Important Information About App Permissions for Android Devices

Before you download an app on Google Play (and other app providers), you might need to give the app permission to access specific capabilities or information on your device. The various categories of capabilities and information an app can access on your mobile device are known as permission groups.

Review permissions on app download screens!

Google Play shows you which permission groups an app will be able to access. This information can help you decide whether you want to install the app.

You'll see the most important permission groups on every download screen. If you want to see the full list of permissions an app can access on your device, follow the instructions under "See all permissions for a specific app" below.

Once you've allowed an app to access a permissions group, the app may use any of the individual permissions that are part of that group. You won't need to manually approve individual permissions updates that belong to a permissions group you've already accepted.

Additional app security on Google Play

Apps on Google Play must also follow Google Play's policies. Google removes apps that are found to violate these policies. Google also has systems that analyze new and existing apps, along with developer accounts to help protect users against potentially harmful software. Despite these protections, though, it's up to us as consumers to know just exactly what we're allowing each app to access or change, and then decide whether those uses are acceptable to us.

See all permissions for a specific app

You can review individual permissions and groups used by the latest version of an app available on the Google Play Store, or by looking at apps you have already downloaded to your mobile device.

Using the Play Store app

1. Open the app for the Google Play Store. 
2. Go to an app's detail page.
3. Under "Developer," select **Permission details**.

Using the Settings app on your device (for apps you've already downloaded)

1. On your device, open your main **Settings** app.
2. Select **Apps** or **Application Manager.** The name varies; it might be called something different but similar on your device.
3. Select an app.
4. Scroll down to "Permissions" and select it.

Permission groups: What does each one mean?

Select one of the groups below to learn more about what is included in that permissions group. Any permissions that are not part of a permissions group will be shown as "Other."

Important Notes:

1. Every time you download an update to an app, you should check the permissions, as they often change with updates. See the topics, 'Control permissions you approve during app updates and 'Turn Off Auto-Updates' on the last page of this handout.
2. Over time, the Android operating system may change the way permissions work, including adding or reclassifying certain permissions, so it's important to re-check your apps' permissions from time to time.

In-app purchases: An app can ask you to make purchases inside the app.

Device & app history: An app can do one or more of the following:

- Read sensitive log data
- Retrieve system internal state
- Read your web bookmarks and history
- Retrieve running apps

Cellular data settings: An app can use settings that control your mobile data connection and even has the ability to control the data you receive. Apparently, for the apps that have these permissions, the latter ability is usually seen as meaning 'the app has the potential to control the data you receive, but this rarely happens.'

Identity: An app can use your account and/or profile information on your device. Identity access might include the ability to:

- Find accounts on the device
- Read your own contact card (example: name and contact information)
- Modify your own contact card
- Add or remove accounts

Contacts: An app can use your device's contacts, which might include the ability to read and modify your contacts.

Calendar: An app can use your device's calendar information, which might include the ability to:

- Read calendar events plus confidential information
- Add or modify calendar events and send email to guests without owners' knowledge

Location: An app can use your device's location. Location access might include:

- Approximate location (network-based)
- Precise location (GPS and network-based)
- Access extra location provider commands
- GPS access

SMS: An app can use your device's text messaging (SMS) and/or multimedia messaging service (MMS). This group might include the ability to use text, picture, or video messages.

Important Note!! *Depending on your plan, you might be charged by your carrier for text or multimedia messages*.

SMS access might include the ability to:

- Receive text messages (SMS)
- Read your text messages (SMS or MMS)
- Receive text messages (MMS, like a picture or video message)
- Edit your text messages (SMS or MMS)
- Send SMS messages; this might cost you money
- Receive text messages (WAP)

Phone: An app can use your phone and/or its call history. Depending on your plan, you might be charged by your carrier for phone calls.

Phone access might include the ability to:

- Directly call phone numbers; this might cost you money
- Write call log (example: call history)
- Read call log
- Reroute outgoing calls
- Modify phone state
- Make calls without your intervention

Photos/Media/Files: An app can use files or data stored on your device.

Photos/Media/Files access might include the ability to:

- Read the contents of your USB storage (example: SD card)
- Modify or delete the contents of your USB storage
- Format external storage
- Mount or unmount external storage

Camera: An app can use your device's camera. Camera access might include the ability to:

- Take pictures and videos
- Record video

Microphone

An app can use your device's microphone. Microphone access might include the ability to record audio.

Wi-Fi connection information

An app can access your device's Wi-Fi connection information, like if Wi-Fi is turned on and the name(s) of connected devices. Wi-Fi connection information access might include the ability to view Wi-Fi connections.

Note: Since apps typically access the Internet, you'll only see the Wi-Fi connection information permission group on the download screen when installing an app. Apps no longer display the "full internet access" permission on the download screen, but you can always see the full list of permissions by following the instructions under the "See all permissions for a specific app" section above.

Bluetooth connection information

An app can control Bluetooth on your device, which includes broadcasting to or getting information about nearby Bluetooth devices.

Wearable sensors/activity data

Allows the app to access data from wearable sensors, such as heart rate monitors. Can receive periodic updates on physical activity levels.

Device ID & call information

An app can access your device ID(s), phone number, whether you're on the phone, and the number connected by a call. Device ID & call information might include the ability to read phone status and identity.

Other: An app can use custom settings provided by your device manufacturer or application-specific permissions.

Important: If an app adds a permission that is in the "Other" group, you'll always be asked to review the change before downloading an update.

Other access might include the ability to:

- Read your social stream (on some social networks
- Write to your social stream (on some social networks)
- Access subscribed feeds

You'll see all permissions from the "Other" group listed on the Play Store, including those that weren't shown on the app download screen.

Control permissions you approve during app updates

When an app updates, there might be changes to the permissions group for that app.

If you have automatic updates turned on

Permissions groups you've already accepted for that app: You won't need to review or accept these permissions again.

New permissions groups for that app: If the app needs access to new permissions or permissions in the "Other" group, you'll be asked to accept the update even if you've set up automatic updates.

If you prefer to review each update manually, you may want to consider turning off auto-update via the instructions below. You can also always see permissions for specific apps via the steps above.

Turn off auto-updates

If you want to manually update apps and accept permission updates individually, you can turn off auto-updates.

Turn off auto-updates for specific apps

1. Open the Play Store app .
2. Touch the Menu icon > **My Apps**.
3. Select an app.
4. Touch Menu .
5. If it's not already unchecked, uncheck the box next to "Auto-update."

Turn off auto-updates for all apps

1. Open the Play Store app .
2. Touch the Menu icon > **Settings** > **Auto-update apps** > **Do not auto-update apps**.

Retrieved from
https://support.google.com/googleplay/answer/6014972?p=app_permissions&rd=1
on 8/4/15.