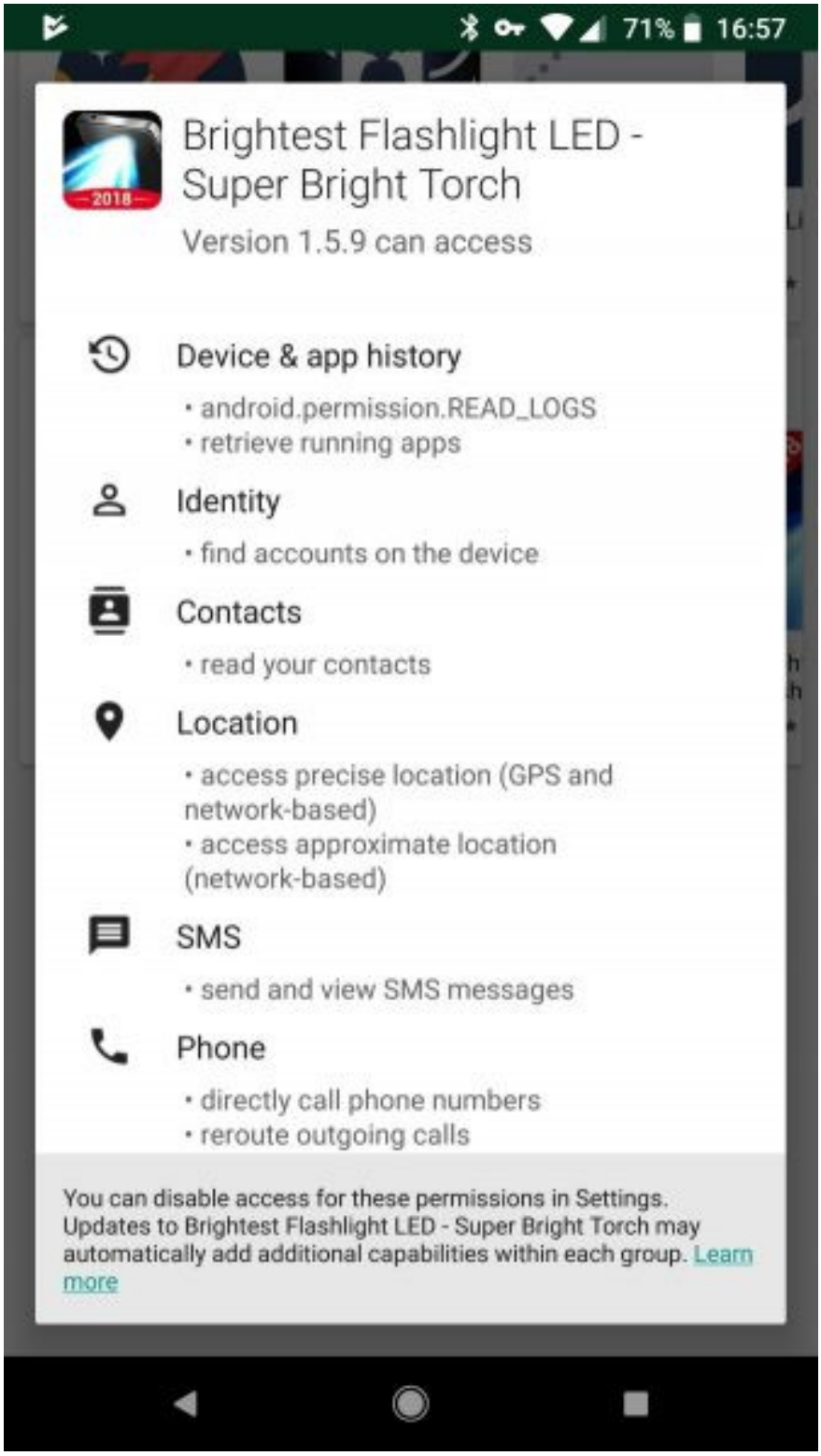
With millions of apps available on smartphones today, it's no surprise that not all apps are reliable. Indeed, many mobile applications are designed to attack users' devices or steal personal information.

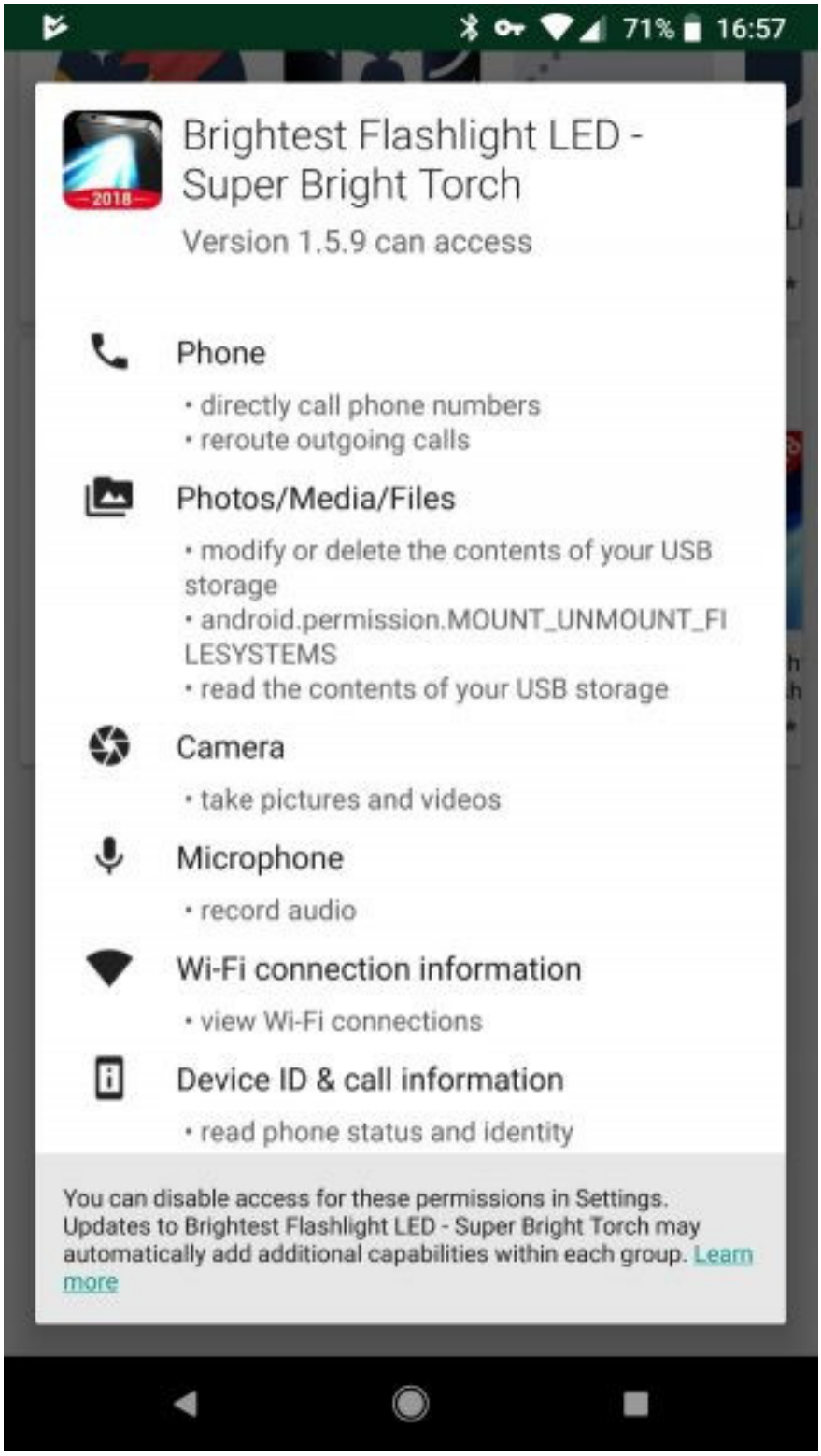
The article will show you some types of unreliable mobile applications and you should stop installing these types today. With these types, Android users should pay special attention because Google Play is less supervised than the App Store, but saying so does not mean that iPhone users do not need to avoid these applications.

1. Compare the two Google Play app markets and the App Store

## 1. Flashlight application


71% 16:58
Flashlight LED
The Brightest Flashlight App
Brightest Flashlight LED - Super Bright Torch
Flashlight APP
Everyone
INSTALL
Contains ads
#1 Top Free Tools
10 MILLION
Downloads
4.7
73,580
Tools
Similar
Get the brightest LED flashlight for FREE! Light your way ANYTIME and ANYWHERE!
READ MORE


71% 16:57
Brightest Flashlight LED - Super Bright Torch
Version 1.5.9 can access
Device & app history
• android.permission.READ_LOGS
• retrieve running apps
Identity
• find accounts on the device
Contacts
• read your contacts
Location
• access precise location (GPS and network-based)
• access approximate location (network-based)
SMS
• send and view SMS messages
Phone
• directly call phone numbers
• reroute outgoing calls
You can disable access for these permissions in Settings. Updates to Brightest Flashlight LED - Super Bright Torch may automatically add additional capabilities within each group. Learn more




**There is no reason to use these applications when your phone has a flashlight.**

People use smartphones like flashlights in emergencies that have been a long time. In the past you needed an application to turn the camera flash or phone screen into a flashlight, but now both Android and iOS phones have a built-in lamp on the operating system. Even so, many people still use flashlight applications filled with advertising and do not provide more useful features than integrated solutions.

Search for ' **flashlight** ' (Google flashlight) on Google Play Store and you'll see dozens of flashlight apps with millions of downloads. The most popular apps have tons of ads and require access like the user's location and contact list. Of course developers use them to sell your data to advertisers to make more money.

Therefore, you should not use these flashlight applications and should only use the built-in function on the phone. On Android, you will find this function by dragging twice from the screen down to open Quick Access. IPhone users can swipe from the bottom of the screen to access the Control Center and use the lights here.

1. How to adjust the Control Center iOS 11 interface

# 2. Keyboard application

**Carefully review the keyboard application you use.**

Android and even Apple started from iOS 8 version that allowed users to replace the default mobile keyboard with a third-party keyboard application. These applications provide predictive features, better functions, but they also provide privacy concerns.

Keep in mind that the keyboard app can see everything you enter, such as passwords, personal messages and financial information. To do this, they download data about specific import types to the company's server. And when the developers of the keyboard violate the data, anything you enter can be stolen. The personal data of ai.type Android keyboard users will be revealed when the company cannot protect their database server with the password as reported by ZDNet. And according to a Reddit user report, Microsoft's owned SwiftKey keyboard application has suggested a personal email address and other predictions for the wrong user.

Thankfully, iOS has a feature that doesn't allow third-party keyboards to access the Internet if you enable the **Full Access** option. But if you use a third-party keyboard or use it on Android, you should carefully choose the right keyboard application. If well-known companies like Microsoft have privacy issues on their keyboards, it is impossible to know what unnamed developers will do with your information.

1. The best 4 free and open source Android keyboard apps

# 3. Free games

**Please note that free games often have hidden costs.**

The proliferation of mobile games has created thousands of 'freemium' games that don't take anything to get started but they can earn a daily amount in other ways. Many applications with in-app purchase titles, ask you to pay to be able to continue playing and almost all free games will have ads. Not surprisingly, most games require access.

Popular free games often require access to contacts, locations, cameras and many other sensitive rights when installing it, although there are many 'legitimate' reasons for that such as sending an invitation to you. friends, etc.

The New York Times reported in late 2017 that hundreds of games on Google Play and the App Store contain software called Alphonso. This is the tool the advertiser uses to use the phone's microphone to get the audio for

the TV show you're watching. In fact, this software can combine this with the location you visit to track your information.

# 4. Antivirus application

**You will be surprised at what security applications can do with what they know about you.**

The iPhone antivirus application is basically useless because Apple's built-in protection can protect you on this operating system. On Android, you really do not need an antivirus application unless the device is rooted or you usually download applications not from Google Play.

1. Top best antivirus application for Android phones
2. The reason why you should only download the app from Play Store and App Store

But another problem is what antivirus applications for mobile devices can do with your data? For the purpose of protecting phones, they have to gather a lot of information and access a lot of data, so there is no longer any secret. If you use an antivirus application on your device, not even doing anything to protect you, it still collects data. So uninstall them to save storage space on the system and prevent antivirus companies from collecting your data.

# 5. Loyalty application

**Getting promotions and discounting by providing shopping habits and paying information storage isn't a wise thing.**

It seems that every restaurant, department store, business provides an application for download by buyers / users. Although installing this application will give you some personal incentives and is a convenient way to pay, but the application also brings some new security risks.

Many restaurant apps allow you to add your credit card so you can easily know your balance after payment. According to a CNN report in 2014, information about Starbucks users has vulnerabilities. A year later, hackers broke into the Starbucks application and used their affiliate card to steal money.

The more payment information you provide, the higher the risk of being attacked. And companies are happy to know more about you when you install their apps.

These are just five types of applications that threaten to violate your privacy but not only that, there are many other applications on the network. Applications that provide basic customization like wallpapers often have full access and advertising rights. Even weather apps can record IP addresses and other unnecessary information. And any application has access to or storing unsafe passwords.

Even health and fitness apps like Fitbit. These applications track you to sleep every night, exercise times, location, and more. It is a lot of information that you should not trust companies to store safely.

There is no sure way to avoid dangerous applications but you should be careful with the above types. And for other applications, consider access rights, security policies before using.

See more:

1. Top 10 great apps only available on Android
2. Essential applications for new iPhone users
3. 5 Security application you should consider removing and replacing

You finished reading the article "**5 types of mobile applications should not be installed on smartphones**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

---