I'm not robot

reCAPTCHA

Continue

I'm not robot

reCAPTCHA

How do i turn off app permissions

Dear Lifehacker, I read your article on Chrome permissions last week, but I want to know about the permissions of the Android app. It seems that all app developers want access to so much on my phone! Do they really need all those authorizations, or are they just collecting my data? Dear Lifehacker, I am a great fan of Google Chrome and I love using extensions. However, I noticed ... Contact ... In accordance with Paranoid AndroidDear Paranoid Android, Android Android, Android Authorizations are simultaneously a best friend and worst friend of Android Developer. Some of the best apps available from even reputable app developers and companies still need some rather profound permissions in order to do basic things. On the other hand, the controversy around Android malware certainly makes the long list of authorizations before installing a new app a scary experience. Let's see if we can set your mind at ease. If you looked at the titles of technological news last week, it is likely that you have heard that AndroidÃ¢ â‚¬ | Take the list of permissions and legal to the characteristics of the app every time you install an app in Android, you are presented the list of permissions The app requires to work. If you are not revised that list before clicking "Install," starts now - you will get better understanding what information they really need an app and what features of your device the app has access only by reading that list. It is tempting simply jumping over, but resist: you should at least watch them so you are aware. The first thing to understand is what all those authorizations you are accepted with to do yes that an app. Some apps ask tons only to work (Facebook, Google+, Gmail, etc.) while others ask for a relatively few. This Thread at Android Forums does a great job to explain how authorizations work and what is all kinds, complete with examples for what it means any type of authorizations. It is a good reading, but in the end it is less important that you understand what it means any type of permissions as you understand why an app is asking when you install or update. Make sure you read the list of permissions and try to correlate each again to a function or function of the app. If you can reasonably make permissions of an app to return to a function (an SMS app that must read SMS messages or caller ID application that needs to access "Read the status of the phone and identity" For example) then there is little to worry about. Let's face it: most of the time, the reason why an app requires the authorizations it does is because it needs them to work. The only remarkable exception to this rule is app that require the root. When you root your Android phone, you give yourself that level of access to the internal work of your phone's operating system. When an app opens a superuser request and asks root, you should seriously think if the app needs it. Apps like ROM manager and titanium backup need root because they are running system level activity on the phone. However, if an application of the clock or even a new startup app requires root, make sure you understand why you need it before clicking "Allow". If you don't, don't do it. I love Android, but the typhus of your phone can give you the opportunity to do so much more than yours ... Morawatch contributions for apps that combine permissions for any reason I talked to Prategor Srivastava, a CS student and Android developer , Though all those authorizations mean and if they are intrinsically dangerous. He explained that most of the permits alone are rather "Even alone, the internet permission cannot do a lot - and it is likely that most apps to view ads. What you should really see is for the apps that combine Willy-Nilly permissions. For example if if they are. I had a file browser application supported by the announcement that required permissions for permissions read your storage, and to the internet to view ads - there is no way to prevent the app from simply publishing your data on file system of your phone (including your camera photos) to the internet. "It is true, true, The apps that seem to have legitimate uses for multiple authorizations could be dangerous. MakeUuryof explains some of the types of authorization you should look for, especially when they are combined in a single app, as Matthew Pettitt does in this great article. It is easy to scare when you see how many information that many apps require - even app from reliable sources - but you must ask yourself these questions when you see these lists Long permission: This app from a reliable developer? Do you look like a malware? Do I understand why this app needs these permissions? The developer explains to me why do they need these permissions? (Are you listed in Google Play, along with the reasons for each authorization request? Often, they are.) If the answer to all three these questions is yes, you are in good shape. If you start answering NO, you should start considering if you really need the app in question. Even the apps of reliable developers can collect a great amount of data, both for advertising and marketing purposes, or because someone screwed. If you have an app from a developer you have never heard of and doesn't explain why it needs permissions that makes it, stay away unless you understand that permissions are needed for the type of app that is.courage Developers to explain their permissions need Google Play Looking at an app that requires a ton of permissions can be scary, but make sure you check the list of apps on Google Play before jumping to the conclusions. As we said above, if the developer explains why any authorization is required for their app to work, you have nothing to worry about unless you think the app is doing something else behind the scenes, and if it It is probably you see the people who talk about this in the app le reviews.check the description of the app on Google Play to see if the developer has listed permissions at the bottom of the function list. More and more devs are doing this, partially because they know they need to fight paranoia, but also be transparent on what information they need their app from you. Even if they don't list it in Google Play, you will find more information on the developer's website. At To-do Manager Any.Do, for example, asks for some rather frightening relationships, but a look at their frequent Android questions should put your fears to rest. If you don't see the permissions explained on Google Play or on the website developer, send them emails and ask. Many apps on Google Play have a link "Visit Developer's Web Site" or a "Privacy Policy" link that will provide you with more information. Even if they don't, they should absolutely have a "Email Developer" link, which you can use to release them a line and ask why their app requires the permissions it does. Encourage them to add this information to their app page in Google Play. Prateek explains: "For developers, Google themselves recommend that you require more permits. The developers are also lazy, for example most developers would require only user account information to identify the user uniquely from your address e-mail or telephone number (this could be for many reasons - perhaps the validation of the server side that the app is not pirated). A better way to do so is outlined here (without any personal information required). " This is the best for which developers must be transparent on the requested permissions, and said, and because users must be careful ... not paranoid "and challenging DevS when they don't know why an app needs permissions That Fa.Monitor and the Authorizations of the Tweak app alone if you really want An app that has questionable permissions, or an app with permits you do not understand (or do not feel necessary for the app to work), there are apps that can help. Some stop the intrusive apps to get the data they want, other monitors will only install the apps that are installed to see if they are doing something fish. For example: PDOID Privacy Privacy (Requires root) is a previously mentioned app that keeps an eye on the types of information that your app request and allows you to allow or not allow a per-app base. You can block access to personal or identifier information for each app installed and will not interrupt the app in the process. Privacy Guard (Requires root) acts a bit like a firewall based on app for Android, notifying you when an app Try to access the data and give you the opportunity to allow or deny it. The key is that if you deny something an app needs to work, it could very well accident, so you'll have to think before touching. Keep in mind that people loved the old version and the new version was not also received in Google Play, so your mileage may vary. PermissionsIdog is another app that we love why it shows you exactly how the apps are dangerous Install at a glance. You can simply say scrolling the list that those are ok and what you should pay great attention. However, you will have to search for: for example, because Google Voice requires access to the phone status, identity, SMS, sleep / wake and other permissions, is labeled dangerous. This is the right classification, but Google Voice passes the smell test.pocket permissions is a complete guide for app permissions. It is useful for Android beginners or anyone else that is interested in the topic, and wants more details about what each type of authorizations specifically means, and what data is available when such authorization is granted. You can use the app to search for permissions and understand why other apps need it, search for authorization to see which apps require, order it for risk or importance and more. Ã $ 2, but it is a useful guide.Research before you are no reason for rage whenever you find an app that requires a good number of authorizations. In many cases, the problem could only be the one you do not understand why the app needs the authorizations that "could be an addiction from Android that the developer had to satisfy so that the app works. It could be a feature in the app that you don't understand fully. Before flying out of the handle and accuse the dev to steal your data, check Google Play or ask them directly. If it seems too effort, do not install the app and find an alternative that is more transparent . "In the end, as a user, you really have to trust the developer of what they are doing with permissions. You can make a good educated hypothesis, but this is about it. As a developer, you must be transparent on what and why you need any authorization. For example if you need to collect analysis on your app and publish the results to the server, you need internet authorization. But if your app is just a clock app - users will be confused because you have permission on the internet. "Good luck, Lifehackerprateek srivastava is an Android developer, creator of app as we installed and timer countdown. He gently offered him experience of him for this story, and thank him. He.