App Permissions & How to Protect Your Device

What are app permissions? App permissions are the files and features of your device than an application has access to, such as your camera, contacts data, and location. Each time you install a new app or update an old app, you should check what permissions the app is asking for to make sure they are appropriate and your information will be safe.

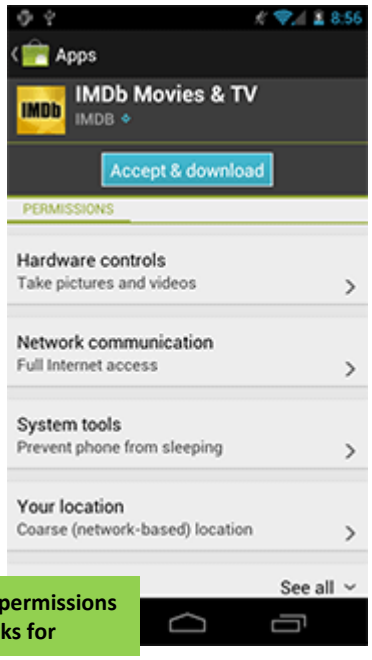

Image: A listing of the permissions the IMDB app asks for

Common App Permissions & When They Are Acceptable:

PERMISSION	WHAT IT DOES	WHEN IS IT ACCEPTABLE
Make Phone Calls	Allows app to make phone call without user having to physically approve the call	Legitimate apps like Google Voice and other phone apps use this permission to make hands-free calls on your behalf. Make sure the app is from a trustworthy source before installing
Send SMS or MMS	Allows app to send text messages on your behalf	Legitimate texting and messaging apps, like WhatsApp and Viber, use this permission to send messages from your device. If an app is NOT explicitly a texting app it should not need this permission.
Modify/delete SD card contacts	Allows app to read, write, and delete files stored on your SD card (external memory)	Many legitimate apps that create new files, such as camera apps, document writing apps, and audio/video apps, need this permission in order to save files you create. Be sure the app is from a trustworthy source before installing.
Read and/or Modify Contacts	Allows app to access and modify your contacts data	Legitimate communication and social media apps may require this permission to work properly. If an app does NOT have any communication or social media features, it should NOT require this permission
Read Social Stream	Allows app to read contents of your social media feeds that are linked to your device (Pinterest, Twitter, Facebook, etc)	Be very careful with this permission; if an app does not explicitly incorporate a social media element, it should not require access to your feeds (and information from your social media feeds can be used to hack your accounts/steal your identity).
Access Microphone or Camera	Allows app to record audio and/or take pictures on your device, sometimes w/o your knowledge	Legitimate communication and media-creation apps may require access to your microphone and camera in order to work properly.

How to Protect Your Device from Malicious Apps:

1. **Use Common Sense**
   Whenever you install a new app, look at the permissions it requires. If the app requires a permission that seems out of place or unnecessary (for example, if a puzzle game asks for access to your precise location, or to your camera & microphone), don't install it.

2. **Look at App Reviews and Ratings**
   Look at what other users have said about an app in the Google Play store before you install it. If an app has a **very low rating** (3 stars or less), has **not been installed by many people**, or has a lot of negative reviews, it's probably not an app you should install.

3. **Research the App Developer**
   Be sure any app you want to install is from a legitimate source. If you can't find any good information on its creator (for example, if they don't have a website or only have negative reviews), you probably shouldn't install the app.

4. **Ask Questions**
   If you don't understand why an application requires certain permissions, ask about it online or by contacting the developer. If you have a question about an app it's likely that others have had the same question before and will be able to help you.

5. **Look at Past App Permissions**
   Looking at the permissions for all apps installed on your device--including apps that you installed a while back--may help you figure out where a problem is coming from if your device gets infected or your data is compromised.